Министерство внутренних дел Российской Федерации

Федеральное государственное казенное образовательное учреждение высшего образования «Казанский юридический институт Министерства внутренних дел Российской Федерации»

Кафедра криминологии и уголовно-исполнительного права

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

на тему Деятельность органов внутренних дел по предупреждению и пресечению преступлений в информационной сфере

Выполнил: Рябцев Евгений Игоревич
40.05.01 – Правовое обеспечение национальной безопасности, год набора 2017
173 учебная группа

Руководитель:
к.ю.н., доцент, начальник кафедры криминологии и уголовно-исполнительного права КЮИ МВД России
полковник полиции
Шалагин Антон Евгеньевич

Рецензент: Помощник начальника управления МВД России - начальник ООРС полковник вн. службы А.А. Федонов.

Дата защиты: «___» _____2022 г. Оценка_____

Казань 2022

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность исследования. Стремительное развитие компьютерных технологий открыло человечеству дополнительные возможности. В условиях современности компьютер является необходимым инструментом в самых различных сферах жизнедеятельности человека. Углубляется зависимость человека, да и общества в целом, от компьютерных и информационных систем. Информатизация современного общества привела к формированию новых видов преступлений, при совершении которых используются вычислительные системы, новейшие средства телекоммуникации и связи, средства негласного получения информации и т.п. За последние 10-15 лет резко увеличилось количество преступлений с использованием вычислительной техники или иной электронной аппаратуры, хищения наличных и безналичных денежных средств. Для совершения преступлений все чаще используются устройства, в основе которых лежат высокоточные технологии их изготовления и функционирования, иными словами, это преступления, в которых используются высокие технологии.

Под компьютерным преступлением (интеллектуальной преступностью) подразумеваются несанкционированный доступ к компьютерным системам и базам данных и причинение ущерба, а также совершение уголовно наказуемого преступления посредством компьютера. Характерные черты подобного рода преступлений — его закрытость, интеллектуальность, многообразие, продолжительность и серьезная опасность, которую они представляют для общества. К таким видам преступлений относят неправомерный доступ к компьютерной информации, создание и распространение вредоносного компьютерного программного обеспечения, нарушение правил хранения, обработки и передачи компьютерной информации, а также интернет-травлю (кибербуллинг). Последнее же явление в условиях современности особенно прогрессирует в связи с тем, что доступ к интернет-ресурсам имеет большое

количество молодёжи. Вследствие этого растет и интерес, уделяемый исследователями феномену кибербулинга.

Впервые данному вопросу было посвящено исследование 1970 г. Д. Олвеуса. Он утверждал, что в качестве буллинга следует понимать процесс, характеризующийся проявлениями агрессивных действий на протяжении длительного времени от одного или нескольких лиц, при этом объект травли находится в постоянном стрессе, однако по различным причинам не может противодействовать нападениям. В настоящее же время кибербуллинг чаще выражается в виде насмешек, угроз или придирок. Стоит отметить, что данный феномен чаще наблюдается среди учащихся школ, причем участниками могут быть как школьники, так и учителя. Именно поэтому особое внимание необходимо обратить на школьные взаимоотношения как наиболее частую причину возникновения кибербуллинга.

Объект исследования: преступления в информационной сфере, в том числе кибербуллинг.

Предмет исследования: предупреждение и пресечение преступлений в информационной сфере.

Цель исследования: изучить деятельность органов внутренних дел по предупреждению и пресечению преступлений в информационной сфере.

Достижению цели работы соответствует выполнение следующих **задач:**

- рассмотреть теоретические, правовые и организационные основы обеспечения кибербезопасности в Российской Федерации;
- дать уголовно-правовую характеристику преступлений в сфере информационно-телекоммуникационных технологий;
- выявить причины и условия совершения преступлений в информационной сфере;
- дать характеристику личности киберпреступника;
- изучить зарубежный опыт противодействия преступлениям с использованием компьютерных технологий;

- проанализировать деятельность органов внутренних дел по профилактике, выявлению и пресечению преступлений в информационной сфере;
- исследовать трансформацию преступности и способы реагирования на новые киберугрозы.

Теоретико-методологической основой исследования является анализ основных понятий «киберпреступлений» (Д.Лэйн, О.Л.Глазман, И.С.Кон), анализ их причин и условий, выявление особенностей кибербуллинга в подростково-молодежной среде (Ю.Л. Макарова, В.Р. Петросянц).

Теоретическая значимость исследования заключается в рассмотрении уголовно-правовых характеристик киберпреступлений в Российской Федерации и за рубежом, существующих понятий «компьютерные преступления», «преступность в информационной сфере», «кибербуллинга», причин и условий киберпреступлений, методов профилактики, предотвращения и пресечения.

Практическая значимость заключается в направленности на решение задач, стоящих перед органами внутренних дел в сфере противодействия преступлениям, совершаемым в информационной среде. Полученные данные могут быть использованы для выработки мер противодействия данным преступлениям.

Структура и объем выпускной квалификационной работы: выпускная квалификационная работа на тему: «Деятельность органов внутренних дел по предупреждению и пресечению преступлений в информационной сфере» состоит из введения, двух глав, семи параграфов, заключения и списка литературы.

ГЛАВА 1. КРИМИНОЛОГИЧЕСКАЯ И УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ В ИНФОРМАЦИОННОЙ СФЕРЕ

§ 1. Теоретические, правовые и организационные основы обеспечения кибербезопасности в Российской Федерации

Переходя к рассмотрению основ обеспечения кибербезопасности в Российской Федерации, стоит отметить нормативно-правовое регулирование изучаемой темы. Так, правовую основу обеспечения кибербезопасности в Российской Федерации составляют Конституция Российской Федерации, Доктрина информационной безопасности, международные нормативно-правовые документы, федеральные конституционные законы, федеральные законы, нормативные правовые акты Президента и Правительства Российской Федерации, федеральных министерств и ведомств, государственных органов местного самоуправления. Основу же составляют следующие нормативно-правовые акты:

- Закон Российской Федерации от 27.07.2006 г. № 149–ФЗ «Об информации, информационных технологиях и о защите информации»;
- Указ Президента Российской Федерации от 12.05.2009 г. № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года»;
- Указ Президента Российской Федерации от 15.01.2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»;

- Указ Президента Российской Федерации от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».[1]

Указанные нормативно-правовые акты являются базой для улучшения системы правового регулирования вопросов кибербезопасности. Однако многие авторы отмечают несовершенство системы. «Правовое регулирование не охватывает всего сложившегося многообразия отношений, возникающих в рамках киберпространства. Анализ показывает, что в официальных российских документах в области информационной безопасности термин «кибербезопасность» не используется отдельно»[2] Вследствие этого в целях совершенствования правового регулирования кибербезопасности видим необходимым проведение мониторингов киберугроз и механизмов кибербпреступлений, а также стимулирование в проведении научных исследований по данной теме.

Под организационными основами обеспечения кибербезопасности в Российской Федерации понимают часть системы обеспечения национальной безопасности страны, предназначенной для реализации государственной политики в информационной сфере. Согласно Доктрине информационной безопасности Российской Федерации организационную основу системы обеспечения информационной безопасности Российской Федерации составляют: Президент, Совет Федерации, Государственная Дума, Правительство, Совет Безопасности, федеральные органы исполнительной власти, межведомственные и государственные комиссии, органы исполнительной власти, органы местного самоуправления, органы судебной власти, общественные объединения, а также граждане, принимающие в

[1] Хоружий В.В., Шульга А.В. Правовые основы кибербезопасности: к постановке проблемы / // Научное обеспечение агропромышленного комплекса: Сборник статей по материалам 73-й научно-практической конференции студентов по итогам НИР за 2017 год, Краснодар, 25 апреля 2018 года / Ответственный за выпуск А.Г. Кощаев. Краснодар: Кубанский государственный аграрный университет имени И.Т. Трубилина, 2018. С. 1265-1268.

[2] Суханов А.Г. Особенности правового регулирования в области обеспечения кибербезопасности критической инфраструктуры // Экономика и социум. 2017. № 3(34). С. 1693–1700.

соответствии с законодательством участие в решении задач информационной безопасности. Рассмотрим функции каждого из них.

Так, Президент Российской Федерации вследствие имеющихся у него конституционных полномочий руководит органами и силами по обеспечению национальной информационной безопасности; санкционирует действия по обеспечению информационной безопасности Российской Федерации; в соответствии с законодательством Российской Федерации формирует, реорганизует и упраздняет подчиненные ему органы и силы по обеспечению информационной безопасности Российской Федерации; посредством ежегодных посланий Федеральному собранию выделяет как приоритетные направления государственной политики в области обеспечения государственной безопасности, так и конкретные меры по ее реализации.

Формированием законодательной базы в сфере реализации кибербезопасности в нашей стране занимаются Совет Федерации и Государственная Дума. Связующим звеном между федеральными органами исполнительной власти и органами исполнительной власти субъектов Российской Федерации является Правительство Российской Федерации, которое координирует работу данных органов, а также занимается вопросами финансирования из средств федерального бюджета федеральных программ в этой области.

Совет Безопасности Российской Федерации выявляет и оценивает угрозы национальной информационной безопасности, оперативно подготавливает проекты решений Президента по предотвращению таких угроз, разрабатывает идеи в вопросах обеспечения информационной безопасности государства, а также следит как за работой органов и сил по обеспечению национальной информационной безопасности, так и за внедрением органами исполнительной власти решений Президента в вопросах кибербезопасности.

Федеральные органы исполнительной власти главным образом следуют законодательству Российской Федерации, реализуют решения Президента и Правительства в области обеспечения информационной безопасности, а также в

пределах своих полномочий разрабатывают нормативно-правовые акты в сфере кибербезопасности и представляют их установленным порядком Президенту и в Правительство.

Межведомственные и государственные комиссии, создаваемые Президентом и Правительством, в рамках своих компетенций занимаются реализацией задач по обеспечению информационной безопасности Российской Федерации.

Органы исполнительной власти субъектов Российской Федерации взаимодействуют с федеральными органами исполнительной власти по вопросам исполнения законодательства Российской Федерации, решений Президента и Правительства в области обеспечения информационной безопасности, а также по вопросам реализации федеральных программ в этой области; совместно с органами местного самоуправления осуществляют мероприятия по привлечению граждан, организаций и общественных объединений к оказанию содействия в решении проблем обеспечения информационной безопасности Российской Федерации; вносят в федеральные органы исполнительной власти предложения по совершенствованию национальной системы обеспечения информационной безопасности государства.

Органы же местного самоуправления обеспечивают соблюдение законодательства Российской Федерации в области обеспечения информационной безопасности Российской Федерации.

Органами судебной власти осуществляются правосудие по делам о преступлениях, связанных с посягательствами на законные интересы личности, общества и государства в информационной сфере. Также ими обеспечиваются судебная защита как граждан, так и общественных объединений, права которых нарушены в связи с обеспечением кибербезопасности Российской Федерации[1].

[1] Яковлев В. В., Корниенко А.А. Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта: учебное пособие. Москва, 2002. С. 213.

Для глубокого анализа теоретических, правовых и организационных основ обеспечения кибербезопасности в Российской Федерации необходимо ознакомиться также с основными понятиями кибербуллинга как одного из видов преступлений, совершаемых в информационной сфере, изучить историю возникновения феномена, виды интернет-травли.

Интернет-травля, или кибертравля – целенаправленные оскорбления, угрозы, инсинуации и сообщения иных компрометирующих данных с помощью средств массовой информации, чаще всего, при помощи информационно-телекоммуникационной сети "Интернет", как правило, в течение длящегося промежутка времени.[1] Также интернет-травля является частью масштабной киберкультуры.

Киберкультура (англ. cyberculture) – это вид современной культуры, формирующийся её носителями в условиях цифровизации современного мира, прежде всего при помощи персональных компьютеров, порождённых наукой кибернетикой. Наиболее распространенной формой киберкультуры можно назвать интернет-культуру, то есть глобальную массовую культуру, имеющую широкий круг пользователей Интернета, а также формирующуюся всеми этими пользователями в ходе использования компьютерных устройств, входящих в общую сеть между собой. Внутри интернет-культуры можно выделить ряд направлений, такие как геймерство (киберспорт), чаты (чаттинг), имиджбординг, свободное ПО, вики-движение, среди которых и интернет-травля, а также многое другое. Англоязычное понятие "cyberculture" определяется Оксфордским словарём как «состояние общества в результате использования средств автоматизации и компьютеризации».[2] Носители киберкультуры являются предметом изучения науки киберпсихологии.

---

[1] Богатырева Ю.В. Подготовка будущих педагогов к обеспечению информационной безопасности школьников: дис. …канд. пед. наук. Тула: Тульский государственный университет, 2014. С. 87.

[2] Сайт Оксфордского английского словаря / URL: https://dictionary.cambridge.org/ru/ (дата обращения: 18.01.2022).

Для обозначения понятия «кибер-травля» используется и дефиниция «кибермоббинг» – это термин, пришедший из английского языка (от англ. Cyber-Mobbing), а также интернет-моббинг (Internet-mobbing), кибербуллинг (cyberbullying), троллинг (trolling – «ловля»), флейм (flame – «пламя»).

В настоящее время одной из актуальных задач является различение длительной кибертравли от кратковременных явлений агрессии, связанных главным образом с использованием гаджетов и электронных технологий. Современными исследователями ситуации кибербуллинга изучаются посредством опроса респондентов, что зачастую не позволяет разграничить продолжительные воздействия агрессоров и грубые единичные, несвязанные между собой эпизоды. Также является необходимым отличать стандартные конфликтные ситуации между людьми от продолжительного воздействия с чётко выделяемыми ролями агрессора и жертвы – травли. На данном этапе изученности вопроса широко применима классификация онлайн-агрессии, где по типу и форме агрессивных проявлений в сети Интернет выделяют хейтинг, троллинг, флэйминг, кибербуллинг и киберсталкинг. В конкретных случаях типология уточняется такими формами, как грифинг и секстинг.

Кибербуллинг (cyberbulling) – это целенаправленный и систематический вред, наносимый кому-то с использованием интернет-технологий, компьютеров, гаджетов и других электронных девайсов.

Троллинг (cyber trolls) – это ситуации, когда со стороны агрессоров происходит публикация и распространение негативной, тревожащей информации на веб-сайтах, страницах социальных сетей, даже на мемориальных страницах, посвященных умершим людям.

Хейтинг (hate)[1] – это негативные комментарии и сообщения, иррациональная критика в адрес конкретного человека или явления, часто без обоснования своей позиции.

Флэйминг (flaming) – это вспышка оскорблений, публичный эмоциональный обмен репликами, часто разгорается в чатах и комментариях в

[1] Лахмытко Н.М. Интернет-травля. Миф или реальность? // Методист. 2015. № 6. С. 21-24.

социальных сетях. Вследствие публичного характера явления происходит привлечение пользователей сети к оскорблениям одной из сторон конфликта. Зачастую целью агрессора и является спонтанное вовлечение большого количества случайных свидетелей в противостояние.

