Министерство науки и высшего образования Российской Федерации
Филиал федерального государственного автономного образовательного учреждения высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»
в г. Нижневартовске
Кафедра «Экономика, менеджмент и право»

ДОПУСТИТЬ К ЗАЩИТЕ

Заведующий кафедрой

/Н.В. Зяблицкая/

28 мая 2021 г.

Уголовно-правовая и криминологическая характеристика киберпреступлений

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

ЮУрГУ – 40.03.01.2021.663.ВКР

Консультанты, (должность)

Руководитель работы
к.ю.н., доцент

/А.Р. Салимгареева/

21 мая 2021 г.

Консультанты, (должность)

Автор работы
Обучающийся Группы НвФл-525

/А.Ф. Раджабова/

20 мая 2021 г.

Консультанты, (должность)

Нормоконтролер

/Н.В. Назарова/

21 мая 2021 г.

Нижневартовск 2021

АННОТАЦИЯ

Раджабова А.Ф. Уголовно-правовая и криминологическая характеристика киберпреступлений. – Нижневартовск: филиал ЮУрГУ, НвФл-525, 77 с., 4 ил., 1 таб., библиогр. список – 45 наим., прил. – нет, 12 л. слайдов

Выпускная квалификационная работа выполнена с целью комплексного исследования теоретических и практических аспектов киберпреступности.

В выпускной квалификационной работе определены понятие и признаки киберпреступлений; проанализированы основания классификации, виды особенности развития киберпреступлений; исследованы проблемы разграничения составов киберпреступлений.

Также в работе проанализированы состояние, структура и динамика киберпреступности на территории ХМАО-Югры; исследованы причины, условия и средства совершения киберпреступлений; разработаны правовые и криминологические меры противодействия преступлениям, совершаемым с использованием киберпространства.

В целях создания системы мер противодействия комплексу киберпреступлений разработаны рекомендации правового и криминологического характера.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования. Процессы глобализации, бурное развитие компьютерных технологий, всеобщая интеграция повлекли за собой возникновение современного информационного общества. Цивилизованное государство и общество не может существовать без виртуального мира. В цифровой реальности находится огромное количество личной и служебной информации, документации, денежных средств, активов. Она представляет собой своеобразную огромную базу по обмену информацией, развлечений, работы и т.д. Стоит отметить, что проводником в виртуальное пространство служит компьютеры и сеть Интернет.

Информатизация и глобальная компьютеризация вносят свои изменения во все сферы жизни общества. Не обошел процесс изменения и преступную среду, а именно появилась новая форма преступлений – преступления в сфере информационных технологий, или киберпреступления.

Важность и актуальность проблемы киберпреступности отражает состояние преступности из статистики МВД РФ. Количество киберпреступлений, особенно в сфере экономики, в последние несколько лет значительно возросло, как и количество мошеннических схем, которые осуществляются через телефоны и смартфоны. За последние три года произошло колоссальное увеличение количества преступлений, совершенных с использованием компьютерных и телекоммуникационных технологий: 2018 год – 12154, 2019 год – 240209, 2020 год – 510396.[1] Кроме того состояние киберпреступности за 2019 год было отражено в новом параграфе статистики МВД РФ «Сведения о преступлениях совершенных с использованием компьютерных и телекоммуникационных технологий».[2]

[1] Показатели преступности России // Портал правовой статистики [сайт]. – URL: http://crimestat.ru/offenses_chart (дата обращения 12.04.2021)

[2] Состояние преступности и результаты расследования преступлений // Интернет-портал МВД РФ: [сайт]. – URL: https://мвд.рф/открытые-данные/ (дата обращения: 12.04.2021)

Данный факт свидетельствует о серьезной угрозе нескольким сферам жизни общества, так как затрагивает и личные права граждан, и экономику целой страны. Однако, усилия правоохранительных органов не дают заметного результата в борьбе с новыми видами преступлений. Качественно проведенная проверка по сообщению о преступлении позволяет выявить основания для возбуждения уголовного дела. Своевременно возбужденное уголовное дело дает возможность найти следы преступления. Несмотря на изложенное, киберпреступлениям свойственны особые признаки и свойства, благодаря которым их очень трудно расследовать. Правоохранительный органы относят данные виды преступлений к наиболее редко раскрываемым.

Изложенное предполагает необходимость изучения уголовно-правовой и криминологической характеристики киберпреступлений.

Объектом исследования являются общественные отношения, складывающиеся в области предупреждения преступлений, образующих в своей совокупности киберпреступность.

Предметом исследования являются российское уголовное законодательство, правоприменительная практика по уголовным делам связанных с совершением данного вида преступлений, а также научная юридическая литература по вопросам квалификации киберпреступности, а также система мер их предупреждения.

Целью выпускной квалификационной работы является комплексное исследование теоретических и практических аспектов киберпреступности, а также разработка рекомендаций правового и криминологического характера по созданию системы мер противодействия комплексу киберпреступлений.

Достижение обозначенной цели предполагает **решение следующих задач**:

– определить понятие и признаки киберпреступлений;

– проанализировать основания классификации, виды особенности развития киберпреступлений;

– исследовать проблемы разграничения составов киберпреступлений;

– проанализировать состояние, структуру и динамику киберпреступности на территории ХМАО-Югры;

– исследовать причины, условия и средства совершения киберпреступлений;

– разработать правовые и криминологические меры противодействия преступлениям, совершаемым с использованием киберпространства.

Методологическую основу исследования составляют следующие методы: историко-правовой, сравнительно-правовой, формально-логический методы, анализ, аналогия, обобщение и систематизация собранных данных.

Теоретическую основу исследования составили работы авторов в области уголовного права, криминологии и информационно-телекоммуникационных технологий: К.Н. Евдокимова,[1] Л.П. Зверянской,[2] Н.Ш. Козаева,[3] П.А. Литвишко[4] и др.

Проблематике киберпреступлений и раскрытию понятия преступлений в IT сфере посвящены исследования М.Е. Батухтина,[5] Т.Н. Бородкиной,[6] Э.Л. Кочкиной[7] и др.

---

[1] Евдокимов, К.Н. Криминологические и уголовно-правовые аспекты противодействия компьютерной преступности в России (социологическое исследование) / К.Н. Евдокимов // Российский следователь. – 2020. – № 11. – С. 41-44.

[2] Зверянская, Л.П. Исторический анализ этапов развития киберпреступности и особенности современных киберпреступлений / Л.П. Зверянская // Научно-методический электронный журнал «Концепт». – 2016. – Т. 15. – С. 881-885.

[3] Козаев, Н.Ш. Противодействие злоупотреблениями современными технологиями: международно-правовые и уголовно-правовые аспекты / Н.Ш. Козаев // Монография. – Москва : Юрлитинформ, 2016. – 177 с.

[4] Литвишко, П.А. Юрисдикционные и международно-правовые аспекты обеспечительных и конфискационных мер в отношении виртуальных активов / П.А. Литвишко // Законность. – 2021. – № 3. – С. 8-14.

[5] Батухтин, М.Е. Киберпреступления: причины, виды, формы, последствия, направления противодействия / М.Е. Батухтин // Проблемы и перспективы развития уголовно-исполнительной системы России на современном этапе Материалы Международной научной конференции адъюнктов, аспирантов, курсантов и студентов. 2018. – С. 142-149.

[6] Бородкина, Т.Н. Киберпреступления: понятие, содержание и меры противодействия / Т.Н. Бородкина, А.В. Павлюк // Социально-политические науки. – 2018. – № 1. – С. 135-137.

[7] Кочкина, Э.Л. Определение понятия «Киберпреступление». Отдельные виды киберпреступлений / Э.Л. Кочкина // Сибирские уголовно-процессуальные и криминалистические чтения. – 2017. – № 3 (17). – С. 162-169.

Анализ последних исследований и публикаций, в которых рассматривались уголовно-правовые и криминологические аспекты киберпреступлений свидетельствует о наличии неразрешенных проблем в данной сфере, что обусловлено стремительным развитием информационных отношений, являющихся объектом посягательства преступников.

Эмпирическую базу исследования составили материалы судебной практики, статистические данные ГИАЦ МВД России, Информационных центров УМВД России по ХМАО-Югре.

Теоретическая и практическая значимость исследования заключается в развитии научных представлений о противодействии преступлениям, совершаемым с использованием киберпространства.

Структура работы: выпускная квалификационная работа состоит из 2 глав и 6 параграфов, присутствует заключение и библиографический список, общий объем работы 77 страниц.

1 УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ В КИБЕРПРОСТРАНСТВЕ

1.1 Понятие и признаки киберпреступлений

В 1980-х годах компьютеры казались вершиной развития в области электроники. Киберпреступность приобрела все большее значение по мере того, как компьютеры стали центральным элементом торговли, развлечений и управления. Из-за раннего и широкого распространения компьютеров и Интернета в Соединенных Штатах Америки, большинство первых жертв и преступников в киберпространстве были американцами. Однако к XXI веку в мире почти не осталось населенных пунктов, которые не были бы затронуты киберпреступностью того или иного рода.

Термин «компьютерная преступность» впервые был использован в юридических текстах, поскольку такие преступления изначально были связаны с компьютерами и без, по крайней мере, двух компьютеров невозможно было установить их связь и, следовательно, создать новое поле человеческой (и преступной) деятельности – виртуальную реальность или киберпространство.

Определение категории «компьютерное преступление» не было общепринятой практикой в теории права. Теоретики уголовного права предложили использовать термин «преступление, связанное с компьютером», в котором учитывается тот факт, что компьютер является «всего лишь инструментом в руках преступников».[1] Этот термин охватывал два элемента: компьютер должен был использоваться в качестве средства или объекта совершения преступления, либо совершение преступления должно было быть результатом экспертного знания преступником компьютера или информационных технологий. Учитывая тот факт, что экспертные знания рассматривались в качестве важного элемента, некоторые эксперты по уголовному праву предлагали

[1] Овчинский, В.С. Основы борьбы с киберпреступностью и кибертерроризмом: хрестоматия / В.С. Овчинский. – Москва : Норма, 2017. С. 56.

использовать термин «преступление в информатике».[1]

Термин «компьютерная преступность» и его производные сегодня считаются либо слишком узкими, либо для обозначения только первого поколения киберпреступности.[2] Компьютеры и их компоненты – микропроцессоры – имеют широкую сферу применения: их можно найти в ручных часах, бытовой технике, транспортных средствах и т.д. Вместо более общего термина «компьютер» более подходящим представляется термин «информационно-коммуникационные технологии».

Помимо компьютеров развитие информационно-коммуникационных технологий привело к появлению других устройств, таких как мобильные телефоны, ладони, автоматизированные сетевые интерфейсы и другие гибридные технологии, которые объединяют существующие отдельные технологии (телевидение, радио, видео, телефония, спутниковая навигация и т.д.). Общим знаменателем этих технологий стало наличие данных и сети – отсюда и термин «преступление в сфере информационно-коммуникационных технологий».

Среди многих информационно-коммуникационных технологий Интернет является специфической сетью, которая использует специальный протокол связи – протокол Интернета (IP). Кроме того, существует множество способов общения в самом Интернете: через службу всемирной паутины (WWW), обеспечивающую доступ к веб-страницам, учетным записям электронной почты, службам интернет-чата, передачи файлов (протокол передачи файлов – FTP), интернет-телефония (протокол передачи голоса через Интернет – VoIP) и т.д. В связи с этим, в теории уголовного права используются термины «интернет-преступность», «электронная преступность» или даже «виртуальная преступность» и «преступность в

[1] Кочкина, Э.Л. Определение понятия «Киберпреступление». Отдельные виды киберпреступлений / Э.Л. Кочкина // Сибирские уголовно-процессуальные и криминалистические чтения. – 2017. – № 3 (17). С. 162.

[2] Киберпреступность: криминологический, уголовно-правовой, уголовно-процессуальный и криминалистический анализ / науч. ред. И.Г. Смирнова; отв. ред. О.А. Егерева, Е.М. Якимова. – Москва, 2016. С. 34.

компьютерных сетях».[1] Все эти термины используются в социологическом дискурсе и менее применимы для правового поля, особенно в уголовном праве с его принципом законности и его компонентом lex certa, являющимся регулирующим принципом. Кроме того, понятие информационной преступности более широкое, чем киберпреступность, поскольку оно охватывает не только компьютерную преступность, но и области, в которых нет компьютеров.

Тем не менее, термин киберпреступность в юриспруденции не совсем уместен, поскольку понятие кибернетики изначально являлось художественным и литературным понятием, введенным Уильямом Гибсоном своим знаменитым киберпанковским романом «Нейромант» в 1984 году.

Всемирная распространенность информационных систем и возникший в результате этого трансграничный характер киберпреступности, являются основными причинами интенсивного стремления сформулировать на международном уровне существенные и процессуальные уголовные нормы против киберпреступности.

Общественная опасность киберпреступлений признана на международном уровне, что выражается в соответствующих решениях международных организаций. В первую очередь, это – определение самого понятия «киберпреступность».

В 1996 году Совет Европы совместно с представителями правительств Соединенных Штатов, Канады и Японии разработал предварительный международный договор, охватывающий компьютерную преступность. Во всем мире группы борцов за гражданские свободы немедленно опротестовали положения договора, требующие от интернет-провайдеров хранить информацию о транзакциях своих клиентов и передавать эту информацию по требованию. Тем не менее, работа над договором продолжалась, и 23 ноября 2001 года Конвенция Совета Европы о киберпреступности была подписана 30 государствами. Конвенция вступила в силу в 2004 году. Дополнительные протоколы,

[1] Третьяк, М.И. Проблема законодательной регламентации преступлений против собственности в сфере высоких технологий / М.И. Третьяк // Законность. – 2016. – № 7. С. 41.

охватывающие террористическую деятельность и киберпреступность на почве расизма и ксенофобии, были предложены в 2002 году и вступили в силу в 2006 году.[1] Кроме того, различные национальные законы, такие как Патриотический акт США 2001 года, расширили полномочия правоохранительных органов по мониторингу и защите компьютерных сетей.

Исчерпывающая формулировка борьбы с «компьютерной преступностью» (как ее тогда называли) началась под эгидой Организации экономического сотрудничества и развития. Его специальная комиссия изучила возможности международной гармонизации уголовного законодательства в борьбе с экономическими преступлениями, связанными с компьютерами. Международные усилия продолжались в Организации Объединенных Наций, когда на Восьмой сессии Организации Объединенных Наций было принято руководство по предупреждению преступлений, связанных с использованием компьютеров, и борьбе с ними.[2] В руководстве описывается явление компьютерной преступности и содержатся некоторые из первых положений материального и процессуального уголовного права.

Важность киберпреступности была дополнительно подчеркнута на конференции «Большой восьмерки» по киберпреступности в 2000 году.[3] Но современные и значительные положения уголовного законодательства о борьбе с киберпреступностью были приняты только в 2001 году на Конвенции Совета Европы о киберпреступности.

Конвенция о киберпреступности является первым всеобъемлющим международным соглашением о борьбе с «высокотехнологичной» преступностью

---

[1] Конвенция о преступности в сфере компьютерной информации (ETS № 185). Заключена в г. Будапеште 23 ноября 2001 г. – [по состоянию на 28 января 2003 г.] // Международные стандарты деятельности правоохранительных органов и уголовно-исполнительной системы. – Екатеринбург, 2003. С. 52-79.

[2] Всестороннее исследование проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора // Интернет-портал Организации Объединенных Наций: [сайт]. – URL: http://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_R.pdf (дата обращения: 12.04.2021)

[3] Там же.

с помощью уголовного права.

С момента принятия конвенции Совет Европы выступил с инициативой борьбы с киберпреступностью с помощью законодательных мер: например, был создан Комитет Конвенции по киберпреступности (T-CY), организованы ежегодные международные конференции, посвященные проблемам киберпреступности.

