УДК 316.4
DOI: 10.19181/snsp.2025.13.1.8
EDN: GVLOLM

Научная статья

КИБЕРСТАЛКИНГ КАК СОВРЕМЕННАЯ УГРОЗА ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ: МЕРЫ ПРОТИВОДЕЙСТВИЯ В РОССИИ И ЗА РУБЕЖОМ

Елена Викторовна Ларина
Институт социологии ФНИСЦ РАН,
Москва, Россия,
elena_shulgina@inbox.ru,
ORCID 0000-0002-4928-4388

Для цитирования: *Ларина Е. В.* Кибersталкинг как современная угроза общественной безопасности: меры противодействия в России и за рубежом // Социологическая наука и социальная практика. 2025. Т. 13, № 1. С. 170–189. DOI 10.19181/snsp.2025.13.1.8. EDN GVLOLM.

Аннотация. Информационно-телекоммуникационные технологии в современном мире становятся неотъемлемой частью социальной реальности, пронизывая все сферы общества. Такая тенденция, помимо безусловного прогресса в разных отраслях, ведёт и к возникновению новых вызовов и угроз, среди которых распространение различных форм кибердевиантности, представляющих опасность как для индивида, так и для общества в целом. Свидетельством актуальности рассматриваемой проблемы являются данные статистики российских правоохранительных органов об увеличении количества преступлений в сфере компьютерной информации, опубликованные сведения одной из ведущих компаний в сфере информационной безопасности о количестве жертв преследования в интернете в разных странах, а также увеличение числа выявленных приложений, направленных на осуществление сталкинга в виртуальном пространстве. Статья посвящена анализу феномена кибersталкинга как одной из наиболее агрессивных форм проявления отклоняющегося поведения в сети интернет, а также оценке мер противодействия рассматриваемому деянию, применяемых в различных странах мира. Распространение кибersталкинга угрожает защищённости, личной, информационной, финансовой безопасности граждан, таким образом создавая риски всей общественной безопасности. В рамках исследования произведён аналитический обзор действующих стратегий защиты безопасности населения в цифровой среде в разных странах мира, в частности, в США, Великобритании, Германии, Сингапуре, Индии, Китае, Японии и др. Рассмотрен статус кибersталкинга в Российской Федерации, а также существующие в отношении него меры противодействия. Обозначены наиболее широко применяемые в мировой практике механизмы борьбы с агрессией в сети. На основании изложенного сделан вывод о целесообразности применения наиболее эффективных мер противодействия кибersталкингу, успешно функционирующих за рубежом, для защиты российского населения в виртуальном пространстве.

Ключевые слова: кибersталкинг, преследование, агрессия, виртуальное пространство, жертва, безопасность, меры противодействия

Введение

Проникновение цифровых технологий во все сферы жизни современного общества, помимо несомненных преимуществ, ведёт и к появлению новых угроз для общественной безопасности. Согласно опубликованным данным Министерства внутренних дел РФ за период январь – декабрь 2023 г., общее количество преступлений, совершённых с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации выросло на 29,7% по сравнению с аналогичным периодом прошлого года. Прирост преступлений в этой сфере составил 270%, в том числе количество случаев неправомерного доступа к компьютерной информации увеличилось на 295,2%, мошенничества – на 41,3%. В общем объёме зарегистрированных преступлений доля совершённых с использованием информационно-телекоммуникационных технологий составляет 34,8%, что превышает аналогичный показатель предыдущего года (26,5%) [1]. Таким образом, преступления в сети представляют реальную угрозу для современного общества. Наибольшую опасность при этом несут действия, совершённые с помощью информационных технологий и направленные на причинение психологического и зачастую физического вреда жертве. Одним из них является киберсталкинг. Острота проблемы актуализирует запрос на комплексный анализ феномена преследования граждан в сети интернет.

Цель статьи заключается в социологическом анализе феномена киберсталкинга как угрозы для безопасности современного общества, обобщении и оценке эффективности мер предотвращения и противодействия данному явлению в российской и зарубежной практике.

Методологическая база исследования

В официальных документах общественная безопасность понимается как «состояние защищённости человека и гражданина, материальных и духовных ценностей общества от преступных и иных противоправных посягательств, социальных и межнациональных конфликтов, а также от чрезвычайных ситуаций природного и техногенного характера»[2]. В научном сообществе понятие общественной безопасности трактуется в широком и узком смысле. И. Е. Ильичёв и Э. В. Богмацера в своём исследовании в качестве широкого понимания общественной безопасности приводят состояние защищённости личности и общества от совокупности различных по характеру угроз, в качестве узкого – состояние

[1] Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2023 года // Министерство внутренних дел Российской Федерации : офиц. сайт. 20 января 2024 г. URL: https://мвд.рф/reports/item/47055751/ (дата обращения: 18.02.2024).

[2] Концепция общественной безопасности в Российской Федерации : утв. Президентом РФ 14 ноября 2013 года № Пр-2685 // Электронный фонд правовых и нормативно-технических документов : сайт. URL: https://docs.cntd.ru/document/499059750 (дата обращения: 11.03.2024).

