МГЮА

приоритет2030^
право для лидерства

Аналитическая справка

Противодействие угрозе кибersталкинга (интернет-слежки) в России и за рубежом

Противодействие угрозе кибersталкинга (интернет-слежки) в России и за рубежом: информационно-аналитическая справка / Д.Е. Гуляев, П.И. Клюева. — Москва, 2024. — 48 с.

Гуляев Дмитрий Евгеньевич,

Директор Центра по обеспечению прав молодежи в цифровом пространстве Университета имени О.Е. Кутафина (МГЮА)

Клюева Полина Игоревна,

Эксперт Центра по обеспечению прав молодежи в цифровом пространстве Университета имени О.Е. Кутафина (МГЮА)

Герасимов Сергей Алексеевич,

обучающийся Университета имени О.Е. Кутафина (МГЮА)

Аналитическая справка

«Противодействие угрозе кибersталкинга (интернет-слежки) в России и за рубежом»

Оглавление

Введение

Цифровые технологии сегодня стремительно проникают во все сферы жизни общества, открывая людям «новые горизонты». Эти возможности существенно облегчают жизнь современного человека, однако, они могут быть использованы злоумышленниками во вред. Поэтому появляются новые и трансформируются существующие угрозы в цифровом пространстве.

Так, сегодня все чаще обсуждаются такие явления как кибербуллинг, фейкинг (воздействие фейков - ложной информации, смешанной со сплетнями, вымыслами, пропагандой и секретами, которая призвана показать какое-либо явление правдоподобным), фишинг (вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей) и другие.

В данной информационно-аналитической справке **предметом исследования** стала не менее актуальная угроза информационно-психологической безопасности, а именно кибersталкинг (интернет-слежка).

Кибersталкинг является производным явлением от «простого» (физического) сталкинга (слежки). Как в науке, так и в юридической практике не выработано единых дефиниций «сталкинга» и «кибersталкинга», при этом возможно выявить общие черты. Несмотря на то, что дефиниции обладают и различиями, ученые солидарны в одном: **кибersталкинг является видом сталкинга**, что подробнее будет раскрыто далее.

Необходимо отметить, что отсутствие специальных норм в законодательстве Российской Федерации, регулирующих отношения, складывающиеся по поводу кибersталкинга, часто приводит к сложностям в юридической квалификации этого явления, что делает исследование **актуальным**.

Цель исследования – провести комплексный анализ проблемы кибersталкинга, его природы и возможных последствий, а также изучить зарубежный опыт противодействия этой угрозе для выработки единого подхода к системе профилактики, а также правовой модели его квалификации

в России в целях совершенствования законодательства и правоприменительной практики для повышения уровня защищенности граждан.

I. Понятия «сталкинга» (слежки) и «кибersталкинга» (интернет-слежка), их соотношение между собой и с понятием «кибербуллинг» (интернет-травля)

1.1 Понятия сталкинга (слежки) и кибersталкинга (интернет-слежки) и их соотношение:

Слово «сталкинг» происходит от английского глагола to stalk, что переводится как «выслеживать, преследовать», согласно Кэмбриджскому словарю, буквальное значение звучит как «близко и тайно следовать за человеком или животным, часто с намерением атаковать»[1].

В правовой плоскости понятие «сталкинг» получило закрепление в отдельных иностранных правопорядках, впервые было использовано в 1990 году в Уголовном Кодексе штата Калифорния была введена ответственность за «преднамеренное, злоумышленное и повторяющееся преследование и домогательство до другого человека»[2]. После этого постепенно в национальном законодательстве различных государств стали закреплять понятие преследования и меры уголовной[3] (например, в Польше[4]) или административной[5] (например, в Молдове[6]) ответственности стали находить отражение, однако единой универсальной дефиниции так и не было выработано. В России на данный момент отсутствуют нормы, способные полноценно защитить жертв сталкинга, но существует уголовная

[1]Cambridge Dictionary: official site.URL:https://dictionary.cambridge.org/ru/?ysclid=m1p7mjkvnx365585243/(дата обращения:24.05.2024)

[2]California Penal Code/ California Legislative Information: official site.URL: https://leginfo.legislature.ca.gov/(дата обращения: 24.05.2024)

[3]«Кто из-за постоянного преследования другого человека или его лица близкого человека вызывает у нее обоснованное обстоятельством чувство опасности, унижение или мучения или существенно нарушает ее частную жизнь, наказывается лишением свободы на срок от 6 месяцев до 8 лет»

[4]Рёрихт А. А. 2013.01.048. Голонка А. упорное преследования как новый тип запрещенного деяния // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4, Государство и право: Реферативный журнал. 2013. №1. URL: https://cyberleninka.ru/article/n/2013-01-048-golonka-a-upornoe-presledovanie-kak-novyy-tip-zapreschennogo-deyaniya-golonka-a-uporczywe-n-kanie-jako-nowy-typ-czynu (дата обращения: 24.05.2024).

[5]«Систематическое преследование лица, вызывающее тревогу, страх за личную безопасность или безопасность близких родственников, вынуждая изменить образ жизни, совершенное путем: выслеживания лица; установления контакта или попытки установления контакта с лицом при помощи любых средств или посредством другого лица»

[6]Кодекс Республики Молдова от 24 октября 2008 года №218-XVI «О правонарушениях» (с изменениями и дополнениями по состоянию на 14.03.2024 г.), ст. 78-2

ответственность за отдельные формы его проявления (например, Клевета (ст. 128.1 УК РФ), Нарушение неприкосновенности частной жизни (ст. 137 УК РФ) и др.)

Основываясь на понятиях, которые закреплены в законодательстве разных стран, можно выявить общие юридически значимые признаки, которые стоит учитывать в случае введения в российское законодательство механизмов привлечения к ответственности за сталкинг и кибersталкинг. Среди таких признаков: систематичность, преднамеренность и наличие умысла. Подробный анализ значения этих признаков и их проявлений будет приведен далее.

Понятие «кибersталкинг» вообще не находит законодательного закрепления. Возможно, причина кроется в том, что в контексте соотношения понятий «сталкинг» и «кибersталкинг» - одно является составной частью (видом) другого, а, следовательно, нет потребности в специальном регулировании этого вопроса.

Однако не стоит недооценивать серьёзность последствий и распространенность этой угрозы. По результатам исследования, проведенного в 2024 году «Лабораторией Касперского»[7], каждый седьмой россиянин сталкивался со сталкингом в Сети тех, с кем находился в любовной связи. В этом признались 15% респондентов.
При этом 28% опрошенных не видят в интернет-слежке ничего страшного, а 32% называют это неприемлемым. Еще 19% относятся к слежке нормально, но только если инициатива взаимна[8]. Такая статистика демонстрирует неоднозначность отношения и беспокойство людей по поводу этой угрозы, что только подтверждает актуальность ее подробного изучения и выработки правовой модели её квалификации.

[7]Опрос проводился Arlington Research по заказу «лаборатории Касперского» в январе 2024 года, в нем принимали участие респонденты из разных стран, в том числе 1000 человек из России.
[8]Kaspersky.ru.сайт URL: https://www.kaspersky.ru/about/press-releases/15-rossiyan-stalkivalis-s-onlajn-slezhkoj-so-storony-novyh-romanticheskih-partnyorov (дата обращения: 25.05.2024)

Изучение данной угрозы актуально, в первую очередь, в контексте обеспечения безопасности детей и молодежи. По данным общероссийского исследования[9], проводимого в 2019 году Фондом Развития Интернета, подростки в возрасте 14-17 лет практически не имеют запретов и ограничений для выхода в Интернет. Это привело к тому, что 45 процентов из них ежедневно проводят в Сети от 1 до 4 часов, а 39 процентов - более 4 часов. При этом 69 процентов большую часть времени проводят именно в социальных сетях и мессенджерах, публикуют личную информацию о себе, что создает риск появления негативных последствий различных киберугроз, в том числе интернет-слежки.

Понятие «интернет-слежка» используется в научной и учебной литературе, например, в Оксфордском словаре социальных сетей это явление описано как «преследование человека с использованием мобильных или онлайн-средств общения, вызывающее у него беспокойство или страх». Энциклопедия Касперского дает такое определение этой угрозы: «систематическое преследование человека, группы лиц или компании, их запугивание и/или домогательство с использованием интернета и других электронных средств коммуникации»[10].

Некоторые ученые, например, доктор юридических наук, профессор, главный научный сотрудник Всероссийского научно-исследовательского института МВД России, П.Н. Кобец, дает более широкое определение: «Кибersталкинг – от англ. cyber (кибер-, компьютерный) и stalking (преследование) – преследование кого-либо с использованием Интернета и других электронных средств»[11].

---

[9]Лебедева, Н. Каждый третий подросток проводит онлайн треть своей жизни. 2019. URL: https://rg.ru/2019/02/13/kazhdyj-tretij-podrostok-provodit-onlajn-tret-svoej-zhizni.html (дата обращения: 25.05.2024)

[10]Кибersталкинг. Энциклопедия Касперского. сайт URL: https://encyclopedia.kaspersky.ru/glossary/cyberstalking/ (дата обращения: 25.05.2024).

[11]Кобец Петр Николаевич Противодействие угрозам кибersталкинга - важнейшей проблеме, исследуемой в рамках совершенствования аспектов информационной безопасности регионов в условиях глобализации информационного пространства // Вестник Прикамского социального института. 2017. №1 (76). URL: https://cyberleninka.ru/article/n/protivodeystvie-ugrozam-kiberstalkinga-vazhneyshey-probleme-issleduemoy-v-ramkah-sovershenstvovaniya-aspektov-informatsionnoy (дата обращения: 25.05.2024).

Некоторые определения включают в себя описания конкретных проявлений интернет-слежки: «этот термин часто используется для обозначения трех видов деятельности: непосредственное общение через электронную почту или текстовые сообщения; интернет-притеснения, когда преступник публикует оскорбительную или угрожающую информацию о жертве в Интернете; и несанкционированное использование, управление компьютером жертвы»[12].