Однако правовые решения Совета Европы, касающиеся киберпреступности, все чаще становятся объектами для споров.[1] Принятые уголовные положения стали полезным инструментом для защиты интересов (т.е. прибыли) наднациональных предприятий (производителей программного обеспечения, поставщиков интернет-контента и т.д.). Таким образом, якобы беспристрастные и независимые правовые решения Совета Европы должны подвергаться тщательному изучению. Особенно критически к конвенции относится международная коалиция НПО, сотрудничающих в рамках Глобальной кампании за свободу Интернета (GILC).[2]

GILC убедительно показал, что правовая деятельность Совета Европы направлена для все более агрессивное уголовное регулирование. Сомнительная деятельность в Интернете становится более криминализированной, чем ее офлайн-аналоги.

Правовые решения Совета угрожают основным правам и свободам человека, демократии и верховенству права Критика правовых решений Совета Европы усилилась в рамках его программы «Проект по борьбе с киберпреступностью», поскольку этот проект в значительной степени финансируется корпорацией Microsoft. Таким образом, корпорация получила

[1] Литвишко, П.А. Юрисдикционные и международно-правовые аспекты обеспечительных и конфискационных мер в отношении виртуальных активов / П.А. Литвишко // Законность. – 2021. – № 3. С. 10.

[2] Всестороннее исследование проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора // Интернет-портал Организации Объединенных Наций: [сайт]. – URL: http://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_R.pdf (дата обращения: 12.04.2021)

эффективный контроль над повесткой дня Совета и полномочия по определению «проблем», заслуживающих внимания Совета.

Вместе с тем, важно отметить, что понятие «киберпреступности» законодательно не закреплено. Кроме того, определения киберпреступности зависят от целей самого термина. Так, Будапештская конвенция не дает прямого указания на термин киберпреступности, но определяет необходимость сдерживания: «…действий, направленных против конфиденциальности, целостности и доступности компьютерных систем и сетей и компьютерных данных, а также против злоупотребления такими системами, сетями и данными, путем обеспечения уголовной наказуемости таких деяний…».[1] Таким образом, можно понимать под киберпреступностью ограниченный круг деяний, направленных против конфиденциальности, целостности и доступности компьютерных систем и сетей и компьютерных данных.

В целом, действующие нормативно-правовые акты международного права содержат в качестве одной из своих составных частей нормативные положения, регулирующие вопросы информационной безопасности и обеспечения прав и интересов субъектов права в этой области. К числу таких документов необходимо в первую очередь отнести: Декларация о преступности и общественной безопасности;[2] Венская декларация о преступности и правосудии;[3] Руководство по предупреждению преступности и многие другие. Указанные акты, в совокупности с нормативными актами, определяющими порядок международного взаимодействия, создают основу для сотрудничества в сфере предупреждения

[1] Конвенция о преступности в сфере компьютерной информации (ETS № 185). Заключена в г. Будапеште 23 ноября 2001 г. – [по состоянию на 28 января 2003 г.] // Международные стандарты деятельности правоохранительных органов и уголовно-исполнительной системы. – Екатеринбург, 2003. С. 57.

[2] Декларация о преступности и общественной безопасности. Принята 12 декабря 1996 г. Резолюцией 51/60 на 82-ом пленарном заседании Генеральной Ассамблеи ООН // Международные стандарты деятельности правоохранительных органов и уголовно-исполнительной системы. – Екатеринбург, 1999. С. 21-48.

[3] Венская декларация о преступности и правосудии: ответы на вызовы XXI века: Резолюция № 55/59 Генеральной Ассамблеи ООН. Принята в г. Нью-Йорке 4 декабря 2000 г. на 81-ом пленарном заседании 55-ой сессии Генеральной Ассамблеи ООН // Бюллетень международных договоров. – 2005. – № 2. С. 3-33.

преступности в целом, так и киберпреступности в частности.

При этом следует отметить, что в разных странах существуют различные подходы к понятию «киберпреступление» и его содержанию. Так, в США под киберпреступлениями понимается любая незаконная деятельность, связанная с компьютером или электронным устройством, подключенным к сети, например мобильным телефоном, сканер, радионяня, и т.д.[1] Таким образом, под киберпреступлениями понимается любая противозаконная деятельность, связанная с электронным устройством, подключенным к сети, начиная со смартфона и заканчивая спутниками.

В России – понятие «киберпреступление» на нормативном уровне отсутствует. Также в российском уголовном законодательстве не используется «кибер»-терминология. Вместо него в УК РФ существует термин «преступления в сфере компьютерной информации».[2] Данный термин употребляется в названии главы 28 Уголовного кодекса Российской Федерации. Связано это, скорее всего, с более упрощенным подходом к данному виду преступлений на основе более понятных российскому уголовному праву, вытекающих из права информационного явлений и процессов, описываемых на основе понятий «компьютер» и «информация».[3]

Помимо международно-правового определения киберпреступлений существует и ряд научных разработок данной проблемы. Например, в своем исследовании Т.М. Хусяинов дает следующую трактовку: «Под термином «интернет-преступление» или «киберпреступление» стоит понимать весь спектр

---

[1] Козаев, Н.Ш. Противодействие злоупотреблениями современными технологиями: международно-правовые и уголовно-правовые аспекты / Н.Ш. Козаев // Монография. – Москва : Юрлитинформ, 2016. С. 89.

[2] Уголовный кодекс Российской Федерации: Федеральный закон от 13 июня 1996 г. № 63-ФЗ. – [по состоянию на 5 апреля 2021 г.] // Собрание законодательства Российской Федерации. – 1996. – № 25. – Ст. 2954.

[3] Одинцов, С.А. Развитие теорий информационного общества и понятия «киберпространство» / С.А. Одинцов, А.В. Ващенко // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – 2016. – № 121 (07). С. 5.

преступных действий в сфере информационных технологий…».[1]

Несколько более широкое понятие описвает в своей работе М.Е. Батухтин: «киберпреступление – это любое преступление в электронной сфере, совершенное при помощи компьютерных средств или виртуальной сети, или против них».[2]

Доктринальные исследования по рассматриваемому вопросу выявили различные подходы к пониманию и нормативно-правовому определению понятия киберпреступности. Однако единого или превалирующего определения в настоящее время привести нельзя, поскольку споры по этому вопросу не привели к какому то устойчивому результату.

Понятие «киберпреступность» охватывает компьютерную преступность (где компьютер – предмет преступления, а информационная безопасность – объект преступления) и другие посягательства, где компьютер является орудиями или способом совершения преступления против собственности, имущественных и неимущественных прав, общественной безопасности и тому подобное. В то время, как под «киберпреступлением» следует понимать любое преступление, совершенное с помощью информационных технологий, либо в информационном пространстве.

Одновременно киберпреступления можно рассматривать как противозаконные действия в сфере автоматизированной электронной обработки информации. В таком случае в качестве главного классифицирующего признака, позволяющего отнести такие деяния в обособленную группу, выделяется общность способов, орудий и объектов посягательств.

Другими словами, объектом посягательства тогда выступает информация, обрабатываемая в виртуальном пространстве. Компьютер же или мобильное

---

[1] Хусяинов, Т.М. Интернет-преступления (киберпреступления) в российском уголовном законодательстве / Т.М. Хусяинов // Уголовный закон Российской Федерации: Проблемы правоприменения и перспективы совершенствования материалы всероссийского круглого стола. 2015. С. 92.

[2] Батухтин, М.Е. Киберпреступления: причины, виды, формы, последствия, направления противодействия / М.Е. Батухтин // Проблемы и перспективы развития уголовно-исполнительной системы России на современном этапе Материалы Международной научной конференции адъюнктов, аспирантов, курсантов и студентов. 2018. С. 144.

(сотовое) средство связи с соответствующим программным обеспечением и выходом на сеть Интернет служат средствами или орудиями посягательства.

Цели этих преступлений разнообразны и варьируются в зависимости от интересов правонарушителя. Кроме того, способы совершения данных преступлений разнообразны и могут достигать только одного пользователя, нескольких пользователей или даже полную сетевую систему.

Анализ сущности киберпреступлений и киберпреступности, позволил выделить следующие их характерные свойства:

1. Глобальный масштаб. Данный признак является основополагающим. Во многих странах резкий всплеск в количестве подсоединений к глобальной сети совпал по времени с экономическими и демографическими преобразованиями, ростом разрыва в доходах, сокращением расходов в частном секторе и снижением финансовой ликвидности. На общемировом уровне отмечается рост уровня киберпреступности в связи с тем, что и частные лица, и организованные преступные группы используют новые возможности для совершения преступлений, руководствуясь стремлением к извлечению прибыли и получению личной выгоды.

Согласно отчетам We Are Social и Hootsuite о глобальном состоянии цифровых технологий на 2020 год в мире аудитория интернета насчитывает 4,5 млрд. человек, что составляет почти 60% от общей численности населения Земли. В социальных сетях зарегистрировано 3,8 млрд. пользователей. 3,7 млрд. человек заходят в социальные сети с мобильных устройств.[1]

Необходимо отметить и географическое распределение пользователей сети Интернет. В частности, около 90% населения Европы, 55% населения Азии, 37% населения Африки, 95% населения Северной Америки и 73% населения Южной Америки являются пользователями Интернета.[2]

[1] Digital 2020: ежегодное глобальное исследование от We Are Social и Hootsuite // Интернет-портал медиааналитического агентства «Exlibris»: [сайт]. – URL: https://exlibris.ru/news/digital-2020-ezhegodnoe-globalnoe-issledovanie-ot-we-are-social-i-hootsuite/ (дата обращения: 12.04.2021)

[2] Там же.

На основе указанных показателей возможно сделать вывод о проникновении информационного пространства в значительную часть человеческой жизнедеятельности.

2. Транснациональность киберпреступности – 62% компьютерных преступлений совершаются в составе организованных групп, которые находятся на территории нескольких стран. Киберпространство существует вне государственных границ и будучи общедоступным позволяет находящемуся на территории одного государства преступнику совершить преступление в отношении лиц иных государств. Следовательно, киберпреступности свойственен транснациональный характер, поскольку преступники для получения преступных доходов, облегчения совершения преступных деяний на территории двух и более государств вынуждены независимо от национальности объединяться в международные преступные группы.

3. Анонимность и неперсонифицированность киберпреступлений – механизмы идентификации глобальной сети (а именно использование программ, которые дают анонимность и использование алгоритмов шифрования) позволяют лицу осуществлять операции анонимно или выдавать себя за другое лицо, изменять биографические данные или социальный статус;

4. Трансграничность выражается в том, что потерпевший и правонарушитель могут быть на любом расстоянии друг от друга, в том числе находится на территории разных государств.

Важным аспектом киберпреступности является ее глобальный характер: действия могут происходить в юрисдикциях, разделенных огромными расстояниями. Это создает серьезные проблемы для правоохранительных органов, поскольку преступления теперь требуют международного сотрудничества. Например, если человек получает доступ к детской порнографии, размещенной на компьютере в стране, которая не запрещает детскую порнографию, возникает ряд вопросов: совершает ли это лицо преступление в стране, где такие материалы являются незаконными? Где именно происходит киберпреступность?

5. Интеллектуальный характер киберпреступности – осуществление киберпреступлению требует определенного набора знаний. При этом киберпреступления, в отличие от других интеллектуальных преступлений, доступны людям невысоких социальных возможностей – для осуществления киберпреступлений не нужно занимать высокое социальное положение, достаточно иметь доступ в Интернет и компьютер.

Подобные свойства киберпреступности свидетельствуют о сложном характере системы реализации киберпреступности, находящейся постоянно в состоянии своего динамического развития, что обуславливается перманентным процессом совершенствования действующих и создания новых кибертехнологий, привлечением в информационные сообщества новых участников, усилением структуры киберпространства посредством увеличения количества пользователей в сети «Интернет», развитием сети мобильных компьютерных устройств, развитием систем электронного документооборота в большом числе организаций, учреждений и предприятий. Кроме того, киберпреступность стала обладать чертами, свойственными экономической преступности, в силу совершения преступлений в финансовой, банковской или корпоративной сферах, а преступная деятельность выбрала основным трендом извлечение прибыли.

Помимо экономики, киберперступления совершаются и в политической, и военной сферах. Они приобретают политическую окраску и совершаются в целях распространения экстремистских материалов, разжигания межнациональных конфликтов, дискредитации государств, или отдельных лиц и т.д. Особая опасность киберпреступности состоит в ее возможности и предпринимаемых попытках трансформации в преступность, обладающую политическим характером. Это связано с усилением в киберпространстве деятельности представителей хакерских движений, различных спецслужб и силовых структур из зарубежных стран, международных организаций экстремистского и террористического толка.

Изложенное подтверждает высокую общественную опасность и

значительную распространенность киберпреступлений. Несмотря на это, до сих пор нет четко определенного и общепринятого понятия данным преступления.

Таким образом, обобщая вышеизложенное, можно заключить, что киберпреступления представляют собой преступления, которые совершаются в так называемом виртуальном пространстве. Киберпреступность – это довольно обширное понятие. К данному виду противоправных деяниям можно отнести и преступления где компьютер, информационная сеть Интернет, данные и т.д. – являются объектом, и преступления, где компьютеры используются как средство и орудие. К этому же понятию многие ученые относят и действия в информационном пространстве для поддержания условий преступной общности, группы, например, использование электронной почты для коммуникации, обмен криминальным опытом и специальными познаниями. Киберпреступность, также называемая компьютерной преступностью, предполагает использование компьютера в качестве инструмента для достижения дальнейших незаконных целей, таких как мошенничество, торговля детской порнографией и интеллектуальной собственностью, кража личных данных или нарушение конфиденциальности.

В уголовном законодательстве РФ понятие «кибер» не используется вовсе, а существующие положения уголовного законодательства, направленные на защиту иных отношений, отражают только вопросы информационных технологий или использования компьютерной техники, не позволяющими признать эту сферу имеющей существенное значение в реализации уголовной политики. Особый отличительный признак исследуемого вида преступлений – его высокотехнологичный характер, который определяется использованием современных кибертехнологий, информационно-коммуникационных сетей, различных компьютерных устройств и носителей компьютерной информации и т.д., обычно выступающих как средства совершения такого рода преступлений.

1.2 Виды киберпреступлений: классификация и особенности развития

Высокий уровень доступности при низкой стоимости использования технологий, максимальные возможности извлечения серьезной прибыли при относительно минимальных рисках и высокой степени анонимности обусловили формирование значительного спектра преступных деяний в обозначенной сфере. Киберпреступления направлены практически на все сферы общественной жизни. При этом отсутствует четкое разделение на конкретные виды киберпреступлений. Перечень так называемых «компьютерных преступлений» сформирован на международном уровне. В Будапештской Конвенции Совета Европы выделены группы компьютерных преступлений, связанных с уголовной ответственностью в сфере использования информационных технологий: незаконный доступ (ст. 2); незаконный перехват (ст. 3); вмешательство в данные (ст. 4); вмешательство в систему (ст. 5).

Существуют и другие классификации, но предложенное в них деление является субъектным, поэтому чаще придерживаются классификации, предложенной Конвенцией о киберпреступлениях.

Так, например, Департамент Юстиции США разделяет киберпреступления на следующие категории: преступления, в которых само устройство является целью; преступления, в которых устройство является орудием преступления; преступления, когда устройство является источником хранения.[1]

Киберпреступления можно разделить на множество наиболее актуальных и распространенных видов:

1) преступления, которые направлены против компьютерных систем и баз данных. К данному виду можно отнести широкий перечень киберпреступлений – это хакерские атаки, заражение интернет вирусами и вредоносными программами и т.д. В качестве примера можно привести частые взломы баз данных мобильных

[1] Хисамова, З.И. Зарубежный опыт уголовно-правовой охраны отношений в сфере использования информационно-коммуникационных технологий / З.И. Хисамова // Юридический мир. – 2016. – № 2. С. 61.