защищённости жизни и здоровья граждан, а также интересов общества от противоправных посягательств в общественных местах законными мерами [1]. Кибersталкинг напрямую посягает на безопасность человека, причём не только в киберпространстве, но и в реальности, наносит ущерб правам и свободам человека и гражданина, прежде всего на неприкосновенность частной жизни. На эти представления автор опирался при формировании методики исследования, результаты анализа данных которого представлены в статье.

Базовой составляющей методики проведённого исследования были сбор, систематизация и анализ материалов оригинальных научных исследований по изучаемой проблематике при помощи специализированных информационно-поисковых систем. Произведён обзор статистических данных и нормативных актов, направленных на противодействие преследованию в офлайн- и онлайн-пространстве. Проанализированы результаты актуальных исследований учёных государственных университетов США (Г. Диллон, К. Дж. Смит), Великобритании (А. Давидович, К. Талбот, К. Брукфилд и др.), Турции (Б. Кукул), Индии (Л. Миноча), Сингапура (Т. Наир), Китая (Ю. Чжан, Ч. Ван, Т. Ву), данные агентств по оказанию помощи жертвам киберпреступлений, специалистов в области зарубежного права (Т. Исиара), компаний в сфере информационной безопасности. Представлены материалы российских исследований, посвящённых феномену кибersталкинга (Я. О. Кучина, Р. Д. Сулейменова, О. Зипельмайер и др.).

Теоретической рамкой исследования является концепция «общества риска», представленная в работах У. Бека [2]. «Общество риска» характеризуется высоким уровнем технологического развития, потребления, а также размыванием границ нормы и отклонения, что сопровождается появлением новых угроз и ростом напряжения в различных сферах жизни. Релятивизм в отношении допустимости тех или иных форм поведения в современном обществе, в частности, проявляется в отсутствии единой оценки уровня опасности преследования людей в виртуальном пространстве. Так, в одних странах в качестве наказания за кибersталкинг предусмотрена уголовная ответственность, в других же данное деяние вообще не криминализировано.

Цифровизация современного мира всё чаще становится предметом исследования в контексте проблем безопасности. Я. И. Гилинский фиксирует переход значительной части преступности в киберпространство, обусловленный высоким уровнем латентности совершения криминальных деяний, большими возможностями сохранения анонимности и ухода от ответственности лиц, совершающих правонарушения [3]. Д. Лаптон анализирует взаимодействие человека и персональных данных, оставляемых им в цифровом пространстве. Такие цифровые персональные данные являются источником информации о людях и способны вносить корректировки в принятые решения, совершения действий этими людьми и по отношению к этим людям, тем самым оказывая влияние на их жизнь в целом. Отсюда с цифровизацией связаны значительные риски, которые необходимо учитывать, оставляя цифровые следы в виртуальном

пространстве [4]. Д. Н. Карпова рассматривает социальную цифровизацию как процесс, который ставит условия существования общества в зависимость от цифровых технологий. Одним из признаков социальной цифровизации становится появление ненамеренных и практически неконтролируемых последствий, что оказывает значительное влияние на общественные отношения, в том числе в сфере безопасности [5]. Ю. Ю. Комлев исследует повсеместное внедрение информационных технологий с точки зрения значительной криминальной угрозы, которую несут в себе киберпреступления, достигшие массового уровня [6]. Он определяет киберпреступность как «множество проявлений негативной кибердевиантности, состоящих в нарушении уголовно-правовых запретов с использованием компьютеров, цифровых технологий и обращённых против компьютерных систем, социальных сетей и их пользователей» [7]. Е. С. Иванова, А. Н. Евдокимова отмечают, что кибербезопасность становится одной из наиболее значимых отраслей современных обществ. Повсеместное использование во всех сферах жизнедеятельности человека информационно-телекоммуникационных технологий привело к уязвимости от различных воздействий в цифровой среде, которые могут быть направлены как на государственную инфраструктуру, предприятия, так и на отдельно взятых граждан [8]. Таким образом, повышение уровня кибербезопасности приобретает важное значение для защиты прав и свобод населения на современном этапе общественного развития.

Результаты исследования

Масштабы распространения и формы киберсталкинга как угрозы для безопасности современного общества. В соответствии с одним из наиболее полных определений киберсталкинг – это «продолжительное навязчивое поведение лица, состоящее из множества повторяющихся действий, направленных на насильственное установление контакта с объектом интереса и навязывание ему общения, совершаемое с использованием возможностей виртуальной среды на основе постоянного отслеживания действий жертвы, сбора информации о ней и её окружении, влекущее причинение морального и психического вреда, а также способное повлечь иные тяжкие последствия» [9, с. 50].

Исследователи-правоведы П. Н. Кобец, К. А. Краснова определяют киберсталкинг как преследование какого-либо лица при помощи интернета и других электронных устройств, включающее в себя угрозы с целью доведения преследуемого до истощения от перенапряжения нервной системы [10, с. 78]. Общественная опасность киберсталкинга заключается в насильственном вторжении в частную жизнь жертвы, наличии оснований у преследуемого опасаться за свою жизнь и здоровье. Научное понимание киберсталкинга через призму психологии содержит описание эмоций, испытываемых жертвой: «киберсталкинг – использование электронных средств для преследования жертвы через повторяющиеся сообщения или звонки, вызывающие страх, тревогу

и раздражение» [11]. С социологической точки зрения, кибersталкинг рассматривается как одна из форм цифровых девиаций, которая носит трансграничный характер и направлена не на компьютерное устройство, а на реального человека – пользователя интернета [7]. Такие цифровые формы девиантного поведения несут в себе большую угрозу для общественной безопасности за счёт расширения группы риска, на которую могут быть направлены, по сравнению с девиациями в офлайн-пространстве [12], а также по причине отсутствия чётко установленных принудительных правовых мер, пресекающих такие деяния.