Кибersталкинг (cyberstalking; to stalk – преследовать, выслеживать) – по средствам информационно-коммуникационных технологий на жертву происходит давление путем повторяющихся угроз о совершении в его отношении преступных действий, в частности, нанесения физического вреда, повреждения имущества и т.д.

Грифинг (griefers) – это преследование одними пользователями в многосубъектиных онлайн-играх других игроков в целях получение удовольствия от самого процесса. Так, «преследователи» в процессе игры предпринимают действия, которые не разрешены в поле игры, используют ненормативную лексику, закрывают доступ к отдельным областям игр, а также незаконно списывают с игровых счетов других пользователей денежные средства.

Секстинг (sexting)[1] – это рассылка или публикация, преимущественно в сети Интернет, фото- и видео порнографического содержания или же демонстрация отдельных частей тела, то есть полуобнаженных людей. Целью секстинга может быть как травля, так и месть бывшему партнеру после разрыва отношений. Данные действия особенно негативно влияют на психику несовершеннолетних, при этом, невозможно в последующем предотвратить установление зависимости детей к секстингу. Исключительной формой предотвращения подобных действий в отношении ребенка является ограничение использования им каких-либо информационных ресурсов и сети Интернет, что так же скажется лишь негативно, так как несовершеннолетних окажется в безинформационном вакууме.

---

[1] Лахмытко Н.М. Интернет-травля. Миф или реальность? // Методист. 2015. № 6. С. 21-24.

Зачастую явление травли осуществляется в информационном пространстве посредством информационно-коммуникационных каналов и средств связи, в том числе в сети Интернет через электронную почту, программы для мгновенного обмена сообщениями (например, ICQ, Viber, What'sUp), в социальных сетях, на форумах, а также посредствомпубликации на видеохостингах (YouTube, Twitch и других) компрометирующих видеоматериалов и сообщений (как правило, с ненормативной лексикой), либо посредством мобильного телефона (например, с помощью SMS-сообщений или надоедливых SPAM-звонков).

«Тролли», «булли» или «мобберы» – современные названия лиц, совершающих хулиганские действия в сети. Они привыкли действовать анонимно, вследствие чего жертве сложно выяснить, от кого проистекают агрессивные действия.

Ежедневное общение в современном мире несомненно претерпевает изменения. Одна из особенностей данной сферы – использование сети и специальных программ как средства для совместного времяпрепровождения. У подростков данное явление с легкостью дополняет, а зачастую и заменяет живое общение. Навыки же, приобретенные посредством электронных систем связи, осваиваются ими быстро и всесторонне.

Вследствие возникновения информационно-телекоммуникационной сети «Интернет», так называемое «виртуальное общение» стало для многих людей одним из основных ресурсов в общении, открывающим новые социальные возможности. В условиях современности чрезвычайно важный для подростков процесс социализации все стремительнее перемещается в Интернет, где помимо знакомств и возникновения новых референтных групп подростки осваивают новые социальные роли, а также нормы поведения. Процессы коммуникации, используемые нами в настоящем общении, по сути «дублируются» и зачастую даже усиливаются и замещаются виртуальным общением. Навыки коммуникации в интернет-пространстве приобретают новые и усиливают привычные черты социального общения.

Отметим, что чрезмерная привязанность подростков к общению в сети Интернет, а в некоторых случаях и замена личному общению, является довольно критичной, так как лица, не достигшие совершеннолетнего возраста, априори не обладают навыками в области пользовательской компетентности и не соблюдают этику общения в сети.[1] Именно неосознание важности следования этическим границам и в условиях виртуального общения, а также анонимность данного процесса приводят к появлению асоциальных и агрессивных моделей общения в сети.

Подростки переносят в киберпространство привычные для своего возраста модели взаимодействия в группе: «отвержение и травля индивидуума группой», «изоляция и самоизоляция» и др.

Анонимность виртуального общения позволяют подростку прибегать к экспериментам разного проявления своего «Я» и использовать различные способы в самоутверждении и достижении отдельных аспектов своего социального статуса, это обусловлено теневой формой общения в сети Интернет, то есть невозможностью рядового пользователя установить настоящие персональные данные лица, а следовательно, и применить в отношении него социальные санкции.

Безличность субъектов общения увеличивает и вероятность встречи подростков в сети с людьми, также использующими вымышленную социальную роль и являющимся не теми, кем они представляются. В виртуальном общении происходит процесс уменьшения у подростка привычного уровня стыдливости и неуверенности в себе, что влечет за собой проявление нетипичных для реальной жизни форм поведения (например, исповедальность, жертвенность, самобичевание и др.).

Однако подростками не учитывается факт возможного раскрытия личности и автора, и участников общения в интернет-пространстве. Подобные случаи могут привести к психологической травме несовершеннолетнего.

---

[1] Проблемы насилия над детьми и пути их преодоления / под ред. Е.Н. Волковой. СПб.: Питер, 2008. С. 14.

Снижение степени личной ответственности агрессора позволяет стать практически элементом симультанной информационной среды и избежать ответных нападений от обиженных.[1]

У несовершеннолетних высокая пользовательская активность в сети сочетается с низким уровнем осведомленности об опасностях Интернет-пространства и способах их избегания или преодоления, в связи с чем становится очевидным необходимость проведения профилактических мероприятий и просвещения подростков по правилам поведения в сети.

Определить исходную точку развития кибербуллинга затруднительно, однако возможно теоретически выделить ключевые этапы. Для установления первого этапа приведем в пример ситуацию Моники Левински, которая называет себя «нулевым пациентом» кибертравли. В 1998 году в средствах массовой информации появились новости о том, что у президента США Билл Клинтон находится в ней в романтических отношениях. Как признавалась Левински, ей понадобилось несколько лет, чтобы не только восстановить свое психологическое состояние, но и восстановить свою честь и достоинство после публичного распространения ложной информации. Как отмечала сама Левински, «СМИ пестрели моими фотографиями; их использовали, чтобы продавать газеты и держать людей у телевизоров».

Следующая потерпевшая от кибербуллинга Фрэнси Дайп вспоминает, как в 13-ти летнем возрасте она перенесла издевательства от собственной подруги: она взломала её электронную почту, периодически удаляла входящие письма и оставляла лишь сообщения с унижениями, отправленные ей с её собственного адреса, а также устанавливала в её календаре напоминания: «Убей себя». [2]

С появлением социальных сетей стало проще прибегать к воздействию на пользователей: благодаря смартфонам мы находимся в Сети практически постоянно и, кажется, единственный способ абстрагироваться от немыслимого

---

[1] Профилактика школьного буллинга: методические материалы / автор-составитель: А. Ненашева. – Южно-Сахалинск, 2015. С. 43.

[2] Hamby S., McDonald R. Trends in violence research // Psychology of Violence. 2014. V. 4 (1). pp. 1-7.

потока информации – полностью перестать пользоваться интернетом, хотя и данное отключение вряд ли остановит поток агрессии. Личные данные, которые хранятся в интернете, анонимные и даже личные угрозы, фейковые страницы жертвы и издевательские паблики – это лишь несколько из множества способов воздействия на жертву.

В настоящее время феномен кибербуллинга получил крайне широкое распространение и вышел за пределы подростковых шуток. Это явление приводит не только к причинению морального вреда, но и к летальному исходу его жертв, обусловленного доведением до самоубийства. Во-первых, сложность борьбы с изучаемым явлением, состоит в том, что кибербуллинг основан на информационных ресурсах и технологиях, что указывает на его регулярную и быструю трансформацию. Во-вторых, субъекты травли, в большинстве случаев, остаются анонимными, в следствие чего это привлекает к осуществлению подобных действие все большее количество подростков. [1]

Тема буллинга является сложной не только для размышления, но и для изучения: во-первых, очень многие в той или иной степени становились жертвами травли, во-вторых, с данным явлением связан целый спектр негативных эмоций, таких как: беспокойство, страх, стыд, беспомощность. Кроме того, переживаемые человеком чувства вследствие травли не принято обсуждать среди других. Сам феномен травли рассматривается как предмет психологической науки и располагается на стыке психологии личности, социальной и клинической психологии.

Зачастую данное явление определяется как регулярное целенаправленное агрессивное поведение среди детей в возрасте до 18 лет при условии неравенства сил или полномочий сторон. Выделяет следующие ключевые характеристики феномена травли — намеренность, регулярность, неравенство силы или власти. Стоит отметить, что за рубежом данный вопрос в качестве одного из ключевых активно исследуется в рамках психологии образования.

---

[1] Интернет в России: его значение для россиян, цели и время использования / URL: http://www.bizhit.ru/index/internet_v_rossii_i_egoznachenie/0-593 (дата обращения: 18.06.2021).

Травля – агрессивное преследование одного из членов коллектива (особенно коллектива школьников и студентов, но также и коллег) со стороны другого. Кроме того, встречаются ситуации травли среди лиц из разных формальных или признаваемых коллективов. Зачастую организатором травли является один человек – лидер, или лидер при помощи сообщников, остальные же люди являются свидетелями. Жертве травли оказывается невозможным обезопасить себя от агрессии – в этом и заключается главное отличие данного явления от конфликта, где силы сторон примерно равны. Травля может выражаться не только в физической, но и в психологической форме. Данное явление прослеживается среди всех возрастных и социальных групп. Крайним же проявлением травли являются некоторые черты групповой преступности.

Выделяют также особую форму травли – групповую («травля толпы»), где организаторами агрессивных нападков является весь коллектив (микросообщество) или его большая часть, а также зачастую сам начальник или работодатель (жарг. «моббинг»).

Исследователями выделяются следующие проявления травли: оскорбления, угрозы, физическая агрессия, регулярная негативная оценка как жертвы, так и результатов её деятельности, отказ в доверии и делегировании полномочий и так далее.

Таким образом, нами были проанализированы теоретические, правовые и организационные основы обеспечения кибербезопасности в Российской Федерации. Выяснилось, что существует сформировавшаяся законодательная база нормативно-правовых актов, регулирующих вопросы кибербезопасности в Российской Федерации, однако зачастую данные документы не в состоянии охватить все многообразие возникающих в рамках киберпространства отношений. Также была рассмотрена организационная составляющая процесса – выделены структурные элементы, а именно органы власти, непосредственно регулирующие кибербезопасность нашей страны. Кроме того, были рассмотрены основные понятия кибербезопасности, изучена история преступлений в информационной среде, а также особенности интернет-травли.

§ 2. Уголовно-правовая характеристика преступлений в сфере информационно-телекоммуникационных технологий

В настоящее время имеется самая неблагоприятная тенденция развития среды Интернет с позиции формирования в ней пространства для процветания преступности. В свою очередь и меры, принимаемые правоохранительными органами страны, которые будут рассмотрены в данном параграфе, нельзя назвать в полной мере эффективными, поскольку наблюдается стремительный рост интернет-преступности, а раскрываемость данных преступлений не достигает даже 50%. Вследствие этого существует необходимость внедрения более совершенствованных методик расследования преступлений, совершаемых в сфере информационно-телекоммуникационных технологий.

Следует определиться с понятием уголовно правовой характеристики преступления. Рассмотрим определение данного термина В. Ф. Козловым[1], по мнению которого под уголовно-правовой характеристикой преступления следует понимать совокупность и содержание информационных данных, сведений о признаках элементов состава конкретного вида уголовного преступления.

Следует отметить, что данное определение является несколько узким, поскольку не затрагивает правовую базу, ведь именно на основании УК РФ и строится уголовно-правовая характеристика любого преступления. При этом, ключевыми аспектами и задачами деятельности лиц из числа правоохранительных органов при формировании уголовно-правовой характеристики преступления, являются детализация сведений об элементах состава преступления согласно УК РФ, а также описание корреляционных связей между ними. Рассмотрим некоторые статьи УК РФ, которые

[1] Козлов В. Ф. К вопросу о соотношении уголовно-правовой, криминологической и криминалистической характеристик преступления / URL: https://justicemaker.ru/view-article.php?id=22&art=3518 (дата обращения: 19.04.2022).

затрагивают преступления в сфере информационно-телекоммуникационных технологий.

- ст. 110, ст. 110.1, ст. 110.2 УК РФ, в которой говорится о доведении до самоубийства, в том числе с использованием сети Интернет;
- ст. 128.1 УК РФ, в которой говорится о клевете, в том числе с использованием сети Интернет;
- ст. 137 УК РФ, в которой говорится о нарушении неприкосновенности частной жизни, в том числе с использованием сети Интернет.

Однако большая часть положений УК РФ не конкретизирует те существующие преступления, которые могли бы совершаться и с применением информационных технологий. Например:

- ст. 119 УК РФ, в которой говорится об угрозах убийством или причинением тяжкого вреда здоровью. Представляется, что данные преступления могут быть совершены с применением сети Интернет, однако в положении речь об этом не идет;
- ст. 133 УК РФ, в которой говорится о понуждениях к действиям сексуального характера. Речи о возможном осуществлении данного вида преступления в Сети так же не идет;
- ст. 147 УК РФ, в которой говорится о нарушениях изобретательских и патентных прав. Такое преступление вполне может быть совершено с использованием дистанционных технологий, однако в данной статье нет указаний на это.

Заметим, что интернет развивается стремительно, и с каждым годом возникает все больше и больше возможностей для совершения уголовных преступлений дистанционным способом. Возможно, уже в недалеком будущем каждая статья УК РФ будет содержать в себе оговорку «с использованием информационно-телекоммуникационных технологий и сетей (включая сеть «Интернет»)». В настоящее время многие положения УК РФ делают акцент на возможности совершения тех или иных деяний с помощью интернета, что уже несколько упрощает процедуру расследования данных преступлений,

поскольку и сам сотрудник правоохранительных органов, и граждане, тем самым, осведомлены о недопустимости совершения тех или иных преступлений с использованием интернета. Однако система требует тщательного пересмотра.

Уголовно-правовой аспект кибербуллинга как одного из видов преступлений в сфере информационно-телекоммуникационных технологий считается наиболее интересным для рассмотрения. По действующему российскому законодательству кибербуллинг наказуемым не является, и его криминализация стоит под вопросом, в отличие от зарубежной уголовной практики. При этом кибербуллинг представляет общественную опасность охраняемым правам и свободам граждан, но данный вопрос законодательством недооценивается и обсуждается лишь на уровне общественно-социальных инициатив. В связи с этим считаем необходимым доказать криминальную основу кибербуллинга и необходимость уголовной ответственности за него.

Отечественное законодательство признает определенные общественные деяния опасными и криминализирует их, то есть признает их преступными, что следует из анализа различных определений процесса криминализации. Так, Г.А. Злобин и С.Г. Келина криминализацию определяют следующим образом: легальное определение в качестве преступления определенного действия или бездействия[1]. А.М. Яковлев же под криминализацией рассматривает определение в уголовном законе деяния в качестве общественно опасного, виновного и наказуемого[2]. Р.Р. Галиакбаровым понятие рассматривается шире: криминализацией является не только закрепление в уголовном законе

[1] Злобин Г.А., Келина С.Г. Некоторые теоретические вопросы криминализации общественно опасных деяний // Проблемы правосудия и уголовного права. М., 1978. 109 с.