операторов с дальнейшим использованием полученной информации в различных целях (получении паспортных данных, рекламные рассылки, последующее использование в мошеннических целях и т.д.). Киберпреступность наиболее ярко проявляется в случае кражи личных данных;

2) преступления, связанные с получением экономической выгоды, например, фишинг – самый распространенный вид мошенничества в интернете. Главная цель данной «преступной махинации» – завладеть логином и паролем виртуальной учетной записи пользователя, и как следствие воспользоваться его личными данными в преступных целях (данные банковских карт, электронные кошельки, «очень личная информация» с перспективой вымогательства и т.д.). Для доступа к учетной записи пользователь предоставляет карту и личный идентификационный номер (PIN-код). Преступники разработали средства для перехвата как данных на магнитной полосе карты, так и PIN-кода пользователя. В свою очередь, эта информация используется для создания поддельных карт, которые затем используются для вывода средств со счета. Особенно эффективной формой мошенничества является использование банкоматов в торговых центрах и магазинах. Там банкоматы стоят отдельно и физически не являются частью банка. Преступники могут легко настроить их для сбора информации о пользователях. Учитывая, что банкоматы являются предпочтительным методом выдачи валюты во всем мире, мошенничество с банкоматами стало международной проблемой;

3) фарминг. Данный способ заключается в перенаправлении пользователей, которые совершают действия в сети Интернет на ложные IP-адреса. Данный способ используется для имитации проверенных и надежных сайтов. Этот способ сложен в исполнении, но гораздо менее заметный, чем фишинг;

4) преступления против свобод и неприкосновенности личности. К данным понятием можно отнести кибербуллинг, грумминг и секстинг. Основные жертвы данных преступлений – это несовершеннолетние. Кибербуллинг, или интернет-травля – это осознанные и целенаправленные оскорбления, угрозы, компроматы в

виртуальном пространстве, которые длятся в течение продолжительного периода времени. Данная травля осуществляется посредством электронных писем, социальных сетей, видеопорталов и т.д. Данное преступное деяние можно трактовать как вмешательство в личное пространство и ущемление свобод и достоинств личности. Как показывает статистика, большинство жертв кибербуллинга – это подростки в возрасте от 12 до 17 лет.[1] Интернет-грумминг – это своеобразный подход взрослого человека к несовершеннолетним с сексуальными целями по средствам интернета; это виртуальное домогательство, совращение несовершеннолетних. Многие аналитики считают, что грумминг в условиях современного мира – это идеальное орудие для педофилов.[2] Секстинг – пересылка информации интимного содержания по средствам информационных технологий (фотографии, видео, сообщения и т.д.). Однако данное понятие в законодательствах многих государств попадает под уголовную ответственность, и рассматривается как синоним распространения детской порнографии;

5) преступления, связанные с содержание контента и нарушением авторских прав. Примерами данных противоправных деяний выступает незаконное распространение фильмов, музыки т.д. В течение 1990-х годов продажи компакт-дисков были основным источником дохода для звукозаписывающих компаний. Хотя пиратство, то есть незаконное копирование материалов, защищенных авторским правом, всегда было проблемой, распространение в университетских кампусах недорогих персональных компьютеров, способных записывать музыку с компакт-дисков и делиться ею в сети Интернет стало значительной проблемой индустрии звукозаписи.

В начале XXI века владельцы авторских прав начали приспосабливаться к идее коммерческого цифрового распространения. Примеры включают онлайн-

[1] Всестороннее исследование проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора // Интернет-портал Организации Объединенных Наций: [сайт]. – URL: http://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_R.pdf (дата обращения: 12.04.2021)

[2] Бородкина, Т.Н. Киберпреступления: понятие, содержание и меры противодействия / Т.Н. Бородкина, А.В. Павлюк // Социально-политические науки. – 2018. – № 1. С. 136.

продажи в iTunes Store (управляемом Apple Inc.) и Amazon.com музыки, телевизионных шоу и фильмов в загружаемых форматах, с ограничениями DRM и без них. Кроме того, провайдеры кабельного и спутникового телевидения, многие электронные игровые системы (PlayStation 3 корпорации Sony и Xbox 360 корпорации Microsoft) и потоковые сервисы, такие как Netflix, разработали сервисы «видео по запросу», которые позволяют клиентам загружать фильмы и шоу для немедленного (потокового) или последующего воспроизведения.

Обмен файлами привел к фундаментальной реконструкции отношений между производителями, дистрибьюторами и потребителями художественного материала. По мере распространения широкополосных подключений к Интернету киноиндустрия сталкивается с аналогичной проблемой, хотя цифровой видеодиск вышел на рынок с шифрованием и различными встроенными попытками избежать проблем, связанных с видео-пиратством. Однако появились сайты, специализировались на обмене такими большими файлами, как фильмы и электронные игры;

6) кибероружие. Данный вид активно применяется для нарушения или уничтожения инфраструктуры. Такие вирусы могут быть несерьезными и направленными на спам или блокирование работы компьютеров, смартфонов и других электронных устройств обычных пользователей, а могут являться действительно серьезной угрозой для систем государственного значения или для банковских систем и других финансовых организаций. Создаются такие вредоносные программы высокоуровневыми профессионалами, которые могут пользоваться продуктом в своих целях или продавать его другим злоумышленникам.

7) киберртерроризм. Данное понятие возникло вследствие очень сильной интеграции виртуального пространства с государством и основными сферами жизни общества. Под данным термином понимают преступные действия, направленные на дезорганизацию электронной, информационной системы общества, вследствие которых может быть причинен большой вред человеку,

обществу и государству. Основная особенность данного вида киберпреступления – масштабность. Главная цель данного противоправного деяния – нанести как можно больший вред человеку, чтобы показать авторитет или, как правило, воздействовать на решения органов власти.

Киберпреступления зачастую предполагают перешедшую в электронную сферу версию обычных преступлений:

1) киберпорнография. К этой категории относятся ресурсы, которые дают пользователям возможность пользователям просматривать материалы эротического содержания с лицами, в том числе, которые не достигли совершеннолетнего возраста. Помимо распространения запрещенных материалов, Интернет также предоставляет педофилам беспрецедентную возможность совершать преступные действия с помощью чатов для выявления и заманивания жертв. Здесь виртуальный и материальный миры пересекаются особенно опасным образом;

2) киберторговля наркотиками. Наркоторговля в сети является наиболее распространенным видом такой торговли в настоящий момент времени. При использовании такого метода преступники используют коды шифрования при отправлении на адреса покупателя писем, в которых содержится информация о местах, где происходит бартер наркотических веществ на деньги;

3) теневые рынки. На так называемых черных рынках продаются разного рода товары, которые в том числе являются незаконными или содержат конфиденциальную информацию физических лиц, которая запрещена к распространению. Добытые путем кражи вещи, сканы и фотографии паспортов также покупаются злоумышленниками для совершения преступлений как в сети Интернет, так и за ее пределами;

4) подделка документов и денег. До недавнего времени создание фальшивых денежных банкнот требовало значительных навыков и доступа к технологиям, которыми граждане обычно не владеют, таким как печатные станки, гравировальные пластины и специальные чернила. Появление недорогих,

высококачественных цветных копировальных аппаратов и принтеров привело к массовому распространению подделок. Широкое развитие и использование компьютерных технологий побудило Казначейства различных стран переработать бумажную валюту, включив в нее различные технологии борьбы с мошенничеством. Кроме того, валюта не является единственным копируемым документом. Так, иммиграционные документы являются одними из самых ценных, и их гораздо легче подделывать, чем денежные банкноты.

Отдельно следует отметить ряд возможных интернет-угроз, которые тесно связаны и в определенном смысле раскрывают данное понятие. Большинство киберпреступлений направлены против виртуальных данных пользователей, а получить доступ к виртуальной среде возможно только по средствам сети Интернет. Среди основных угроз можно выделить:

1) спам – так называемая вредоносная реклама. Электронная почта породила одну из наиболее значительных форм киберпреступности – спам, или нежелательную рекламу товаров и услуг, которая, по оценкам экспертов, составляет примерно 50% электронной почты, циркулирующей в Интернете.[1] Спам является преступлением против всех пользователей Интернета, поскольку он расходует ресурсы как хранилища, так и сетевых возможностей интернет-провайдеров. Тем не менее, несмотря на различные попытки законодательно запретить его существование, остается неясным, как можно устранить спам, не нарушая свободу слова в демократическом государстве. В отличие от нежелательной почты, с которой связаны почтовые расходы, спам почти бесплатен для злоумышленников. Кроме того, данная «рекламная информация» либо уже содержит шпионское программное обеспечение, либо переводит пользователей на сайт с вредоносной программой;

2) интернет атаки – направленная деятельность злоумышленников на

[1] Всестороннее исследование проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора // Интернет-портал Организации Объединенных Наций: [сайт]. – URL: http://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_R.pdf (дата обращения: 12.04.2021)

взлом компьютеров и кражи данных по средствам сети Интернет. В последнее время стали популярны PDF-атаки. Связана такая популярность с малозащищенностью и уязвимостью PDF-фалов;

3) социальные сети – актуальное и перспективное направление реализации киберпреступлений. На просторах социальных сетей распространяется огромное количество вредоносных ссылок и программ;

4) веб-приложения – относительно новое направление интернет угроз. Злоумышленники завладевают целыми базами данных пользователей через «поддельные» приложения;

5) интернет мошенничество – очень популярный вид реализации интернет преступлений. Схемы обмана изобилуют в Интернете. Среди наиболее известных – нигерийская, или афера «419» – число является ссылкой на раздел нигерийского законодательства, который нарушает данная деятельность. Хотя эта афера использовалась как с факсом, так и с традиционной почтой, Интернет дал ей новую жизнь. В рамках этой схемы физическое лицо получает электронное письмо, в котором утверждается, что отправителю требуется помощь в переводе крупной суммы денег из Нигерии или другой отдаленной страны. Обычно эти деньги находятся в форме актива, который будет продан, например, нефть, или большой суммы наличных денег, которая требует «отмывания», чтобы скрыть свой источник; вариации бесконечны, и постоянно разрабатываются новые особенности. В сообщении содержится просьба к получателю покрыть некоторые расходы по переводу средств из страны в обмен на получение гораздо большей суммы денег в ближайшем будущем. Если получатель отвечает чеком или денежным переводом, ему говорят, что возникли осложнения и требуется больше денег. Таким образом, существует огромное количество разнообразных схем от банальных до очень сложных (сюда можно отнести «лотереи», «подружка», «приглашение на работу», «ошибка», «нигерийская афера» и др.).

Самым крупным источником мошенничества является «неуплата/недоставка», когда товары и услуги либо доставляются, но не

оплачиваются, либо оплачиваются, но не доставляются. В отличие от кражи личных данных, когда кража происходит без ведома жертвы, эти более традиционные формы мошенничества. Жертва добровольно предоставляет частную информацию, которая позволяет совершить преступление, следовательно, это транзакционные преступления. Несмотря на огромное количество просветительской работы, интернет-мошенничество остается перспективной отраслью для преступников.

Все эти виды деятельности существовали до того, как префикс «кибер» стал широкоупотребимым. Киберпреступность, особенно связанная с Интернетом, представляет собой расширение существующего преступного поведения наряду с некоторыми новыми незаконными действиями.

Перечисленные виды киберпреступлений также получили широкое распространение в России, где хорошо развиты услуги интернет банков, приложения на Android и IOS, а также сайты в сети Интернет, через которые пользователи осуществляют денежные операции. Экспертами международной компании Group-IB, специализирующейся на предупреждении или расследованиях киберпреступлений, определено, что к основным преступным деяниям, образующим «рынок киберпреступности» в Российской Федерации, следует отнести мошенничество в системах интернет-банкинга; фишинг; хищение электронных денег; услуги по обналичиванию иных нелегальных доходов; спам-рассылки; продажу трафика; продажу эксплойтов; продажу загрузок; анонимизацию; DDoS-атаки.[1] Большинство из указанных деяний еще не нашло своего отражения в уголовном законодательстве РФ, не говоря о разрабатываемых новых кибернетических технологиях.

Действующим УК РФ в общем перечне отношений в сфере информации, подлежащих уголовно-правовой охране, законодательством в отдельную группу

[1] Всестороннее исследование проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора // Интернет-портал Организации Объединенных Наций: [сайт]. – URL: http://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_R.pdf (дата обращения: 12.04.2021)

выделяются отношения, которые возникают в связи с противоправными посягательствами, затрагивающими сферу компьютерной информации (гл. 28 УК РФ), поэтому основной категорией уголовно-правового регулирования выступает «компьютерная информация».

Сущность имеющихся в правовых нормах гл. 28 УК РФ запретов заключается в недопущении общественно опасных деяний, которые могут посягать на безопасность как компьютерной информации, так и систем ее обработки. Поэтому группа выделенных преступлений против компьютерной информации является первой группой преступлений в сфере информационно-коммуникационных сетей и компьютерной информации. Исходя из деления по объекту и субъекту преступления, предметом этой группы преступлений выступает сама компьютерная информация, что вытекает из сути противоправных деяний, установленных в ст. ст. 272, 273 и 274, 274.1 УК РФ. Во вторую группу преступлений следует определить те преступления, где компьютерная информация служит средством совершения преступления. К преступлениям, составы которых находятся в других разделах уголовного закона, можно отнести преступления, предусмотренные ст. ст. 138, 159.6, 171.2, 185.3, ч. 2 ст. 228.1, ч. 2 ст. 242.2 УК РФ и др.

Приведенные различия в подходах к классификации киберпреступлений вызывают необходимость более точного определения видов данных преступлений. На основе выделенных характерных особенностей киберпреступлений, а также с учетом анализа положений Европейской Конвенции по киберпреступности и внутрироссийских нормативных актов и документов, касающихся материальных норм права, возможно структурировать типы и виды киберпреступлений, которые представляют угрозу для национальной безопасности:

1) преступления против конституционных прав и свобод человека и гражданина;

2) преступления против жизни и здоровья;

3) преступления против чести и достоинства лица;

4) преступления против собственности;

4) финансовые преступления, сущность которых заключается в применении фишинговых сайтов и приемов социальной инженерии для получения доступа к персональным данным клиентов финансовых услуг;

5) преступления в сфере компьютерной информации, в первую очередь – неправомерный доступ к информации и созданию, использованию и распространению вредных программ;

6) преступления против общественной нравственности;

7) преступления в сфере незаконного оборота наркотических средств и психотропных веществ;

8) преступления против безопасности государства;

9) кибертерроризм и киберэкстремизм.

Таким образом, подводя итог изложенному, можно сделать вывод, что киберпреступность охватывает широкий спектр видов деятельности. Киберпреступность затрагивает как виртуальные, так и реальные объекты, но последствия для каждого из них различны. Кибернетическая преступность выступает как особая разновидность преступности, которая находится в тесной взаимосвязи с иными видами преступлений в Российской Федерации в силу того, что кибернетическим преступлениям часто свойственно использование способов совершения иных уголовно наказуемых деяний. Проведенный анализ позволил констатировать отсутствие четкого понимания возможностей механизма уголовного законодательства при осуществлении противодействия новым способам криминальной деятельности в сфере реализации кибертехнологий, круга таких преступлений, недостаточное и противоречивое правовое закрепление терминологического аппарата в российском уголовном законодательстве.

1.3 Проблемы разграничения составов киберпреступлений

Перевод имущественных отношений в Интернет-пространство способствует и появлению и распространению имущественных киберпреступлений. Необходимость о криминализации некоторых преступлений против собственности, совершаемых при помощи высоких технологий, обосновывалась достаточно давно.[1] Сегодня данные научные идеи нашли отражение в уголовном законе и оказались весьма своевременными. Однако тесное переплетение посягательств на имущество, совершаемых при помощи высоких технологий, с уголовно наказуемыми деяниями в сфере компьютерной информации, а также между собой способно внести путаницу в процесс квалификации.

Многоаспектный характер киберпреступлений осложняется проблемами их разграничения со смежными составами преступных посягательств, предметом которых также выступает компьютерная информация.

Особенностью объективной стороны преступлений в сфере информационно-коммуникационных сетей и компьютерной информации выступает способ их совершения. Ввиду инновационности способа совершения преступлений порождаются не только многочисленные вопросы их раскрытия и расследования (сбора доказательственной базы, реализации результатов оперативно-розыскных мероприятий и т.д.), но, в первую очередь, вопросы квалификации и отграничения от смежных составов преступлений.

Если речь идет о мобильной связи и сети Интернет, где находит свое отражение компьютерная информация, основными составами, граничащими с составами преступлений рассматриваемой группы, будут являться преступления в сфере компьютерной информации.

Объективная сторона исследуемых групп преступлений достаточно схожа.

---

[1] Зверянская, Л.П. Исторический анализ этапов развития киберпреступности и особенности современных киберпреступлений / Л.П. Зверянская // Научно-методический электронный журнал «Концепт». – 2016. – Т. 15. С. 881.