Таким образом, кибersталкинг – это не только одна из форм девиантного поведения, требующая профилактических мер, данный феномен включает и криминологический аспект, т. е. является преступлением, поскольку нарушает одно из главных прав человека, закреплённых в конституции – право на неприкосновенность частной жизни, а также несёт угрозу психологическому и физическому здоровью преследуемого.

Официально статистика относительно количества случаев кибersталкинга в России не ведётся. По данным одной из крупнейших компаний в сфере информационной безопасности «Лаборатория Касперского», во всём мире число пострадавших от кибersталкинга пользователей в 2022 году составило 29 312 человек, что в целом соответствует аналогичному показателю 2021 года [1]. Однако в полученное количество включены лишь пользователи продукции данной компании, а реальное число пострадавших может быть несоизмеримо больше.

По имеющимся данным, в 2022 году ежемесячно в среднем 3 333 человека становились новыми жертвами преследования: пик пришёлся на март – 3 891 человек и январь – 3 685 человек, спад – на июль – 2 930 человек и июнь – 2 969 человек [2].

С 2019 года, в соответствии с данными «Лаборатории Касперского», тройка стран – лидеров по количеству случаев кибersталкинга, остаётся неизменной: Россия, Бразилия, Индия. Причём в 2022 году по числу пострадавших Россия существенно опережает остальные страны – 8 281 человек (Бразилия – 4 969 человек, Индия – 1 807 человек). Для сравнения, по данным того же источника, количество жертв преследования в 2022 году в Европе – 3 158 человек, в США – 1 585 [3].

По данным исследователей среди жертв, подвергшихся кибersталкингу, преобладают женщины и молодёжь 18–29 лет [13]. В соответствии с результатами опроса американского Центра помощи предотвращения и информирования о преследовании (SPARC), примерно каждая третья женщина и каждый шестой мужчина подвергались преследованию [4]. Статистическая информация, пред-

[1] О состоянии сталкерского ПО в 2022 году // securelist by Kaspersky : сайт. URL: https://securelist.ru/the-state-of-stalkerware-in-2022/106956 (дата обращения: 01.02.2024).
[2] Там же.
[3] Там же.
[4] Fact sheets & infographics // SPARC : сайт. URL: https://www.stalkingawareness.org/fact-sheets-and-infographics/ (дата обращения: 29.01.2024).

ставленная в исследовании «Технологии защиты детей в интернете», также подтверждает, что жертвами большинства различных проявлений кибersталкинга чаще становились женщины, хоть и не всегда с большим перевесом (см. табл. 1).

Таблица 1

Распределение по полу жертв различных проявлений кибersталкинга, %

Проявления кибersталкинга	Пол	
	Мужчины	Женщины
Сексуальные домогательства в интернете	26,1	73,9
Навязчивые попытки установить контакт онлайн	26,6	73,4
Сталкеринг с использованием идентичности других людей	46,4	53,6
Домогательства в интернете (не сексуального характера)	47,7	52,3
Угрозы	53,8	46,2

Источник данных: исследование «Технологии защиты детей в интернете»[1]. В таблице приводятся доли мужчин и женщин в общем количестве проявлений каждого вида.

Кибersталкинг, как правило, осуществляют люди в той или иной степени знакомые со своей жертвой. В то же время, в среднем около трети (32,6%) выбирают в качестве цели преследования незнакомцев [2]. Среди кибersталкеров преобладают мужчины различного возраста. Так, например, по данным европейского исследования подростков от 16 до 19 лет (N=8000) 27% из них осуществляли киберпреследование в течение последнего года [3]. Что касается личностных характеристик кибersталкеров, то, как правило, такие люди испытывают трудности в установлении социальных контактов, склонны к проявлению агрессии и зависти [4]. По данным исследования, включающем психодиагностику 137 сталкеров, лишь у 28% из них не было выявлено никаких признаков психических расстройств. Остальные 72% характеризовались теми или иными расстройствами психики, наиболее распространённые из которых – антисоциальные, нарциссические, пограничные личностные расстройства (более 50%), алкогольная и/или наркотическая зависимость (46%), тревожный невроз/аффективные расстройства (31%), психоз (10%) [14].

---

[1] Исследование «Технологии защиты детей в интернете». 2022. URL: https://www.company.rt.ru/social/kids-safety/Технологии_защиты_детей_Результаты_исследования.pdf (дата обращения: 04.02.2024).

[2] Там же.

[3] *Milmo D.* Risky online behaviour “almost normalized” among young people, says study // The Guardian : сайт. 5 декабря 2022 г. URL: https://www.theguardian.com/technology/2022/dec/05/risky-online-behaviour-almost-normalised-among-young-people-says-study (дата обращения: 05.02.2024).