Проводя соотношение дефиниций «сталкинг» и «кибersталкинг», ученые не пришли к единому мнению. В основном спор ведется о том, является ли понятие сталкинга более широким и «поглощающим» кибersталкинг. Некоторые считают, что кибersталкинг представляет собой новую форму девиантного поведения, поэтому его стоит отличать от офлайн-сталкинга (вне Интернета). Существует позиция, что основное различие между сталкингом и кибersталкингом заключаются в мотивах совершения соответствующих действий: в отличие от офлайн-сталкинга мотивы для кибersталкинга могут быть различными[13]. Однако, это мнение не популярно, так как, анализируя судебную практику зарубежных стран, где преследование криминализировано, можно заметить, что мотивы преследования также различны (подробнее в параграфе «Правовые механизмы противодействия кибersталкингу (интернет-слежке) в иностранных правопорядках»), что не позволяет отличить слежку от интернет-слежки.

Другие исследователи придерживаются точки зрения, что границы между киберпреследованием и преследованием уже давно стерты, ведь преследование человека давно не обходится без поиска информации о нем в Интернете, с помощью технических устройств[14]. Более того, кибersталкинг с

[12]Барышева К.А. Определение понятия и общественно опасной природы кибersталкинга // Адвокат. 2016. N 10. С. 60 - 66.

[13]Кобец Петр Николаевич Противодействие угрозам кибersталкинга - важнейшей проблеме, исследуемой в рамках совершенствования аспектов информационной безопасности регионов в условиях глобализации информационного пространства // Вестник Прикамского социального института. 2017. №1 (76). URL: https://cyberleninka.ru/article/n/protivodeystvie-ugrozam-kiberstalkinga-vazhneyshey-probleme-issleduemoy-v-ramkah-sovershenstvovaniya-aspektov-informatsionnoy (дата обращения: 25.05.2024).

[14]Барышева К.А. Определение понятия и общественно опасной природы кибersталкинга // Адвокат. 2016. № 10. С. 60 - 66.

легкостью переходит в офлайн-преследование, и наоборот. Лицо может собирать сведения о своей жертве, получить доступ к компьютеру, выяснить адрес и телефон, но ничего не мешает перенести преследование в реальный мир, встретиться с жертвой, а также совершить более серьезные деяния, охватываемые составами преступлений.

В связи со всем вышесказанным, более убедительным видится мнение, что киберсталкинг является видом сталкинга, отвечающим признакам последнего, но при этом обладающим своей спецификой, связанной с широким применением новых возможностей цифровых технологий.

Проанализировав существующие легальные понятия преследования и доктринальные понятия интернет-преследования, можно выделить общие существенные признаки и сформировать исчерпывающее определение. Интернет-слежка – это систематическое преднамеренное преследование лица посредством использования Интернета и информационных технологий с целью причинения психологического, а в будущем возможно физического и иного вреда, который может подпадать под состав преступления.

1.2. Соотношение киберсталкинга (интернет-слежки) и кибербуллинга (интернет-травли):

Еще одним существенным аспектом исследования проблемы интернет-слежки является его соотношение с угрозой кибербуллинга. Для этого необходимо определить место кибербуллинга и киберсталкинга в контексте информационной безопасности.

Доктрина информационной безопасности определила информационную безопасность как состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность Российской Федерации[15]. В Стратегии

[15]Указ Президента РФ «Об утверждении Доктрины информационной безопасности Российской Федерации» от 05.12.2016 N 646 // «Собрание законодательства РФ», 12.12.2016, N 50, ст. 7074

Национальной безопасности РФ от 2021 года, утвержденной Указом Президента РФ[16], были упомянуты две категории информационных угроз, связанных с:

1. деструктивным информационно-психологическим воздействием
2. деструктивным информационно-техническим воздействием

Отсюда можно выделить 2 вида информационной безопасности: информационно-психологическую безопасность (безопасность от деструктивного воздействия) и информационно-техническую (безопасность информации и критический информационной инфраструктуры). Как кибербуллинг, так и киберсталкинг относятся к угрозам информационно-психологической безопасности. Это следует из определений: кибербуллинг – систематическое вербальное издевательство, совершаемое путем нападок через информационно-коммуникационную сеть «Интернет» с причинением нравственных и душевных страданий жертве (например, угрозы, обидные высказывания, связанные с внешним видом, умственными способностями и т.д[17]). Киберсталкинг– это систематическое преднамеренное преследование лица посредством использования Интернета и информационных технологий с целью причинения психологического, а в будущем возможно физического и иного вреда, который может подпадать под состав преступления. Оба явления связаны с деструктивным информационно-психологическим воздействием.

Риски информационно-психологической безопасности можно разделить на контентные (связаны с процессом «ознакомления» интернет-пользователей с информацией в виде текстового, фото-, аудио- и видеоматериала) и коммуникационные (связаны с процессом общения интернет-пользователей путем использования одной из сторон деструктивных речевых стратегий)

[16]Указ Президента Российской Федерации «О Стратегии национальной безопасности Российской Федерации» от 02.07.2021 №400 // Российская газета. - 2021

[17]Willard N. E. Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social Aggression, Threats, and Distress. Champaign, 2007

риски[18]. Интернет-травля и интернет-слежка относятся к коммуникационным угрозам, так как возникают в процессе коммуникации агрессора с жертвой.

Из представленной выше дефиниции следует, что кибербуллинг и киберсталкинг обладают общими чертами, например, систематичность, преднамеренность, причинение вреда. Однако, некоторые содержательно различаются. Во-первых, в контексте систематичности интернет-травля должна повторяться, чтобы жертва не имела возможности абстрагироваться от негативного воздействия, чтобы не была утрачена специфика запугивания. В интернет-слежке же систематичность выражается в самом факте совершения нескольких действий, направленных на собирание личной информации о жертве, независимо от того, знает она об этом или нет. Из этого следует, что при кибербуллинге обязательным условием является наличие повторяющейся, как правило, двусторонней коммуникации с жертвой, что необязательно для киберсталкинга.

Из вышесказанного следует и различие этих угроз по целям. Обе направлены на причинение вреда, но характер вреда различается. Вред при интернет-преследовании может быть значительнее вреда от интернет-травли. Основная цель интернет-травли сводится к запугиванию и появлению у жертвы негативных эмоций, вызывающих существенный дискомфорт, то есть к психологическому и эмоциональному вреду. При киберсталкинге же агрессор может собирать персональную информацию не только для создания у жертвы эмоционального напряжения, но и для иных, в том числе преступных целей, к примеру, для дальнейшего похищения, причинения вреда здоровью и др., то есть как для причинения психологического, так и в дальнейшем физического, материального вреда.

При этом, интернет-травля включает в себя больший спектр действий (форм) проявления, способных вызвать негативные эмоции у жертвы, чем киберсталкинг. Среди форм кибербуллинга выделяют хэйтинг (публичное

[18]Галяшина Е. И., Никишин Д. Информационно-мировоззренческая безопасность в интернет-медиа: монография. — Москва:Блок-Принт, 2023.- 424 с.

выражение ненависти в интернет-пространстве с определённой частотой ее проявлений), хэппислэппинг (нападение на человека с ведением записи нападения и последующей его публикацией в сети «Интернет») и др. Интернет-слежка же включает в себя конкретные действия, направленные на сбор, а иногда и распространение персональных данных о личности конкретного человека. Подробный анализ будет приведен в последующих параграфах.

Несмотря на приведенные различия, эти угрозы обладают сходствами. Для обеих, как правило, характерна персонифицированность, то есть наличие тесной личной связи с жертвой, общность целей, ведь обе угрозы направлены, в первую очередь, на причинение психологического вреда. Также схожи последствия обеих явлений.

Более того, в этом вопросе некоторые современные исследователи придерживаются мнения, что кибersталкинг является одной из форм кибербуллинга[19], поэтому разумно полагать, что анализируя интернет-слежку и ее проявления, имеют место характеристики и интернет-травли.

[19]Профилактика кибермоббинга и кибербуллинга в среде несовершеннолетних: методическое пособие / Т.А. Дёгтева и др. – Ставрополь: Ставропольское издательство «Параграф», 2017 г, С.- 9

II. Признаки кибersталкинга (интернет-слежки)

Из всех проанализированных определений кибersталкинга наиболее оптимальным для выведения его характерных признаков видится определение, данное в Энциклопедии Касперского[20], так как оно в отличие от всех остальных содержит перечисление отдельных признаков этого явления, а не его формы. Из данной дефиниции можно выделить следующие признаки: систематичность, осуществление посредством сети «Интернет» и цифровых технологий.

Учитывая наличие взаимосвязи с кибербуллингом и «простым» сталкингом, о которых было сказано выше, возможно выделить такой признак как преднамеренность, а также сформулировать общую цель - причинение вреда. Исходя из анализа существующих примеров, а также зарубежной судебной практики, стоит выделить ряд дополнительных специфических признаков: персонифицированнность, анонимность, продолжительность.

Признаки сталкинга и кибersталкинга совпадают, кроме признака «осуществление посредством сети «Интернет» и цифровых технологий», что обоснованно спецификой среды совершения последнего.

Важно учитывать, что все эти признаки в совокупности образуют акт преследования или интернет-преследования. Обязательными и юридически значимыми среди всех этих признаков можно считать систематичность, преднамеренность, причинение вреда как основная цель агрессора и персонифицированность. Именно эти признаки свойственны всем проявлениям преследования и интернет-преследования, остальные же носят факультативный характер и во многом зависят от конкретного случая.

1. Систематичность

Для этой угрозы характерны систематические акты преследования. Это может выражаться в комплексе как однородных, так и разнородных действий.

[20] Кибersталкинг. Энциклопедия Касперского.сайт URL: https://encyclopedia.kaspersky.ru/glossary/cyberstalking/ (дата обращения: 25.05.2024).

Например, однократное посещение страницы лица с целью узнать о нем какую-либо информацию не является кибersталкингом. При этом ежедневное посещение страницы другого человека, собирание его личных данных, отправка навязчивых сообщений свидетельствуют об акте интернет-преследования.

2. Преднамеренность

Случайный характер действий невозможен. Лицо, осуществляющее кибersталкинг, осознает, что создает для жертвы дискомфорт, часто своими действиями заставляет чувствовать страх, беспокойство и даже ужас. Но порой действия агрессора могут быть анонимными и незаметными. Иногда интернет-слежка осуществляется исключительно как приготовление к совершению преступлений в реальности, к примеру, приготовление к похищению человека (ст. 126 УК РФ).