Воздействие на компьютерную информацию происходит как собственно в целях неправомерного доступа к ней, так и с целью совершения преступления против собственности. Вместе с тем, если в первом случае воздействие на компьютерную информацию выступает в роли собственно деяния, то во втором случае указанное воздействие является средством совершения преступления. Неправомерный доступ к компьютерной информации либо создание и использование вредоносных компьютерных программ, нарушение правил эксплуатации средств хранения информации, являясь самостоятельными преступлениям, при совершении преступлений против собственности выступают в качестве подготовительных действий.

Таким образом, если лицо совершило, к примеру, неправомерный доступ к компьютерной информации с целью приготовления к совершению преступления против собственности, но, по не зависящим от него обстоятельствам, не смогло совершить посягательство на имущество (например, хакерская атака была выявлена сотрудниками правоохранительных органов), его действия следует квалифицировать по ст. 272 УК РФ, а также (при наличии умысла и при условии, что преступление относится к категории тяжких), по ч. 1 ст. 30 и ч. 3 или ч. 4 ст. 159.6 УК РФ. Подобной точки зрения придерживаются и суды. Так, в обзоре судебной практики по делам о мошенничестве, присвоении и растрате указано, что, если не наступили последствия в виде материального ущерба собственнику или иному обладателю имущества по причинам, не зависящим от воли виновного при совершении мошенничества путем воздействия на компьютерную информацию, его действия следует квалифицировать как покушение на данное преступление и по совокупности с действиями, ответственность за которые предусмотрена ст. 272 или 273 УК РФ.[1]

Но таким образом имеет место применение принципа двойного вменения, что противоречит постулату «не дважды за одно и то же». Тогда можно сделать

[1] О судебной практике по делам о мошенничестве, присвоении и растрате: Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 // Бюллетень Верховного Суда РФ. – 2018. – № 2.

вывод, что включение ст. 159.6 в УК РФ не вполне обоснованно.

С одной стороны, введение отдельной статьи в Уголовный кодекс упрощает задачу правоприменителям в выявлении и расследовании преступлений, с другой – содеянное, как и ранее, можно квалифицировать по совокупности преступлений, охватывая умысел основного состава мошенничества. На практике также нет единого мнения по поводу применения нормы, поскольку четко обозначенные рекомендации Верховного Суда РФ относительно применения указанной нормы отсутствуют.

Вместе с тем, при совершении преступлений против собственности, доступ к компьютерной информации может осуществляться и правомерно, однако, действия, производимые с данной информацией, будут противоправными. Показателен приговор в отношении М., вынесенный Железнодорожным районным судом г. Читы Забайкальского края. М. приобрела сим-карту для личного пользования. К данной сим-карте ошибочно была подключена услуга «Мобильный банк» (возможно номер указанной карты ранее использовался иным владельцем). М. при активации указанной сим-карты получила смс-оповещение о перечислении на счет К. 10000 рублей.

У М. возник умысел на хищение указанных денежных средств, который был ею реализован.[1] В данном случае М., являясь собственником сим-карты, имела правомерный доступ ко всей информации, содержащейся в телефоне и поступающей на принадлежащий ей абонентский номер, однако неправомерно воспользовалась указанной информацией, в связи с чем суд справедливо квалифицировал ее действия лишь по ч. 2 ст. 159.6 УК РФ.

Существует мнение, что мошенничество, составляющее более 70% от общего числа преступлений против собственности, совершаемых посредством мобильной связи или сети Интернет, является своего рода продолжением, следующей ступенью развития неправомерного доступа к компьютерной

[1] Приговор Железнодорожного районного суда г. Читы (Забайкальский край) от 22 апреля 2016 г. № 1-166/2016 // Интернет-портал «Судебные и нормативные акты Российской Федерации»: [сайт]. – URL: https://sudact.ru/ (дата обращения: 12.04.2021)

информации и создания, использования или распространения вредоносных компьютерных программ.[1] Как показывает практика, чаще всего ст. 159.6 УК РФ применяется по совокупности со ст. 272 УК РФ, предусматривающей ответственность за неправомерное завладение компьютерной информацией. Так, например, для хищения «электронных денег» преступнику необходимо сначала получить код доступа. Однако подобная квалификация вызывает сомнения у ряда ученых. Например, Р.Д. Шарапов полагает, что «по существу неправомерный доступ к охраняемой законом компьютерной информации в целях хищения чужого имущества или приобретения права на чужое имущество, является способом нового вида мошенничества в сфере компьютерной информации. Вследствие этого уголовно-правовые нормы, предусмотренные ст. 159.6 и ст. 272 УК РФ, состоят между собой в отношениях конкуренции частей и целого, где ст. 159.6 предусматривает норму-целое».[2] Данную позицию можно признать справедливой лишь отчасти, поскольку, несмотря на присутствие в диспозиции ст. 272 УК РФ указания на корыстную заинтересованность лица, объект, подлежащий охране, в указанных случаях все-таки различен.

Очевидное отличие составов преступлений против собственности, совершаемых посредством мобильной связи или сети Интернет, от компьютерных преступлений, состоит в предмете посягательства. В первом случае предметом выступают денежные средства и иное имущество, а во втором случае – компьютерная информация. Следует также учитывать тот факт, что компьютерная информация при совершении преступления против собственности скорее будет относиться к средству совершения преступления.

Субъективная сторона рассматриваемых преступлений отличается преимущественно целью. Для преступлений против собственности характерна цель завладения имуществом или причинения имущественного ущерба, для

[1] Простосердов, М.А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им: дисс. … канд. юрид. наук / М.А. Простосердов. – Москва, 2016. С. 137.

[2] Особенности противодействия киберпреступности подразделениями уголовного розыска / под ред. Б.П. Михайлова, Е.Н. Хазова. – Москва : ЮНИТИ-ДАНА: Закон и право, 2016. С. 50.

компьютерных преступлений цель может быть самой разнообразной: получение сведений, составляющих государственную или коммерческую тайну, плагиат, уничтожение важной для потерпевшего компьютерной информации из желания отомстить или по другой причине и т.п.

Особую роль в субъективной стороне рассматриваемых преступлений играет мотив. Для посягательств на имущество характерен корыстный мотив, для компьютерных преступлений возможно наличие любого мотива (мести, хулиганских побуждений, вражды и пр.). Однако следует отметить, что в статьях 272 и 273 УК РФ предусмотрен квалифицирующий признак «совершенное из корыстной заинтересованности». И.А. Клепицкий определяет корыстную заинтересованность как мотивацию, направленную на извлечение какой-либо имущественной (исчисляемой деньгами) выгоды для себя или другого лица.[1] В таком случае возникает вопрос о том, каким образом отграничивать мошенничество в сфере компьютерной информации от неправомерного доступа к компьютерной информации, совершенного из корыстной заинтересованности. И.А. Клепицкий, принимая статью 159.6 УК РФ за специальную норму по отношению к статье 272 УК РФ, указывает, что при наличии в содеянном всех признаков мошенничества в сфере компьютерной информации содеянное квалифицируется по ст. 159.6 УК РФ и дополнительная квалификация по ст. 272 УК РФ не требуется.[2] При отграничении рассматриваемых составов друг от друга следует учитывать наличие или отсутствие всех признаков конкретного состава. Так, например, корыстная заинтересованность при неправомерном доступе к компьютерной информации может заключаться в получении вознаграждения за такой доступ от заинтересованного лица, либо информация может быть получена с целью последующего шантажа потерпевшего, а также с целью вымогательства.

В данном случае компьютерная информация не выступает средством обмана или злоупотребления доверием, не является она также средством,

[1] Научная платформа: дискуссия и полемика: сборник материалов Международной научно-практической конференции (30 октября 2020 г.). – Кемерово : ЗапСибНЦ, 2020. С. 11.

[2] Там же. С. 12.

облегчающим доступ к денежным средствам или иному имуществу (т.е. неким «ключом от сейфа»). Компьютерная информация должна расцениваться как предмет преступления. Если при совершении преступления против собственности компьютерная информация является одной из составляющих «структуры способа», то в случае с преступлениями в сфере компьютерной информации последняя выступает предметом.

Несмотря на внешнюю схожесть рассмотренных составов преступлений, они все же обладают существенными отличиями, чем и обусловлено размещение норм об ответственности за данные преступления в разных разделах уголовного закона. В процессе квалификации все обозначенные особенности должны быть учтены во избежание двойного вменения и нарушения принципа справедливости. В связи с этим отсутствует возможность неправильной квалификации преступления из-за схожести с другими составами преступления.

Таким образом, подводя итог изучению уголовно-правовой характеристики преступлений, совершаемых в киберпространстве, можно заключить, что единого и широко распространенного определения киберпреступности до сих пор не существует. Хотя положения Конвенции о киберпреступности, являются мощными инструментами для гармонизации борьбы с киберпреступностью, законодатели различных стран используют различные термины для обозначения группы преступлений, связанных с использованием информационно-коммуникационных технологий.

Каждая из статей киберпреступлений обладает составом уникальных отличительных признаков. В связи с этим отсутствует возможность неправильной квалификации преступления из-за схожести с другими составами преступления.

Четкое разграничение киберпреступности от других преступных деяний позволяет проводить конкретную внешнюю и внутреннюю политику в области борьбы с постоянно развивающимся спектром киберугроз, восполнять многие правовые пробелы и лазейки, которыми могут воспользоваться преступники во избежание уголовной ответственности за свои преступные деяния.

2 КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ В КИБЕРПРОСТРАНСТВЕ

2.1 Состояние, структура, динамика киберпреступности на территории ХМАО-Югры

Согласно статистическим данным Главного информационно-аналитического центра МВД России на территории Ханты-Мансийского автономного округа за 2020 год зарегистрировано совершение 20977 преступлений, что на 1621 ниже уровня 2016 года. Уровень регистрируемой преступности за анализируемый период снизился на 7,17% (рисунок 2.1).

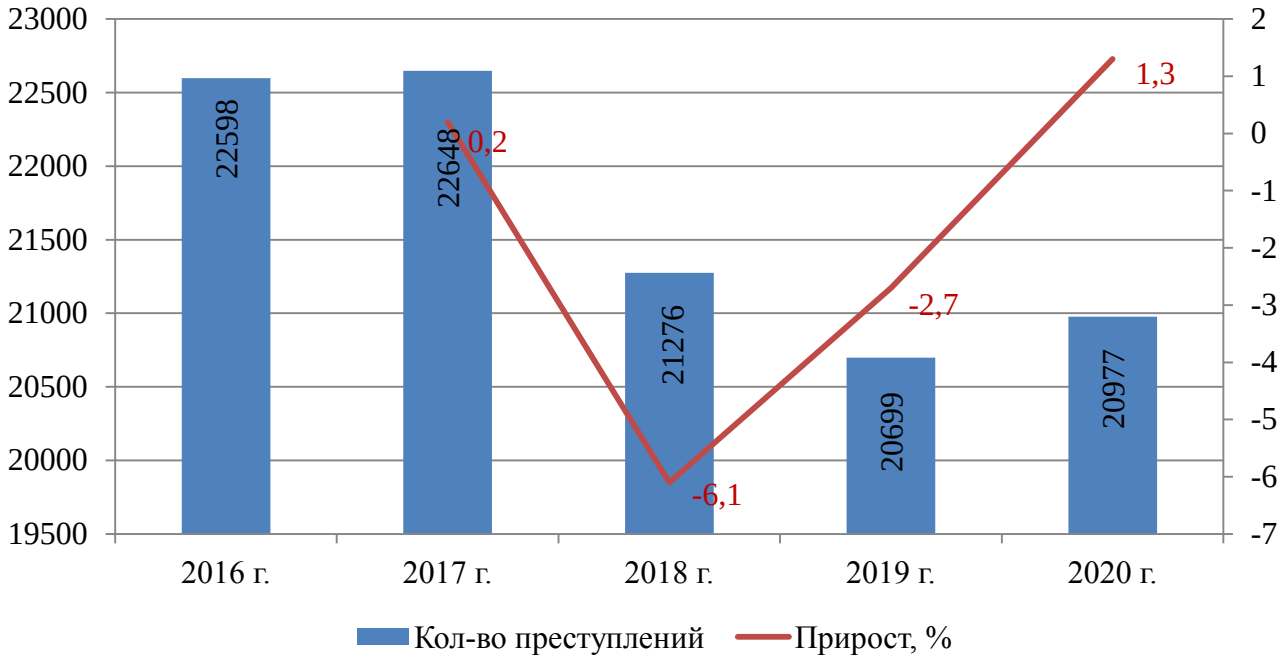

Рисунок 2.1 – Количество преступлений, зарегистрированных в ХМАО-Югре[1]

Несмотря на положительную динамику, Ханты-Мансийский автономный округ возглавляет рейтинг регионов, где происходит наибольшее количество преступлений с использованием информационно-телекоммуникационных технологий.

Так, за период с 2016 по 2020 г. доля преступлений с использованием

[1] Преступность в регионах // Портал правовой статистики [сайт]. – URL: http://crimestat.ru/regions_chart_total (дата обращения 12.04.2021)

информационно-телекоммуникационных технологий возросла до 39,9% (рисунок 2.2).

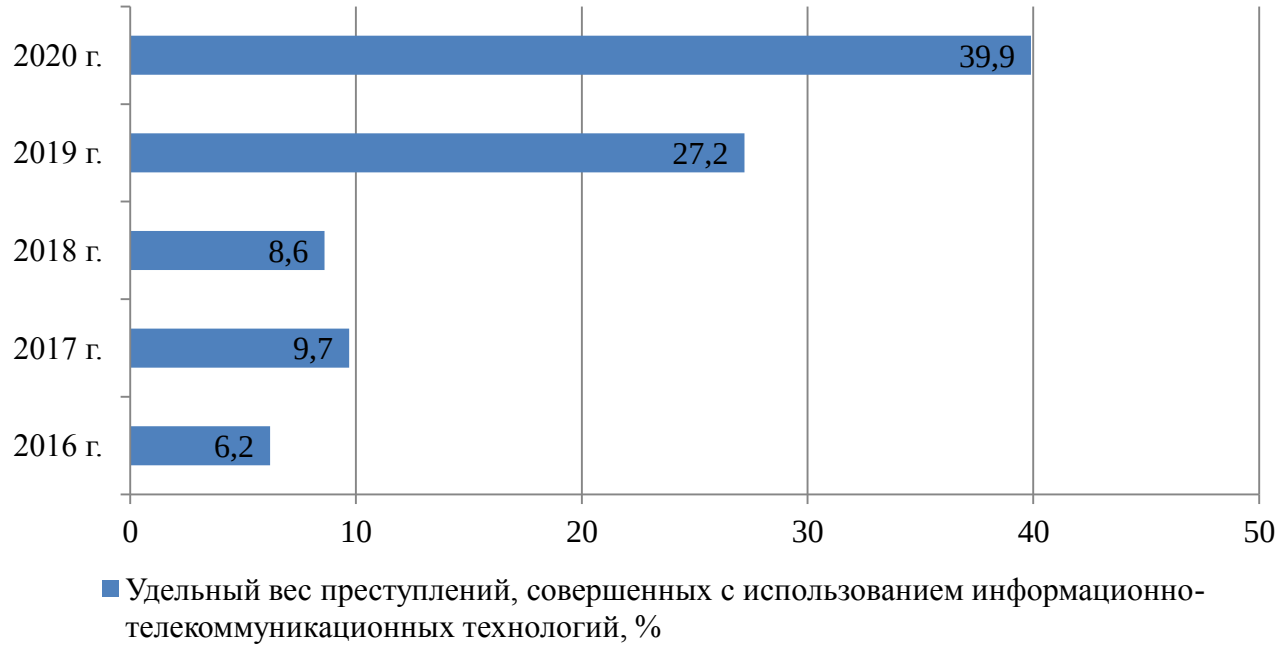

Рисунок 2.2 – Доля преступлений, совершенных с использованием информационно-телекоммуникационных технологий в общем количестве преступлений, зарегистрированных в ХМАО-Югре, %[1]

Там в 2018 году на территории округа 27,2% всех преступлений были связаны с информационно-телекоммуникационной сферой. В 2019 году в ХМАО-Югре был зафиксирован самый высокий процент преступлений с использованием информационно-телекоммуникационных технологий – 39,9%.