[2] Яковлев А.М. Криминализация деяний в системе социального контроля и социального планирования // Планирование мер борьбы с преступностью: сборник статей / Отв. ред. В.М. Коган. М., 1982. 257 с.

определенных признаков новых составов преступлений, но и повышение верхних пределов санкций в рамках определенных составов преступлений[1].

Центральным звеном криминализации является отнесение противоправного деяния к составу преступления. Докажем общественную опасность кибербуллинга. Так, объектом кибербуллинга главным образом является не только благополучие личности и общества, но и жизнь и здоровье человека. Преступление совершается дистанционно – в информационной среде, между агрессором и жертвой нет физического контакта, что затрудняет поиски преступников. Однако последствия кибербуллинга могут быть чрезвычайно опасны – агрессор на расстоянии может довести жертву до самоубийства, распространять личную информацию.

Несомненно, дистанционный характер преступления делает его сложным в раскрытии. Агрессор чувствует анонимность и некую защищенность от правосудия. Информационное пространство становится местом связи агрессора с жертвой, однако пострадавшие не могут определить ни пол, ни возраст, ни отличительные признаки агрессора. Все, что удается выявить правоохранительным органам – IP-адрес компьютера виновного, однако, если кибербуллинг совершался в общественной сети Интернет, данные сведения оказываются невозможными для определения[2].

Также общественную опасность доказывает и мотив совершения киберпреступления – зачастую агрессорами кибербуллинг совершается умышленно, по подготовленному сценарию. Лишь в редких случаях кибертравля осуществляется случайно, как бы легкомысленно.

Таким образом, уголовно-правовая характеристика преступлений, совершаемых в сфере информационно-телекоммуникационных технологий, отражена в положениях УК РФ, который требует внесения поправок; статьи УК

---

[1] Галиакбаров Р.Р. Проблемы криминализации многосубъектных общественно опасных деяний // Актуальные проблемы криминализации и декриминализации общественно опасных деяний: сборник научных трудов. Омск, 1980. 324 с.

[2] Путинцева А.В. Уголовно-правовой аспект криминального кибербуллинга // Общественная безопасность, законность и правопорядок в III тысячелетии. 2020. № 6-1. С. 115-120.

РФ неисчерпывающие, совершить преступление дистанционным образом можно и по другим статьям, при чем, с каждым годом таких возможностей становится больше. Вышеизложенная информация полагает утверждать, что кибербуллинг является преступлением, так как представляет общественную опасность правам и свободам личности. Вследствие этого вопрос криминализации кибербуллинга в условиях российского законодательства является наиболее актуальным.

§ 3. Причины и условия совершения преступлений в информационной сфере

Определенной платой за информационный прогресс можно считать преступления в сфере компьютерной информации. С ростом совершенства компьютерной техники возрастает изощренный характер компьютерной преступности. Соответственно должны совершенствоваться способы борьбы с этим видом преступлений. Эти методы должны носить системный характер и учитывать причины и условия совершения преступлений данного вида.

Наиболее типичными причинами и условиями совершения преступлений в сфере компьютерной информации являются:

- рост числа ЭВМ и как следствие увеличение объемов информации, обрабатываемой и хранимой в ЭВМ;
- недостаточность мер по защите ЭВМ, систем ЭВМ и их сетей;
- недостаточность защиты программного обеспечения;
- рост информационного обмена через мировые информационные сети;
- отступление от технологических режимов обработки информации;
- отсутствие, несовершенство или отступление от правил эксплуатации программ для ЭВМ, баз данных и аппаратных средств обеспечения сетевых технологий;
- отсутствие или несоответствие средств защиты информации ее категории;

- нарушение правил работы с охраняемой законом компьютерной информацией;
- низкий уровень специальной подготовки должностных лиц правоохранительных органов, которые должны предупреждать, раскрывать и расследовать преступления в сфере компьютерной информации;
- отсутствие государственной политики в сфере обеспечения информационной безопасности.

Наряду с вышеперечисленными, специалистами выделяются следующие причины, способствующие совершению преступлений данного вида, это:

- недостаточная защита средств электронной почты;
- небрежность в работе пользователей ЭВМ;
- непродуманная кадровая политика в вопросах приема на работу и увольнения;
- нарушение технологического цикла проектирования, разработки, испытаний и сдачи в промышленную эксплуатацию компьютерных систем;
- совмещение функций разработки и эксплуатации программного обеспечения в рамках одного структурного подразделения;
- нарушение сроков изменения паролей пользователей;
- нарушение установленных сроков хранения копий программ и компьютерной информации, а иногда полное их отсутствие;
- необоснованность использования ЭВМ в конкретных технологических процессах и операциях;
- отсутствие должного контроля со стороны администрации за деятельностью своих работников, задействованных на чувствительных этапах обработки компьютерной информации;
- психологически неправильные межличностные взаимоотношения должностных лиц с подчиненными и другими работниками.

Теперь же перейдем к рассмотрению причин и условий кибербуллинга как одного из видов преступлений в информационной сфере. Участниками кибербуллинга чаще всего становятся подростки. Вследствие этого причины и условия возникновения кибербуллинга в большей мере будут рассматриваться в подростковой среде.

Компания McAfee, входящая в состав Intel Security, опубликовала данные своего изучения «Подростки за компьютером-2014: вопросы защиты личной информации, общения в социальных сетях и кибербуллинга». Данное исследование проводится ежегодно, в нем подвергаются анализу поведение в виртуальном пространстве и специфика интернет-общения детей подросткового возраста. Консалтинговая фирма The Futures Company со 2 по 14 апреля 2014 г. провела устный опрос, респондентами которого стали 1 502 молодых людей и девушек-американцев в возрасте от 10 до 18 лет[1]

В 2014 г. была зафиксирован резкий скачок лиц, которые стали свидетелями кибербуллинга, составив 87% от общего числа респондентов, заметим, что в 2013 г. указанный показатель находился в пределах лишь 27%. Что касается непосредственно жертв кибербуллинга, то данный показатель установить затруднительно, так как большое количество подростков не хотят признаваться, что в отношении них применилось физические или психическое насилие. Среди тех, кто признался, что был объектом кибербуллинга удалось выяснить в чем именно, по их мнение, состояли причины травли:

- 72% опрошенных указали в качестве основной причины внешность и ее изъяны;
- 26% – национальность или вероисповедание;
- 12% - личные неприязненные отношения, чаще всего, основанные на отказе состоять в близких отношениях.

[1] McAfee: исследование «Подростки за компьютером-2014: вопросы защиты личной информации, общения в социальных сетях и кибербуллинга // Технологии в образовании: новости и события / URL: http://educationevents.ru/2014/06/19/mcafee-research-about-internet-safety-for-teens/ (дата обращения: 12.05.2021).

Так, многие авторы, такие как: Г.Е. Ураева, О.Н. Боголюбова, Н.А. Селиверстова, Питер Мак-Ларен, считают, что причины проявления агрессии у подростков основаны именно на особенностях психологической деятельности. Анализ и обобщение исследований в области кибербуллинга позволяют выделить наиболее распространенные причины изучаемого явления:

1. Стремление к превосходству над другими;

А. Адлер считает, что желание превосходства представляет собой ключевой законом всей человеческой жизни. Желание выделиться среди другие и быть лучшим относится к врожденному чувству, это стремление мы проносим всю жизнь. Механизм запускается в возрасте пяти лет, когда цель как фокус жизненного стремления начинает свое формирование. Спустя время она организовывает нашу жизнь и является мотиватором, в основе которого лежат все поступки человека.

Но желание превосходства, а вместе с ним и вся человеческая деятельность может быть направлена как в позитивное русло, так и в негативное. Если человек, руководствуясь желанием превосходства, определит источником достижения цели позитивные блага, то его деятельность может быть основана на проявлении героизма, общественно-полезной деятельности, помощи нуждающимся и т.д.

В противоположном случае, деятельность лица основана на противоправных действиях, нарушении социальных норм и правил поведения. К данному направлению относится и кибербуллинг.

2. Комплекс неполноценности - совокупность психологических и эмоциональных факторов, которые способствуют оценке себя в обществе как ненужного и бесполезного элемента. Данный комплекс основан на дискриминации, отсутствии должного внимания в семье, душевные травмы, собственных неудачах и т. д. Первооткрывателем в области исследования комплекса неполноценности является венский психоаналитик Альфред Адлер. Он считал, что в попытках устранить имеющийся комплекс неполноценности,

человек не находит иных вариантов, как проявить превосходство над более слабым.

3. Зависть;

Зависть выражается в скрытой необходимости опередить другого человека в интеллектуальном развитии, физической подготовке, социальном авторитете и т.д.

Зависть является своего рода ограничителем – возникает желание добиться того, чего уже добились другие. В том случае, если человек по объективным причинам не обладает возможностью достижения аналогичных ресурсов или навыков, другим способом уравновешивания позиций является лишение человека имеющихся возможностей. Возникновение же зависти среди подростков возможно благодаря многим причинам, охватывающим как внешний вид, так и жизненные успехи в целом. Кибербуллинг, в данном случае, выступает возможностью сбалансировать умения, навыки, возможности, пусть и временно[1]

4. Месть;

Местью считаются действия, осуществляемые побуждениями ответить на реальную или мнимую несправедливость, причиненную ранее.

Явление имеет следующий механизм: приступ возмущения, похожий на внутренний взрыв вследствие несправедливых событий, запускает желание «дать сдачи», которое придает человеку энергии и сил за отстоянную гордость. Обиженные же вследствие кибербуллинга видят в мести способность защитить себя и исправить сложившуюся ситуацию. Как правило, эти люди не считают свои поступки выходящими за пределы нормы, наоборот, жертва интернет-травли уверена в правильности своих действий. При этом возникает чувство облегчения и оправдания за то, что они пережили.

5. Развлечение;

---

[1] Карепова Э.В. Феномен зависти: палач и жертва в одном чувстве / URL: http://psyfactor.org/lib/envy.htm (дата обращения: 12.04.2021).

По мнению, Л.А. Найденова, И.С. Осипова, П.Ю. Еремеева, кибербуллинг изначально может иметь форму шутки или незначительной насмешки. Но шутки довольно быстро могут перерасти в открытую травлю. В свою очередь, люди, которые стал объектами насмешек, приобретают подавленное состояние, снижение работоспособности и чувство неполноценности. Вследствие постоянного нахождения в ситуации страха человек старается избегать компании людей. Зигмунд Фрейд, изучавший человеческие бессознательные мотивации, расценивал юмор как символическое уничтожение врага. Вообще, уничтожение преследует целью неприкрытую яростную агрессию, а юмор является одним из способов возвыситься перед окружающими – я смешной и остроумный, а остальные – нет. То есть, как и во всех других случаях конфликтогенного поведения, внутренние мотивы направления юмора на партнера — это самовозвышение за счет унижения другого.

6. Проблемы в семейных взаимоотношениях;

К проблемам в семье относится: отсутствие должного внимания родителей к ребенку, чрезмерная вседозволенность, чрезмерно жесткий контроль родителей и т.д.

Все вышеперечисленные причины приводят к тому, что ребенок ищет иную форму общения и находи ее в Интернете, а свою агрессию, которую он не имеет возможность проявить в обычной жизни, реализует при помощи интернет-травли, которая служит единственной возможность отстаивания собственного «я».

7. Низкий уровень развития эмпатии;

Эмпатия (от греч. empatheia - сопереживание) – высокий уровень эмоционального развития, выражающийся в осознании и понимании эмоционального состояния окружающих. Термин «эмпатия» введен Э. Титченером. По мнению ученых, Т.П. Гаврилова и И.М. Юсупова, эмпатия - личностное свойство, имеющее социальный генез и, как любое социально обусловленное свойство, поддается целенаправленному формированию.

Подростковый возраст характеризуется И.М. Юсуповым как период маргинальной социализации. Подросток находится как бы в промежуточном, пограничном положении между различными социальными и возрастными группами, что накладывает определенный отпечаток на его психику и может выражаться в повышенной тревожности, неконтактности в общении, агрессивности, эгоцентричности, а также проявляться в реакциях эмансипации, компенсации, группирования со сверстниками и т. д. В подростковом возрасте как один из ведущих видов деятельности считается создание прочных отношений со сверстниками, которые предполагают стремление к полному пониманию и принятию другого, определяя интимно-личностный характер общения. Однако подростки, занимающиеся кибербуллингом, считают данную деятельность вполне хорошим способом установления межличностного взаимодействия. Некоторые исследования показали, что 40 % студентов не сочувствуют своим жертвам в Интернете и их не мучает совесть. Вместо этого, многие подростки сообщили, что занятия травлей в сети позволили получить ощущения веселья, популярности и силы в глаза окружающих.

8. Отсутствие умения разрешать конфликты;

Конфликты, возникающие в подростковом возрасте, являются формой социализации личности, а также служит способом развития. В межличностных отношениях причины конфликта многогранны и имеют сложную структуру – это всё то, что относится к области вкусов, моды и другим подобным мотивам. Только конструктивный диалог способствует нахождению компромисса с целью разрешения конфликтной ситуации, выявлению скрытых проблем и налаживанию нормальные доверительные взаимоотношения. Но, учитывая особенности развития личности в пубертатный период, мы понимаем, что подросток еще не способен прибегнуть к конструктивному диалогу с оппонентом; даже для многих взрослых людей данная задача является весьма сложной.

Подростки могут перенести конфликт в интернет-среду, так как не могут найти наиболее удачный способ разрешения конфликта, считают свою позицию

превосходствующей над мнением оппонента, не принимая другую сторону ситуации. Там в их распоряжение попадает огромная аудитория слушателей, которая придает чувства силы и открывает новый уровень отстаивания своих интересов. В кибербуллинге наблюдается перевес сил на стороне одного из участников конфликта, кроме того, другой участник даже не догадывается, кто его оппонент. Неравновесность сил приводит к тому, что унижаемая жертва не может в полной мере постоять за себя, неспособен к сопротивлению, полностью беззащитен.

9. Индивидуально-личностные характеристики индивида (акцентуации характера, проблемы в эмоционально-волевой сфере и др.) Рассмотрим некоторые из них.

Акцентуация характера – это крайний вариант нормы, усиление отдельных черт характера, вследствие чего обнаруживается определенная уязвимость в отношении некоторого рода психогенных воздействий, при одновременно хорошей устойчивости к другим. Иными словами, акцентуация считается вариантом психического здоровья (нормы), но при котором наблюдается особая выраженность, заостренность, непропорциональность некоторых черт характера всему складу личности, что способствует возникновению определенной личностной дисгармонии. Именно при наличии какой-либо явной акцентуации подросток может быть наиболее склонен к кибербуллингу. Тому пример истероидный или демонстративный тип личности, которым присущи следующие особенности: эгоцентризм, крайнее себялюбие, ненасытная жажда внимания, потребность в почитании, в одобрении и признании действий и личных способностей. Многое из особенностей характера находя удовлетворение в Сети, а именно в кибербуллинге: собственная личность не задевается, большое количество внимания и поддержка огромной аудитории, возвышение себя за счет принижения другого. Или, например, эпилептоидный тип, которому присущи склонность к злобно-тоскливому настроению с накапливающейся агрессией, проявляющейся в виде приступов ярости и гнева (иногда с элементами

жестокости), конфликтность, вязкость мышления, скрупулезная педантичность. Кибербуллинг для таких акцентуированных личностей становится способом выплеснуть агрессию в онлайн-пространство, при этом заняв доминирующую позицию в конфликте.