[4] *Григорьевых А.* «Я знаю о тебе всё». Что такое кибersталкинг и как защититься от преследований в интернете // Такие дела : сайт. 29 сентября 2023 г. URL: https://takiedela.ru/notes/ya-znayu-o-tebe-vse-chto-takoe-kiberstal/ (дата обращения: 05.02.2024).

На современном этапе развития информационно-телекоммуникационных технологий появилось большое количество средств, при помощи которых стало возможным достаточно легко осуществлять преследование: специальные программы и приложения для прослушки разговоров и чтения переписок, удалённое получение доступа к камерам видеонаблюдения, установленным в общественных местах, мониторинг фото- и видеоматериалов, точек геопозиции, выкладываемых в виртуальных социальных сетях, и др. В открытом доступе можно найти специальные сталкерские программы, направленные на сбор разнообразных сведений о жертве преследования: от текстовых сообщений и фотографий до конкретных координат местонахождения выслеживаемого устройства. Причём обнаружить такие программы на гаджетах жертв достаточно сложно ввиду их работы в фоновом режиме, незаметном для неподготовленных пользователей. В 2023 году специалистами было выявлено 182 различных сталкерских приложения, чаще всего распространяемых под видом программ, предназначенных для осуществления родительского контроля или для защиты безопасности гаджета [1].

Противодействие кибersталкингу в России и в зарубежной практике. В целях противодействия кибersталкингу в разных странах мира применяется широкий диапазон мер от простого информирования о возможности столкнуться с данной опасностью до уголовного наказания агрессора.

Безусловно, одним из наиболее серьёзных направлений противодействия преследованию в интернете является правоприменительная практика, предусматривающая различные виды ответственности от денежного штрафа до реального лишения свободы. Так, в Канаде преследование было криминализировано ещё в 1993 году. Уголовная ответственность, в соответствии с законом, наступает за такие действия, как постоянно повторяющиеся звонки со сбросом после снятия трубки, нежелательный поток рассылок текстовых и голосовых сообщений, навязывание контакта в интернете, выведывание персональных данных через знакомых жертвы и др. [15]. В Великобритании среди законов, направленных на борьбу с киберпреступностью, выделяют Закон о вредоносных коммуникациях, принятый в 1988 году, и Закон о защите от преследования 1997 года. В качестве вредоносных коммуникаций упомянутый закон квалифицирует отправку одним лицом другому определённых предметов и/или сообщений неприличного или оскорбительного характера, содержащих угрозу или заведомо ложную информацию, с целью вызвать беспокойство или причинить страдания [16]. В Японии национальный закон против преследования был принят в 2000 году. С тех пор он периодически дополнялся посредством включения новых способов преследования. Сначала он содержал запрет на преследования офлайн, а также при помощи повторяющихся телефонных звонков, затем произошло включение электронной почты и далее платформ социальных сетей в качестве инструментов преследования. Дополненный закон криминализировал как повторную отправку сообщений в социальных сетях при условии, что

[1] О состоянии сталкерского ПО в 2022 году // securelist by Kaspersky : сайт. URL: https://securelist.ru/the-state-of-stalkerware-in-2022/106956 (дата обращения: 01.02.2024).

получатель не хочет их получать, так и оставление нежелательных комментариев. В 2014 году был принят Основной закон о кибербезопасности, который лежит в основе всей политики Японии по борьбе с преступностью в сети [17]. С 2007 года сталкинг является уголовно наказуемым в Германии. В качестве преступления рассматриваются различные действия, которые можно отнести к преследованию, в частности ограничение привычного образа жизни жертвы, попытки установить контакт при помощи средств связи или третьих лиц, угрозы причинения вреда жизни, здоровью и свободе преследуемого. Даже намерение агрессора повлиять на образ жизни жертвы квалифицируется в качестве преступления. Кроме того, в тексте закона содержится пункт, указывающий, что список перечисленных действий не является исчерпывающим и может быть дополнен в каждом конкретном случае [16]. В 2022 году преследование было официально внесено в Уголовный кодекс Турции как преступление, характеризующееся постоянным причинением одним лицом серьёзного беспокойства другому лицу за свою безопасность или безопасность своих родственников посредством осуществления физической слежки или попыток установления контакта при помощи любых средств связи, информационных систем или третьих лиц. За данное деяние предусмотрено наказание в виде лишения свободы на срок от шести месяцев до двух лет [16]. В Сингапуре в 2022 году был обновлён ряд законодательных актов, касающихся преступлений против личности. В них добавлены положения о совершении преступлений онлайн. Так, в соответствии с Законом о защите от преследований, акты кибersталкинга, публикация частной информации о лице в интернете со злым умыслом (доксинг) теперь квалифицируются как преступления и предусматривают наказание в виде значительных штрафов и/или лишения свободы. Отдельно был принят Закон о преступном вреде в интернете, который содержит список конкретных правонарушений и наделяет правительство более широкими полномочиями в сфере борьбы с преступной деятельностью в сети [18].