Количество регистрируемых киберпреступлений варьируется в зависимости от конкретного состава. На преступления, связанные с незаконным оборотом наркотических средств и психотропных веществ, приходится лишь 9,22% всех преступлений, на экономические – 3,4%. Постепенно меняется и структура краж – грабители осваивают интернет и телекоммуникации.

Динамика киберпреступлений в разрезе соответствующих норм УК РФ

[1] Состояние преступности в Югре // Управление МВД России по Ханты-Мансийскому АО – Югре [сайт]. – URL: http:// 86.мвд.рф/Dejatelnost/Sostojanie_prestupnosti_v_JUgre (дата обращения 12.04.2021)

представлена в таблице 2.1.

Таблица 2.1 – Динамика преступлений, совершенных в ХМАО-Югре с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации[1]

Показатели	Значение, количество преступлений				
	2016 г.	2017 г.	2018 г.	2019 г.	2020 г.
Всего преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации	1401	2197	1830	5630	8370
из них					
тяжких и особо тяжких	679	1065	887	2729	4388
в том числе					
1) совершенных с использованием или применением:					
расчетных (пластиковых) карт	164	257	214	658	3119
компьютерной техники	87	136	113	349	470
программных средств	30	47	39	120	165
фиктивных электронных платежей	5	7	6	19	23
сети «Интернет»	747	1172	976	3003	4925
средств мобильной связи	553	867	722	2221	3587
2) по видам:					
кража ст. 158 УК РФ	470	737	614	1889	2844
мошенничество ст. 159 УК РФ	571	895	745	2293	3452
мошенничество с использованием электронных средств платежа ст. 159.3 УК РФ	77	120	100	309	424
мошенничество в сфере компьютерной информации ст. 159.6 УК РФ	3	5	4	13	13
незаконные организация и проведение азартных игр ст. 171.2 УК РФ	4	6	5	16	13
публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма ст. 205.2 УК РФ	1	2	1	4	4
изготовление порнографических материалов ст. 242, 242.1, 242.2 УК РФ	9	14	12	37	34

[1] Состояние преступности в Югре // Управление МВД России по Ханты-Мансийскому АО – Югре [сайт]. – URL: http:// 86.мвд.рф/Dejatelnost/Sostojanie_prestupnosti_v_JUgre (дата обращения 12.04.2021)

Продолжение таблицы 2.1

Показатели	Значение, количество преступлений				
	2016 г.	2017 г.	2018 г.	2019 г.	2020 г.
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 ст. 228.1 УК РФ	117	184	153	472	772
публичные призывы к осуществлению экстремистской деятельности ст. 280 УК РФ	1	2	2	5	6
преступления в сфере компьютерной информации глава 28 УК РФ	14	22	18	55	74
в том числе					
неправомерный доступ к компьютерной информации ст. 272 УК РФ	11	18	15	46	67
создание, использование и распространение вредоносных компьютерных программ ст. 273 УК РФ	3	4	3	9	7

В 2016 г. на территории округа было зарегистрировано 1401 преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, к 2020 г. таких преступлений стало почти в 6 раз больше – 8370.

Примечательно, что преступлений, предусмотренных ст. 274 УК РФ о нарушении правил эксплуатации средств хранения, обработки или передачи компьютерной информации, не зарегистрировано за анализируемый период. Количество преступлений, предусмотренных ст. 272 УК РФ, о неправомерном доступе к компьютерной информации, напротив, возросло до 67 в 2020 г. по сравнению с 11 случаями в 2016 г. В целом преступления в сфере компьютерной информации глава 28 УК РФ составляют менее 1% в структуре киберпреступлений округа.

Самыми популярными киберпреступлениями являются кража (ст. 158 УК

РФ), мошенничество (ст. 159 УК РФ), а также мошеннические действия, совершенные с использованием электронных средств платежа (ст. 159.3 УК РФ). Преступники, представляясь близкими родственниками (знакомыми) потерпевших, просят о передаче или перечислении электронным платежом определенной суммы денежных средств для разрешения сложившейся в их жизни неблагоприятной ситуации. К примеру, в связи с необходимостью освобождения их от уголовной ответственности. Нередко злоумышленники сами представляются сотрудниками органа правопорядка (рисунок 2.3).

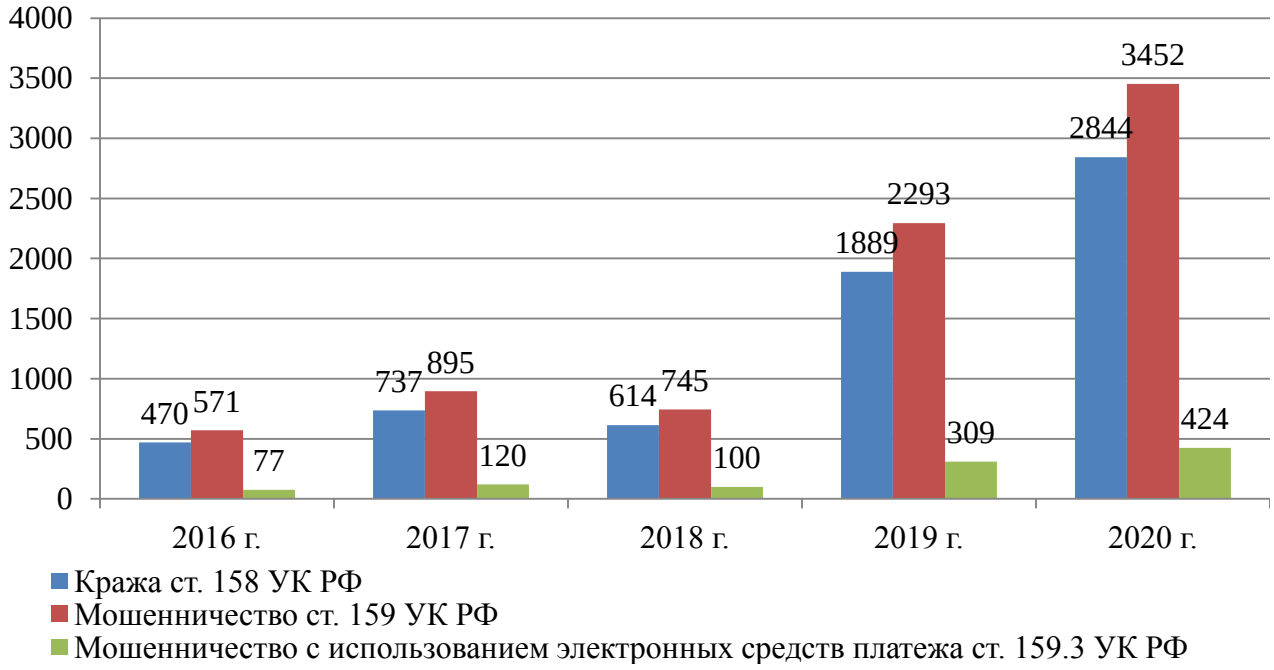

Рисунок 2.3 – Динамика наиболее распространенных киберпреступлений, зарегистрированных в ХМАО-Югре[1]

Рост преступлений, предусмотренных ст. 159.3 УК РФ наблюдался в 2019 г. – темп роста составил 209%. В 2020 г. темп роста замедлился, составив 37,2%.

К основным видам мошенничества с использованием платежных карт относят использование неполученных, поддельных украденных или утерянных карт, проведение транзакций с использованием украденных реквизитов,

[1] Состояние преступности в Югре // Управление МВД России по Ханты-Мансийскому АО – Югре [сайт]. – URL: http:// 86.мвд.рф/Dejatelnost/Sostojanie_prestupnosti_v_JUgre (дата обращения 12.04.2021)

несанкционированное использование персональных данных держателя карты и информации по счету клиента и пр.

Наряду с крайне высокими темпами роста киберпреступности, отмечается низкий уровень раскрываемости данной группы преступлений.

Количество расследованных преступлений по рассмотренным статьям уменьшилось в 2020 году на 3,56 процентных пункта. Общая раскрываемость составила 18,60%.

Рисунок 2.4 – Динамика раскрываемости киберпреступлений, зарегистрированных в ХМАО-Югре[1]

Низкий уровень раскрываемости киберпреступлений обусловлен следующими факторами:

1) несовершенство действующего уголовного законодательства: имеющихся уголовно-правовых норм в сфере использования информационно-телекоммуникационных технологий или компьютерной информации недостаточно, они сложны и запутанны для понимания как субъектов судебного

[1] Состояние преступности в Югре // Управление МВД России по Ханты-Мансийскому АО – Югре [сайт]. – URL: http:// 86.мвд.рф/Dejatelnost/Sostojanie_prestupnosti_v_JUgre (дата обращения 12.04.2021)

процесса, так и сотрудников правоохранительных органов. Кроме того, они не отражают весь спектр современных киберпреступлений (майнинг, DDoS);

2) санкции за совершение киберпреступлений преимущественно предусматривают условное наказание;

3) киберпреступления расследуют сотрудники МВД с юридическим образованием, тогда как во многих странах мира следователи по киберпреступлениям – это, прежде всего, технические эксперты с дополнительным юридическим образованием.

Преступления в сфере высоких технологий являются сложными для расследования, они требуют специальных знаний, опыта и ресурсов со стороны сотрудников правоохранительных органов. Очередь на проведение компьютерных экспертиз в государственных экспертных учреждениях, как правило, превышает полгода, специалистов в области киберрасследований в полиции крайне мало и большинство из них находится в Москве. Существенная часть бытовых киберпреступлений (взлом социальных сетей или мессенджеров, вирусные атаки на домашние компьютеры) не фиксируется.[1]

4) низкий уровень защищенности. Пользователи информационно-телекоммуникационных технологий нередко имеют минимальные знания о компьютерной гигиене и правилах безопасной работы в Интернете;

Низкий уровень раскрываемости киберпреступлений связан не с появлением новых способов совершения киберпреступлений, а со специфичным понятийным аппаратом и необходимостью проведения большого объема процессуальных действий.

Таким образом, методы совершения преступлений постоянно эволюционируют, при этом преступниками активно используются современные информационно-телекоммуникационные технологии, которые зачастую просты в использовании и доступны неограниченному числу пользователей сети Интернет.

[1] Демин, Ю.В. Организационно-правовые основы выявления и раскрытия краж, совершаемых с банковского счета, а равно в отношении электронных денежных средств / Ю.В. Демин // Российский следователь. – 2021. – № 1. С. 66.

2.2 Причины, условия и средства совершения киберпреступлений

Среди причин и условий возникновения такого преступного явления как киберпреступность выделяют основные: непосредственно сам процесс компьютеризации и автоматизации (усовершенствование информационных технологий и расширение производств; виртуальных форм финансовых расчетов и платежей), а также уровень развития страны, то есть ее экономическая составляющая. Компьютерные и телекоммуникационные сети позволяют совершать атаки злоумышленникам, которые могут быть значительно удалены от жертв. Кроме этого выделяют такие условия и мотивы как доступность, прибыльность и факт удаленности, которые благоприятно влияют на сложность раскрытия таких преступлений.

С точки зрения жертвы, интернационализация информационно-коммуникационных технологий привела к широкому распространению виктимизации. В информационных обществах пользователями высокотехнологичного оборудования являются корпорации (т.е. компании и государственные органы) и частные лица. У многих пользователей нет необходимого уровня технических знаний и времени, необходимого для обслуживания их компьютеров (обновления программного обеспечения и установки различных программ безопасности). Из данных, предоставленных Интерполом, ясно, что наиболее частыми жертвами кибератак являются коммерческие компании, а затем государственные учреждения. Причины, по которым корпоративный мир и само современное политическое государство являются главными жертвами киберпреступности, имеют структурную причину. Культура хакеров, которая все еще находится в эпицентре Интернета, была в первую очередь основным фактором интернализации Интернета. В то же время культура хакеров остается диаметрально противоположной «культуре» жертв, которые преследуют цели максимизации прибыли и монополизации выгод об их интеллектуальном участии в киберпространстве. Именно столкновение этих двух

культур порождает конфликт.

Однако большинство пострадавших субъектов не выступают за раскрытие информации о нападении, которому они подвергаются, поскольку это часто только выявило бы их уязвимость и подверженность ошибкам. Такие разоблачения могут нанести ущерб дальнейшему экономическому успеху этих жертв, поскольку они проявили низкий уровень ответственности к обеспечению безопасности финансовых операций и разглашение информации может повлечь снижение доверия общественности. Последствия такого раскрытия особенно серьезны с точки зрения политического государства, объективность и возможности которого являются непременным условием его деятельности. Другими словами, вторичная виктимизация этих субъектов больше, чем первичная виктимизация (деяние, совершенное преступником), и латентность преступлений оценивается как крайне значительная. Изложенное способствует дальнейшей преступной деятельности.

Однако эти факты могут служить препятствиями для уголовных расследований и научных исследований, поскольку многое просто остается неизвестным или нераскрытым: например, субкультурные особенности, такие как мотивы преступников, конкретный способ действий и т.д.

Статистические данные показывают, что кибератаки были преимущественно мотивированных любопытством преступников. Исследователи подчеркивают, что эта тенденция меняется, поскольку продолжающиеся атаки становятся более серьезными, более разрушительными, лучше спланированными и более изощренными.[1] Несмотря на этот человеческий фактор, сама природа киберпространства также является чрезвычайно криминогенной из-за расплывчатости границ, отделяющих законное от незаконного и «нормальное» от «ненормального» поведения. Помимо «преступников из любопытства» остается еще одна группа преступников. Криминологический тезис о том, что жертвы

[1] Евдокимов, К.Н. Криминологические и уголовно-правовые аспекты противодействия компьютерной преступности в России (социологическое исследование) / К.Н. Евдокимов // Российский следователь. – 2020. – № 11. С. 42.

очень похожи (в поведении, отношении к государственной власти, образе жизни и т.д.) на преступников в данной сфере, подтверждается также в контексте киберпреступности. В одной узкой области кибер-девиантности, то есть спама, жертвы фактически становятся преступниками, поскольку именно основные жертвы наводняют Интернет спамом. Исследования показали, что 70% спама поступает с зараженных компьютеров, которые на самом деле принадлежат его первоначальным получателям.[1]

В литературе одним из условий совершения киберпреступлений является наличие значительных технических знаний. Однако статистические данные показывают, что киберпреступники преимущественно имеют уровень полного среднего образования.[2]

В ранние годы развития информационно-коммуникационных технологий лица, совершающие киберпреступления, должны были обладать высокими знаниями и навыками в сфере компьютеризации, но в настоящее время для совершения киберпреступления достаточно иметь доступ в Интернет. Таким образом, в настоящий момент для совершения киберпреступления более не требуется обладание сложными навыками или знание сложных методов.

Чаще всего одним из отличительных признаков киберпреступности являются получение финансовых благ и выгоды. Почти все преступления охватываемые диапазоном киберпреступности совершаются для достижения этой цели.

Помимо этого некоторые криминологи определяют некую зависимость между киберпреступностью и организованными группами.[3] Организованные преступные группы используют новые возможности для совершения

[1] Малов, А.А. Международные правовые стандарты истребования электронных доказательств от иностранных юрисдикций / А.А. Малов // Международное уголовное право и международная юстиция. – 2021. – № 1. С. 19.

[2] Евдокимов, К.Н. Криминологические и уголовно-правовые аспекты противодействия компьютерной преступности в России (социологическое исследование) / К.Н. Евдокимов // Российский следователь. – 2020. – № 11. С. 43.

[3] Овсюков, Д.А. Использование информационно-телекоммуникационных сетей при совершении вымогательства / Д.А. Овсюков // Актуальные проблемы российского права. – 2021. – № 2. С. 142.

преступлений, руководствуясь стремлением к извлечению прибыли и получению личной выгоды.