Стоит понимать, что все вышеперечисленные причины взаимодополняют и взаимообуславливают друг друга. Так, например, испытывая чувство собственной неполноценности, подросток испытывает зависть к более развитым и успешным сверстникам, вследствие чего стремится превосходить окружающий его социум. Также и проблемы в семейных взаимоотношениях провоцируют возникновение нарушений в личностной сфере подростка и могут усугублять протекание подросткового возрастного кризиса. Так, часть причин как раз являются возрастными особенностями личности подростка: конформизм, инфантилизм, стремление быть принятым сверстниками, иметь среди них высокий социальный статус и др. [1]

Но, помимо причин кибербуллинга, существуют так называемые благоприятные условия его протекания. К ним относятся:

- непрерывное развитие информационной среды и высоких технологий;
- Высокий уровень латентности кибербуллинга;
- Большой объем навыков современных подростом по использованию информационно-телекоммуникационных ресурсов;
- иллюзия анонимности;
- указание на личных станицах исчерпывающие данные о себе и близких;
- безнаказанность со стороны администрации сайтов и закона;
- отсутствие компьютерной компетентности и этики у подростков[2].

---

[1] Gordon S. 8 Reasons Why Kids Cyberbully Others // About Health / URL: http://bullying.about.com/od/Cyberbullying/a/8-Reasons-Why-Kids-Cyberbully-Others.htm (дата обращения: 01.05.2021).

[2] Баранов А.А., Рожина С.В. Психологический анализ причин подросткового кибербуллинга // Вестник Удмуртского университета. Серия «Философия. Психология. Педагогика». 2015. №1. С. 13-14.

Таким образом, основными причинами и условиями совершения преступлений в сфере компьютерной информации являются: информационный прогресс общества, отсутствие или несоответствие средств защиты информации, отсутствие служб информационной безопасности, а также высокая латентность преступлений данного вида, позволяющая преступникам избегать наказания и совершать новые преступные посягательства. Социальная сущность совершения компьютерных преступлений лежит в аномии, в транзитивности российского общества, в расхождении темпов нравственного и научного развития. Также было выяснено, что кибербуллинг как один из основных и масштабных видов преступлений в информационной среде активно развивается в среде подростков. Причины возникновения данного явления многообразны; относятся как к психологическим, личностным, так и социальным факторам.

§ 4. Личность киберпреступника и её характеристики

Изучение основ психологии киберпреступников позволит разработать стратегии противодействия киберпреступности, оценить соответствие уголовного законодательства психологии преступника, а также разработать тактику ведения процессуальной деятельности.

Профессор Университета Райдер (США) Джон Шулер (John Suler) для обозначения эффекта, который киберпространство оказывает на человека, делая возможным действовать более свободно, нежели в реальном социуме, ввел понятие «эффект онлайн дезингибиции»[1]. Основу этого эффекта, по мнению Шулера, составляют:

- дисассоциативная анонимность («ты меня не знаешь»), сущность которой состоит в том, что в условиях анонимности люди могут отделить свои действия в киберпространстве от реального мира и реальной личности, в

[1] John Suler. The Psychology of Cyberspace / URL: http://users.rider.edu/~suler/psycyber/psycyber.html (дата обращения: 06.03.2022)

таком случае человек полагает, что может не брать на себя ответственность за свои действия;

- невидимость («ты меня не видишь») – позволяет избегать установления психологического контакта;
- асинхронность («увидимся позже») – возможность общаться в отдельных случаях без необходимости немедленной реакции на слова или действия собеседника, что является немаловажным дезингибирующим фактором;
- солиптическая интроекция («это все в моей голове») – вероятность того, что при онлайн-общении может возникнуть ощущение, что все происходит исключительно в нашем собственном воображении;
- минимизация власти («мы равны») – возникает из-за опосредованного восприятия атрибутов более высокого социального положения, а также возможности их игнорировать. Тем не менее, необходимо учитывать, что в киберсоциуме можно говорить о существовании качественно другой, но все-таки иерархии.

Психологическая характеристика отдельных киберпреступников, безусловно, важная составляющая изучения киберпреступности, однако вследствие большого количества видов киберпреступлений является чрезвычайно объемной. Поэтому считаем необходимым представить только основные группы киберпреступников. За основу же предлагаемой классификации берется вид совершенного преступления и уровень компьютерных навыков преступников.

1. Преступники специального киберпреступного типа. Данная категория преступников не только специализируется на совершении специальных киберпреступлений, но также каждый из киберпреступников данного типа совершает их самостоятельно и обладает «профессиональными» техническими знаниями, необходимыми для совершения преступлений данного рода. Критерий наличия специальных знаний является на сегодня крайне важным вследствие того, что на виртуальном «черном рынке» достаточно программного обеспечения, информации и предложения услуг, которые позволяют совершать

специальные киберпреступления без наличия соответствующих знаний. Наличие же специальных знаний фактически означает принадлежность такого преступника к субкультуре хакеров (крэкеров).

2. Преступники общекиберпреступного типа совершают при помощи электронных устройств неспецифические для киберпространства деяния (мошенничество, кражи, отмывание денежных средств, незаконное распространение порнографических материалов и проч.), не используя при этом специальные технические знания либо используя только поверхностные знания и приобретенные программные средства. Как уже говорилось, условия киберпространства существенно отличаются от реальных, поэтому необходима дифференциация киберпреступников в зависимости от локализации их преступной деятельности. Критерий локализации имеет существенное значение для установления процесса возникновения преступного умысла, его природы, а также степени общественной опасности данного лица. Таким образом, можно выделить три основных группы.

1. Киберпреступники, ведущие основную преступную деятельность только в киберпространстве. Преступные установки у таких лиц сформировались в высококриминогенных условиях киберпространства, следовательно, в случае устранения криминогенных факторов такие лица могут представлять значительно меньшую социальную опасность, нежели реальные преступники.

2. Киберпреступники, занимающиеся в равной степени преступной деятельностью как в киберпространстве, так и реальной жизни. Психология преступников данной категории является типично преступной при незначительном влиянии условий киберпространства.

3. Лица, совершившие ранее преступления, не относящиеся к киберпреступлениям, совершающие киберпреступления в настоящее время. Появление этой категории киберпреступников обусловлено, в первую очередь, пристальным вниманием организованных преступных сообществ к широким возможностям Интернета. Обладая хорошими организаторскими

способностями, такие киберпреступники используют лиц, имеющих специальные знания, для совершения преступлений, при этом основные усилия направляют на максимальное получение прибыли и усиление собственного влияния.

В зависимости от мотивации преступного поведения можно выделить следующие типы киберпреступников.

Корыстный тип. Помимо характерных для обыкновенного корыстного типа преступников свойств, киберпреступники могут совершать преступления для получения специфических предметов, имеющих особую ценность в киберпространстве, например игровых предметов, без цели их дальнейшей продажи.

Насильственный тип. Несмотря на отсутствие физического контакта, такие насильственные преступления, как доведение до самоубийства или угроза убийством, могут быть совершены при помощи электронных
устройств и сетей. В связи с рядом самоубийств несовершеннолетних, совершенных в том числе под воздействием оскорблений или угроз, сделанных с помощью различных онлайн-сервисов, в США обсуждается возможность введения уголовной ответственности за киберзапугивание (cyberbullying) и киберпреследование (cyberstalking) для предотвращения трагических последствий.

Сексуальный тип. Для данного типа преступников характерно совершение таких преступлений, как незаконное распространение порнографических материалов или предметов, без цели наживы, понуждение к действиям сексуального характера, развратные действия. Вероятно, что в некоторых случаях совершение преступлений в отношении несовершеннолетних будет иметь место насильственно-сексуальный тип преступника.

Социально дезорганизующий тип, основной целью которого является само нарушение обеспеченных законодательно социальных норм и оказание деструктивного влияния на социум и общественные отношения.

Идеологически или политически мотивированный тип. В последнее время совершение специальных киберпреступлений становится распространенной формой протеста и политической или идеологической борьбы.

Статусный тип. Преступники этого типа, совершая преступления, стремятся получить более высокий неформальный социальный статус, зачастую в сообществах киберсоциума. Хотя по своей природе статусность как стимул к совершению преступлений является дополнительным фактором или оказывает кратковременное влияние на преступную деятельность, в среде хакеров (крэкеров) может иметь достаточно серьезное мотивирующее значение.

Исследовательский тип характерен для лиц, совершающих специальные киберпреступления. Основой для их мотивации служит изучение программных и аппаратных составляющих электронных устройств и их сетей, поиск уязвимостей, возможности их использования и устранения. Данные цели были характерны для первых поколений немногочисленных хакеров, а также отдельных современных преступлений, хотя сейчас в большинстве случаев они выступают только дополнительным мотивом. Преступники данного типа, в первую очередь, направляют свои действия на устранение ошибок и развитие защиты устройств и сетей и поэтому являются социально «полезными».

Изучение же феномена травли позволяет выделить субъекты, роли кибербуллинга, к которым относятся жертва, агрессор и свидетель. По мнению психологов, негативные результаты данного явления будут наблюдаться у всех трёх групп участников.

Наиболее тяжёлые последствия травли находят свое проявление у жертвы агрессии. Зачастую результатом травли для жертвы является потеря уверенности в себе. Кроме того, возможны более тяжелые исходы ситуаций буллинга: психические отклонения различной тяжести, психосоматические заболевания, а в ряде случаев самоубийство или спланированное нападения на

место учебы или работы жертвы. В таких случаях наиболее важно доказать человеку, что его травят, и объяснить, как поступать в таком случае.

Свидетели травли также, как уже было сказано выше, получают негативный опыт, так как оказываются бессильными перед властью толпы, а в дальнейшем стыдятся за нерешительность вступится за жертву из страха оказаться на ее месте.

Кроме того, опыт насилия деструктивен особенно для личности агрессора. Действия лидера способствуют угасанию любых чувств, отрицанию близких взаимоотношений с людьми, а в конечном итоге — к деструктивным, асоциальным чертам личности. Личности агрессора становится все сложнее доверять остальным, строить близкие отношения с окружающими, партнёрами и родственниками, в том числе и с собственными детьми. И в некоторых ситуациях наблюдается месть агрессору со стороны отчаявшейся жертвы посредством нанесения тяжких травм.

Участникам буллинга присущи определенные личностные и поведенческие характеристики, а также ряд сопряженных с ролями социальных рисков.

Жертвы же травли обладают такими характерологическими особенностями, как чувствительность, тревожность, склонность к слезам, физическая слабость, низкая самооценка. Такие люди зачастую не имеют достаточной поддержки извне, у них мало близких людей. Дети же большую часть своего свободного времени проводят в кругу взрослых. Образец жертвы травли – замкнутый ребенок с чертами девиантного поведения, отрицательными убеждениями о самом себе и трудностями в установлении социальных связей. Такие черты могут выступать и как последствия травли, и в качестве возможных предпосылок для других детей и общества в целом сделать данного ребенка жертвой.

Агрессоров же характеризуют как людей, обладающих высоким эмоциональным интеллектом, так как им легко удается распознать чужие эмоции, психические состояния и с успехом манипулировать детьми. Среди

основных побуждений к буллингу выделяют желание власти, чувство удовлетворения от причинения вреда другим и вознаграждение, как материальное (деньги, сигареты, и любые другие вещи жертвы), так и психологическое (приобретаемый престиж, повышение социального статуса). Но систематическое поведение в роли агрессора влечет ряд негативных последствий, а именно: низкая успеваемость и прогулы, драки, воровство, вандализм, хранение оружия, употребление алкоголя и табака, в некоторых случаях, наркотических средств.

Однако около 3% детей могут занимать роли и агрессора, провоцировать других детей на причинение себе вреда; или же в некоторых случаях такой ребенок является организатором травли, а в других – становится жертвой – это так называемые «преследователи/жертвы», или «провоцирующие жертвы». Таким детям также присущи такие характерологические особенности, как гиперактивность, импульсивность, неуклюжесть, вспыльчивость в сочетании с нарушениями поведения, низкой способности к самоконтролю, низкой социальной компетентностью, трудностями с концентрацией внимания и, как следствие, проблемами в учебе, тревожностью и проявлениями депрессии. В целом такие дети инфантильнее своих сверстников. Несмотря на то, что такой тип детей встречается редко, учителям наиболее сложно с ними работать, и вследствие этого ребенку не хватает сочувствия и поддержки от других детей. Именно поэтому для них наиболее характерно суицидальное и аутоагрессивное характеристики поведения.

Переходя к третьей и наиболее многочисленной группе участников буллинга – свидетелям, стоит отметить, что она является наиболее благоприятной для профилактики травли. Особенно важно отметить, что большая часть (но чем старше, тем реже) детей испытывают чувства жалости к жертве и сообщают об этом, но лишь немногие стараются предотвратить ситуации травли. Реакция свидетелей является ключевой в разворачивающейся ситуации: следование лидеру и проявления одобряющего поведения (улыбка, смех и тому подобное) со стороны свидетелей выступает в качестве поощрения

лидерам, а оказание сопротивления и несогласия, попытки поддержать жертву не дают преследователям продолжить давление. Важно подчеркнуть, что в таких ситуациях свидетель борется сам с собой: попытка помочь жертве находит отрицание в виде чувства собственной небезопасности и страха лишиться социального статуса в детском коллективе. Отрицательные последствия становления свидетелем травли находят отражение в восприятии окружающей среды как заведомо небезопасной, чувствах страха, беспомощности и стыда за свое бездействие, а также одновременно в мотиве стать одним из преследователей. Кроме того, у свидетелей слабеет способность к эмпатии.

Существует целый ряд факторов, которые способствуют зарождению и развитию травли среди детских сообществ. Чаще всего, это зависит от типа воспитания в семье и микроклимате того образовательного учреждения, куда попадают дети для получения образования.

Однако и взрослые участники школьных взаимоотношений, сами этого не замечая, могут участвовать в травле и даже способствовать ей посредством:[1]

- публичного оскорбления или унижения ученика в отношении уровня его знаний, внешности и т.д.;
- демонстрации угрожающих жестов (замахиваний, ударов по близлежащим ученику объектам др.);
- разделение учеников на группы по принципу «нравятся или не нравятся».

Также способствовать травле и провоцировать её могут следующие факторы:

- наличие в классе признанного «лидера», который основан на агрессии и отношениях власти- подчинения;
- острый открытый конфликт между учениками;

[1] Глазман О. Л. Психологические особенности участников буллинга // Известия Российского государственного педагогического университета им. А. И. Герцена. 2009. С. 159-165.