3. Причинение вреда

По аналогии со сталкингом, при квалификации действий как актов кибersталкинга следует обращать внимание на цель агрессора. Причинение вреда является общей целью для кибersталкера. Проанализировав зарубежный опыт в этой области, можно заметить, что только некоторые государства выделяют причинение вреда в качестве обязательного признака сталкинга. Например, в Польше обязательному доказыванию подлежит наличие негативных последствий для жертвы: существенное причинение вреда как физического, так и материального, появление чувства страха, тревоги и опасения за свою жизнь и жизнь близких, то есть реальный характер угрозы[21]. Однако в силу специфики осуществления кибersталкинга посредством сети «Интернет», можно говорить преимущественно о причинении эмоционального и психологического вреда жертве. Постоянное психологическое давление в цифровом пространстве способно сделать жизнь жертвы невыносимой: нежелательные звонки, сообщения, электронные

[21]Барышева Ксения Александровна Преследование как новый вид уголовно-наказуемого деяния // Пробелы в российском законодательстве. 2016. №8. URL: https://cyberleninka.ru/article/n/presledovanie-kak-novyy-vid-ugolovno-nakazuemogo-deyaniya (дата обращения: 25.05.2024).

письма оказывают непосредственное негативное воздействие на жизнь и здоровье личности. При этом сложно исключать цель причинить в будущем физический или материальный вред в ряде случаев, когда онлайн-преследование переходит в офлайн.

4. **Осуществление посредством сети «Интернет» и цифровых технологий**

Применение технических средств, таких как: отправка электронных сообщений через различные мессенджеры, собирание личной информации, сохранение фотографий и иных данных о жертве и др.

5. **Персонифицированность**

Агрессор обладает особой личной связью с жертвой. Как показывает ряд исследований, преследование, в том числе, интернет-преследование всегда основано на личном отношении агрессора к жертве, на тех эмоциях, которые вызвала жертва и которые с ней связаны[22]. Эта связь может быть обоснована различными мотивами. Более того, связь может быть, как двусторонней, так и односторонней, то есть жертва может не видеть и даже не подозревать об этой связи, но в сознании агрессора она существует.

6. **Анонимность (в ряде случаев)**

В некоторых случаях агрессор действует скрытно, осуществляя преследование так, чтобы жертва не замечала соответствующих действий или же подозревала, но не понимала, кто именно выступает источником опасности. Это называется иллюзией анонимности, она проявляется в возможности отсутствия сведений об агрессоре, в связи с чем киберагрессор чувствует себя менее уязвимым. Анонимность проявляется, например, в отправке анонимных сообщений, звонках с неизвестных номеров телефона, общении с жертвой под фейковым аккаунтом.

7. **Продолжительность**

[22]Mohandie K. et al., The RECON Typology of Stalking: Reliability and Validity Based Upon a Large Sample of North American Stalkers. Journal of Forensic Sciences. Jan. 2006. pp. 147–155

Статистика по сталкингу показывает, что преследование может носить длительный характер, агрессор способен преследовать свою жертву от 6 месяцев до 20 лет[23].

[23]Collins P.I., The Psychiatric Aspects of Stalking in J. Cornish, K. Murray, P.I. Collins, eds., The Criminal Lawyers' Guide to the Law of Criminal Harassment and Stalking. Aurora, Ontario: Canada Law Book, 1999. pp. 35-37

III. Формы и типы киберсталкинга (интернет-слежки)

3.1. Формы киберсталкинга (интернет-слежки):

Понятие «**формы** киберсталкинга» не разработано в процессе исследования этой угрозы. Под формами в рамках настоящего исследования предлагается понимать те конкретные действия, которые в совокупности могут свидетельствовать о том, что интернет-преследование происходит в действительности, не является плодом воображения жертвы. Сложность состоит в том, что таких проявлений множество в различных вариациях. В киберсталкинге эти формы можно разделить по этапам: сбор личных данных о жертве, использование полученных данных с целью нанесения психического или эмоционального вреда жертве. Для каждого из этих этапов характерно совершение разных действий.

1. **Сбор личных данных о жертве** – это подготовительный этап, на котором, как правило, жертва не осознает, что в отношении нее ведется преследование. Киберсталкер изучает цифровой профиль оппонента, то есть совокупность всей информации о лице, которая содержится в социальных сетях, на страницах самых разных сайтов, в сети «Интернет». Преследователь идет по его «цифровым следам» посредством посещения личных страниц, поиска данных о его семье, друзьях, работе и интересах; анализа профилей тех, на чьи публикации жертва оставляет лайки, реакции, комментарии; использования вредоносных программ для получения доступа к информации с устройств жертвы и иными подобными способами. **Цель этого этапа** состоит в подготовке к вступлению в контакт с жертвой и последующему психологическому воздействию на нее или к совершению более серьезных деяний в реальности. Однако этот этап факультативен, а также он может осуществляться параллельно с использованием данных с целью нанесения психического или эмоционального вреда.

2. **Использование данных с целью нанесения вреда жертве** – это основной этап, в ходе которого агрессор вступает в коммуникацию с жертвой. Он пишет навязчивые сообщения, звонит, публикует оскорбительную или

угрожающую информацию о жертве в сети «Интернет» (например, посредством создания фейковой страницы своей жертвы), угрожает вступлением в контакт в реальной жизни/иными более серьёзными действиями (к примеру, убийством) и иным образом дает понять, что за ней следят. Кибersталкер порой действует анонимно, чтобы сильнее запугать преследуемого. Более того, не всегда становится понятно, сколько человек наблюдают за тобой по «ту» сторону экрана и знакомые ли это люди. **Цель этого этапа** состоит в прямом причинении вреда (в зависимости от изначальных целей преследователя как психологического, так и физического).

3.2. Типы кибersталкинга (интернет-слежки):

Типы кибersталкинга можно выделить по различным критериям. Например, в своих исследованиях доценты Рохамптонского университета Лондона, Лерой МакФэрлэйн и Пол Босич выделяли типы кибersталкнга по критерию мотивов, которые подтолкнули агрессора к преследованию. Нужно заметить, что кибersталкинг совершается по самым разным мотивам, значительно зависящим от личности агрессора и его отношения к жертве. Ученые выделили мстительный, сквозной, интимный и коллективный типы кибersталкинга[24].

1. **Мстительный** кибersталкинг – агрессором движет желание возмездия. Он может мстить как за реальное оскорбление, так и за предполагаемое оскорбление, которое является его собственной фантазией. Этот тип отличается особой жестокостью, особенно страшные и даже маниакальные способы воздействия на жертву.

2. **Сквозной** кибersталкинг – агрессор не стремится установить прямой контакт с жертвой, терроризирует свою жертву иными путями. Он хочет, чтобы она постоянно находилась в эмоциональном напряжении. Ему кажется, что таким образом он контролирует ситуацию. Ему нравится быть теневой фигурой и дергать свою жертву «за ниточки», словно марионетку.

[24]Leroy McFarlane, Paul Bocij. An exploration of predatory behaviour in cyberspace: Towards a typology of cyberstalkers // First Monday. — 2003-08-04. — Т. 8, вып. 9.

3. **Интимный** кибersталкинг – агрессор предпринимает настойчивые и многократные попытки добиться взаимного чувства или внимания объекта своей страсти. Можно разделить на “бывших-близких” и “влюбленных”. Первые пытаются возобновить отношения с человеком, с которым раньше их связывали близкие отношения. Даже если бывший возлюбленный не стремится к воссоединению, кибersталкер продолжает постоянно напоминать о себе. «Влюбленные» могут преследовать как своих кумиров, так и обычных людей, к которым испытывают чувства. Однако в ситуациях с публичными личностями признак причинения вреда как цели деяния может отсутствовать, поэтому такое деяние не является проявлением кибersталкинга.

Часто агрессоры страдают от эротомании – ложной убежденности человека в том, что он любим другим, в действительности обычно не питающим к нему никаких чувств или не подозревающем о его существовании. Эти кибersталкеры считают, что должны любой ценой добиться внимания своей жертвы.

4. **Коллективный** кибersталкинг – агрессором чаще всего выступает группа людей, особенно распространено в рабочих коллективах. На первый взгляд в коллективе все может быть спокойно, но коллективные кибersталкеры разворачивают настоящую «виртуальную войну», давая понять определенному человеку, что если он не уйдет, то его репутация будет испорчена. Жертвы просто вынуждены увольняться, что и является целью преследователей.

Похожая классификация, однако в рамках характеристики угрозы сталкинга была изложена в работе врача-психиатра П. Мюллена. Она включает деление на:

1. **Отверженных** — с надеждой на примирение или с целью отомстить преследуют близких друзей, с которыми в ссоре.

2. **Искателей близких отношений** — преследуют человека, в которого влюблены, но он не отвечает им взаимностью.

3. **Злопамятных** — преследуют жертву, чтобы отомстить за реальную или придуманную субъектом травму.

4. **Сталкеров-хищников** — преследуют жертву с целью совершения сексуального контакта, чаще неправомерного.[25]

В 2022 году Центром по контролю и профилактике заболеваний США было опубликовано исследование, согласно которому сталкерами чаще всего становятся бывшие или нынешние партнеры (43.4% – в случаях с женщинами и 32.4% – в случаях с мужчинами) и знакомые (40.3% – в случаях с женщинами и 44.2% – в случаях с мужчинами)[26], поэтому можно сделать вывод, что самым распространенным является интимный сталкинг и кибersталкинг.

Однако вышепредставленные классификации не в полной мере соответствуют выбранному основанию (по мотивам). Так, к примеру, коллективный кибесталкинг возможен и из желания отомстить, поэтому этот вид «выпадает» из данной классификации. В рамках классификации по мотивам видится целесообразным рассматривать только мстительный, сквозной и интимный типы.

Благодаря анализу признаков этого явления, а также существующих классификаций, можно выделить еще несколько классификаций интернет-слежки:

- **по критерию анонимности:**

- анонимный – вид, при котором жертва не знает, кто именно ее преследует (например, агрессор отправляет навязчивые сообщения с одноразовых электронных почт и пишет, что найдет свою жертву);
- личный – вид, при котором жертва знакома лично/заочно с агрессором (например, агрессором выступает знакомый парень, с которым у девушки не сложились романтические отношения).