В Индии наиболее широко применяемым против кибersталкинга является Закон об информационных технологиях, в соответствии с которым нарушение конфиденциальности и неприкосновенности частной жизни в виртуальном пространстве наказывается тюремным заключением до двух лет и/или существенным денежным штрафом [19]. Однако исследователи утверждают, что данный закон, принятый ещё в 2008 году, не защищает население от агрессии в сети. В качестве мер, повышающих эффективность противодействия киберпреступности, индийские эксперты указывают на необходимость ужесточения наказания – киберпреследование должно быть признано тяжким преступлением, за совершение которого следует увеличить тюремное заключение до семи лет и повысить взыскание минимального штрафа в 20 раз. Кроме того, необходимо реформировать сам текст закона, который не распространяется на преследование мужчин со стороны женщин и/или других мужчин. Язык закона делает его конкретным для преследователя мужчины и жертвы женщины. В качестве преступления не рассматриваются угрозы. Несмотря на серьёзный вред состоянию

физического и психологического здоровья жертвы, который наносят сами угрозы совершения преступления, необходимо дождаться их реализации. Более того, если совершённое киберпреследование не повлекло за собой таких значительных последствий, как преступление сексуального характера, кража личных данных, террористические акты, то преступник подлежит освобождению под залог [19]. Помимо реформирования законодательства, в целях упрощения борьбы со случаями киберпреследования упоминается также необходимость сокращения количества посещений жертвой отдела полиции, сохранение конфиденциальности пострадавших для их защиты от социальной стигматизации, предоставление возможности подавать жалобы онлайн [19].

В Китае нет единого закона, охватывающего различные формы кибersталкинга, однако есть положения о кибербезопасности, закреплённые в конституции. К ним относятся нарушения прав на личную информацию, намеренное занесение в компьютерную систему вирусов, установка шпионских программ и др. По данным положениям предусмотрено наказание в виде штрафа, ареста и тюремного заключения. В 2017 году был принят специальный закон, регулирующий сбор, хранение и передачу личных данных сетевыми операторами. Этот закон устанавливает строгие требования к локализации данных и ограничения на трансграничную передачу личной информации и других важных сведений [20].

Не менее значимым направлением противодействия кибersталкингу является комплекс реабилитационных мер для пострадавших. В США работают сайты агентств по оказанию помощи жертвам различных преступлений, в частности кибersталкинга. Они содержат практические советы по предотвращению опасного поведения в сети, с которыми в свободном доступе может ознакомиться любой желающий. Среди них рекомендации создавать двухфакторную аутентификацию, избегать отправку личной информации через общедоступный Wi-Fi, использовать антивирусное и антишпионское программное обеспечение для периодического сканирования компьютера, закрывать веб-камеру, когда она не используется, и др. Предоставляется телефон горячей линии, куда можно обратиться за помощью в случае столкновения с киберпреследованием [1]. В Великобритании функционируют различные организации поддержки жертв преследования. К ним относятся, например, Сеть по борьбе с преследованием (Network for surviving stalking), Защита от преследования (Protection against stalking). Действует бесплатная Национальная линия помощи жертвам преследования. Министерство юстиции при правительстве Великобритании оказывает помощь пострадавшим и предоставляет рекомендации на всех этапах – от сообщения о преследовании до поиска поддержки на местном уровне [19]. В Берлине уже больше десятилетия функционирует консультативный центр, специализирующийся на сталкинге – Stop-Stalking. Причём данный центр предоставляет консультирование и психологическую поддержку не только жертвам, но и самим преследователям.

[1] *Wendell T.* Eight Tips to Protect Yourself from Cyberstalking // SafeHorizon : сайт. URL: https://www.safehorizon.org/stories/protect-yourself-from-cyberstalking/ (дата обращения: 08.02.2024).

В центре оказывают свои услуги психологи, социальные педагоги и юристы. Вся помощь для пострадавших оказывается бесплатно и защищается законом о неразглашении сведений частной жизни. Ежегодно в центр обращаются около 500 жертв и 120 агрессоров [14]. Среди предпринимаемых мер в Сингапуре следует выделить создание специальных онлайн-сообществ в целях обеспечения эмоциональной поддержки людей, имеющих травмирующий опыт, обсуждения волнующих вопросов, обмена жизненными историями и формирования чувства общности пострадавших [18]. Создан специализированный центр поддержки жертв онлайн-ущерба, призванный обеспечить комплексную помощь и безопасное пространство, в который могут обратиться те, кто столкнулся с агрессивным поведением в сети. Данный центр имеет свою телефонную линию помощи, линию текстовых сообщений, команду профессиональных специалистов, оказывающих бесплатные консультационные услуги и юридическую помощь.

Отдельно следует отметить, что в Японии предусмотрены специальные социальные программы для сталкеров. Так, например, программа STEP направлена на образование и реабилитацию выявленных и осуждённых сталкеров. Специалисты данных программ подчёркивают необходимость остановить и «перевоспитать» агрессоров, пока их действия не привели к ещё более серьёзным последствиям [19].