Киберпреступники всегда выбирают простой способ заработать большие деньги. Они нацелены на состоятельных людей или крупные организации, такие как банки, казино и финансовые организации, где ежедневно поступает значительное количество денег, и взламывают конфиденциальную информацию. Поймать таких преступников трудно. Следовательно, это увеличивает количество киберпреступлений по всему миру. Компьютеры уязвимы, поэтому необходимы законы для их защиты и защиты от киберпреступников. Можно выделить ряд причин уязвимости компьютеров:

– простота доступа. Проблема защиты компьютерной системы от несанкционированного доступа заключается в том, что существует множество возможностей взлома из-за сложной технологии. Хакеры могут украсть коды доступа, изображения сетчатки глаза, продвинутые диктофоны и т.д., могут легко обмануть биометрические системы и брандмауэры, чтобы обойти многие системы безопасности;[1]

– емкость для хранения данных в сравнительно небольшом пространстве. Компьютер обладает уникальной характеристикой хранения данных в очень небольшом пространстве. Это значительно облегчает преступникам кражу данных из любого другого хранилища и использование их для собственной выгоды;

– пробелы программирования. Компьютеры работают на операционных системах, и эти операционные системы запрограммированы на миллионы кодов. Человеческий разум несовершенен, поэтому они могут совершать ошибки на любом этапе. Киберпреступники пользуются этими пробелами;[2]

[1] Приговор Нижневартовского городского суда Ханты-Мансийского автономного округа – Югры от 28 июля 2020 г. по делу № 1-521/2020 // Интернет-портал «Судебные и нормативные акты Российской Федерации»: [сайт]. – URL: https://sudact.ru/ (дата обращения: 12.04.2021)

[2] Приговор Нижневартовского городского суда Ханты-Мансийского автономного округа – Югры от 17 июля 2020 г. по делу № 1-97/2020 // Интернет-портал «Судебные и нормативные акты Российской Федерации»: [сайт]. – URL: https://sudact.ru/ (дата обращения: 12.04.2021)

– небрежность. Небрежность является одной из характеристик поведения человека. Таким образом, существует вероятность того, что, защищая компьютерную систему, человек может совершить любую небрежность, которая обеспечивает киберпреступный доступ и контроль над компьютерной системой;

– потеря доказательств. Данные, связанные с преступлением, могут быть легко уничтожены. Потеря доказательств стала очень распространенной и очевидной проблемой, которая парализует систему расследования киберпреступлений.[1]

Серьезным фактором, осложняющим как профилактику, так и борьбу с киберпреступлениями, выступает высокая степень ее латентности по разным видам уголовно наказуемых деяний, что во многом обуславливается определенными объективными факторами, среди которых нежелание жертв искать защиты в правоохранительных органах, незаметность компьютерных преступлений для подавляющего большинства населения по причине их совершения в киберсреде, сложность в выявлении компьютерных преступлений и т.д.

Высокий уровень латентности данных преступлений связан со многими причинами, такими как незначительный ущерб, нежелание потерпевшего обращаться к правоохранительным органам, не возможность выявления самого факта преступления и т.д. Стоит также подчеркнуть, что данная безнаказанность служит своего рода импульсом для популярности киберпреступлений.

Вторая причина выражена в высоком уровне профессионализма преступников. Как правило, киберпреступники, или так называемые хакеры, имеют очень высокий уровень теоретических и практических знаний. У некоторых данный талант проявляется довольно в раннем возрасте. Например, известен случай, когда 14-летний подросток взломал сервер NASA для того,

[1] Приговор Нефтеюганского районного суда Ханты-Мансийского автономного округа – Югры от 6 июля 2020 г. по делу № 1-342/2020 // Интернет-портал «Судебные и нормативные акты Российской Федерации»: [сайт]. – URL: https://sudact.ru/ (дата обращения: 12.04.2021)

чтобы хранить там свои виртуальные данные.[1]

Третья проблема заключается в сборе доказательств совершения киберпреступления. Для привлечения к ответственности киберпреступника необходимо доказать его причастность к данному деянию. «Виртуальные следы» противоправного деяния легко скрыть ввиду легкости изменения и уничтожения компьютерной информации. Очень сложна, а порой и не возможна процедура оформления, изъятия данных доказательств. Данные факты затрудняют доказывание вины и причастности лица к виртуальному преступлению, тем самым способствую увеличению процента нераскрытых преступлений.

Следующая причина выражена в юридической проблеме. Сюда следует отнести малорегламентированность или вовсе отсутствие регламентации со стороны нормативно-правовых актов. Суть данной проблемы заключается в отсутствии актуального законодательства, которое отвечало бы современным реалиям. Порой вообще отсутствует уголовная или иные виды ответственности за деяния в виртуальной сфере.

Следующая причина – отсутствие необходимых технических средств противодействия киберпреступлениям, или техническая проблема. Зачастую техника преступников в разы превосходит технику правоохранительных органов. Данный факт показывает невозможность раскрытия некоторых преступлений в связи с некой отсталостью в «технологиях».[2]

Кроме того, невозможность оперативно скоординировать деятельность правоохранительных органов через государственные границы, пределы юрисдикций и многообразие законодательных систем государств, приводят к длительности или неэффективности действий при раскрытии данного вида преступлений.

---

[1] Роль и место информационных технологий в современной науке: сборник статей Международной научно-практической конференции (17 января 2019 г, г. Самара). В 3 ч. Ч. 2. – Уфа : OMEGA SCIENCE, 2019. С. 75.

[2] Русскевич, Е.А. Международно-правовые подходы противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий / Е.А. Русскевич // Международное уголовное право и международная юстиция. – 2018. – № 3. С. 12.

Так как обычные сотрудники полиции не обладают должными знаниями в сфере компьютерных технологий, поэтому они не имеют возможности эффективно бороться с хакерами и другими киберпреступниками. В России в 1997 г. в связи с вступлением в действие нового Уголовного кодекса РФ для раскрытия и работы со спецификой незаконной деятельности в области компьютерных средств и технологий была создана отдельная структура в правоохранительных органах – Управление «К». Данное подразделение МВД России – это особое управление, основная деятельность которого направлена на борьбу с преступлениями в киберпространстве. Также в его задачи входит пресечение преступлений по пропаганде различных экстремистских идей, движений и направлений, которые совершаются с использованием сети Интернет, а также пресечение совершения правонарушений по незаконному обороту наркотических и психотропных средств, которые используют сеть Интернет для бесконтактного способа оплаты и сообщения о месте нахождения «пакета» с наркотиками.

Для защиты персональных данных и баз данных автоматизированных систем от незаконного доступа создано в прокуратуре РФ специальное подразделение, занимающее мониторингом Интернет-пространства, обнаружением вредоносных программных продуктов, установлением их возникновения и устранением воздействия угроз на незаконный доступ к неизменной хранимой информации.

Учитывая транснациональный характер данной деятельность, следует усилить международное сотрудничество органов уголовной юстиции в данной сфере для повышения эффективности противодействия данной преступной деятельности.

Другим значимым фактором развития кибернетической преступности служит ее высокоорганизованный характер и тесная взаимосвязь с организованной преступностью, т.к. значительному количеству совершенных киберпреступлений (DDoS-атакам, банкингу, фишингу, созданию ботнетов и пр.)

свойственна их реализация организованными преступными сообществами, члены которых являются представителями «высокопрофессиональных» групп специалистов. Это во многом обусловлено и тем, что лица, совершающие киберпреступления, обладают компьютерной преступной специализацией, при этом они не совершают иных видов преступных деяний; извлекают преступный доход только благодаря данному виду преступной деятельности; обладают необходимыми знаниями, навыками и умениями в сфере компьютерных технологий; устанавливают понятия, терминологию, правила поведения и специфические законы, благодаря которым общаются, обмениваются опытом и находят единомышленников.

Способы совершения таких преступлений зачастую не отличаются друг от друга и имеют схожие сценарии. Преступник может отправить SMS сообщение, в котором говорится о несуществующем выигрыше в лотерею. Данный способ является хорошим примером социальной инженерии, где злоумышленник использует в качестве точки давления стремление человека к деньгам, доверчивость, а также входит в доверие иными способами, вроде имитации номера банка, например, Сбербанка (900).[1]

Часто встречающимся видом преступлений является SMS рассылка с просьбой перечисления денежных средств под предлогом попадания в экстренную или непредвиденную ситуацию, что является целевым фишингом.[2]

Распространенным способом преступлений, совершаемых по телефону является вымогательство, которое осуществляется с помощью шантажа и угроз распространения имеющимися у правонарушителя данных, порочащих честь и

[1] Решение Октябрьского районного суда г. Барнаула Алтайского края от 20 июля 2020 г. по делу № 2-1330/2020 // Интернет-портал «Судебные и нормативные акты Российской Федерации»: [сайт]. – URL: https://sudact.ru/ (дата обращения: 12.04.2021)

[2] Приговор Нижневартовского городского суда Ханты-Мансийского автономного округа – Югры от 26 февраля 2019 г. по делу № 1-1036/2017 // Интернет-портал «Судебные и нормативные акты Российской Федерации»: [сайт]. – URL: https://sudact.ru/ (дата обращения: 12.04.2021)

достоинство потерпевшего или членов его семьи.[1]

Характерной чертой для таких преступлений, как и для киберпреступлений является анонимность преступника. Статистика показывает, что преступления в сети Интернет, а также преступления по телефону совершаются чаще всего одним лицом не как разовый акт, а как целая серия преступлений.[2]

Таким образом, киберпреступность набирает обороты с развитием информационно-коммуникационных технологий. Расследовать такие преступления, несмотря на все предпринимаемые усилия остается очень сложно, ввиду целого ряда отягчающих факторов, среди которых есть и техническая сложность вопроса, и низкий уровень обращений граждан, которые стали потерпевшими в результате атаки киберпреступников.

С учетом того, что развитие киберпреступности осуществляется двумя взаимосвязанными способами, где первым выступает появление новых, неизвестных ранее преступлений, вторым – использование преступниками кибертехнологий при совершении выходящих за пределы «компьютерных» статей УК РФ деяний, то к основным проблемам необходимо отнести несоответствие действующего российского уголовного законодательства, в котором отсутствует прогностичность регламентации ответственности за совершение киберпреступлений при наличии достаточно быстро устаревающего официального закрепления и той ограниченной группы деяний, использующих термин «компьютерная информация».

Изложенные причины, условия и средства совершения киберпреступлений, а также высокий уровень виктимизации и латентности в данной области, свидетельствуют о необходимости разработки правовых и криминологических мер противодействия киберпреступлениям.

---

[1] Приговор Нижневартовского городского суда Ханты-Мансийского автономного округа – Югры от 3 мая 2018 г. по делу № 1-1/2018 // Интернет-портал «Судебные и нормативные акты Российской Федерации»: [сайт]. – URL: https://sudact.ru/ (дата обращения: 12.04.2021)

[2] Показатели преступности России // Портал правовой статистики [сайт]. – URL: http://crimestat.ru/offenses_chart (дата обращения 12.04.2021)

2.3 Правовые и криминологические меры противодействия преступлениям, совершаемым с использованием киберпространства

Современное общество развивается в условиях стремительно развивающихся информационно-коммуникационных технологий, поэтому одной из главных проблем здесь является построение комплексной правовой системы мер информационной безопасности.

Инструментами киберпреступности считаются Интернет, электронная почта и социальные сети, но перечень инструментов с каждым годом расширяется. Следовательно, меры кибербезопасности должны осуществляться за пределами страны (защита от преступлений, совершенных другими странами и преступными группами против отдельных граждан) и в рамках национального пространства (защита от преступлений, совершенных другими гражданами), особенно с учетом того, что развитие глобальной киберпреступности приняло прогрессивный оборот.

Проблемы кибербезопасности в настоящее время находятся в центре внимания исследователей, особенно в некоторых областях, затронутых необходимостью борьбы с киберпреступностью: например, фишинг, кибersталкинг и нарушение авторских прав. Для предотвращения распространения инновационных киберпреступлений требуются специальные программы, которые будут уведомлять граждан о том, как такая незаконная деятельность может угрожать их имуществу и безопасности, знакомить их с основными тенденциями киберпреступности и методами борьбы с кибермошенничеством.

Киберпреступность в сфере финансовой деятельности – это еще одна сторона проблемы. До тех пор, пока влияние киберпреступности на финансовый сектор является значительным, киберпреступность требует больших вложений в технические средства. Соответственно, денежные средства, вложенные компаниями в развитие кибербезопасности, увеличит стоимость

киберпреступности в этой области, что повлечет за собой препятствия для совершения преступлений.

Кибербезопасность является приоритетной сферой корпоративной информационной безопасности, поскольку цифровые технологии глубоко укоренились в бизнесе, меняя деловую этику, модели и виды занятости (количество удаленных сотрудников, которые подключаются к корпоративным сетям удаленно, продолжает расти и т.д.).

Кибертерроризм является одной из наиболее опасных форм киберпреступности, о чем свидетельствуют многочисленные кибератаки, которые в последнее время имели место в мире и представляли угрозу международной безопасности. В результате чего акцент был сделан на установлении глобальных международных правил и методов расследования киберпреступности.

В настоящее время многие международные организации сосредоточили свои усилия на борьбе с киберпреступностью, поскольку национальные законы, действующие в отдельных странах, не могут справиться с этой проблемой. Эффективная защита от кибертерроризма (и защита от киберпреступности в целом) требует объединения ресурсов уголовного права с техническими ресурсами для расследования и квалификации преступлений, чтобы меры по борьбе с компьютерными преступлениями, такими как хакерство, кибертерроризм, информационная война и все остальное, действительно могли работать. В условиях кибервойны, международных стандартов и глобальных меры по борьбе с киберпреступностью приобретают все большее значение. Кибервойна началась в 2007 году, когда Таллинн стал центром расследования киберпреступности и местом, где разрабатываются контрмеры.

Для эффективной борьбы с киберпреступностью необходимо наладить многомерное сотрудничество между государственным и частным секторами, правоохранительными органами, отраслью информационных технологий, организациями по информационной безопасности, интернет-компаниями и финансовыми учреждениями.

Необходимо учитывать международный опыт в вопросе предотвращения киберпреступлений, в связи с чем целесообразно принятие Закона о киберпреступности, который будет определять стандарты приемлемого поведения для пользователей информационно-коммуникационных технологий; устанавливать правовые санкции за киберпреступность; защищать пользователей ИКТ в целом и смягчать и/или предотвращать причинение вреда физическим и юридическим лицам, данным, системам, услугам и инфраструктуре; защищать права человека; обеспечивать расследование и судебное преследование преступлений, совершенных в Интернете (за пределами традиционных условий реального мира); и облегчать сотрудничество между странами по вопросам киберпреступности. Закон о киберпреступности должен предусматривать правила поведения и стандарты поведения в отношении использования Интернета, компьютеров и связанных с ними цифровых технологий, а также действий государственных, правительственных и частных организаций; правила доказывания и уголовного судопроизводства и другие вопросы уголовного правосудия в киберпространстве; и регулирование для снижения риска и/или смягчения вреда, причиненного отдельным лицам, организациям и инфраструктуре в случае совершения киберпреступности. Соответственно, закон о киберпреступности включает материальное, процессуальное и превентивное право.

При этом превентивное право фокусируется на регулировании и снижении рисков. В контексте киберпреступности превентивное законодательство должно быть направлено либо на предотвращение киберпреступности, либо, по крайней мере, на смягчение ущерба, причиненного в результате совершения киберпреступности. Законы о защите данных (например, Федеральный закон Российской Федерации «О персональных данных»,[1] Общее положение ЕС о защите данных от 2016 года и Конвенция Африканского союза о

[1] О персональных данных: Федеральный закон от 27 июля 2006 г. № 168-ФЗ. – [по состоянию на 1 марта 2021 г.] // Собрание законодательства Российской Федерации. – 2006. – № 31. – Ст. 3451.

кибербезопасности и защите персональных данных от 2014 года) и законы о кибербезопасности (например, Закон Украины об основных принципах обеспечения кибербезопасности Украины от 2017 года) призваны уменьшить материальный ущерб от преступных нарушений частных данных в случае киберпреступности и/или свести к минимуму уязвимость частных лиц к киберпреступности. Другие законы позволяют органам уголовного правосудия выявлять, расследовать и преследовать в судебном порядке киберпреступность, обеспечивая наличие необходимых инструментов, мер и процессов для облегчения этих действий (например, инфраструктура поставщиков услуг телекоммуникаций и электронных коммуникаций такова, что она позволяет прослушивать и сохранять данные). К примеру, в США действует с 1994 года Закон о коммуникационной помощи правоохранительным органам, согласно которому правоохранительные органы вправе требовать от поставщиков телекоммуникационных услуг и производителей оборудования, чтобы их услуги и продукты позволяли государственным учреждениям законно получать доступ к коммуникациям.