- **по ролевой структуре:**

[25]Мюллен П. Организация помощи сталкерам // Обзор современной психиатрии. 2003. № 18. С. 34.
[26]Report on stalking // National Intimate Partner and Sexual Violence Survey // URL: https://www.cdc.gov/violenceprevention/datasources/nisvs/summaryreports.html // (дата обращения 25.05.2024)

- простой – как на стороне агрессора, так и на стороне жертвы находится по 1 человеку (например, одна сестра следит за другой и пишет ей угрожающие сообщения);
- сложный – как на стороне агрессора, так и на стороне жертвы может быть несколько человек (группа агрессоров/жертв) (например, агрессор шантажирует сразу нескольких жертв, угрожает публикацией порочащих их сведений).

Но в обоих видах не исключено наличие свидетелей.

- **по способу преследования:**

- коммуникативный – преследование осуществляется при двусторонней связи с жертвой (например, агрессор пытается пообщаться с жертвой, создать доверительные отношения при помощи манипулятивных конструкций для дальнейшего преследования);
- наблюдающий – преследование осуществляется при односторонней связи с жертвой (например, посредством сбора личных данных и преследования без коммуникации).

IV. Последствия кибersталкинга (интернет-слежки)

Говоря о **последствиях** кибersталкинга, нужно заметить, что они имеют место как для преследуемого лица, так и для преследователя.

Последствия для преследуемого находятся в тесной связи с индивидуальными особенностями его личности. Более того, последствия зависят и от того, в какой связи с жертвой находится агрессор: двусторонней или односторонней, а также от конкретных целей агрессора.

При двусторонней связи жертва находится в контакте с агрессором и осознает, что ее преследуют. Она может лично не знать агрессора, но знает о его существовании и неблагоприятных намерениях, поэтому последствия в виде причиненного психологического и эмоционального вреда преимущественно имеют место.

Такие последствия обладают схожими чертами с последствиями кибербуллинга. Они также носят скрытый характер и, как правило, заключены на уровне психики жертвы. Кибersталкер вызывает душевные страдания, в результате которых у преследуемого могут развиться внутренние комплексы, неуверенность в себе, тревожность, апатия и др., что может привести к психическим расстройствам, социальной дезадаптации и иным негативным последствиям.

Однако не исключаются и последствия, связанные с причинением физического и материального вреда. Примерами таких последствий служат перемена привычного образа жизни (смена места жительства и др.), попытки самоубийства со стороны жертвы, проявления потребности в членовредительстве к себе (селфхарм) и иные вынужденные действия, в том числе в попытки скрыться от преследователя.

Риск наступления физического или материального вреда присутствует и при односторонней связи жертвы с агрессором, но он напрямую связан с действиями кибersталкера. Примерами таких последствий может стать совершение уже в офлайн-пространстве правонарушений и даже преступлений. Преследователь может осуществлять собирание информации о

жертве посредством использования сети «Интернет» для дальнейшего совершения преступлений против собственности (например, кража, разбой), причинения вреда жизни и здоровью (например, убийство, причинение тяжкого вреда здоровью), похищения человека и других.

При этом остается дискуссионным вопрос о том, относится ли к кибersталкингу простое собирание данных о личности, которая и не подозревает о преследовании (односторонняя связь), если преследователь не наносит ни физический, ни материальный вред, при этом использует только открытые источники.

Последствием же для самого кибersталкера является привлечение к юридической ответственности. Как было описано выше, возможно привлечение к ответственности как за отдельные формы, так и за совокупность действий, составляющих преследование, а также за те деяния, для которых этап сбора информации о жертве послужил приготовлением. В различных правопорядках предусмотрены разные виды ответственности и санкции (административная или уголовная).

V. Меры защиты от кибersталкинга (интернет-слежки)

Чтобы избавить себя в будущем от возможного посягательства, необходимо знать о превентивных мерах в отношении кибersталкинга, их можно разделить на несколько групп, а именно:

- **Профилактические меры** – это меры и правила, соблюдение которых обеспечит наибольший уровень защищенности от возможного в будущем посягательства. Профилактика в отношении угрозы интернет-слежки представляет собой перечень довольно простых правил поведения в цифровом пространстве:

1. **Обезопасьте свои персональные данные следующими способами:**

- **Осознанно формируйте свой цифровой профиль**. Нередко наши «цифровые следы» могут скомпрометировать нас, а тем самым быть полезны агрессору. Перед публикацией какой-либо личной информации о себе или окружающих в аккаунтах и социальных сетях оцените, не может ли эта информация быть использована злоумышленниками во вред вам или вашим близким;

- **Устанавливайте настройки приватности в социальных сетях.** Они позволят ограничить доступ незнакомым и нежелательным лицам к данным профиля, публикациям и прочей информации, а также ограничат возможность коммуникации (например, посредством личных сообщений);

- **Осуществляйте фильтрацию интернет-знакомств.** Нередко к нам в друзья в социальных сетях добавляются неидентифицируемые личности, а также фейк-аккаунты. Существует вероятность, что под ними скрываются преследователи. Чтобы обезопасить себя, исследуйте такие аккаунты на приемлемость до того, как начать с ними активное взаимодействие. Для этого достаточно будет проанализировать содержимое профиля потенциального друга, изучить контент, который он публикует, оценить его достоверность и безопасность для других пользователей. Иногда уже по имени пользователя можно понять, что скорее всего страница

фейковая, например, в случаях, когда пользователь представлен под именем публичной личности. В подобных ситуациях понять, кто на самом деле скрывается за этим цифровым профилем, просто не представляется возможным.

- **Тщательно подбирайте пароли для социальных сетей, электронных почт и т.д.** Выбирая простой и запоминающийся пароль, вы увеличиваете шансы посторонним людям завладеть вашим аккаунтом. Также, стоит придерживаться правила: один аккаунт – один пароль.

Надежный пароль должен соответствовать 3 основным условиям:

- во-первых, не содержать ту информацию, которую Вы размещаете о себе в свободном доступе (дата рождения, место учебы и т.д.);
- во-вторых, длина пароля должна быть не менее 10-12 символов;
- в-третьих, пароль не должен быть единым для всех Ваших цифровых ресурсов, в противном случае, получив доступ к одному аккаунту, злоумышленник «по цепочке» сможет обеспечить себе доступ и ко всем остальным.

Кроме того, для защиты своих профилей можно использовать двухфакторную аутентификацию. Такая аутентификация помимо ввода логина и пароля запрашивает дополнительное подтверждение по электронной почте, SMS или с использованием биометрии - системы распознавания людей по одной или более физическим, или поведенческим чертам (например, отпечаток пальца или Face ID, которые невозможно подделать).

Хранить пароли лучше всего в голове, но, если всё же записывать – лучше хранить материальный носитель в месте, к которому имеет доступ минимальное количество людей.

- **Не разрешайте сбор данных cookie.** Многие сайты запрашивают это разрешение, не предоставляя альтернативы. Для того, чтобы скрыть баннер и начать знакомиться с интересной информацией, многие просто нажимают OK. Но с помощью такой функции легче всего осуществлять сбор

данных по конкретному пользователю, поэтому лучше не облегчать задачу потенциальным злоумышленникам и не давать согласие на сбор таких данных.

2. **Проверьте личные устройства на наличие шпионских программ[27].**

С помощью шпионского ПО злоумышленники могут **отслеживать местоположение владельца устройства, записывать его звонки и читать переписки, воровать пароли от аккаунтов в социальных сетях,** читать электронную почту, смотреть личные фотографии. Есть ряд **косвенных признаков того, что на устройстве есть сталкерское или шпионское ПО**:

- Устройство работает медленно, время отклика увеличено;
- Неожиданно появляются рекламные сообщения и всплывающие окна (шпионское и рекламное ПО часто идут вместе);
- Слишком быстро разряжается батарея;
- При входе на защищенные сайты возникают проблемы (если вам удалось войти на сайт со второй попытки, возможно, первая была на его поддельной версии и ваш пароль был передан злоумышленникам, а не банку);
- Расходуется слишком большой трафик. Это может означать, что шпионская программа ищет ваши данные и отправляет их посторонним[28].

Но однозначно ответить на вопрос, заражено устройство или нет, можно только **используя мобильные защитные решения (антивирусные ПО и другие подобные программы) или прибегнув к помощи специалистов по кибербезопасности.**

- **Пресекательные меры** – это меры, которые применимы в момент, когда посягательство только началось, но еще не завершилось, поэтому возможно его предотвращение. Также применение этих мер целесообразно, чтобы киберпреследование не перешло в преследование в реальности. Если у вас появляются подозрения, что за вами следят в Сети, то возможно воспользоваться следующими средствами:

[27]Что такое кибersталкинг и как от него защититься // Kaspersky.ru: сайт URL: https://www.kaspersky.ru/resource-center/threats/how-to-avoid-cyberstalking (дата обращения: 28.05.2024)
[28]Как обнаружить шпионское ПО и защитить свою приватность? // Kaspersky.ru: сайт URL: https://www.kaspersky.ru/resource-center/threats/how-to-detect-spyware (дата обращения: 28.05.2024).

Пресекательные меры в контексте этой угрозы представляют собой **самозащиту.** Суть данного способа заключается в самостоятельном принятии пользователем мер по борьбе с агрессорами: блокирование, отключение звука, применение «невидимости» на своего аватара, прекращение коммуникации с агрессором, жалоба администрации платформы и т.п.

Поэтапные шаги по пресечению кибersталкинга:

- **Не реагируйте, прекратите общение с агрессором.**

Целью агрессора является нарушение эмоционального равновесия жертвы, ее ответная реакция. Получив отклик, он продолжит свои нападки, обрекая жертву на ухудшение состояния. Дайте преследователю понять – обязательно в письменном виде, – что не хотите с ним общаться. Предупредите, что обратитесь в полицию, если он/она не оставит Вас в покое. После этого прекратите общение.

- **Внесите агрессора в черный список, отключите звук уведомлений.**

Данная мера поможет дистанцироваться от проявлений преследования. Используйте для этого настройки приватности, затем сообщите о нарушении администрации цифровой платформы.

- **Зафиксируйте факты кибersталкинга.**

Для этого достаточно сделать скриншоты. Такое действие в будущем поможет привлечь агрессора к ответственности, если она предусмотрена законодательством.