- недостаточный уровень контроля за взаимоотношениями учащихся.

Помимо поведения взрослых людей, которое способствует развитию буллинга в школьном сообществе, существует ряд факторов, провоцирующих возникновению травли непосредственно среди детей:

- низкие моральные качества несовершеннолетних;
- неадекватная заниженная или завышенная самооценка;
- высокий уровень импульсивности;
- недостаточный уровень самоконтроля;
- злоупотребление алкогольными и психотропными веществами, а также компьютерными играми;
- индивидуальные психические отклонения;
- желание проявлять властные полномочия над другими;
- раннее нахождение лица в статусе жертвы буллинга;
- смена воспитателей (отчим, мачеха), появление второго ребёнка в семье;
- семейное и сексуальное насилие;
- внутрисемейные конфликты;
- низкий социально-экономический статус семьи;
- завышенные требования к успеваемости, которые не всегда соответствуют способностям и возможностям ребёнка;
- гиперопека или равнодушие со стороны родителей;
- склонение совершеннолетних к противоправным действиям;
- случаи приводов в полицию, ранняя судимость.

Фаза полового созревания способствует не только возникновению затруднений физиологического и психологического характера, но и началу формирования критического мышления, которое позволяет ставить под сомнение поступки взрослых, препятствовать их социальным установкам. Наблюдаются сложности в школьной успеваемости и явление навешивания так

называемых ярлыков (учителя и родители говорят, что ребёнок неисправим, плохо воспитан или глуп). Ученики, которые имеют затруднения в успеваемости, используют проявления агрессии в качестве компенсации сложностей в учебной деятельности. Именно поэтому цель травли определяется как желание скрыть за агрессивным поведением свою неполноценность.

Таким образом, в настоящее время достижения, полученные в изучении психологии киберпреступников, уже активно применяются в других странах при расследовании преступлений, в основном, при определении типа преступников. Исследования в данной сфере являются также важным теоретическим материалом и могут способствовать развитию изучения психологии девиантного поведения. Как показывает сложившаяся ситуация, в борьбе с киберпреступностью и ее профилактике необходим мультидисциплинарный подход, в котором не последнее место занимает психология. Поэтому создание эфективной системы противодействия киберпреступлениям требует активизации исследований психологии киберпреступников и подготовки кадров в данном направлении.

Кроме того, нами были рассмотрены психологические составляющие субъектов кибербуллинга как одного из видов информационных преступлений, а именно то, как кибертравля оказывает влияние как на жертв и свидетелей, так и на агрессоров.

ГЛАВА 2. СТРАТЕГИЯ И ТАКТИКА ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В СФЕРЕ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

§ 1. Зарубежный опыт противодействия преступлениям с использованием компьютерных технологий

Совершенствование компьютерной техники, стремительное развитие информационных технологий порождает качественное изменение преступлений в сфере компьютерной информации. И, конечно же, проблемы противостояния таким хищениям остро стоят перед мировым сообществом, которое адекватно оценивает сложившуюся ситуацию, признавая обязательность принятия безотлагательных международных мер.

Первые шаги, предпринятые в этих целях, – Рекомендация №89 (9), содержащая список компьютерных правонарушений, принятая 13 сентября 1989 года на заседании Комитета министров Совета Европы; Окинавская хартия Глобального информационного общества, принятая 22 июля 2000 года главами государств и правительств «Группы восьми». В связи с этим целесообразно обратить внимание на то, как на современном этапе международные организации развивают свою деятельность в этом направлении.

Значительный вклад в решение проблемы противодействия киберпреступности вносит ООН. Управлением ООН по наркотикам и преступности в целях изучения проблемы противодействия, разработки предложений по совершенствованию международных правовых мер и национальных законодательств проведено всестороннее исследование проблемы киберпреступности. Для проведения исследования по просьбе Генеральной Ассамблеи ООН (резолюция от 1 апреля 2011 г. №65/230) Комиссией по предупреждению преступности и уголовному правосудию была создана межправительственная группа экспертов открытого состава, которая

определила темы и методологию исследования, приняла к сведению само исследование, а также ответные меры на него со стороны государств-участников, международного сообщества и частного сектора и уже в 2017 году предложила выполнять функции платформы для дальнейшего обсуждения вопросов, касающихся киберпреступности, внимательно следить за новыми тенденциями.

В первую очередь необходимо проанализировать Конвенцию Совета Европы о киберпреступности, принятую 23 ноября 2001 года, известную также как Будапештская конвенция (далее – Конвенция). В настоящее время это единственный глобальный документ международного уровня, являющийся обязательным для государств-участников, который регулирует действия по борьбе с киберпреступностью. Конвенция определила виды киберпреступлений и обязала договаривающиеся стороны принять законодательные и иные меры, необходимые для того, чтобы квалифицировать деяния в качестве уголовных преступлений согласно внутригосударственному праву.

В вопросах противодействия киберпреступности Совет Европы не ограничился разработкой и принятием Конвенции. Им создан Комитет по Конвенции о киберпреступности (T-CY), который представляет государства-участников, содействует эффективному использованию и реализации положений Конвенции, обмену информацией и рассмотрению поправок к ней. Кроме этого, помощь государствам в консолидации их возможностей в решении проблем, связанных с киберпреступностью, оказывает Управление Совета Европы по вопросам киберпреступности (C-PROC).

Если обратиться к документам, принятым Европейским Союзом в целях построения системы борьбы с правонарушениями в информационном пространстве, то необходимо отметить, что наряду с актами об электронной коммерции, персональных данных, об атаках на информационные системы, против детской порнографии, в 2001 году принято Рамочное решение по борьбе с мошенничеством и подделкой безналичных платежных средств, которое

обязало каждого участника признать такие деяния, если они совершены умышленно, преступлением.

Проблема же интернет-травли имеет большой размах и признается во всем мировом сообществе. Так, многие развитые государства законодательно закрепили меры по борьбе с травлей в сети. Например, в Южной Корее такой закон был принят еще в 2007 году. К уголовной ответственности за травлю в интернете могут привлечь и в Германии, а во Франции учителей обязали следить за блогами своих учеников и помогать жертвам кибербулинга. Агрессорам-учащимся между тем грозит исключение из школы.

В США нет федерального закона о кибербуллинге, однако ответственность за травлю закреплена в законодательстве некоторых штатов. Первыми такой закон приняли в Джорджии. В 1999 году власти ввели запрет на травлю в интернете и через мобильную связь.

Позднее похожие меры приняли и в Неваде, где ввели уголовное наказание за устные или письменные угрозы. Кроме того, в США сформирована общественная организация BullyPolice, которая защищает подвергшихся интернет-травле детей и оказывает поддержку пострадавшим. Помимо этого, организация обращает внимание на законодательную сторону контроля кибербуллинга.

В Канаде между тем функционирует целая система борьбы с интернет-травлей. Ее разработали в организации Promoting Relationships and Eliminating Violence Network (PREVNet), в которую входят 130 ученых-исследователей и 62 национальные молодежные организации.

Кроме того, в 2015 году власти обновили уголовный кодекс: он стал наказывать тех, кто отправляет интимные фотографии человека без его согласия.

Проблемой кибербуллинга озабочены и в Австралии. Там в 2019 году стартовал процесс реформы закона о диффамации (оглашение в печати позорящих сведений). Группа. Формулировавшая закон, пришла к выводу, что существующие нормативы не учитывают век современных технологий. В ходе подготовки реформы на обсуждение был вынесен ряд вопросов: о привлечении

соцсетей к ответственности за публикации пользователей, о введении ограничений на подачу новых исков для людей, которые на самом деле серьезно не пострадали от клеветы, о компенсациях, опровержении, критериях невиновности социальных сетей и других агрегаторов цифрового контента[1].

Для наилучшего понимания зарубежного опыта противодействия преступлениям с использованием компьютерных технологий, а именно кибербуллингу, изучим данный вопрос параллельно с состоянием проблемы в Российской Федерации, что позволит глубже проанализировать подходы к борьбе с информационной преступностью.

Что касается Российской Федерации, то большая часть жителей (49%) уверена, что уровень агрессии в интернете вырос за период пандемии коронавируса, показало исследование Mail.RuGroup. Лидерами по объемам распространения деструктивного контента стали иностранные интернет-платформы, а именно — Instagram и Twitter. Весомая доля аудитории этих площадок — несовершеннолетние пользователи, которым намного сложнее справится с кибербуллингом в отличие от взрослой части населения.

В России уже имеются специальные нормы, которые закреплены в гражданском кодексе и призваны регулировать вопросы защиты чести, достоинства и деловой репутации в сети, о чем отмечает председатель комиссии по правовому регулированию обеспечения цифровой экономики московского отделения АЮР Александр Журавлев.

Если же речь идет о клевете или каких-либо уголовно наказуемых деяниях, то практика неоднозначна. Очень часто проблема заключается в том, что нельзя установить конкретного ответчика. Это происходит вследствие нераскрытия информации о пользователях иностранными площадками, не имеющими представительства на территории РФ, даже по запросу российских правоохранительных органов. Вторая проблема — различная правоприменительная практика. В настоящее время редко

[1] Уровень агрессии растет: как в России борются с кибербуллингом // Газета.ru. URL: https://www.gazeta.ru/tech/2020/12/15_a_13401170.shtml (дата обращения: 13.03.2022).

правоохранительными органами возбуждаются дела за совершенные нарушения в Сети.

Александр Журавлев видит решением проблемы внесение на рассмотрение в Госдуму законопроект о правилах саморегулирования интернет-платформ. Необходимо обязать правоохранительные органы оперативно выявлять и пресекать случаи кибербуллинга, а также быстро реагировать на обращения пользователей. Такой законопроект позволил бы регламентировать правила саморегулирования и специальные виды ответственности за нарушение этих правил.

Директор Регионального общественного центра интернет-технологий Сергей Гребенников в свою очередь призывает приравнять ответственность за преступления, совершенные в реальной в жизни и интернете. Он считает, что в век современных технологий граница между онлайном и оффлайном давно стерлась, а делить преступления, совершаемые в жизни и виртуальном пространстве, совершенно неправильно. Победить же и предотвратить травлю в сети позволило бы повышение цифровой грамотности населения, убежден эксперт, ведь кибербуллинг – это степень межличностных взаимоотношений, улучшить которые возможно лишь повышением уровня культуры.

Отметим, что в России уже проводят профилактические работы по предотвращению интернет-травли с детьми школьного возраста и их родителями. Специалисты общественных организаций оказывают помощь школьникам в ликвидации последствий буллинга в Сети, учат цифровой грамотности детей, что при столкновении с ситуациями кибербуллинга знать алгоритм действий и предпринимаемых мер. Общественники также проводят встречи с родителями, обращая их внимание на способы предотвращения негативного влияния интернета на детей. В частности, по всей стране проводятся бесплатные уроки безопасного интернета, на которых детям рассказывают о возможных киберугрозах.

Таким образом, обзор деятельности международных организаций позволяет заключить, что мировое сообщество активно предпринимает меры по

борьбе с киберпреступлениями, прилагает усилия по реформированию законодательства. Но при этом, признавая, что эффективное противостояние возможно лишь при совместных комплексных, согласованных действиях, оно пока не добилось положительных результатов в этом направлении. Принятые документы международных и региональных организаций характеризуются определенной степенью фрагментации с точки зрения криминализации деяний. Обзор деятельности в сфере борьбы с кибертравлей международных сообществ не вызывает сомнений о деятельной работе по реформированию законодательства, введении новых сообществ и организаций по борьбе с киберпреступлениями и помощи жертвам кибербуллинга. В Российской Федерации также проводится совершенствование законодательства, однако нормативно-правовое регулирование вопроса требует доработки.

§ 2. Деятельность органов внутренних дел по профилактике, выявлению и пресечению преступлений в информационной сфере

В каталоге федеральных органов исполнительной власти МВД России отведена важнейшая роль: оно выступает в качестве ключевого органа, осуществляющего исполнительно-распорядительные полномочия и противодействующего хищениям, совершаемым с использованием современных информационных технологий.

В соответствии с приказом МВД России от 17 января 2006 г. № 19 «О деятельности органов внутренних дел по предупреждению преступлений» (далее — Приказ о предупреждении преступлений) конкретные обязанности по предупреждению преступлений, в том числе являющихся предметом рассмотрения в настоящей работе, закреплены за различными подразделениями Министерства.

Так, в обязанности участковых уполномоченных полиции (далее – участковые) входит:

- систематический анализ актуальной оперативной обстановки на обслуживаемых участках;
- внесение предложений, направленных на повышение эффективности принимаемых среди населения профилактических мер по предупреждению тех или иных видов преступлений (например, информирование граждан о новых способах совершения хищений с использованием информационных технологий, а также о методике и тактике, которые используются преступниками);
- привлечение граждан обслуживаемого участка, различных охранных предприятий и общественных объединений, осуществляющих свою деятельность в сфере правоохраны, для организации совместной работы по предупреждению IT-преступлений;
- установление конфиденциальных контактов и доверительных отношений с гражданами обслуживаемого участка (для получения сведений, которые могут быть использованы в целях предупреждения и раскрытия преступлений, совершаемых с использованием информационных технологий);
- содействие соответствующим правоохранительным органам в преследовании и задержании лиц, подозреваемых в совершении рассматриваемой категории преступлений.

Обязанностями сотрудников подразделений дознания являются:

- профилактическая работа с лицами, в отношении которых были совершены преступления с использованием информационно-телекоммуникационных технологий (такая работа очень часто позволяет жертвам преступлений «отойти» от соответствующего виктимного поведения);
- своевременная передача сведений, полученных в ходе расследования преступлений, в соответствующие подразделения органов внутренних дел (далее — ОВД) и органов государственной власти.

К обязанностям сотрудников уголовного розыска относятся:

- выявление причин, обусловливающих совершение IT-преступлений, а также их устранение в рамках имеющихся полномочий;
- выявление лиц и последующее применение необходимых мер к лицам, имеющим отношение или непосредственно занимающимся приготовлением или покушением на совершение преступлений с использованием информационных технологий;
- взаимодействие с участковыми, в том числе в ходе реализации мероприятий по выявлению и предупреждению IT-преступлений, совершаемых лицами, которые раньше уже совершали подобные преступления и были судимы за это;
- участие в совместных комплексных мероприятиях оперативно-профилактической направленности;
- розыск лиц как совершивших, так и подозреваемых или обвиняемых в совершении IT-преступлений, а также лиц, скрывающихся от органов дознания, следствия или суда;
- осуществление оперативно-разыскных мероприятий в отношении лиц, представляющих оперативный интерес (например, тех, кто был осужден за совершение IT-преступлений, но при этом наказание не связано с лишением такого лица свободы).

Необходимо отметить, что в Приказе о предупреждении преступлений не нашли своего закрепления некоторые функции подразделений уголовного розыска, которые, тем не менее, на практике повсеместно реализуются, например: анализ преступлений, совершенных с использованием информационных технологий; выявление и обобщение при помощи средств массовой информации способов совершения рассматриваемой категории преступлений и др.