Поскольку киберпреступники ведут свой бизнес не только в пределах одной страны, международное сотрудничество в борьбе с киберпреступностью имеет важное значение. Для этого необходимы современные правовые акты, которые учитывали бы особенности национального законодательства и конкретные ролевые программы по индивидуализированному предупреждению киберпреступности.

Так, целесообразно квалифицировать в качестве уголовных преступлений следующие деяния:

– незаконная эмиссия или подделка электронных денег;

– неправомерное воздействие на функционирование системы (DoS, DDoS-атаки);

– подлог с использованием компьютеров и компьютерных систем;

– хищение с использованием компьютеров и компьютерных систем, а

также в части, касающейся преступлений, связанных с охраняемой внутригосударственным правом информацией, и другие кибердеяния, совершаемые с применением информационных коммуникационных технологий.

Предотвратить крупную технологическую катастрофу возможно только при обеспечении эффективного взаимодействия и координация усилий на глобальном уровне. Для этого необходимы политическая воля руководителей различных государств и создание самых передовых технологий.

Территориальную подсудность киберпреступлений следует определять с учетом места начала и места окончания деяния. При этом указанные категории должны быть закреплены в Постановлении Пленума Верховного Суда РФ для каждого преступления в сети Интернет отдельно, поскольку отдельно взятое деяние обладает своими специфическими характеристиками.

Особое внимание необходимо уделить именно месту окончания преступления. Иными словами, устранение проблемы с определением территориальной подсудности преступлений в киберпространстве возможно достичь только с помощью закрепления места окончания определенного киберпреступления в соответствующем акте Пленума Верховного Суда РФ. Можно предположить, что в дальнейшем данная категория преступлений станет основной формой преступлений, поэтому изложенные проблемы не могут оставаться без рассмотрения.

Меры профилактики любого вида преступлений обычно делятся на общие, специальные и индивидуальные. Они связаны друг с другом, но все же имеют определенные особенности. Индивидуальные меры (меры, направленные на отдельных лиц) представляются наиболее важными, поскольку они позволяют проецировать прямое влияние на потенциальных (или реальных) киберпреступников, а также на лиц, которые могут стать жертвами таких преступлений. Статистические данные доказывают, что для предотвращения киберпреступности необходимы индивидуальные меры, поскольку наибольшее количество киберпреступлений происходит дома, в интернет-кафе и школах с

использованием персональных гаджетов (около 81%).[1]

Индивидуальные меры противодействия предполагают, что профилактика киберпреступности будет сосредоточена на определенных лицах, которые уже совершили преступления против кибербезопасности или склонны к их совершению. Кроме того, эти меры должны охватывать лиц, которые могут стать жертвами киберпреступности. Наиболее эффективными мерами профилактики киберпреступлений являются следующие:

– прогнозирование возможных опасных киберпреступлений в профилактических целях путем проведения исследований с использованием официальных статистических и эмпирических данных;

– определение наиболее опасных сфер, в которых информационные технологии используются в качестве инструментов совершения преступлений (терроризм, фашизм и тому подобное);

– закрепление международной правовой базы, содержащей правила и инструменты для статистического анализа киберпреступности в глобальном и национальном измерениях;

– формирование глобальной (международной) стратегии борьбы с киберпреступностью и разработка международных соглашений о сотрудничестве в обеспечении международной безопасности;

– разработка концептуального аппарата для определения отношений между людьми и организациями в сети;

– активизация информационно-просветительской деятельности населения в целях обеспечения национальной безопасности;

– своевременное выявление внешних и внутренних угроз кибербезопасности и их нейтрализация в рамках системы уголовного правосудия.

Представляется необходимым формировать физическим лицам привычку быть осторожными, избегая опасности или риска, и принимать превентивные

[1] Кудрявцев, О.А. Фишинг в электронной почте, sms-сообщениях, мессенджерах и социальных сетях / О.А. Кудрявцев, О.В. Щекочихин // Поведение молодежи в современном интернет-пространстве: стратегии, риски, защита. – 2018. С. 25.

меры, чтобы не стать жертвами киберпреступности. В первую очередь это касается молодежи, поскольку именно этот сегмент населения находится в группе риска. Для этого необходимы специальные программы, направленные на формирование у молодежи законопослушного поведения и уважения основных прав, свобод и законных интересов.

Следует также иметь в виду опасность, которую представляют киберзапугивание и фишинг (мошенническая попытка получить от доверчивых или невнимательных пользователей персональные данные тех, кто пользуется онлайн-аукционами, услугами перевода или обмена валюты, интернет-магазинами). Поэтому специальные программы также должны нивелировать или ослаблять влияние факторов виктимизации, связанных с киберпреступностью.

Можно предложить следующие наиболее эффективные индивидуальные профилактические меры:

1) совершенствование киберкультуры среди физических лиц, особенно детей и подростков, посредством образовательных и научно-популярных проектов, направленных на формирование у людей высокой культуры поведения в киберпространстве. Как государственные, так и неправительственные организации могут реализовывать такие программы, направленные на создание так называемой «Киберэтики». Доказано, что такая профилактическая мера необходима после успешной реализации подобной программы в Нигерии с участием 218 студентов.[1] В долгосрочной перспективе это может способствовать предотвращению киберпреступности. В рамках данного направления можно выделить следующие меры:

– использование надежных паролей. Следует применять различные комбинации паролей и имен пользователей для каждой учетной записи и не сохранять их в памяти браузера. Простые пароли могут быть легко взломаны с

[1] Преступления, связанные с использованием компьютерной сети / X конгресс ООН по предупреждению преступности и обращению с правонарушителями // Интернет-портал Организации Объединенных Наций: [сайт]. – URL: https://www.unodc.org/documents/ (дата обращения: 12.04.2021)

помощью определенных методов атаки. Наиболее частыми ошибками, влекущими взлом пароля, являются использование шаблонов клавиатуры для паролей, например, qwerty; использование простых комбинаций, например, Alina1998; использование паролей по умолчанию, например, Welcome123; дублирование пароля и имени пользователя;

– соблюдение мер кибербезопасности в социальных сетях: обязательное сохранение профилей в социальных сетях (Вконтакте, Instagram, Facebook, Twitter, YouTube и т.д.) закрытыми, проверка настроек безопасности, осторожность с информацией, размещаемой пользователем в Интернете;

– защита мобильных устройств. Многие пользователи не знают, что их мобильные устройства также уязвимы для вредоносных программ. Мерами предосторожности в данном случае являются загрузка приложений только из надежных источников, поддержание операционной системы в актуальном состоянии, установление антивирусного программного обеспечения и использование безопасного экрана блокировки. В противном случае злоумышленник может получить доступ ко всей личной информации пользователя на его телефоне, или установить вредоносное программное обеспечение, которое может отслеживать каждое движение пользователя через GPS;

– защита данных. Необходима защита данных, используя шифрование для наиболее конфиденциальных файлов, таких как финансовые отчеты и налоговые декларации. Осведомленность о способах киберпреступлений позволяет пользователям оставаться на шаг впереди преступника, получая информацию о мошенничестве и стилях взлома в Интернете;

– защита личности в Интернете при предоставлении личных данных, таких как имя, адрес, номер телефона и/или финансовая информация в Интернете. Данное направление включает в себя включение настроек конфиденциальности при использовании/доступе к веб-сайтам;

– обновление программного обеспечения. Один из лучших способов

защиты от злоумышленников – это применение исправлений и обновлений программного обеспечения, когда они становятся доступными. Регулярное обновление программного обеспечения блокирует злоумышленникам возможность воспользоваться недостатками программного обеспечения (уязвимостями), которые они могли бы использовать для взлома;

– применение родительского контроля. В эпоху онлайн-технологий родители должны следить за всеми действиями своих детей в Интернете. Родители должны быть осторожны и регулярно следить за историей браузера и учетными записями электронной почты. Лучший способ обеспечить безопасность – включить родительский контроль в мобильных приложениях, браузерах и на уровне маршрутизатора для получения доступа только к защищенным сайтам. Многие приложения, такие как Netflix и YouTube, предлагают персонализированный контент только для детей, чтобы защитить детей от правонарушений;

– обращение за помощью. При обнаружении незаконного онлайн-контента, кражи личных данных или любого другого преступления, необходимо сообщить об этом в отдел полиции и администратору веб-сайта.

Правильное использование Интернета и использование защищенных веб-сайтов являются основой кибербезопасности пользователей;

2) привлечение внимания к общим явлениям и процессам киберпреступности, а именно к пропаганде борьбы с кибербуллингом и фишингом, формирование негативного отношения к преступным деяниям и осведомленность об ответственности за совершение киберпреступлений. Этот комплекс мер должен быть реализован соответствующими государственными органами (правоохранительными и судебными органами). Эти меры должны заключаться в выделении основных детерминант киберпреступности, разработке эффективных нормативно-правовых средств борьбы с ее ростом и объяснением наиболее распространенных и наиболее опасных противоправных действий против кибербезопасности. Следует отметить, что согласно статистическим

данным, киберзапугивание становится все более распространенным, особенно в социальных сетях: Вконтакте и Facebook – более 80% случаев, в то время как другие 20% приписываются другим социальным сетям (Instagram, Twitter и т.д.).[1] На данный момент указанные меры крайне необходимы;

3) проведение агрессивной восстановительной кампании по устранению криминогенных факторов, провоцирующих позитивное или нейтральное отношение к киберпреступности. Эти меры также должны приниматься соответствующими государственными органами, действующими в целях улучшения уровня жизни. Статистические данные по странам с высоким и низким уровнем киберпреступности представляются информативными, демонстрируя зависимость роста киберпреступности от средств массовой информации и кибертехнологий, а также от общего уровня жизни в стране: самые высокие показатели были зафиксированы в Китае (57,2%) и Тайване (49,15%), в то время как самый низкий – в Норвегии (20,51%) и Финляндия (20,32%).[2] Изложенное свидетельствует об эффективности этой меры;

4) использование индивидуальных стратегий профилактики в отношении лиц, склонных к совершению преступлений против кибербезопасности. Это профилактическое мера связана с деятельностью конкретных государственных органов, осуществляющих выявление таких лиц. На данном этапе требуются специальные критерии для выявления лиц, склонных к совершению киберпреступлений, прежде чем они направят все свои усилия на их совершение. Актуальность такой меры очевидна из того факта, что число случаев фишинга увеличилось на 36% в период с 2019 по 2020 год, когда ежедневно совершалось 4000 преступлений. Кроме того, ежедневно появляется около 230000 вредоносных

[1] Евдокимов, К.Н. Криминологические и уголовно-правовые аспекты противодействия компьютерной преступности в России (социологическое исследование) / К.Н. Евдокимов // Российский следователь. – 2020. – № 11. С. 43.

[2] Digital 2020: ежегодное глобальное исследование от We Are Social и Hootsuite // Интернет-портал медиааналитического агентства «Exlibris»: [сайт]. – URL: https://exlibris.ru/news/digital-2020-ezhegodnoe-globalnoe-issledovanie-ot-we-are-social-i-hootsuite/ (дата обращения: 12.04.2021)

программ;[1]

5) разработка специальных правительственных и неправительственных программы по снижению кибервиктимизации путем формирования способности к сопротивлению у людей, которые легко могут стать жертвами киберпреступности. Эта мера основана на критериях виктимности потерпевших, и эффективных (насколько это возможно) рычагах, направленных на снижение склонности становиться жертвами киберпреступности. Такие программы должны разрабатываться при участии специальных государственных органов и неправительственных организаций. Указанные программы необходимы, так как 78% людей знают о рисках, которые возникают при открытии незнакомых программ или писем, но все же делают это оно. Кроме того, такая мера пригодится частным предпринимателям, так как 43% кибератак нацелены на малый бизнес.[2]

Технология сама по себе не может гарантировать безопасность в сфере обмена информацией в киберпространстве. Поэтому основную роль в обеспечении кибербезопасности играет индивидуализированная профилактика киберпреступности. Без новых индивидуальных мер по предотвращению киберпреступности и усиления уголовного законодательства (как национального, так и международного) наиболее важные и уязвимые области кибербезопасности не могут быть защищены.

В частности, бдительность и осведомленность как неформальный метод предотвращения киберпреступности вызывают определенные сомнения, поскольку они могут быть превентивным инструментом только для конкретных целей, но не будут работать с потенциальными (или реальными) преступниками.

[1] Digital 2020: ежегодное глобальное исследование от We Are Social и Hootsuite // Интернет-портал медиааналитического агентства «Exlibris»: [сайт]. – URL: https://exlibris.ru/news/digital-2020-ezhegodnoe-globalnoe-issledovanie-ot-we-are-social-i-hootsuite/ (дата обращения: 12.04.2021)

[2] Всестороннее исследование проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора // Интернет-портал Организации Объединенных Наций: [сайт]. – URL: http://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_R.pdf (дата обращения: 12.04.2021)

В то же время защита киберпространства требует не только новейших технологических ресурсов, но и значительных инвестиций, поскольку затраты на кибербезопасность постоянно растут. Если цель состоит в сокращении расходов, инвестирование в технологическое развитие кибербезопасности недостаточно. На данном этапе государственная уголовная политика должна быть сосредоточена на защите киберпространства от преступных посягательств с использованием различных средств, включая специальные программы индивидуальной профилактики.

В рамках борьбы и предотвращения киберпреступности следует придерживаться регулирования предоставления персонального контента физическим лицам, поскольку в киберпространстве существует реальная угроза, связанная с защитой персональных данных и интеллектуальной собственности на цифровом рынке. В то же время правила, закрепляющие право на предоставление персональных данных для обработки, могут нарушать основные права, свободы и интересы лица, ее отправляющего. Поэтому подход к кибернетике в сочетании с достижениями криминологии является эффективным путем при формировании правового реагирования на киберпреступность.

Еще одним фактом, свидетельствующим о необходимости наиболее эффективных индивидуализированных мер борьбы с киберпреступностью, является то, что этот вид преступлений доминирует среди преступлений против личности. Киберпреступления также подвергают общественность опасности, подвергая рост виктимизации среди людей, особенно подростков, посредством запугивания. Это, в свою очередь, создает довольно серьезную угрозу современному обществу.

Следующей проблемой является разработка уголовных мер, направленных на обеспечение кибербезопасности несовершеннолетних. Учитывая тот факт, насколько важно обеспечить нормальное развитие несовершеннолетних и их безопасность на всех уровнях, эта проблема представляется крайне актуальной. К примеру, проблема защиты детей от сексуальной эксплуатации вызвана

трудностями в выявлении таких преступлений и их расследовании. Эта проблема может быть решена только при условии принятия соответствующего международного и национального законодательства. Разработка специальных программ, специально направленных на борьбу с киберпреступностью и ее влиянием на несовершеннолетних, является одним из наиболее эффективных направлений в этой области. Такие программы должны разрабатываться с учетом национальных особенностей каждой страны, но поскольку это проблема носит международный характер, необходима определенная международная программа, которая будет разработана в качестве образца для национальных программ.

Таким образом, с быстрым распространением киберпреступности все большее значение приобретают превентивные меры, направленные на отдельных лиц, склонных к совершению киберпреступлений. Для борьбы с киберпреступностью необходимы специальные программы снижения уровня виктимизации путем укрепления кибербезопасности лиц, которые могут стать жертвами киберпреступлений. Разработка таких программ приведет к снижению активности киберпреступности.

Конкретные государственные органы и неправительственные организации должны принимать участие в превентивном процессе. Всеобъемлющие превентивные меры по борьбе с киберпреступностью, приближающиеся к международному уровню, позволят разработать конкретные пилотные программы для индивидуальной профилактики.

ЗАКЛЮЧЕНИЕ

Подводя итог проведенному исследованию, можно сделать следующие выводы.