- **При необходимости обратитесь в полицию, прокуратуру или в суд.**

Необходимо представить соответствующие доказательства и, если известны данные преследователя, то следует указать их в своем заявлении. Если имеются сомнения в вопросе – обращайтесь в полицию, а именно в территориальный орган МВД России. В настоящее время в МВД создано специальное Управление по организации борьбы с противоправным

использованием информационно-коммуникационных технологий (УБК)[29] для обращения в подобных ситуациях.

- **При наличии подозрений о наличии шпионского ПО не используйте это устройство до момента его проверки техническим специалистом.**
- **Смените пароли к электронной почте и важным сервисам, если подозреваете, что они могут быть взломаны.**

[29]Приказ МВД России от 29.12.2022 N 1110 "Об утверждении Положения об Управлении по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации". URL: https://www.consultant.ru/document/cons_doc_LAW_439373/ (дата обращения: 25.05.2024).

VI. Правовые механизмы противодействия киберсталкингу (интернет-слежке) в иностранных правопорядках

6.1. Правовая квалификация и меры юридической ответственности за киберсталкинг (интернет-слежку):

Перед проведением детального анализа специфики правовой квалификации и мер юридической ответственности за рубежом, необходимо сказать, что в законодательстве стран, где криминализован сталкинг, как правило, отсутствует специальная норма, предусматривающая ответственность за киберсталкинг. Те государства, которые работают в этом направлении, чаще всего включают отдельный пункт в статью за сталкинг/преследование, который предусматривает юридическую ответственность за осуществление преследования посредством использования информационно-телекоммуникационных технологий и сети «Интернет».

Однако есть и страны, избравшие иной подход. Например, в законодательстве Германии[30] и Канады[31] присутствуют нормы, запрещающие оффлайн-преследование, но нет пунктов, которые прямо предусматривают санкцию за киберпреследование.

1. Германия:

Так в Уголовном Уложении **Германии** (далее – УУ ФРГ) есть §238 Преследование: «лишением свободы на срок до трёх лет или денежным штрафом наказывается тот, кто способом, пригодным для значительного ухудшения качества жизни другого лица, недозволенно преследует его тем, что систематически:

1. ищет пространственной близости этого лица,

2. **пытается установить с этим лицом контакт, используя телекоммуникационные средства,** иные средства коммуникации или через третьи лица,

3. злоупотребляя личными данными этого лица, a) заказывает для него товары или услуги или b) привлекает третьих лиц к установлению с ним контакта или

[30]https://www.uni-potsdam.de/fileadmin/projects/ls-hellmann/Forschungsstelle_Russisches_Recht/Neuauflage_der_kommentierten_StGB-%C3%9Cbersetzung_von_Pavel_Golovnenkov.pdf
[31]https://laws-lois.justice.gc.ca/eng/acts/c-46/page-38.html#docCont

4. угрожает этому лицу причинением вреда жизни, телесной неприкосновенности, здоровью или свободе его самого или другого близкого ему лица, или

5. действует иным сравнимым образом»[32].

Перечень форм сталкинга в конструкции этой нормы является открытым, поэтому возможны и иные проявления, в том числе относящиеся к кибersталкингу. Более того, пункт 2 нормы содержит формулировку «пытается установить с этим лицом контакт, используя телекоммуникационные средства», которая может быть отнесена к проявлениям и кибersталкинга.

Интересно, что в первоначальной редакции[33] этот состав считался материальным и сводился к наличию такого последствия как «существенное ухудшение качества жизни потерпевшего», относящегося скорее только к категории материального вреда. Иными словами, если потерпевший не поддался оказываемому на него давлению и не позволил изменить к худшему условия своей жизни, ответственность за оконченное неправомерное преследование / за покушение на него по § 238 УУ ФРГ не наступала.

В последней редакции, проанализированной выше, субъективное восприятие сталкинга потерпевшим (то есть страх, стресс и иной психологический вред) принимаются во внимание, решающим является не столько значительное ухудшение качества жизни потерпевшего, сколько объективная пригодность деяния для наступления подобного преступного последствия.

Некоторые из проявлений неправомерного преследования наказуемы в соответствии с общими составами, направленными на защиту телесной неприкосновенности и свободы личности (например, принуждение в § 240 УУ ФРГ, угроза в § 241 УУ ФРГ). Однако законодатель предусмотрел отдельный состав для преследования, чтобы была возможность наиболее комплексно охватить то разнообразие моделей поведения, которые свойственны преследованию. Кроме того, основным защищаемым правовым благом в данном составе является именно свобода формирования воли и действий личности в отношении собственного жизнеустройства[34], а физическая неприкосновенность и жизнь потерпевшего в этом составе выступают

[32]П.В. Головненков. Уголовное уложение Федеративной республики Германия – Strafgesetzbuch (StGB) –. Научно-практический комментарий и перевод текста — Москва: Проспект, 2023.- 494 с.
[33]BT-Drs. 18/9946, S. 10f.; 18/10654, S. 1
[34]BT-Drs. 15/5410 S. 6; 16/1030 S. 6; Eisele, in: Schönke/Schröder, 29. Aufl., § 238 Rn. 4 mwN.

дополнительным объектом[35], поэтому введение отдельного состава при наличии мер ответственности за отдельные проявления видится разумным.

Целесообразно будет сравнить предложенное Германией правовое регулирование с государствами, где присутствует регулирование именно кибersталкинга как вида сталкинга. Было решено рассмотреть законодательство США и Великобритании ввиду бОльшей разработанности правовых норм, и наличия судебной практики по данному вопросу.

2. США:

В 1996 г. Конгресс США определил преследование как федеральное преступление. В последующие 3 года по данным Национальной конференции законодательных собраний штатов, по состоянию на июнь 2000 года в 22 штатах США были приняты законы о киберпреследовании, а в законодательных собраниях еще 15 штатов находились на рассмотрении законопроекты о киберпреследовании. Этому послужило массовое появление прецедентов кибersталкинга посредством электронной почты в штатах, где это явление не было криминализовано. Об этих прецедентах будет сказано подробнее далее.

Позже в федеральное законодательство были внесены поправки, которые расширили возможности уголовно-правовой защиты жертв от преследования, были введены новые виды составов – преследование, причиняющие значительный моральный вред; преследование, **с использованием электронных коммуникаций, с помощью системы GPS**[36]. Преследование по законодательству США – это комплекс действий, «связанных не только с причинением физического вреда, но также направленных на причинение беспокойства (слова, действия, направленные на конкретного человека, не имеющие никакой специальной цели, кроме как досадить, вызвать чувство тревоги), действия, вызывающие эмоциональные страдания, депрессию, психическое расстройство, чувство стыда, панику, шок, смущение, страх»[37]. В правовой норме США применяется конструкция материального состава преступления, то есть важно, чтобы наступили последствия в форме причинения вреда.

Говоря о юридической ответственности, можно заметить, что система наказаний достаточно сурова, Статья 2261 Федерального Кодекса США

[35] BT-Drs. 15/5410 S. 6, 16/1030 S. 6

[36]Code of Laws of the United States of America, Title 18 § 2261A, 18 U.S.C. § 2261A(2)(B), 18 U.S.C. § 2261A(2)(A). https://www.law.cornell.edu/uscode/text/18/2261A

[37]Барышева Ксения Александровна Преследование как новый вид уголовно-наказуемого деяния // Пробелы в российском законодательстве. 2016. №8. URL: https://cyberleninka.ru/article/n/presledovanie-kak-novyy-vid-ugolovno-nakazuemogo-deyaniya (дата обращения: 25.05.2024).

предусматривает, что: «лицо должно быть оштрафовано и заключено в тюрьму:

(1) пожизненно или на любой срок в течение нескольких лет, если наступит смерть потерпевшего;

(2) на срок не более 20 лет в случае необратимого уродства или опасного для жизни телесного повреждения потерпевшего;

(3) на срок не более 10 лет, если потерпевшему причинено тяжкое телесное повреждение или если при совершении преступления преступник применил опасное оружие;

(4) на срок не более 5 лет, в ином случае».

Важно заметить, что санкция ужесточается, если потерпевшим выступает ребенок, а именно на 5 лет увеличивается срок тюремного заключения в соотношении с максимальным сроком, предусмотренным в общем порядке для состава преследования.

При этом штаты в региональном законодательстве имеют право устанавливать более специализированное регулирование. К примеру, в Уставе штата Иллинойс в главе, посвященной уголовным правонарушениям, есть отдельная статья, посвященная именно кибersталкингу[38].

Этот состав не обладает спецификой с точки зрения конструкции состава или санкции, но выделяется в качестве отдельной статьи, что говорит об уделении особого внимания этому правонарушению. При этом, представляется, что специфика кроется скорее в наличии разъяснений в самой статье относительно отдельных понятий и категорий, которые в ней встречаются. Например, в статье выделяются понятия «эмоциональный стресс», «несогласованный контакт», «шпионское ПО» и иные, которые обладают особым значением для конкретного состава. Также присутствует пункт, содержащий перечень действий, которые не могут быть квалифицированы по этой статье.

3. Великобритания:

Понятие сталкинга в Великобритании введено Законом о защите свобод (Protection of Freedoms Act), вступившим в силу 25 ноября 2012 года[39].В настоящее время в Великобритании существует несколько уголовно наказуемых деяний, связанных с преследованием: домогательства;

[38]Устав штата Иллинойс, глава 720. Уголовные преступления § 5/12–7.5. Кибersталкинг – последнее обновление: 1 января 2022 г. URL: https://codes.findlaw.com/il/chapter-720-criminal-offenses/il-st-sect-720-5-12-7-5/

[39] Protection of Freedoms Act 2012. URL: https://www.legislation.gov.uk/ukpga/2012/9/section/111

преследование (сталкинг); действия, вызывающие чувство угрозы насилия; преследование, связанное с угрозой насилием, вызывающие страх, чувство тревоги и стресс; нарушение гражданского запрета на преследование; нарушение запретительного ордера. В соответствующей статье Закона о защите свобод не дается определения преследования, перечисляются действия, которые являются его проявлениям: «Ниже приведены примеры действий или бездействия, которые при определенных обстоятельствах могут быть связаны с преследованием —

(a) следить за человеком,

(б) вступать в контакт или пытаться связаться с человеком любыми способами,

(в)публиковать любые заявления или другие материалы, относящиеся или предполагающие, что они относятся к какому-либо лицу, или исходящие от какого-либо лица,

(d) **отслеживающие использование каким-либо лицом Интернета, электронной почты или любой другой формы электронного общения,**

(e) слоняться без дела в любом месте (будь то общественном или частном),

(f) вторгаться в любое имущество, находящееся во владении человека,

(g) наблюдать за человеком или шпионить за ним».