Следует также выделить некоторые обязанности, присущие следственным подразделениям:

- установление обстоятельств, способствовавших совершению преступления с использованием информационных технологий;
- письменное информирование в трехдневный срок заинтересованного подразделения ОВД о подозреваемых и обвиняемых, в отношении которых избрана мера пресечения, не связанная с заключением под стражу, а также в отношении которых уголовное преследование прекращено по нереабилитирующим основаниям, по месту совершения хищения в указанной сфере, по месту жительства или месту пребывания указанных лиц для постановки их на профилактический учет;
- передача в заинтересованное подразделение ОВД данных, полученных в результате расследования уголовных дел и которые в дальнейшем могут быть использованы в целях предупреждения и раскрытия IT-преступлений;
- реализация профилактических мероприятий в отношении лиц, пострадавших от совершения IT-преступлений (цель таких мероприятий сводится к изменению виктимного поведения последних).

Особое место в предупреждении преступлений, в частности, преступлений, совершаемых при помощи информационно-телекоммуникационных технологий, отводится подразделениям информации и общественных связей МВД России, которые выступают в качестве связующего элемента для всех перечисленных выше подразделений, средств массовой информации и граждан. К обязанностям подразделений информации и общественных связей относятся:

- распространение в СМИ и сети Интернет информации, связанной с предупреждением IT-преступлений;
- подготовка и проведение для всех заинтересованных лиц встреч, пресс-конференций, брифингов, «круглых столов» с участием руководства ОВД по вопросам, касающимся предупреждения IT-преступлений.

Также в области противодействия преступлениям в сфере информационных технологий в структуре МВД РФ существует важнейшее

подразделение, а именно, Бюро специальных технических мероприятий МВД России — отдел «К», активно противодействующий преступлениям в киберпространстве, в том числе осуществляющий профилактические мероприятия посредством издания пособий и методических рекомендаций для сотрудников ОВД по противодействию преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий.

Рассматривая деятельность органов внутренних дел по профилактике, выявлению и пресечению кибербуллинга как одного из видов преступлений в информационной сфере, можно сказать, что на сегодняшний день отсутствует четкость в организации мероприятий по регулированию кибербуллинга на территории Российской Федерации. Сейчас проводится контроль лишь за определенными видами буллинга, не полностью затрагивающие те формы травли, которые существуют. Необходимо сказать о том, что современные законопроекты, имеющие отношение к проявлению кибербуллинга были приняты лишь несколько лет назад. Проведем анализ эффективного использования подходов к проявлению государственного регулирования в сфере кибербуллинга с использованием нормативно-правовых актов.

Затрагивая управленческий подход, можно сказать, что имеющиеся на сегодняшний день законы не до конца проработаны, что сказывается в целом на эффективности в борьбе с кибербуллингом. Существует определенное затруднение в определении полученной травмы самой жертвы кибербуллинга, что отражается на решении суда.

Если говорить с правовой точки зрения, то предоставленные законы не затрагивают все сферы, где существует вероятность в столкновении с кибербуллингом. Все это в совокупности отражается на недовольстве общества и появляются общественные резонансы, где присутствуют конкретные примеры.

С точки зрения социально-экономического подхода принятые законопроекты неоднозначно восприняты самим обществом и поэтому

возникает дисбаланс между самим обществом и защитой их прав в тех сферах, где возникают прецеденты, имеющие отношение к кибербуллинга.

Проведенный выше анализ позволяет утверждать, что система противодействия кибербуллингу со стороны органов внутренних дел разрозненна и несовершенна, так как отсутствует четкая законодательная база вследствие сложности контроля всех сфер кибербуллинга. При этом обеспечение своевременности и эффективности предупредительной деятельности в сфере информационно-телекоммуникационных технологий представляет собой определенную проблему для органов внутренних дел, решение которой во многом зависит от комплексного подхода к разрешению организационных, правовых и методических аспектов специального предупреждения данного вида преступлений. Стоит отметить, что профилактические же мероприятия сотрудниками органов внутренних дел наиболее разработаны. Ознакомимся с ними.

Предупреждение преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, является одним из приоритетных направлений деятельности органов внутренних дел. На наш взгляд, профилактические мероприятия должны проводиться регулярно и в ходе повседневной служебной деятельности. Среди основных направлений предупреждения киберпреступлений, а именно кибербуллинга, выделяют:

- выявление ранее осужденных лиц по киберпреступлениям против личности с целью усиления контроля за их поведением;
- так как жертвами буллинга часто становятся дети и подростки, важно выявлять нарушителей законодательства РФ в области защиты детей от информации, причиняющей вред их здоровью и развитию;
- проведение с родителями или законными представителями профилактических бесед, которые направлены на активизацию контроля со стороны взрослых за электронной информацией, потребляемой детьми в сети Интернет; использование программного обеспечения «Родительский контроль», позволяющего контролировать сайты и

программы, которые посещает ребенок, а также ставить определенные ограничения на вход и просмотр; в случае начальных этапов развития кибербуллинга обращаться в психолого-педагогические центры за квалифицированной помощью; а также объяснение необходимости обращения в полицию при зафиксированных случаях кибербуллинга в отношении несовершеннолетних.

Предполагается, что данной профилактической и просветительской работой будет заниматься инспекция по делам несовершеннолетних следующими способами:

- сочетание лекций с семинарами с применением материалов из практики, к которым могут относиться уголовные дела, решения судебных органов;
- разъяснение положений законодательства, защищающего детей от информации, причиняющей вред их здоровью и развитию;
- информирование и методическая поддержка образовательных организаций буклетами, научно-методической литературой по предупреждению, видам и распознаванию кибербуллинга.[1]

Стоит отметить, что все большее количество специалистов сходится во мнении, что в будущем количество IT-преступлений будет только увеличиваться, что связано, в первую очередь, со способностью преступников быстро и эффективно приспосабливаться к стремительному развитию и обновлению современных высоких технологий. Представляется, что ключевым фактором в деле успешного предупреждения рассматриваемой категории преступлений станет всеобщее повышение грамотности в области информационно-телекоммуникационных технологий. В связи с этим важным является разработка на государственном уровне специальной программы, предусматривающей систематическое информирование населения о правилах безопасной работы с цифровыми устройствами. Оценка же законодательной

[1] Панфилов И.А. О роли подразделении полиции в профилактике деструктивного воздействия электронных масс-медиа на человека // Закон и право. 2021. №4.

базы по противодействию кибербуллингу показала, что в целом формирование основы для регулирования кибербуллинга на территории России включает в себя цель создания, прецеденты, имеющие отношение к нарушению законодательной базы. Проведение подобного рода оценки позволит выявить современную ситуацию, в котором находится система кибербуллинга.

§ 3. Трансформация преступности и способы реагирования на новые киберугрозы

Уровень подготовки злоумышленников растет из года в год — и уже сегодня можно пронаблюдать трансформацию киберпреступности и выделить несколько классов преступников. Если основная цель киберхулиганов — нанести компании репутационный ущерб путем остановки ее систем и появления сбоев у клиентов, то киберкриминальные группировки предпочитают массово атаковать сектор (например, с помощью фишинга и заражения устройств вредоносными программами), чтобы найти в нем «слабое звено» — компанию с низкой защитой. Киберкриминал ориентирован на прямую монетизацию атаки — получение выкупа за украденную информацию или за восстановление данных, продажу данных на «черном рынке». Работают такие группировки в рамках заложенного бюджета и действуют максимально экономично.

Также в последние годы выделился еще один, более продвинутый, класс хакеров — кибернаемники, которые работают по заказу и атакуют конкретную организацию. В рамках своих кампаний они проводят разведку, ищут тех, кто «сольет» данные, или разрабатывают уникальный набор инструментов. Цели кибернаемников могут быть самыми разными: ущерб репутации, остановка инфраструктуры, влекущая финансовые потери, кража конкурентно значимых материалов, шпионаж и так далее. Противодействие таким группировкам требует все более высокой интеграции и взаимодействия всех служб организации.

Верхушку этой иерархии занимают группировки, чья квалификация соответствует уровню спецслужб. Их цели — контроль над критической информационной инфраструктурой (КИИ) и получение стратегически значимых конфиденциальных данных. Для этого применяются самые продвинутые техники и инструментарий: самостоятельно найденные ранее неизвестные уязвимости в ПО, разработанные и внедренные «закладки» и т.д. Злоумышленники этого типа действуют максимально скрытно и способны довольно долго оставаться незаметными для стандартных средств мониторинга и защиты. Справиться с ними самостоятельно организация вряд ли сможет — в данном случае не обойтись без высококвалифицированной помощи профильных экспертов.

Одним из способов реагирования на новые киберугрозы видится создание коммерческими организациями высокого порога входа, чтобы атаки стали для киберпреступников нецелесообразными. В этом могут помочь профильные киберучения, где внешняя команда «атакующих» адаптируется под профиль, компетенции и принципы работы определенных группировок киберкриминала и кибернаемников, а затем проверяют внутренние системы безопасности.

Требуется сформировать план экстренного восстановления систем при сбое или атаке и отработать все взаимодействия внутри этого плана, чтобы они были слаженными. Работу должна контролировать независимая группа профессионалов, которые организуют киберучения. Отдельного внимания требует повышение киберграмотности как сотрудников, так и граждан — это позволит вовремя распознать методы социальной инженерии, используемой хакерами[1].

Теперь перейдем к рассмотрению трансформации кибербуллинга и способов реагирования на травлю в Интернете, что является наиболее острой проблемой в современном обществе.

---

[1] Киберхулиганы и кибернаемники: как бороться с новыми угрозами инфобеза. РБК / URL: https://trends.rbc.ru/trends/industry/61c1951e9a79475fdac24d4c (дата обращения: 21.04.2022)

Современное состояние профилактики кибербуллинга на сегодняшний день оценивается как развитие по следующим направлениям. Во-первых, предполагается развитие технических устройств, которые смогли бы ограничить доступ к нежелательному контенту, которые можно увидеть в социальных сетях и веб-сайта. Такого рода технические возможности заключаются в использовании фильтра, цензуры, а также кнопок тревоги, которые помогают оповестить сотрудника того или иного сайта о возникновении конфликтной ситуации, противоречащей законодательству Российской Федерации. Помимо этого, сейчас большинство сайтов обладают специальными настройками конфиденциальности, которые позволяют скрыть личную информацию от посторонних лиц. Во-вторых, происходит обучение пользователей Интернета основным правилам поведения и безопасности, а также выражения своего мнения по отношению к другим пользователям.

Зарубежная практика показывает, что существует необходимость в создании специальных веб-сайтов, которые направлены на увеличение интернет-грамотности, что позволит осуществлять корректное и рациональное общение в среде Интернет, не используя при этом агрессивные и вективные методы поведения.

На просторах российских Интернет-ресурсов можно увидеть проведение работ по введению цензуры контента и совершенствования фильтров. Ежегодно проводятся проекты, посвященные данному вопросу «Дети онлайн», «Дружественный Рунет», где происходит обсуждение актуальных вопросов в отношении проявления кибербуллинга, а также демонстрируется технические рекомендации, то есть возможности заблокировать, агрессивного лица, обозначение важности в реализации родительского контроля за деятельностью своих детей в Интернет-среде. В тоже время отсутствует необходимые рекомендации в преодолении киберпреследования, в число которого входят особенность переживания и поведения жертвы, свидетелей и самого агрессора. Следует уделять достаточно внимание установлению личных границ жертвы и навыков, способствующих их устойчивости, в случае, когда отсутствуют

«реальные» взаимоотношения между самим агрессором и его потенциальной жертвой.

Говоря о проявлении родительского контроля по отношению к своему ребенку как о залоге его безопасности, можно считать данное направление достаточно противоречивым, поскольку ставится под вопрос доверие родителей к своему ребенку, его последующей открытости и выстраивании взаимоотношений между родителями и детьми. В тоже время стоит понимать, что ребенок должен проявлять самостоятельность, осознавать каждое сое действие и сознанию принимать соответствующее решение для отражения своего понимания и чужих мотивов. Взаимоотношения, выстраиваемые между родителями и ребенком, выступает фундаментом для отработки навыков самостоятельного принятия решения, что в последующем отражается на социализации в Интернете. Для снижения риска того, что ребенок может оказаться в роли предмета киберпреследования необходимо развивать осознанное и ценностное отношение проявления своего поведения в Интернет-среде, а также предоставлять комплекс мер предосторожности.

Профилактика кибербуллинга заключается прежде всего в проведении диагностики. В ходе данной диагностики происходит определение факторов риска у аудитории, которые выступают в качестве потенциальных жертв кибербуллинга. Основные методы, позволяющие провести диагностику с целью определения факторов риска представлены в виде анкетирования и тестирования.

Выделяют также основные правила противодействия кибербуллингу. Для начала необходимо не реагировать на провокации и не комментировать оскорбительные посты, которые могут задеть вас, не отвечать обидным сообщениям. Тем более нет необходимости опускаться до уровня агрессора.

Не стоит испытывать вину или стыд. Кибербуллинг не является результатом неосторожного поведения, неправильных слов и ошибок. В качестве жертвы может стать любой человек, при этом если постоянно обдумывать данную ситуацию в голове облегчения не наступит. Не надо

перечитывать постоянно оскорбительные сообщения или каким-либо образом не затрагивать данную тему.

Следующим правилом является уменьшение возможности в общении с агрессором. В качестве одного из наиболее простых вариантов служит ограничение агрессора в осуществлении коммуникации. Существует возможность в использовании черного списка и блокировке телефонного номера и электронной почты.

Обязательным пунктом будет освещение своей проблемы, лучше всего с теми, кому можно довериться, в данном случае это могут быть родители или друзья. Также существует горячая линия психологической поддержки.

Стоит понимать и не бояться обращаться в правоохранительные органы в отношении проявления угроз или клеветы со стороны агрессора. Также можно обратиться в поддержку социальных сетей. Ежедневно социальные сети борются с буллингом, поэтому удаляют несомнительные или нежелательные посты или комментарии, в том числе банят агрессивных пользователей и сомнительные паблики.

Особенно важно делать скриншоты, которые могут представить себя как доказательства для суда. В случае если агрессор является несовершеннолетним, то можно отправить данную информацию его родителям или учителям.

Другим правилом является способность поставить агрессора на место. В случае, когда есть достаточно смелости и сил, то можно провести диалог с агрессором. Однако, в данном случае диалог не должен принимать вид переговоров или способа окупиться. Необходимо донести до обидчика все возможные способы его наказания, вплоть до обращения в суд.

Стоит бороться со стрессом. Проявление Интернет-травли выступает в качестве ситуации выхода из обычной зоны комфорта. Для того, чтобы не обращать внимания на возникающие онлайн-конфликты, необходимо повышать стрессоустойчивость. В качестве таких методов могут выступать творческие хобби, медитации и ароматерапия.

Необходимо проанализировать свое поведение в Интернет-среде. Стоит уменьшить социальную активность, меньше выкладывать фотографии и постов относительно себя. Также можно закрыть страницы закрытой, необходимо тщательнее изучать тех, кто добавляется в друзья.