Киберпреступления представляют собой преступления, которые совершаются в так называемом виртуальном пространстве. Киберпреступность – это довольно обширное понятие. К данному виду противоправных деяниям можно отнести и преступления где компьютер, информационная сеть Интернет, данные и т.д. – являются объектом, и преступления, где компьютеры используются как средство и орудие. К этому же понятию многие ученые относят и действия в информационном пространстве для поддержания условий преступной общности, группы, например, использование электронной почты для коммуникации, обмен криминальным опытом и специальными познаниями. Киберпреступность, также называемая компьютерной преступностью, предполагает использование компьютера в качестве инструмента для достижения дальнейших незаконных целей, таких как мошенничество, торговля детской порнографией и интеллектуальной собственностью, кража личных данных или нарушение конфиденциальности.

В уголовном законодательстве РФ понятие «кибер» не используется вовсе, а существующие положения уголовного законодательства, направленные на защиту иных отношений, отражают только вопросы информационных технологий или использования компьютерной техники, не позволяющими признать эту сферу имеющей существенное значение в реализации уголовной политики. Особый отличительный признак исследуемого вида преступлений – его высокотехнологичный характер, который определяется использованием современных кибертехнологий, информационно-коммуникационных сетей, различных компьютерных устройств и носителей компьютерной информации и т.д., обычно выступающих как средства совершения такого рода преступлений.

Киберпреступность охватывает широкий спектр видов деятельности.

Киберпреступность затрагивает как виртуальные, так и реальные объекты, но последствия для каждого из них различны. Кибернетическая преступность выступает как особая разновидность преступности, которая находится в тесной взаимосвязи с иными видами преступлений в Российской Федерации в силу того, что кибернетическим преступлениям часто свойственно использование способов совершения иных уголовно наказуемых деяний. Проведенный анализ позволил констатировать отсутствие четкого понимания возможностей механизма уголовного законодательства при осуществлении противодействия новым способам криминальной деятельности в сфере реализации кибертехнологий, круга таких преступлений, недостаточное и противоречивое правовое закрепление терминологического аппарата в российском уголовном законодательстве.

Единого и широко распространенного определения киберпреступности до сих пор не существует. Хотя положения Конвенции о киберпреступности, являются мощными инструментами для гармонизации борьбы с киберпреступностью, законодатели различных стран используют различные термины для обозначения группы преступлений, связанных с использованием информационно-коммуникационных технологий.

Несмотря на различия в определениях, основными характеристиками киберпреступности являются: техническая сложность, быстрое развитие (расширение уязвимости и расширение возможностей для нарушений) и криптография (как мера защиты и препятствие для обнаружения преступников).

В понятие киберпреступности включают следующие особенности:

1) новое (виртуальное) место преступления;

2) распространение девиантного поведения: это включает в себя старые формы девиантного поведения в новых формах (например, кража данных) и совершенно новые виды преступлений (например, взлом, компьютерные атаки вирусами и др.);

3) новые методы расследования преступлений и новые правила для юрисдикции и наказания.

Определение киберпреступности, которое может принято в юридическом дискурсе, представляет собой совокупность следующих характеристик:

1) преступление, угрожающее информационной и сетевой безопасности (преступление против целостности компьютера или киберпреступность в узком смысле);

2) преступление с использованием информационно-коммуникационных технологий для совершения традиционных видов преступлений (преступление, связанное с компьютером);

3) преступление, связанное с контентом, таким как детская порнография, ненавистнические высказывания и нарушение прав интеллектуальной собственности (преступление, связанное с компьютерным контентом).

Методы совершения преступлений постоянно эволюционируют, при этом преступниками активно используются современные информационно-телекоммуникационные технологии, которые зачастую просты в использовании и доступны неограниченному числу пользователей сети Интернет.

Киберпреступность набирает обороты с развитием информационно-коммуникационных технологий. Расследовать такие преступления, несмотря на все предпринимаемые усилия остается очень сложно, ввиду целого ряда отягчающих факторов, среди которых есть и техническая сложность вопроса, и низкий уровень обращений граждан, которые стали потерпевшими в результате атаки киберпреступников.

С учетом того, что развитие киберпреступности осуществляется двумя взаимосвязанными способами, где первым выступает появление новых, неизвестных ранее преступлений, вторым – использование преступниками кибертехнологий при совершении выходящих за пределы «компьютерных» статей УК РФ деяний, то к основным проблемам необходимо отнести несоответствие действующего российского уголовного законодательства, в котором отсутствует прогностичность регламентации ответственности за совершение киберпреступлений при наличии достаточно быстро устаревающего

официального закрепления и той ограниченной группы деяний, использующих термин «компьютерная информация».

Изложенные причины, условия и средства совершения киберпреступлений, а также высокий уровень виктимизации и латентности в данной области, свидетельствуют о необходимости разработки правовых и криминологических мер противодействия киберпреступлениям.

С быстрым распространением киберпреступности все большее значение приобретают превентивные меры, направленные на отдельных лиц, склонных к совершению киберпреступлений. Для борьбы с киберпреступностью необходимы специальные программы снижения уровня виктимизации путем укрепления кибербезопасности лиц, которые могут стать жертвами киберпреступлений. Разработка таких программ приведет к снижению активности киберпреступности.

Конкретные государственные органы и неправительственные организации должны принимать участие в превентивном процессе. Всеобъемлющие превентивные меры по борьбе с киберпреступностью, приближающиеся к международному уровню, позволят разработать конкретные пилотные программы для индивидуальной профилактики.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1 Нормативно-правовые акты

1.1 Конституция Российской Федерации. Принята всенародным голосованием 12 декабря 1993 г. (с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 года) // Собрание законодательства Российской Федерации. – 2020. – № 12. – Ст. 1855.

1.2 Декларация о преступности и общественной безопасности. Принята 12 декабря 1996 г. Резолюцией 51/60 на 82-ом пленарном заседании Генеральной Ассамблеи ООН // Международные стандарты деятельности правоохранительных органов и уголовно-исполнительной системы. – Екатеринбург, 1999. – С. 21-48.

1.3 Венская декларация о преступности и правосудии: ответы на вызовы XXI века: Резолюция № 55/59 Генеральной Ассамблеи ООН. Принята в г. Нью-Йорке 4 декабря 2000 г. на 81-ом пленарном заседании 55-ой сессии Генеральной Ассамблеи ООН // Бюллетень международных договоров. – 2005. – № 2. – С. 3-33.

1.4 Конвенция о преступности в сфере компьютерной информации (ETS № 185). Заключена в г. Будапеште 23 ноября 2001 г. – [по состоянию на 28 января 2003 г.] // Международные стандарты деятельности правоохранительных органов и уголовно-исполнительной системы. – Екатеринбург, 2003. – С. 52-79.

1.5 Уголовный кодекс Российской Федерации: Федеральный закон от 13 июня 1996 г. № 63-ФЗ. – [по состоянию на 5 апреля 2021 г.] // Собрание законодательства Российской Федерации. – 1996. – № 25. – Ст. 2954.

1.6 О персональных данных: Федеральный закон от 27 июля 2006 г. № 168-ФЗ. – [по состоянию на 1 марта 2021 г.] // Собрание законодательства Российской Федерации. – 2006. – № 31. – Ст. 3451.

2 Научная и учебная литература

2.1 Батухтин, М.Е. Киберпреступления: причины, виды, формы, последствия, направления противодействия / М.Е. Батухтин // Проблемы и перспективы развития уголовно-исполнительной системы России на современном этапе

Материалы Международной научной конференции адъюнктов, аспирантов, курсантов и студентов. 2018. – С. 142-149.

2.2 Бородкина, Т.Н. Киберпреступления: понятие, содержание и меры противодействия / Т.Н. Бородкина, А.В. Павлюк // Социально-политические науки. – 2018. – № 1. – С. 135-137.

2.3 Всестороннее исследование проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора // Интернет-портал Организации Объединенных Наций: [сайт]. – URL: http://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_R.pdf (дата обращения: 12.04.2021)

2.4 Демин, Ю.В. Организационно-правовые основы выявления и раскрытия краж, совершаемых с банковского счета, а равно в отношении электронных денежных средств / Ю.В. Демин // Российский следователь. – 2021. – № 1. – С. 64-68.

2.5 Евдокимов, К.Н. Криминологические и уголовно-правовые аспекты противодействия компьютерной преступности в России (социологическое исследование) / К.Н. Евдокимов // Российский следователь. – 2020. – № 11. – С. 41-44.

2.6 Зверянская, Л.П. Исторический анализ этапов развития киберпреступности и особенности современных киберпреступлений / Л.П. Зверянская // Научно-методический электронный журнал «Концепт». – 2016. – Т. 15. – С. 881-885.

2.7 Киберпреступность: криминологический, уголовно-правовой, уголовно-процессуальный и криминалистический анализ / науч. ред. И.Г. Смирнова; отв. ред. О.А. Егерева, Е.М. Якимова. – Москва, 2016. – 244 с.

2.8 Козаев, Н.Ш. Противодействие злоупотреблениями современными технологиями: международно-правовые и уголовно-правовые аспекты / Н.Ш. Козаев // Монография. – Москва : Юрлитинформ, 2016. – 177 с.

2.9 Кочкина, Э.Л. Определение понятия «Киберпреступление». Отдельные виды киберпреступлений / Э.Л. Кочкина // Сибирские уголовно-процессуальные и криминалистические чтения. – 2017. – № 3 (17). – С. 162-169.

2.10 Кудрявцев, О.А. Фишинг в электронной почте, sms-сообщениях, мессенджерах и социальных сетях / О.А. Кудрявцев, О.В. Щекочихин // Поведение молодежи в современном интернет-пространстве: стратегии, риски, защита. – 2018. – С. 22-26.

2.11 Литвишко, П.А. Юрисдикционные и международно-правовые аспекты обеспечительных и конфискационных мер в отношении виртуальных активов / П.А. Литвишко // Законность. – 2021. – № 3. – С. 8-14.

2.12 Малов, А.А. Международные правовые стандарты истребования электронных доказательств от иностранных юрисдикций / А.А. Малов // Международное уголовное право и международная юстиция. – 2021. – № 1. – С. 19-23.

2.13 Научная платформа: дискуссия и полемика: сборник материалов Международной научно-практической конференции (30 октября 2020 г.). – Кемерово : ЗапСибНЦ, 2020. – 70 с.

2.14 Овсюков, Д.А. Использование информационно-телекоммуникационных сетей при совершении вымогательства / Д.А. Овсюков // Актуальные проблемы российского права. – 2021. – № 2. – С. 140-145.

2.15 Овчинский, В.С. Основы борьбы с киберпреступностью и кибертерроризмом: хрестоматия / сост. В.С. Овчинский. – Москва : Норма, 2017. – 528 с.

2.16 Одинцов, С.А. Развитие теорий информационного общества и понятия «киберпространство» / С.А. Одинцов, А.В. Ващенко // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. – 2016. – № 121 (07). – С. 1-13.

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

2.18 Пибаев, И.А. Алгоритмы в механизме реализации конституционных прав и свобод: вызовы цифровой эпохи / И.А. Пибаев, С.В. Симонова // Сравнительное конституционное обозрение. – 2020. – № 6. – С. 31-50.

2.19 Показатели преступности России // Портал правовой статистики [сайт]. – URL: http://crimestat.ru/offenses_chart (дата обращения 12.04.2021)

2.20 Преступность в регионах // Портал правовой статистики [сайт]. – URL: http://crimestat.ru/regions_chart_total (дата обращения 12.04.2021)

2.21 Преступления, связанные с использованием компьютерной сети / X конгресс ООН по предупреждению преступности и обращению с правонарушителями // Интернет-портал Организации Объединенных Наций: [сайт]. – URL: https://www.unodc.org/documents/ (дата обращения: 12.04.2021)

2.22 Простосердов, М.А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им: дисс. … канд. юрид. наук / М.А. Простосердов. – Москва, 2016. – 232 с.

2.23 Роль и место информационных технологий в современной науке: сборник статей Международной научно-практической конференции (17 января 2019 г, г. Самара). В 3 ч. Ч. 2. – Уфа : OMEGA SCIENCE, 2019. – 269 с.

2.24 Русскевич, Е.А. Международно-правовые подходы противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий / Е.А. Русскевич // Международное уголовное право и международная юстиция. – 2018. – № 3. – С. 10-13.

2.25 Состояние преступности и результаты расследования преступлений // Интернет-портал МВД РФ: [сайт]. – URL: https://мвд.рф/открытые-данные/ (дата обращения: 12.04.2021)

2.26 Сборник стандартов и норм Организации Объединенных Наций в области предупреждения преступности и уголовного правосудия // Интернет-

портал Организации Объединенных Наций: [сайт]. – URL: https://www.unodc.org/documents/justice-and-prison-reform/R_ebook.pdf (дата обращения: 12.04.2021)

2.27 Состояние преступности в Югре // Управление МВД России по Ханты-Мансийскому АО – Югре [сайт]. – URL: http:// 86.мвд.рф/Dejatelnost/Sostojanie_prestupnosti_v_JUgre (дата обращения 12.04.2021)

2.28 Третьяк, М.И. Проблема законодательной регламентации преступлений против собственности в сфере высоких технологий / М.И. Третьяк // Законность. – 2016. – № 7. – С. 41-46.

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

2.30 Хусяинов, Т.М. Интернет-преступления (киберпреступления) в российском уголовном законодательстве / Т.М. Хусяинов // Уголовный закон Российской Федерации: Проблемы правоприменения и перспективы совершенствования материалы всероссийского круглого стола. 2015. – С. 90-95.

2.31 Digital 2020: ежегодное глобальное исследование от We Are Social и Hootsuite // Интернет-портал медиааналитического агентства «Exlibris»: [сайт]. – URL: https://exlibris.ru/news/digital-2020-ezhegodnoe-globalnoe-issledovanie-ot-we-are-social-i-hootsuite/ (дата обращения: 12.04.2021)

3 Материалы правоприменительной практики

3.1 О судебной практике по делам о мошенничестве, присвоении и растрате: Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 // Бюллетень Верховного Суда РФ. – 2018. – № 2.

3.2 Приговор Железнодорожного районного суда г. Читы (Забайкальский край) от 22 апреля 2016 г. № 1-166/2016 // Интернет-портал «Судебные и нормативные акты Российской Федерации»: [сайт]. – URL: https://sudact.ru/ (дата обращения: 12.04.2021)

3.3 Решение Октябрьского районного суда г. Барнаула Алтайского края от 20 июля 2020 г. по делу № 2-1330/2020 // Интернет-портал «Судебные и нормативные акты Российской Федерации»: [сайт]. – URL: https://sudact.ru/ (дата обращения: 12.04.2021)

3.4 Приговор Нижневартовского городского суда Ханты-Мансийского автономного округа – Югры от 26 февраля 2019 г. по делу № 1-1036/2017 // Интернет-портал «Судебные и нормативные акты Российской Федерации»: [сайт]. – URL: https://sudact.ru/ (дата обращения: 12.04.2021)

3.5 Приговор Нижневартовского городского суда Ханты-Мансийского автономного округа – Югры от 3 мая 2018 г. по делу № 1-1/2018 // Интернет-портал «Судебные и нормативные акты Российской Федерации»: [сайт]. – URL: https://sudact.ru/ (дата обращения: 12.04.2021)

3.6 Приговор Нижневартовского городского суда Ханты-Мансийского автономного округа – Югры от 28 июля 2020 г. по делу № 1-521/2020 // Интернет-портал «Судебные и нормативные акты Российской Федерации»: [сайт]. – URL: https://sudact.ru/ (дата обращения: 12.04.2021)

3.7 Приговор Нижневартовского городского суда Ханты-Мансийского автономного округа – Югры от 17 июля 2020 г. по делу № 1-97/2020 // Интернет-портал «Судебные и нормативные акты Российской Федерации»: [сайт]. – URL: https://sudact.ru/ (дата обращения: 12.04.2021)

3.8 Приговор Нефтеюганского районного суда Ханты-Мансийского автономного округа – Югры от 6 июля 2020 г. по делу № 1-342/2020 // Интернет-портал «Судебные и нормативные акты Российской Федерации»: [сайт]. – URL: https://sudact.ru/ (дата обращения: 12.04.2021)