Один из блоков мер профилактики кибersталкинга в разных странах представлен организацией информационно-просветительских программ. В Великобритании много внимания уделяется обучению различных социальных групп в сфере информационно-коммуникационных технологий. Так, подчёркивается важность формирования у молодёжи соответствующих навыков и различных способов вмешательства, если они стали свидетелями преступления в сети, предоставляется обратная связь, т. е. конкретная информация о случаях, когда и как подобное вмешательство помогало жертвам [21]. Исследователи также предлагают создать специальные группы социальных работников, обладающих навыками и знаниями в сфере IT-технологий, которые будут консультировать жертв кибер-агрессоров, в частности, по таким вопросам, как безопасно дистанцироваться от преследователя в цифровом пространстве, адекватно оценить возможный риск, не допустить эскалации насилия [22]. В американскую образовательную систему включены различные программы профилактики. Одна из наиболее широко распространённых из них – DARE. Изначально она была разработана для борьбы с потреблением наркотиков и их негативными последствиями, в настоящий момент данная программа включает в себя уроки по безопасности в интернете. В США также действуют различные специализированные некоммерческие организации. Например, работа организации Enough is Enough направлена на повышение осведомлённости общественности об опасностях в сети и способах противодействия им [1]. Сеть поддержки против киберпреступности (Cybercrime Support

[1] Who we are: our mission // Enough is Enough : сайт. URL: https://enough.org/aboutus (дата обращения: 08.02.2024).

Network) предоставляет помощь и консультации частным лицам и организациям до, во время и после случаев столкновения с киберпреступлениями [1].

Американские исследователи делают акцент на сильной системе ценностей, разработанной для противодействия киберпреследованию. Они считают, что такая система может помочь сдерживать преступную деятельность в сети. Например, раннее выявление негативного поведения в интернете может быть осуществлено при помощи оценивания того, насколько индивид следует семейным ценностям, и связанного с этим социального давления [23]. Важную роль играет также личная ответственность пользователей, т. е. каждый человек должен внимательно и ответственно относиться к тому, какую информацию о себе он выкладывает в публичную сферу интернета. Предотвращению кибersталкинга способствует повышение осведомлённости не только посредством информационно-просветительских программ, но также привития детям надлежащего онлайн-этикета родителями или другими авторитетными лицами.

В Сингапуре с 2021 года в школьную программу введён курс по воспитанию характера и гражданственности (Character and Citizenship Education), в рамках которого подчёркивается важность следования моральным ценностям, комфортного пользования интернетом и уважения личных границ как офлайн, так и онлайн. Данный курс также направлен на повышение осведомлённости о различных опасностях, которые может содержать виртуальное общение [18]. В июле 2022 г. Министерство связи и информации Сингапура разработало ряд информационно-просветительских и образовательных программ для обеспечения поддержки жертв киберпреследования, а также в целях пропаганды ответственного поведения в интернете.

В Индии эксперты также подчёркивают важность повышения уровня информированности в школах, т. к. использование интернета начинается в раннем возрасте, дети должны быть хорошо осведомлены о том, как безопасно вести себя в сети. Количество информации о киберпреступности и методах борьбы с ней должно увеличиваться с повышением возраста учащихся. Кроме того, сотрудники, поступающие на место работы, также должны пройти обучение по предотвращению киберпреступности и, в частности, кибersталкинга, дополненное отраслевыми знаниями по профессии [19].

Помимо повышения осведомлённости в рамках профилактики агрессии в сети внедряется специальное программное обеспечение и современные правила интернет-площадок, направленные на организацию безопасного пребывания в сети. В США созданы специальные сервисы, которые могут отслеживать и защищать личную информацию в интернете, обеспечивать комфортное пребывание пользователей в сети, а также предоставляются дополнительные инструменты безопасности при обмене персональными данными, среди которых усиленные настройки конфиденциальности или методы частного просмотра веб-страниц [23]. Ещё одним важным шагом в борьбе с кибersталкингом в Америке является сведение

[1] Cybercrime Support Network. Official site. URL: https://fightcybercrime.org (дата обращения: 08.02.2024).

к минимуму возможности компаний и частных лиц отслеживать действия людей в интернете, данные об их местоположении. Так, одна из самых популярных американских социальных сетей после протеста пользователей отозвала функцию, которая отправляла подписчикам аккаунта сообщения с информацией о покупках его владельца на различных сайтах. В качестве необходимой задачи указывается также работа с приложениями и сайтами, навязывающими пользователям раскрытие информации об их местонахождении [23]. В Сингапуре функционирует специальный портал Агентства кибербезопасности (GoSafeOnline), который предоставляет целенаправленную информацию для повышения осведомлённости об опасностях интернета, консультации для жертв агрессии онлайн [18].

Китайскими учёными были проведены исследования, в результате которых сформулированы конкретные рекомендации по работе виртуальных социальных платформ, снижающие вероятность распространения киберпреследования. К таким рекомендациям относятся: устранение ощущения полной анонимности пользователей посредством ввода хотя бы одного обязательного проверяемого идентификатора владельца аккаунта; усиление мониторинга при помощи системы предупреждений агрессивного поведения в сети; снижение асинхронности общения пользователей между собой, т. к. отсутствие непосредственной реакции жертвы, откладывание её во времени способствует затормаживанию дальнейших действий агрессора [20].