Еще одним правилом является следование правилам цифровой грамотности. Не следует переходить по незнакомым или сомнительным ссылкам, не стоит разговаривать с незнакомцами, не скачивать подозрительные файлы.

Таким образом, можно сделать следующие выводы:

- киберпреступления в условиях современности стремительно трансформируются, чему способствует информационный прогресс. Выделяются новые виды информационных преступлений, а коммерческие организации разрабатывают системы реагирования на кибератаки;
- во всех популярных соцсетях уже осознали масштаб проблемы кибербуллинга. В Твиттере, Инстаграме, Фейсбуке, ВКонтакте и других платформах есть инструменты, которые помогут ограничить взаимодействие с нежелательными пользователями, сообщить о нарушении закона и преследовании;
- кибербуллинг детей — острая проблема. В интернете легче сохранить кажущуюся анонимность, и это, в свою очередь, порождает вседозволенность вкупе с сопутствующими проблемами. Важно вовремя отследить, что у ребёнка проблемы в Сети. Об этом говорят некоторые симптомы: подавленность, постоянное использование гаджетов, злость или непривычная замкнутость. Есть разные способы защититься от кибербуллинга — горячие линии, жалобы на контент в интернете.

ЗАКЛЮЧЕНИЕ

Таким образом, преступления в информационной сфере в последнее время стали популярным и быстро распространяющимся явлением в связи с информационным прогрессом и широкой распространенностью сети Интернет. Компьютерно-информационные технологии функционируют относительно давно, и их развитие происходит огромными темпами, что связано с большой заинтересованностью ими широких слоев населения. Преступления, связанные с использованием компьютерной техники, – это лишь специализированная часть преступной деятельности в информационной сфере. К данной категории относятся и преступления, при совершении которых осуществляется неправомерный доступ к охраняемой законом компьютерной информации. Компьютерные преступления – это преступления, совершаемые людьми, использующими информационные технологии для преступных целей.

Остается актуальной проблема борьбы с организованной преступностью, которая, прибегая к услугам высококвалифицированных специалистов, стала все чаще использовать различные технические средства - от обычных персональных компьютеров и традиционных средств связи до сложных вычислительных систем и глобальных информационных сетей, в том числе и Интернет. Сфера применения компьютерных технологий в преступных целях весьма обширна.

Особую яркость среди всех преступлений, совершаемых в сфере информационно-коммуникационных технологий, приобрел кибербуллинг, выражающийся к главным образом в психологической травле в Сети. Чаще феномен возникает среди подростков как индивидуальная демонстрация своей агрессии или же как антисоциальная групповая деятельность, несформированность, а чаще отсутствие ценностно-ориентационной сплоченности группы и т.д.

Было вывлено, что в кибербуллинге выделяются три основополагающие стороны – это агрессор, жертва и наблюдатели. Наиболее сложные последствия кибербуллинга накладываются на жертву – возникает психологический стресс, а это может повлечь за собой появление таких симптомов, как истощение организма, обезвоживание, потеря общего тонуса, возникновение тревожности, раздражительности, упадок сил, депрессия, бессонница, нарушение памяти и т.д., что ведет к серьезным психическим и психологическим заболеваниям.

Поставленная цель исследования была достигнута. Задачи, которые способствовали достижению цели, так же были выполнены, а именно: рассмотрены теоретические, правовые и организационные основы обеспечения кибербезопасности в Российской Федерации, что позволило выделить недостаточное правовое регулирование вопроса. Дана уголовно-правовая характеристика преступлений в сфере информационно-телекоммуникационных технологий на примере кибербуллинга, которая выявляет непризнание отечественным законодательством кибербуллинга как преступления. Выявлены причины и условия совершения преступлений в информационной сфере, а именно психологическая характеристика и причины возникновения явления кибербуллинга, к которым относятся как психологические, так и социальные причины и условия. Дана характеристика как личности киберпреступника, так и личностям жертвы и свидетелей. Изучен зарубежный опыт противодействия преступлениям с использованием компьютерных технологий, который подтверждает признание зарубежным законодательством кибербуллинга преступлением. Далее была проанализирована деятельность органов внутренних дел по профилактике, выявлению и пресечению преступлений в информационной сфере, выявлено отсутствие должного объема законодательной базы для выявления и пресечения кибербуллинга, отмечены положительные профилактические меры в данной области. А также были исследованы актуальные трансформации преступности и способы реагирования на новые киберугрозы.

Таким образом, результаты научных исследований и юридическая практика свидетельствуют о том, что, несмотря на длительность и разносторонность исследования феномена киберпреступлений, значимость проблемы для социума нарастает не только в нашей стране, но и во всем мире. Возникает необходимость поиска эффективных способов профилактики киберперступлений, а также кибербуллинга в образовательной среде, требующая привлечения не только специалистов психолого- педагогического профиля, социальных работников, но и родителей.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Монографии, учебники, учебные пособия

1. Галиакбаров, Р.Р. Проблемы криминализации многосубъектных общественно опасных деяний [Текст] / Р.Р. Галиакбаров // Актуальные проблемы криминализации и декриминализации общественно опасных деяний: сборник научных трудов. – Омск, 1980. – 324 с.

2. Джимерсон, С.Р. Справочник по вопросам школьного насилия и школьной безопасности: международное исследование и практика [Текст] / С.Р. Джимерсон. – Нью-Йорк, 2019.

3. Ильин, Е.П. Психология агрессивного поведения [Текст] / Е.П. Ильин. – СПб.: Питер, 2019. – 368 с.

4. Яковлев, А.М. Криминализация деяний в системе социального контроля и социального планирования [Текст] / А.М. Яковлев // Планирование мер борьбы с преступностью: сборник статей / Отв. ред. В.М. Коган. – М., 1982. – 257 с.

5. Яковлев, В. В. Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта : учебное пособие [Текст] / В. В. Яковлев, А. А. Корниенко. – Москва: 2002. – 328 с.

Статьи, научные публикации

1. Ачитаева, И.Б. Деструктивные взаимоотношения в учебных группах образовательных учреждений [Текст]: автореф. дис... канд. психол. наук / И.Б. Ачитаева. – Москва, 2010. – 25 с.

2. Баранов, А.А. Психологический анализ причин подросткового кибербуллинга [Текст] / А.А. Баранов, С.В. Рожина // Вестник Удмуртского университета. Серия «Философия. Психология. Педагогика». – 2015. – №1.

3. Бочавер, А.А. Буллинг как объект исследований и культурный феномен [Текст] / А.А. Бочавер, К.Д. Хломов // Психология. Журнал Высшей школы экономики. – 2013. – Т. 10. – № 3. – С. 149-159.

4. Буллинг [Электронный ресурс]. – Режим доступа: https://www.kp.ru/putevoditel/sovety-dlya-roditelej/bulling-v-shkole/, свободный

5. Бязырова, А.Т. Психолого-педагогические условия профилактики школьного буллинга [Текст] / А.Т. Бязырова, А.А. Гадзиев // Проблемы современного педагогического образования. – 2017. – № 55-8. – С. 105-111.

6. Волкова, Е.Н. Подростковый буллинг: направления профилактической работы и организация помощи [Текст] // Вестник практической психологии образования. – 2019. – № 3 (3). – С. 50-57.

7. Волкова, И.В. Характеристика подросткового буллинга и его определение [Текст] // Вестник Мининского университета. – 2016. – № 2 (15). – С. 26.

8. Глазман, О.Л. Психологические особенности участников буллинга [Текст] //Изв. РГПУ им. А.И. Герцена. – 2019. – № 105. – С. 159-165.

9. Гришина, Т.Г. Исследование буллинга среди школьников: обзор зарубежных исследований [Текст] / Т.Г. Гришина // Современная прикладная психология: теория и практика: сборник статей Международной научно-практической конференции: в 2 т. / под ред. Т.Н. Мельникова, Н.Т. Колесник. Т. 2. – М.: ИИУ МГОУ, 2017. – С. 14-17.

10. Гудзовская, А.А. Школьный буллинг как отражение развития группового субъекта деятельности [Текст] / А.А. Гудзовская, А.М. Манухина, А.А. Проскурина // Социальные явления. – 2017. – №1 (7).

11. Екимова, В.И. Жертвы и обидчики в ситуации буллинга: кто они? [Текст] / В.И. Екимова, А.М. Залалдинова // Современная зарубежная психология. – 2019. – т. 4. – № 4. – С. 5-10.

12. Ермолова, Т.В. Буллинг как групповой феномен: исследование буллинга в Финляндии и скандинавских странах за последние 20 лет (1994-

2014) [Текст] / Т.В. Ермолова, Н.В. Савицкая // Современная зарубежная психология. – 2015. – Т. 4. – № 1. – С. 65-90.

13. Злобин, Г.А. Некоторые теоретические вопросы криминализации общественно опасных деяний [Текст] / Г.А. Злобин, С.Г. Келина // Проблемы правосудия и уголовного права. – М., 1978. – С. 109.

14. Карепова Э.В. Феномен зависти: палач и жертва в одном чувстве [Электронный ресурс]. – Режим доступа: http://psyfactor.org/lib/envy.htm, свободный

15. Карпук, В. А. Личностные особенности молодых людей, вовлеченных в буллинг и кибербуллинг [Текст] / В.А. Карпук // Психология стресса и совладающего поведения: вызовы, ресурсы, благополучие: материалы V Междунар. науч. конф. – Кострома, 2019. – Т. 1. – С. 186—190.

16. Киберхулиганы и кибернаемники: как бороться с новыми угрозами инфобеза. РБК [Электронный ресурс]. – Режим доступа: https://trends.rbc.ru/trends/industry/61c1951e9a79475fdac24d4c, свободный.

17. Кожухарь, Г.С. Феноменология разных форм психологического насилия в молодежной среде: зарубежные исследования [Текст] // Психологическая наука и образование. – 2018. – №1.

18. Козлов, В. Ф. К вопросу о соотношении уголовно-правовой, криминологической и криминалистической характеристик преступления [Электронный ресурс]. – Режим доступа: https://justicemaker.ru/view-article.php?id=22&art=3518, свободный

19. Корзун, С.А. Буллинг как форма проявления агрессии в подростковом возрасте [Текст] / С.А. Корзун, О.В. Страпко // Актуальные проблемы гуманитарных и социально-экономических наук. – 2017. – Т. 11. – № 8. – С. 107-111.

20. Королева, Д. О. Исследование повседневности современных подростков: присутствие в социальных сетях как неотъемлемая составляющая общения [Текст] // Современная зарубежная психология. – 2016. – Т. 5. – № 2. – С. 55-61.

21. Костенко, Е.С. Психологические предпосылки буллинга [Текст] / Е.С. Костенко, С.Ю. Баскунович // Лучшая студенческая статья 2017. – 2017. – С. 283-285

22. Кочнева, Е.М. Социометрическая позиция школьника и его роль в структуре буллинга [Текст] / Е.М. Кочнева, И.Е. Емелина, А.А. Симанина // Проблемы современного педагогического образования. – 2019. – № 63–4.

23. Кошенова, М.И. Моббинг как маркер системного неблагополучия современного российского общества? [Текст] / М.И. Кошенова // Социально-психологическая оценка рисков современной реальности: очевидное и вероятное: монография / Под научн. Ред. О.А. Белобрыкиной. – Новосибирск: НГПУ, 2017. – С. 53–69.

24. Кривцова, С.В. Школьный буллинг: об опыте исследований распространенности буллинга в школах Германии, Австрии, России [Текст] / С.В. Кривцова, А.А. Белевич, АН. Шапкина // Образовательная политика. – 2016. Т. 3. – № 73. – С. 2-25.

25. Лахмытко, Н.М. Интернет-травля. Миф или реальность? [Текст] // Методист. – 2015. – № 6. – С.21-24.

26. Маракушина, И.Г. Возрастной подход к анализу психолого-педагогических проблем современного младшего подростка [Текст] / И.Г. Маракушина, А.Н. Буторина, О.Е. Кузнецова // Человек и образование. – 2017. №2. – С.152-156.

27. Мигунова, А.В. Возможности социальной работы в решении школьных проблем [Текст] // Вестник Нижегородского университета им. Н.И. Лобачевского. – 2017. – № 4 (32). – С.62-67.

28. Миронов, Д.Д. Сущность понятия девиантное поведение подростков [Текст] // Вестник Челябинского государственного педагогического университета. – 2017. – №10. – С.70-73.

29. Молчанова, Д.В. Противодействие школьному буллингу: анализ международного опыта [Текст] / Д.В. Молчанова, М.А. Новикова // Высшая школа экономики. – М.: НИУ ВШЭ, 2020. – С. 72.

30. Неволина, В.В. Психолого-педагогические условия саморазвития личности в юношеском возрасте [Текст] // Казанский педагогический журнал. – 2018. – №2. – С.167-171.

31. Нестерова, А.А. Психологические особенности детей, склонных к виктимности в ситуации школьной травли [Текст] // Личность в экстремальных условиях и кризисных ситуациях жизнедеятельности. – 2018. – № 5. – С. 277-285.

32. Неустроева, О.В. Психологическая характеристика подросткового возраста в концепциях Д.Б.Эльконина и Д.И.Фельдштейна [Текст] // Europeanresearch. – 2018. – №6 (7). – С.69-73.

33. Новикова, М.А. Семейные предпосылки вовлеченности ребенка в школьную травлю: влияние психологических и социальных характеристик семьи [Текст] / М.А Новикова, А.А. Реан // Психологическая наука и образование. – 2018. – Т. 23. – № 4. – С. 112-120.

34. Петросянц, В.Р. Проблема буллинга в современной образовательной среде [Текст] // Вестн. ТГПУ. – 2019. – № 6. – С. 151–154.

35. Поливанова, К.Н. Что в профиле тебе моем: данные «ВКонтакте» как инструмент изучения интересов современных подростков [Текст] / К.Н. Поливанова, И.Б. Смирнов // Вопросы образования. – 2017. – №2. – С.134-151.

36. Реан, А.А. Буллинг в среде старшеклассников: распространенность и влияние социо-экономических факторов [Текст] / А.А. Реан, М.А. Новикова // Мир психологии. Научно-методический журнал. – 2019. – Том 97. – № 1. – С. 165– 177.

37. Родионова, Е.Л. Психолого-педагогические и социальные модели профилактики асоциального поведения несовершеннолетних [Текст] / Е.Л. Родионова, А.Л. Нелидов // Министерство образования и науки Нижегородской области. – Н.Новгород: Нижегородский гуманитарный центр, 2004. – С. 5-86

38. Селифанова, А.И. Буллинг в подростковой среде [Текст] / А.И. Селифанова, Л.А. Мартиросян, О.В. Захарова, Е.К. Абдулина // Перспективы развития науки и образования: сборник научных трудов по материалам

международной научно-практической конференции. – 2017. – С. 104-105.

39. Смирнягина, М.М. Возрастные границы и психологическое содержание стабильного периода подросткового возраста [Текст] // Вестник ЮУрГУ. – 2019. – №5. – С.56-61.