Сравнивая предусмотренные меры юридической ответственности, нужно сказать, что предусмотренная в США санкция за подобное деяние намного существеннее, чем в Великобритании. В соответствии с Законом о защите свобод, виновный подлежит наказанию в упрощенном порядке в виде тюремного заключения на срок до 51 недели или штрафа.

Проводя сравнение 3 различных правопорядков можно сделать некоторые выводы. Основное отличие кроется в конкретных деяниях, комплекс которых составляет сталкинг и кибersталкинг. Их перечень может быть как закрытым, так и открытым, также различное место в системе этих проявлений занимают те, которые относятся именно к интернет-слежке. Так, в региональном законодательстве США для кибersталкинга выделяются отдельные статьи с подробными дефинициями, а в УУ ФРГ практически не содержится проявлений именно кибersталкинга.

Во всех правопорядках состав является материальным, так как основным условием наступления уголовной ответственности за действия, образующие как онлайн-, так и оффлайн-преследование, является причинение,

как минимум психологического вреда потерпевшему, то есть учитывается именно субъективное восприятие жертвой действий агрессора.

Также законодатель применяет тождественные санкции к обвиняемым, а именно лишение свободы или штраф, в зависимости от модели поведения обвиняемого и тяжести причиненного вреда.

6.2. Зарубежная судебная практика/кейсы:

Германия:

Фабула: С 2006 по конец 2007 года гражданин N состоял в отношениях с гражданкой А. После расставания неоднократно возникали ссоры, так как гражданин N не хотел соглашаться на расставание. Гражданка А 7 января 2008 г. добилась судебного запрета в соответствии с Законом о защите от насилия в отношении гражданина N (было запрещено вступать в контакт с гражданкой А и приближаться к ней в радиусе 100 метров).

Однако и после наложения этого запрета гражданин N продолжал доставлять неудобство и страх гражданке А, он находил ее на работе, приходил к ее дому, кричал, оскорблял и угрожал, что «выбьет ей щеки до синевы» и что убьет. Также он постоянно писал по электронной почте и звонил жертве, пытался выяснить, где она находится в конкретный момент. Гражданке А угрозы показались довольно реалистичными, поэтому она по возможности больше не выходила из своей квартиры и из страха больше не открывала входную дверь. Она перестала включать свет в квартире по вечерам, чтобы могла притвориться, что ее нет дома. Из-за беспокойства она существенно похудела и стала часто болеть. Преследование продлилось до 2010 года.

Итог: обвиняемый был приговорен к лишению свободы сроком на 1 год[40].

Анализ: Нужно заметить, в первую очередь, что в фабуле содержатся как многократные акты преследования, так и черты интернет-преследования. Деяние обладает таким признаками как: преднамеренность, систематичность, причинение вреда (в особенности психологического, эмоционального), а также персонифицированность.

Исходя из выделенных классификаций преследования, необходимо обозначить, что по мотивам этот кейс относится к интимному сталкингу, так как агрессор стремится добиться взаимных романтических чувств от жертвы.

[40] Entscheidungen des Bundesgerichtshofs. URL: https://www.bundesgerichtshof.de/DE/Entscheidungen/entscheidungen_node.html

По критерию анонимности – личный, ведь жертва четко понимает, кто выступает агрессором, а агрессор не пытается скрыть свою личность.

По ролевой структуре – простой, в обеих ролях выступает по 1 человеку (Гражданин N и гражданка А)

По способу преследования – коммуникативный, агрессор старается вступить в личный контакт с жертвой, по началу уговорить, а затем даже принудить к совершению определенных действий.

США:

(1) Фабула: В Калифорнии в апреле 1999 года частный охранник из Лос-Анджелеса признал себя виновным по обвинению в том, что он пытался использовать Интернет для подстрекательства к изнасилованию знакомой женщины.

Он признал, что выдавал себя за свою жертву, женщину, которая его отвергла, в интернет-чатах на секс-тематику, размещая персональные объявления от имени женщины, то есть выдавая себя за нее. На объявления откликнулись многие мужчины, он прислал им ответные сообщения по электронной почте, утверждая, что женщина мечтала о том, чтобы ее изнасиловали. В электронных письмах он указал имя женщины, ее физическое описание, адрес и номер телефона. В своих сообщениях он также дал советы о том, как обойти систему домашней безопасности женщины. Шестеро мужчин пришли к женщине домой и заявили, что хотят ее изнасиловать.

Итог: обвиняемый был приговорен к шести годам лишения свободы в тюрьме штата Калифорния, однако следователи столкнулись с трудностями при получении ордеров на обыск в других штатах, где у него были открыты учетные записи электронной почты и где не было законодательства о киберпреследовании[41]. Мужчины, которые пришли к женщине домой, не были привлечены к юридической ответственности, так как ими не были совершены деяния, запрещенные законодательством.

Анализ: В фабуле содержатся многократные акты интернет-преследования. Деяние обладает таким признаками как: преднамеренность, систематичность, причинение вреда (в особенности психологического, эмоционального), персонифицированность, а также такой признак как анонимность (в виде факта выдачи себя за другого лица, а также отсутствие у жертвы представления о личности преследователя и об осуществлении слежки).

[41]§ 1:68. State laws in the United States—Cyberstalking, 1 World Online Business Law § 1:68

Исходя из выделенных классификаций преследования, необходимо обозначить, что по мотивам этот кейс относится к мстительному кибersталкингу, так как агрессор хоть и состоял в романтических отношениях с жертвой, не стремится добиться взаимности от нее, а стремится отомстить ей за отказ.

По критерию анонимности – анонимный, ведь жертва не могла представить, кто именно выступил агрессором.

По ролевой структуре – простой, в обеих ролях выступает по 1 человеку. Шестеро мужчин не могут быть отнесены к группе, действующей на стороне агрессора, так как их действия не охватывались умыслом агрессора, они не знали и не подозревали, что за страницей жертвы в социальных сетях может скрываться ее бывший возлюбленный, стремящийся отомстить.

По способу преследования – наблюдающий, агрессор осуществил преследование посредством сбора личных данных о жертве, при этом использование этих данных не предполагало прямой коммуникации с жертвой.

(2) Фабула: С 2019 года гражданин N писал оскорбительные сообщения с просьбами за деньги созваниваться с ним по видео и осуществлять действия интимного характера. Гражданка А согласилась, а в ходе одного из таких видеозвонков Гражданин N записал ее действия на видео. Через пару месяцев он связался с Гражданкой А под другим псевдонимом в социальной сети и отправил ей видеозапись одного из их предыдущих звонков, пригрозил отправить видео ее родителям, если она не будет участвовать в более откровенных видеозвонках с ним. Опасаясь смущения, унижения, Гражданка А согласилась.

В течение 2020 года Гражданин N неоднократно связывался с Гражданкой А, используя многочисленные псевдонимы, угрожая отправить откровенные записи с ней членам ее семьи, если она не выполнит его требования о видеочате с ним.

В 2021 году она связалась с Федеральным бюро расследований (ФБР) и встретилась с агентами ФБР. Она предоставила агентам фотографию лица, которую он ей отправил, и агенты идентифицировали его как человека на фотографии посредством обратного поиска изображений. Последовал арест Гражданина N.

Итог: обвиняемый был приговорен к тюремному заключению сроком на 42 месяца с последующим тридцатишестимесячным освобождением под надзор[42].

Анализ:

В фабуле содержатся как многократные акты именно интернет-преследования. Деяние обладает таким признаками как: преднамеренность, систематичность, причинение вреда (в особенности психологического, эмоционального), а также такой признак как анонимность (в виде того, что агрессор скрывал свою личность от жертвы, используя для этой цели несколько аккаунтов).

Исходя из выделенных классификаций преследования, необходимо обозначить, что по мотивам этот кейс относится к сквозному кибersталкингу, так как агрессору важна не столько личная связь с жертвой, сколько возможность контролировать ее действия, а также приятен факт сохранения у жертвы эмоционального напряжения.

По критерию анонимности – анонимный, ведь жертва не могла представить, кто именно выступил агрессором, более того, агрессор скрывал свою личность посредством использования разных аккаунтов в социальной сети.

По ролевой структуре – простой, в обеих ролях выступает по 1 человеку.

По способу преследования – коммуникативный, агрессор старается вступить в личный контакт с жертвой, по началу уговорить, а затем даже принудить к совершению определенных действий.

Великобритания:

Фабула: Шон Маккуэйг создавал фейковые изображения, используя фоторедактор, фотографии голых девушек из Интернета и фотографии, где есть лица тех подростков, которым он собирался присылать подобные фотографии. Далее он многократно и навязчиво писал им с нескольких аккаунтов, присылал эти фотографии с угрозами, что опубликует их, если жертвы не будут присылать ему откровенные фото. Из-за чувства испуга, стыда и ужаса подростки исполняли требования агрессора. Некоторые из жертв проинформировали своих родителей или учителей, и в июне 2017 года, действуя на основании информации о хранении непристойных изображений, сотрудники полиции посетили дом ответчика. Исследование обнаруженного

[42]British and Irish Legal Information Institute. URL: https://www.bailii.org/

компьютерного оборудования установило его ответственность за различные правонарушения, совершенные в отношении девяти заявителей. Кроме того, было обнаружено 2653 непристойных неподвижных изображения детей.

Итог: обвиняемый был приговорен к тюремному заключению сроком на 6 лет по совокупности преступлений[43].

Анализ:

В фабуле содержатся многократные акты интернет-преследования. Деяние обладает таким признаками как: преднамеренность, систематичность, причинение вреда (в особенности психологического, эмоционального), а также такой признак как анонимность (в виде того, что агрессор скрывал свою личность от жертв, используя для этой цели несколько аккаунтов).

Исходя из выделенных классификаций преследования, необходимо обозначить, что по мотивам этот кейс относится к сквозному кибersталкингу, так как агрессору важна не столько личная связь с жертвами, сколько возможность контролировать их действия, а также приятен факт сохранения у жертв эмоционального напряжения.