В Японии организован специальный Совет по стабильному использованию интернета, который в рамках своей деятельности сформировал руководящие принципы по противодействию кибератакам и конфиденциальности коммуникаций, а также Комиссия по защите личной информации, Национальный центр готовности к инцидентам и стратегии кибербезопасности (NISC). В качестве необходимых мер правительство страны работает над повышением отслеживаемости и прозрачности киберпространства, а также поощрением жертв киберпреступлений сообщать о них в полицию и специализированные государственные органы с целью минимизации условий для преступности в сети [1].

Что касается Российской Федерации, то здесь кибersталкинг не криминализирован, т. е. официально не рассматривается в качестве преступления. При этом существует ряд положений административного и уголовного кодексов, предусматривающих наказание за определённые проявления агрессии в виртуальном пространстве: ст. 128.1. УК РФ – клевета, совершённая с использованием интернета; ст. 137 УК РФ – незаконный сбор и распространение сведений о частной жизни других лиц без их согласия; ст. 119 УК РФ – угроза убийством или причинением тяжкого вреда здоровью; ст. 110 УК РФ – доведение до самоубийства [2]. В то же время, пока жертва агрессивного поведения в сети не докажет

[1] Cybersecurity strategy. The Government of Japan, September 28, 2021. URL: https://www.nisc.go.jp/eng/pdf/cs-senryaku2021-en.pdf (дата обращения: 15.02.2024).
[2] УК РФ Статья 128.1. Клевета // КонсультантПлюс : сайт. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/8a73d26dba7976d6c43cc94aa1515368fef256f0/ (дата обращения: 20.02.2024).

реальную опасность поступаемых ей угроз либо не получит фактический вред своей жизни и здоровью со стороны преследователя, реакция правоохранительных органов не последует.

Ещё в 2019 году в Госдуме РФ состоялось заседание круглого стола по проблеме кибersталкинга и противодействия ему, по итогам которого был принят проект резолюции, содержащий предложение по введению уголовной ответственности за назойливое преследование в интернете [1]. Однако данной статьи в уголовном кодексе РФ до сих пор нет.

Вместе с тем необходимо отметить, что российская правовая сфера постепенно развивается в направлении повышения уровня обеспечения информационной безопасности. В конце 2022 г. Верховный Суд РФ опубликовал постановление, уточняющее некоторые вопросы, которые возникают в судебной практике по уголовным делам в сфере компьютерной информации [2]. Данное постановление позволяет более точно квалифицировать преступные деяния, совершённые в киберсфере, а также обязывает суды при рассмотрении дел, связанных с неправомерным доступом к компьютерной информации, устанавливать общественно опасные последствия, которые такой доступ за собой повлёк.

30 декабря 2024 г. Правительство РФ утвердило «Концепцию государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий»[3]. В тексте данной концепции официально признана проблема отсутствия в стране необходимого уровня информационной безопасности, обозначена одна из главных целей государства – защита граждан от противоправных действий, в том числе от нарушения неприкосновенности частной жизни при использовании информационных технологий. Концепция содержит перечень основных задач, которые ставит перед собой государство в сфере информационной безопасности, среди них совершенствование средств противодействия различным правонарушениям с использованием информационно-коммуникационных технологий, создание соответствующих специализированных подразделений, повышение уровня безопасности персональных данных, обеспечение систематического широкого информирования населения о новых угрозах, развитие пользовательской культуры и грамотности поведения населения в цифровом пространстве и др. Для выполнения поставленных задач предполагается создание

[1] В ГД обсудили идею ввести уголовную ответственность за кибersталкинг // РИА Новости : сайт. URL: https://ria.ru/20191206/1562060603.html (дата обращения: 19.02.2024).

[2] Постановление Пленума Верховного суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершённых с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»» // КонсультантПлюс : сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_434573/7ad11c1823e584a73bbfbac49e996e617343f1ca/ (дата обращения: 19.12.2024).

[3] Распоряжение Правительства Российской Федерации от 30.12.2024 № 4154-р // Официальное опубликование правовых актов : сайт. URL: http://publication.pravo.gov.ru/document/0001202501090003?index=1 (дата обращения: 15.01.2025).

специализированной платформы, призванной обеспечить оперативный обмен данными между различными ведомствами и правоохранительными органами с целью раскрытия и пресечения противоправных действий в сети; организация системы профилактики; своевременное совершенствование законодательства для ответа на новые виды преступлений и др. Актуальность поставленных задач и средств для их выполнения не вызывает сомнений, однако ввиду недавнего принятия данной Концепции, в настоящее время не представляется возможным оценить эффективность её реализации.

Проблема сталкинга, в том числе совершаемого в виртуальном пространстве, не находит достаточного освещения в российском информационном поле, что создаёт иллюзию её незначительности и неактуальности. Так, несмотря на представленные выше данные специализированных организаций о большом числе жертв преследования, петиция, созданная ещё в декабре 2016 г. с целью введения в уголовный кодекс РФ статьи о сталкинге, на момент написания статьи набрала только чуть больше половины необходимых подписей – 81 151 из 150 000 [1].