40. Собкин, В.С. Буллинг в стенах школы: влияние социокультурного контекста (по материалам кросскультурного исследования) [Текст] / В.С. Собкин, М.М. Смыслова // Социальная психология и общество. – 2019. – Том 5. – № 2. – С. 71–86.

41. Соловьёв, Д.Н. Использование потенциала первичного коллектива в профилактике буллинга среди школьников подросткового возраста [Текст]: автореф. дис. на соиск. учен. степ. канд. пед. наук / Д.Н. Соловьев. – Тюмень: Тюм.гос.ун-т., 2019. – 24 с.

42. Соловьёв, Д.Н. Модель профилактики буллинга среди школьников подросткового возраста [Текст] // Интернет-журнал «НАУКОВЕДЕНИЕ». – 2014. – № 3. – Режим доступа: https://elibrary.ru/download/elibrary_22285304_62543160.pdf.

43. Соловьёв, Д.Н. Способы командообразования в предупреждении буллинга в подростковом возрасте [Текст] // Гуманитарные исследования. – 2019. – №1. – С.94-97.

44. Суханов, А.Г. Особенности правового регулирования в области обеспечения кибербезопасности критической инфраструктуры [Текст] // Экономика и социум. – 2017. – № 3(34). – С. 1693-1700.

45. Травля в школе [Электронный ресурс]. – Режим доступа: https://www.ya-roditel.ru/parents/base/experts/travlya-v-shkole/.

46. Трофименко, Г.С. Некоторые особенности личностной идентичности современных подростков [Текст] // Педагогическое образование в России. – 2019. – №3. – С.135-141.

47. Уровень агрессии растет: как в России борются с кибербуллингом [Электронный ресурс]. – Режим доступа: https://www.gazeta.ru/tech/2020/12/15_a_13401170.shtml.

48. Хапачева, С.М. Формирование мотивации учения в период адаптации подростков ко второй ступени обучения [Текст] //Концепт. – 2019. – №4 (апрель). – С.1-8.

49. Хоружий, В.В. Правовые основы кибербезопасности: к постановке проблемы [Текст] / В.В. Хоружий, А.В. Шульга // Научное обеспечение агропромышленного комплекса : Сборник статей по материалам 73-й научно-практической конференции студентов по итогам НИР за 2017 год, Краснодар, 25 апреля 2018 года / Ответственный за выпуск А.Г. Кощаев. – Краснодар: Кубанский государственный аграрный университет имени И.Т. Трубилина, 2018. – С. 1265-1268.

50. Шалагинова, К.С. Игры и упражнения для профилактики буллинга в подростковом возрасте [Текст] // Справочник педагога-психолога. Школа. – 2016. – №12. – С. 56-66

51. Gordon, S. 8 Reasons Why Kids Cyberbully Others [Электронный ресурс] // About Health. – Режим доступа: http://bullying.about.com/od/Cyberbullying/a/8-Reasons-Why-Kids-Cyberbully-Others.htm.

52. McAfee: исследование «Подростки за компьютером-2014: вопросы защиты личной информации, общения в социальных сетях и кибербуллинга [Электронный ресурс] // Технологии в образовании: новости и события. – Режим доступа: http://educationevents.ru/2014/06/19/mcafee-research-about-internet-safety-for-teens/.

АНТИПЛАГИАТ
ОБНАРУЖЕНИЕ ЗАИМСТВОВАНИЙ

СПРАВКА

о результатах проверки текстового документа
на наличие заимствований

Казанский юридический институт МВД России

ПРОВЕРКА ВЫПОЛНЕНА В СИСТЕМЕ АНТИПЛАГИАТ.ВУЗ

Автор работы: Рябцев Евгений Игоревич
Самоцитирование рассчитано для: Рябцев Евгений Игоревич
Название работы: Деятельность органов внутренних дел по предупреждению и пресечению преступлений в информационной сфере
Тип работы: Выпускная квалификационная работа
Подразделение: 173 учебной группы, очной формы обучения, 2017 года набора, по специальности 40.05.01 –

РЕЗУЛЬТАТЫ

■ **ОТЧЕТ О ПРОВЕРКЕ КОРРЕКТИРОВАЛСЯ:** НИЖЕ ПРЕДСТАВЛЕНЫ РЕЗУЛЬТАТЫ ПРОВЕРКИ ДО КОРРЕКТИРОВКИ

ЗАИМСТВОВАНИЯ	29.64%	ЗАИМСТВОВАНИЯ	29.64%
ОРИГИНАЛЬНОСТЬ	52.79%	ОРИГИНАЛЬНОСТЬ	52.79%
ЦИТИРОВАНИЯ	17.56%	ЦИТИРОВАНИЯ	17.56%
САМОЦИТИРОВАНИЯ	0%	САМОЦИТИРОВАНИЯ	0%

ДАТА ПОСЛЕДНЕЙ ПРОВЕРКИ: 22.06.2022

ДАТА И ВРЕМЯ КОРРЕКТИРОВКИ: 22.06.2022 19:21

Модули поиска: ИПС Адилет; Библиография; Сводная коллекция ЭБС; Интернет Плюс; Сводная коллекция РГБ; Цитирование; Переводные заимствования (RuEn); Переводные заимствования по eLIBRARY.RU (EnRu); Переводные заимствования по Интернету (EnRu); Переводные заимствования издательства Wiley (RuEn); eLIBRARY.RU; СПС ГАРАНТ; Модуль поиска "КЮИ МВД РФ"; Медицина; Сводная коллекция вузов МВД; Диссертации НББ; Перефразирования по eLIBRARY.RU; Перефразирования по Интернету; Патенты СССР, РФ, СНГ; Коллекция СМИ; Шаблонные фразы; Кольцо вузов; Издательство Wiley

Подпись Шалагина А.Е.
УДОСТОВЕРЯЕТСЯ
ОД и Р КЮИ МВД России

Работу проверил: Шалагин Антон Евгеньевич
ФИО проверяющего

Дата подписи: 22.06.22

Подпись проверяющего

Чтобы убедиться в подлинности справки, используйте QR-код, который содержит ссылку на отчет.

Ответ на вопрос, является ли обнаруженное заимствование корректным, система оставляет на усмотрение проверяющего. Предоставленная информация не подлежит использованию в коммерческих целях.

Отзыв о работе
обучающегося 173 учебной группы, очной формы обучения, 2017 года набора, по специальности 40.05.01 – Правовое обеспечение национальной безопасности
Рябцева Евгения Игоревича
в период подготовки выпускной квалификационной работы
на тему «Деятельность органов внутренних дел по предупреждению и пресечению преступлений в информационной сфере»

Тема выпускной квалификационной работы выбрана автором из перечня, предложенного кафедрой. Совместно с научным руководителем разработан план исследования, который имеет логичную структуру и последовательно раскрывает исследуемую проблему. В соответствии с темой исследования сформулированы цель и задачи, определены методы исследования.

Рябцев Е.И. при постановке цели и задач, выборе методов и способов описания результатов исследования проявил высокую степень инициативности. Контакты с научным руководителем, необходимые для научно-методического обеспечения работы, поддерживал своевременно, в соответствии с имеющимися потребностями и утвержденным планом-графиком.

Эмпирический материал, учебная, научная, справочная литература автором подобраны в достаточном объёме. В ходе исследования Е.И. Рябцев продемонстрировал достаточно высокий уровень заинтересованности в проведении исследования, самостоятельности, творческой активности.

При подготовке выпускной квалификационной работы им использовались общенаучные, частно-научные и специальные методы исследования. Научную, юридическую терминологию, следственно-судебную практику по теме исследования автор изучил и уверенно применял.

Результатом проведённого исследования явились выводы и предложения в сфере деятельности органов внутренних дел по предупреждению и пресечению преступлений в информационной сфере, что указывает на умение выявлять и анализировать практико-ориентированные материалы. Выявленные в ходе исследования проблемы весьма актуальны для правоохранительной деятельности.

Выводы автора подготовленной работы сформулированы логично, последовательно, отражают достаточную эффективность научного поиска и обобщения эмпирического материала по теме выпускной квалификационной работы. По результатам исследования можно полагать, что Рябцев Е.И. приобрел способность к самостоятельному формулированию обоснованных (достоверных) выводов и предложений.

Процесс подготовки выпускной квалификационной работы планировался

правильно и своевременно. Выполнение мероприятий по подготовке работы, а также указания научного руководителя осуществлялись в установленные сроки. Работа по устранению выявленных недостатков проведена корректно и своевременно. Отмечаются умения и навыки работы с необходимым компьютерным программным обеспечением, информационно-справочными ресурсами и сетью «Интернет».

Выпускную квалификационную работу Е.И. Рябцева следует признать завершенной, имеющей актуальность, научную новизну, теоретическую и практическую значимость в сфере противодействия информационной преступности. Исследование проведено на достаточном научном уровне, с анализом и проработкой выявленных проблем. Задачи, поставленные при проведении исследования, в целом решены, выводы и заключение сформулированы корректно. Уровень оригинальности выпускной квалификационной работы соответствует предъявляемым требованиям.

Подготовленная работа «Деятельность органов внутренних дел по предупреждению и пресечению преступлений в информационной сфере» является оконченным научным исследованием. В связи с чем, она может быть рекомендована к публичной защите.

Руководитель:
начальник кафедры криминологии и
уголовно-исполнительного права
Казанского юридического института
МВД России
кандидат юридических наук, доцент
полковник полиции
«17» 05 2022 г. А.Е. Шалагин

С отзывом ознакомлен Е.И. Рябцев

«17» 05 2022 г.

Подпись Шалагина А.Е.
УДОСТОВЕРЯЕТСЯ
ОД и Р КЮИ МВД России

РЕЦЕНЗИЯ
на выпускную квалификационную работу
обучающегося 173 учебной группы, очной формы обучения, 2017 года набора, по специальности 40.05.01 –
Правовое обеспечение национальной безопасности
Рябцева Евгения Игоревича
на тему «Деятельность органов внутренних дел по предупреждению и пресечению преступлений в информационной сфере»

Представленная на рецензирование выпускная квалификационная работа выполнена на актуальную, теоретически и практически значимую тему. В настоящее время отмечается рост преступлений в информационной среде. В условиях развития современного мира все большее количество людей сталкиваются с проблемой кибербуллинга, киберпреследования. Стоит отметить, что данный феномен чаще всего наблюдается среди учащихся школ, причем участниками могут быть как школьники, так и молодежь.

В роли жертв могут выступать дети, педагоги, родители или другие работники учебного заведения. Большинство исследователей считают, что причиной возникновения данной проблемы является характер и психологические особенности ребенка, условия его воспитания в семье, взаимоотношения со сверстниками. Ситуация осложняется тем, что данные преступления все чаще совершаются с использованием сети Интернет, а также отсутствием в Уголовном кодексе Российской Федерации специальной нормы, предусматривающей ответственность за интернет травлю. Противодействие такого рода преступлениям должно осуществляться наступательно и системно, с привлечением широкого круга субъектов профилактики преступлений и правонарушений. Особую роль в противодействии преступлениям в информационной среде играют органы внутренних дел.

Структура работы включает в себя введение, две главы, семь параграфов, заключение и список использованной литературы. Во введении

обосновывается актуальность темы исследования, определяется цель, задачи, объект и предмет исследования, теоретическая, нормативная и методологическая основы работы. В первой главе автор рассматривает криминологическую характеристику преступлений в информационной среде, в том числе показатели преступности данного вида, ее причинный комплекс, криминологическую характеристику преступника и жертвы. Во второй главе исследуются меры предупреждения и пресечения преступлений в информационной сфере. Изучены новые способы совершения данных преступлений. Особое внимание обращено на вопросы взаимодействия органов внутренних дел с государственными и общественными организациями при предупреждении и предотвращении данных преступлений. В заключении сформулированы выводы и предложения по теме исследования.

Цель и задачи исследования в целом достигнуты. Научные положения, выводы и рекомендации, представленные в работе, заслуживают поддержки. Выпускная квалификационная работа «Деятельность органов внутренних дел по предупреждению и пресечению преступлений в информационной сфере» соответствует предъявляемым требованиям, содержит элементы научной новизны, творческого мышления и заслуживает положительной оценки.

Рецензент

Помощник начальника управления МВД России пог. Кизан _____ А.А. Фефилов

«16» 05 2022 г.

С рецензией ознакомлен(а) _____ Е.И. Рябцев

«16» 05 2022 г.

Кафедра криминологии и уголовно-исполнительного права

УТВЕРЖДАЮ
Начальник кафедры криминологии и уголовно-исполнительного права кандидат юридических наук, доцентполковник полиции

_____ А.Е.Шалагин

"15" 06 2021г.

ПЛАН-ГРАФИК
выполнения выпускной квалификационной работы

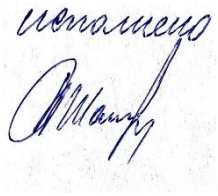
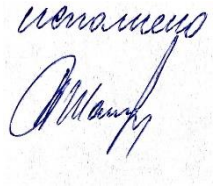
Тема: Деятельность органов внутренних дел по предупреждению и пресечению преступлений в информационной сфере

Курсант: Рябцев Евгений Игоревич Учебная группа № 173

(фамилия, имя, отчество)

Специальность 40.05.01 – правовое обеспечение национальной безопасности

Форма обучения очная Год набора 2017

N п/п	Характер работы (главы, параграфы и их содержание)	Примерный объем выполнения (в %)	Срок выполнения	Отметка руководителя о выполнении
1	Глава 1.Криминологическая и уголовно-правовая характеристика преступлений, совершаемых в информационной сфере. § 1. Теоретические, правовые и организационные основы обеспечения кибербезопасности в Российской Федерации.	10%	До 02.10.2021	
2	§ 2. Уголовно-правовая характеристика преступлений в сфере информационно-коммуникационных технологий	15%	До 20.11.2021	

3	§ 3. Причины и условия совершения преступлений в информационной сфере	10%	До 10.12.2021	исполнено
4	§ 4. Личность киберпреступника и её характеристики	10%	До 20.01.2022	исполнено
5	Глава 2. Стратегия и тактика противодействия преступлениям в сфере информационно-коммуникационных технологий. § 1. Зарубежный опыт противодействия преступлениям с использованием компьютерных технологий	15%	До 13.02.2022	исполнено
6	§ 2. Деятельность органов внутренних дел по профилактике, выявлению и пресечению преступлений в информационной сфере	10%	До 19.02.2022	исполнено
7	§ 3. Трансформация преступности и способы реагирования на новые киберугрозы.	15%	До 01.04.2022	исполнено
8	Введение, заключение, список использованной литературы	15%	До 20.04.2022	исполнено

Подпись выпускника

"15" 06 2021г.

СОГЛАСОВАНО
Начальник кафедры
криминологии и
уголовно-исполнительного права
полковник полиции
«15» 06 2021 г.

А.Е. Шалагин

Подпись Шалагина А.Е
УДОСТОВЕРЯЕТСЯ
ОД и Р КЮИ МВД России