По критерию анонимности – анонимный, ведь жертвы не могли представить, кто именно выступил агрессором, более того, агрессор скрывал свою личность посредством использования разных аккаунтов в социальной сети.

По ролевой структуре – сложный, в роли жертвы выступало сразу несколько человек.

По способу преследования – коммуникативный, агрессор старается вступить в личный контакт с жертвой, по началу уговорить, а затем даже принудить к совершению определенных действий.

[43]МакКуэйг (Шон) против Адвоката Ее Величества, 2018 WL 04539008

VII. Правовые механизмы противодействия кибersталкингу (интернет-слежке) в России

В России не сформировано единого подхода к регулированию проблемы слежки и интернет-слежки, кроме того, не существует специальных норм, предусматривающих юридическую ответственность за эти деяния.

Научное сообщество относит кибersталкинг к уголовно-наказуемым деяниям, причем родовым признаком определена личность, ее права и свободы[44]. В понятие «кибersталкинг» закладывают клевету, похищение и использование «цифровой личности», угрозы убийством, собирание информации, которая может быть использована для запугивания или домогательств, но при условии систематичности таких действий. При малозначительности деяния или при отсутствии прямых угроз убийством или иной формой расправы деяния относят к административным правонарушениям. Однако, в практике отсутствуют уголовно-правовые нормы, которые бы предусматривали запрет и санкцию как за преследование в целом, так и за интернет-слежку, в частности.

Стоит отметить, что в научном сообществе нет единого мнения касательно криминализации этих явлений. Некоторые ученые предлагают варианты включения сталкинга и кибersталкинга в Уголовный кодекс Российской Федерации в качестве отдельной статьи, используя зарубежный опыт квалификации[45]. При этом возникает проблема соотношения различных форм преследования, домогательств, травли, эмоционального террора, которые криминализированы в законодательстве зарубежных стран и которые аналогичным образом предлагают криминализировать в законодательстве России.

Более того, в области преступлений против личности, ее прав и свобод в законодательстве Российской Федерации уже существуют определенные положения, провести разграничение с которыми будет не просто. Среди таких норм есть те, в соответствии с которыми в настоящее время наказываются и деяния, фактически относящиеся к сталкингу и кибersталкингу. Они представляют собой скорее отдельные формы и проявления этих угроз, но их специфика в сравнении с преследованием состоит в отсутствии

[44]Корнилова Татьяна Владимировна, Емельянова Жанна Эдиковна Ответственность за преследование (сталкинг) в России и за рубежом // Вестник СурГУ. 2022. №3 (37). URL: https://cyberleninka.ru/article/n/otvetstvennost-za-presledovanie-stalking-v-rossii-i-za-rubezhom (дата обращения: 25.05.2024).

[45]Рыжова Ольга Александровна, Корнишина Юлия Сергеевна Об ответственности за сталкинг в Российской Федерации и в зарубежных странах // Наука. Общество. Государство. 2018. №4 (24). URL: https://cyberleninka.ru/article/n/ob-otvetstvennosti-za-stalking-v-rossiyskoy-federatsii-i-v-zarubezhnyh-stranah (дата обращения: 25.05.2024).

систематичности. Среди норм Уголовного кодекса Российской Федерации, которые применяются и могут быть применимы к правовому регулированию интернет-слежки:

- Доведение до самоубийства (ст. 110 УК РФ);
- Склонение к совершению самоубийства или содействие в совершении самоубийства (ст. 110.1 УК РФ);
- Угроза убийством или причинением тяжкого вреда здоровью (ст. 119 УК РФ);
- Клевета (ст. 128.1);
- Нарушение неприкосновенности частной жизни (ст. 137 УК РФ);
- Вымогательство (ст. 163 УК РФ);

Некоторые исследователи также отмечают, что проявления кибersталкинга можно рассматривать и в свете административного права, например:

- Мелкое хулиганство (ст. 20.1 КоАП РФ);
- Оскорбление (ст. 5.61 КоАП РФ);
- Клевета (ст. 5.61.1 КоАП РФ).

Отдельного внимания заслуживает вопрос о разграничении этих составов правонарушений и кибersталкинга.

Помимо статьи 137 УК РФ, которая наиболее близка к кибersталкингу по объективной стороне (будет рассмотрена подробнее в следующем разделе), можно выделить статью 163 УК РФ «Вымогательство». Нередко злоумышленники узнают те или иные сведения, порочащие честь и достоинство потерпевшего или подрывающие его репутацию, с целью шантажа последнего. В данном случае отграничить такой состав от кибersталкинга можно по цели и периодичности действий. Вымогательство является корыстным преступлением, совершаемым для извлечения выгоды, в то время как интернет-слежка является преступлением против личности, в первую очередь совершаемый для нанесения вреда (психологического) потерпевшему.

Кроме того, вымогательство, как правило не носит систематический характер, в отличие от кибersталкинга. В случае если имеет место длящееся вымогательство, необходимо обратить внимание на цель – если единственной целью является передача имущества потерпевшего, значит данное деяние следует квалифицировать как вымогательство.

Сложнее отграничить статьи 110 УК РФ «Доведение до самоубийства» и 110.1 «Склонение к совершению самоубийства или содействие в совершении

самоубийства» от кибersталкинга. Интернет-преследование далеко не всегда приводит к смерти жертвы, однако последствия в указанных выше составах преступления с высокой долей вероятности могли стать результатом кибersталкинга. Доведение до самоубийства достаточно трудно доказывается, об этом свидетельствует относительно небольшое количество дел из судебной практики, закончившихся обвинительным приговором. Данный состав изначально предполагал частичное затрагивание других составов против жизни и здоровья, в связи с чем Верховный Суд в своем постановлении Пленума[46] указал: «Самоубийство потерпевшего либо покушение на него дополнительной квалификации по статьям о преступлениях против жизни и здоровья не требует…»

Таким образом, в случаях, когда имело место доведение до самоубийства, равно как и склонение к совершению самоубийства, целесообразным было бы применять нормы именно этих статей.

Еще одним смежным с кибесталкингом составом преступления является статья 119 УК РФ «Угроза убийством или причинение тяжкого вреда здоровью». Действительно, кибersталкеры могут угрожать причинением тяжкого вреда здоровью или даже убийством, однако для квалификации по статье 119 УК РФ необходимо, чтобы имелись достаточные основания опасаться осуществления этой угрозы.

[46]Постановление Пленума Верховного Суда РФ от 18 мая 2023 года № 11 «О практике рассмотрения судами уголовных дел против военной службы». URL: https://www.consultant.ru/document/cons_doc_LAW_447521/ (дата обращения: 25.05.2024).

Подтверждает сложность доказывания угрозы убийством судебная практика[47] (Определение № 10-УДП21-11-А4[48]).

В отдельных случаях ответственность за кибersталкинг может наступать по статье 128.1 УК РФ «Клевета». Клевета, как правило, не отличается систематичностью, поэтому в большинстве случаев проблемы с квалификацией деяния не возникает, однако можно представить и такие случаи, в которых преступник на постоянной основе распространяет заведомо ложные сведения, порочащие честь и достоинство другого лица. В таком случае необходимо обратить внимание на последствия данного деяния.

Как уже отмечалось, интернет-преследование следует рассматривать в качестве материального состава преступления, в то время как клевета является формальным составом, для совершения которого достаточно самого распространения таких сведений. Если в результате систематического распространения таких сведений лицу не был нанесен какой-либо вред (в том числе, если не будет доказано, что эти действия подорвали его деловую репутацию), данное деяние следует квалифицировать по по ч.2 ст. 128.1 УК РФ. При этом необходимо помнить о целях, которые преследует кибersталкер: подрыв деловой репутации сам по себе не является его целью, главной целью остается постановка жертвы в такое положение, в котором она будет испытывать страх, тревогу, угрозу безопасности, стыд и другие чувства, способные существенно изменить ее поведение.

---

[47]Б. был признан виновным в угрозе убийством потерпевшему, у которого имелись основания опасаться осуществления этой угрозы. По приговору мирового судьи судебного участка № 32 Шадринского судебного района Курганской области от 18 июня 2020 г. (оставленному судами апелляционной и кассационной инстанций без изменения) Б. осужден по ч. 1 ст. 119 УК РФ.

В кассационной жалобе адвокат в защиту интересов осужденного просил отменить приговор и вынести оправдательный приговор в связи с отсутствием в действиях Б. состава преступления. В жалобе указано, что описание объективной стороны деяния, признанного судом доказанным, заключается в нанесении побоев потерпевшему без квалифицирующих признаков, предусмотренных ст. 116 и 116.1 УК РФ, и образует состав административного правонарушения.

Судебная коллегия по уголовным делам Верховного Суда Российской Федерации 22 июля 2021 г. отменила приговор и все последующие судебные решения в отношении Б. и дело передала на новое судебное разбирательство в суд первой инстанции иным составом суда, указав следующее: «Статьей 119 УК РФ предусмотрена уголовная ответственность за угрозу убийством или причинением тяжкого вреда здоровью, если имелись основания опасаться осуществления этой угрозы. Из приговора усматривается, что угроза убийством выражалась в том, что осужденный в ходе конфликта с потерпевшим Т., имея умысел на создание реальной угрозы жизни и здоровью Т., умышленно нанес удары руками, металлическим предметом и ногами по различным частям тела потерпевшего, что явилось недостаточным для квалификции деяний по статье 119 УК РФ».

В приведенном выше деле даже нанесение телесных повреждений может не явиться основанием опасаться убийства. Данный состав имеет место только в случае, если можно с уверенностью сказать о том, что лицо намеревается именно убить, что достаточно сложно. Поэтому частые ситуации, в которых жертвам пишут угрозы убить ее или членов ее семьи почти никогда не подпадают под состав, указанный в статье 119 УК РФ, ввиду невозможности доказать, что имелись основания опасаться осуществления этой угрозы.

[48]«Обзор судебной практики Верховного Суда Российской Федерации № 3 (20210» (утв. Президиумом Верховного Суда РФ 10.11.2021), п. 48

В силу сложностей квалификации и отделения уже существующих составов от предполагаемого отдельного состава «Преследование», ученые предлагали вместо введения отдельной статьи внести изменения в существующие статьи.

Например, в своей работе[49] к.ю.н., доцент кафедры уголовного права Университета имени О.Е. Кутафина (МГЮА), И.А. Юрченко, представляла проект внесения изменений в Уголовный Кодекс РФ посредством расширения содержания статьи 137 «Нарушение неприкосновенности частной жизни» и добавления конкретизирующих ее содержание статей 137.1 и 137.2. о незаконном собирании и распространении сведений, составляющих личную и (или) семейную тайну, а также профессиональную тайну лица. Отдельные пункты в этих статьях по возможности полно охватывают угрозы сталкинга и кибersталкинга, а именно в пунктах:

«1. Незаконное вмешательство в какой бы то ни было форме в частную жизнь лица без его согласия – наказывается…
2. То же деяние, совершаемое **систематически,** — наказывается...

3. Деяния, указанные в частях первой и второй настоящей статьи:

а) совершенные **с использованием специальных и иных технических средств**, предназначенных для негласного получения информации, либо с использованием информационно-телекоммуникационных сетей, **включая сеть Интернет, а также в средствах массовой информации**»

В такой конструкции статья предполагает, что за причинение лишь эмоционального или психологического вреда лицо уже будет привлечено к уголовной ответственности за оконченное преступление.

Но, к сожалению, на практике происходит так, что помощь жертве правоохранительные органы оказывают только при наступлении более тяжких последствий, когда сталкер уже совершил более существенные деяния, которые можно квалифицировать по действующим статьям УК РФ.

В следующем разделе будут более подробно проанализированы и изложены предложения по совершенствованию законодательства о сталкинге и кибersталкинге, ведь из уже проведенного исследования явствует необходимость в разрешении этого пробела в праве.

[49]Юрченко Ирина Александровна Сталкер как субъект уголовной ответственности // Вестник Университета имени О. Е. Кутафина. 2018. №12 (52). URL: https://cyberleninka.ru/article/n/stalker-kak-subekt-ugolovnoy-otvetstvennosti (дата обращения: 25.05.2024).

VIII. Предложения по совершенствованию законодательства о сталкинге (слежке) и кибersталкинге (интернет-слежке) в России.

Как уже отмечалось ранее, юридической ответственности за сталкинг, а тем более кибersталкинг в России не установлено, это существенно усложняет процедуру квалификации деяний, посягающих на неприкосновенность частной жизни. Существовали попытки разрешения этого пробела как научным сообществом, так и представителями органов государственной власти. А именно были разработаны предложения по установлению мер административной или уголовной ответственности.

В предыдущем разделе были перечислены различные составы преступлений, по которым могут квалифицироваться формы сталкинга и кибersталкинга, однако наиболее близким составом преступления представляется «Нарушение неприкосновенности частной жизни» (статья 137 УК РФ).

Так, к.ю.н., доцент кафедры уголовного права Университета имени О.Е. Кутафина (МГЮА), И.А. Юрченко, чья позиция представлена в предыдущем разделе, в своей работе предложила достаточно широкую формулировку, объединяющую существующую статью 137 УК РФ и деяния, которые в науке признаются сталкингом и кибersталкингом. Но сама конструкция состава статьи 137 УК РФ по объективной стороне является формальной, то есть наказывается сам факт незаконного собирания данных. При этом отсутствует ужесточенная санкция за материальный состав (за совершение действий с использованием полученных данных, повлекших негативные последствия для жертвы), что зачастую и является основной целью сталкера и кибersталкера. Таким образом, позиция И.А. Юрченко урегулирует проблему преследования только в её небольшой части, связанной с незаконным собиранием данных.

Однако, многие рассмотренные в предыдущих разделах примеры слежки и интернет-слежки связаны с законным собиранием личных данных, через открытые источники информации. Сохранение опубликованных в социальных сетях фотографий, номера телефона и других сведений, которые

агрессор узнал из открытого цифрового профиля потенциальной жертвы. При таких методах собирания данных невозможно привлечение к юридической ответственности, за исключением случаев, когда за собиранием следуют действия, повлекшие негативные последствия для жертвы.

Таким образом, все действия, подходящие под определение интернет-слежки, невозможно законодательно урегулировать без введения отдельной статьи в закон, например, связанной с законным собиранием данных и дальнейшим их использованием, повлекшим негативные последствия.

При этом введение отдельных статей, определяющих ответственность за сталкинг и кибersталкинг, научному сообществу[50] видится нецелесообразным, так как это только создаст излишние сложности в квалификации деяний, которые внешне похожи на уже существующие составы, но при этом поглощаются понятием сталкинга или кибersталкинга.

Несмотря на эти доводы, еще одна модель законодательного закрепления кибersталкинга была предложена в 2024 году представителями органа государственной власти, а именно депутатами партии ЛДПР. Сейчас законопроект[51] находится на стадии предварительного рассмотрения Государственной Думой ФС РФ. В законопроекте предлагается ввести именно отдельную статью в Кодекс РФ об административных правонарушениях в следующей редакции:

«Статья 5.61. Преследование:

1. Преследование – систематическое совершение гражданином действий, направленных на причинение преследуемому гражданину нравственных страданий, выразившееся в попытках общения при явно выраженном несогласии преследуемого гражданина, в имеющих целью

[50]Юрченко Ирина Александровна Сталкер как субъект уголовной ответственности // Вестник Университета имени О. Е. Кутафина. 2018. №12 (52). URL: https://cyberleninka.ru/article/n/stalker-kak-subekt-ugolovnoy-otvetstvennosti (дата обращения: 25.05.2024).

[51]Законопроект № 671685-8 «О внесении изменения в Кодекс Российской Федерации об административных правонарушениях» (в целях установления административной ответственности за преследование, т.е. систематическое совершение лицом действий, направленных на причинение преследуемому им гражданину нравственных страданий). URL: https://sozd.duma.gov.ru/bill/671685-8 (дата обращения: 25.05.2024).

причинить преследуемому гражданину беспокойство демонстрацией присутствия, направлении либо оставлении сообщений, в злоупотреблении правом свободно искать, получать, передавать, производить и распространять информацию о преследуемом гражданине и его близких родственниках, если такие действия не содержат уголовно наказуемого деяния, –

влечет предупреждение или наложение административного штрафа в размере двух тысяч рублей.

2. Те же действия, совершенные с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет» –

влекут наложение административного штрафа в размере трех тысяч рублей.

3. Совершение административного правонарушения, предусмотренного частью 1 или 2 настоящей статьи, гражданином, ранее подвергнутым административному наказанию за аналогичное административное правонарушение, –

влечет наложение административного штрафа в размере пяти тысяч рублей либо административный арест на срок до пятнадцати суток».

Однако, содержание этой статьи абсолютно не раскрывает вопрос о методах собирания данных о жертве. Создается впечатление, что в этой трактовке понятий «преследование» и «интернет-преследование» не предусмотрен этап собирания информации, который является конструирующим, позволяет отделить это деяние от остальных составов.

Исходя из всего вышесказанного, можно сделать вывод о невозможности на сегодняшний день подобрать оптимальную модель установления юридической ответственности за преследование и интернет-преследование ввиду существования множества форм и проявлений этой угрозы, которые частично подпадают под действие других норм уголовного или административного закона. Более того, не все формы слежки и интернет-слежки наказуемы в силу недостаточно высокой степени общественной опасности.

При этом, сталкинг и кибersталкинг – это серьезные угрозы, которые могут нести тяжкие последствия для преследуемого, поэтому возможно предложить модель поступательного урегулирования их отдельных форм. Предлагается начать с введения в законодательство общих дефиниций «преследование» и «интернет-преследование», а также предусмотреть специальные профилактические меры противодействия тем актам слежки, которые связаны с законным собиранием личных данных, ведь именно за эти формы несоразмерно привлечение к уголовной или административной ответственности.

Изучая вопрос того, в какой нормативный правовой акт необходимо интегрировать понятия, было обращено внимание и на обсуждаемую сегодня проблему травли и интернет-травли в молодежной среде. Сейчас депутатами комитета по молодежной политике Государственной Думы ФС РФ рассматриваются различные законодательные модели противодействия этим угрозам[52]. В одном из предыдущих разделов было обозначено, что угрозы интернет-травли и интернет-слежки имеют достаточно общих черт, а некоторые считают, что одной из форм кибербуллинга является кибersталкинг[53]. Исходя из этого, введение понятия «кибersталкинг» как одной из форм кибербуллинга может положить начало борьбе с этой угрозой информационной безопасности. Поэтому видится разумным создание отдельного федерального закона «О противодействии травле и интернет-травле», который будет помимо понятий «травля» и «интернет-травля» раскрывать специфику разных их форм и проявлений, например, кибersталкинга, предусматривать специальные профилактические мероприятия в отношении несовершеннолетних и их родителей, а также «мягкие» механизмы ответственности, действующие для проявлений, не наказуемых УК РФ или КоАП РФ.

[52]В Думе предложили «курс исправления» для школьных буллеров и их родителей. URL: https://www.rbc.ru/society/22/09/2024/66ed88bf9a79473763592490 (дата обращения: 25.05.2024).
[53]Профилактика кибермоббинга и кибербуллинга в среде несовершеннолетних: методическое пособие / Т.А. Дёгтева и др. – Ставрополь: Ставропольское издательство «Параграф», 2017 г, С.- 9

В качестве определения предлагается следующая формулировка: «Интернет-преследование – одна из форм интернет-травли, выражающаяся в собирании личных данных и их использовании против преследуемого лица с целью причинить психологический, а в будущем и иной вред демонстрацией присутствия, попытками установления коммуникации, распространением этих данных среди третьих лиц посредством использования Интернета и информационных технологий».

Предполагается, что при принятии подобного федерального закона, общие для кибербуллинга и кибersталкинга признаки (например, систематичность) должны быть встроены в общее понятие интернет-травли, а понятие интернет-преследования должно включать специфические для этой угрозы черты и проявления.

Таким образом, отдельный закон позволит учесть специфику интернет-слежки как формы интернет-травли, а также ввести постепенно для начала «мягкие» механизмы противодействия этой угрозе для дальнейшего внедрения в законодательство мер ответственности за формы интернет-слежки, связанные именно с незаконным собиранием данных о преследуемом лице.