Заключение

Тотальная виртуализация, пронизывающая все сферы жизнедеятельности современного общества, создаёт не только новые возможности для дальнейшего прогресса в различных областях, но и способствует появлению новых серьёзных вызовов и угроз безопасности. Развитие технологических возможностей послужило толчком для перехода некоторых форм девиантного поведения в цифровую среду. В частности, опубличивание персональных данных посредством размещения их в виртуальном пространстве приводит к формированию зависимости безопасности человека от уровня надёжности сохранения конфиденциальности предоставленных сведений, от цели их использования, от того, в чьи руки данные сведения могут попасть. Особые опасения в связи с этим вызывает лёгкость, с которой злоумышленники, используя современные технологии, могут получить доступ к личной информации жертвы, включая номер телефона, адрес проживания, данные о счетах, имуществе и т. д., скрыто подключиться к телефону или компьютеру преследуемого. В то же время анонимность самих преследователей не только существенно затрудняет пресечение их действий, но и оказывает растормаживающий эффект, снимает немедленное негативное подкрепление неприемлемого поведения.

Несмотря на явную общественную опасность, которую несёт в себе кибер-сталкинг, в настоящее время в России не предусмотрена система мер, направленных на эффективное противодействие ему. В связи с этим представляется целесообразным обратиться к рассмотренному положительному опыту ряда

[1] Ввести в УК РФ статью о сталкинге (преследовании) // Change.org : сайт. 7 декабря 2016 г. URL: https://www.change.org/p/правительство-рф-введите-в-ук-рф-статью-о-сталкинге-преследовании (дата обращения: 22.02.2024).

зарубежных стран, в которых функционируют механизмы защиты безопасности населения в виртуальном пространстве, и перенять наиболее эффективные из них. Результаты проведённого анализа позволяют к таким мерам отнести: криминализацию действий преследования в интернете, постоянный мониторинг актуальной ситуации по безопасности в сети, своевременное реформирование законодательства с учётом появления новых угроз, широкое информирование населения о существующих рисках, с которыми можно столкнуться в цифровой среде, понятное донесение данной информации с учётом возраста и особенностей восприятия целевой аудитории, образовательные кампании, создание специализированных организаций, оказывающих бесплатную разностороннюю помощь жертвам преследования. Официальное признание кибersталкинга преступным деянием закрепляет рассмотрение данного явления в правоприменительной практике в качестве угрозы правам человека и общественной безопасности, предусматривает чётко определённую ответственность за его совершение и предполагает неотвратимость наказания. Организация регулярного мониторинга виртуального пространства на предмет появления новых рисков и угроз правам человека, ценностям и интересам общества способствует оперативному приведению законодательства в соответствие с актуальной ситуацией, что необходимо для оперативного пресечения данных вызовов, постоянного поддержания должного уровня безопасности. Информационно-просветительские программы, ориентированные на разные группы населения, направлены на обеспечение необходимой подготовки граждан к возможным угрозам в сети, на предоставление рекомендаций по защите личной, информационной, финансовой безопасности. Работа специализированных организаций, оказывающих помощь жертвам агрессии, призвана восстановить состояние защищённости личности от противоправных посягательств.

На данный момент в связи с отсутствием чётко регламентированных действий, направленных на предотвращение и пресечение кибersталкинга в России, угроза общественной безопасности со стороны рассматриваемого деяния только возрастает, что подтверждается представленными в работе статистическими данными и результатами специализированных исследований.

СПИСОК ИСТОЧНИКОВ

1. *Ильичев И. Е., Богмацера Э. В.* Общественная безопасность и безопасность общества: соотношение понятий // Проблемы правоохранительной деятельности. 2018. № 1. С. 11–19. EDN YUKGEL.
2. *Бек У.* Общество риска. На пути к другому модерну / У. Бек ; пер. с нем. В. Седельника, Н. Фёдоровой ; посл. А. Филиппова. М. : Прогресс-Традиция, 2000. 384 с. ISBN 5-89826-059-5. EDN RAYTKJ.
3. *Гилинский Я. И.* Очерки по криминологии. СПб : Алеф-Пресс, 2015. 140 с. ISBN 978-5-905966-60-6.
4. *Вершинина И. А., Лядова А. В.* Данные в цифровом мире: новые возможности или дополнительные риски? // Вестник Российского университета дружбы народов. Серия: Социология. 2020. Т. 20, № 4. С. 977–984. DOI 10.22363/2313-2272-2020-20-4-977-984. EDN OPNQCR.

5. *Карпова Д. Н., Проскурина А. С.* Социотехнический поворот в исследовании цифровизации общества // Власть. 2020. Т. 28, № 1. С. 97–105. DOI 10.31171/vlast.v28i1.7048. EDN RDJMRV.
6. *Комлев Ю. Ю.* Преступность: тренды и вызовы на пороге новой технологической революции // Вестник ВЭГУ. 2017. № 4 (90). С. 67–75. EDN ZDAYVB.
7. *Комлев Ю. Ю.* От цифровизации социума к киберпреступности, кибердевиантности и развитию цифровой девиантологии // Российский девиантологический журнал. 2022. Т. 2, № 1. С. 17–26. DOI 10.35750/2713-0622-2022-1-17-26. EDN CLLGON.
8. *Иванова Е. С., Евдокимова А. Н.* Кибербезопасность в основе обеспечения национальной безопасности страны // Журнал прикладных исследований. 2022. Т. 7, № 11. С. 559–563. DOI 10.47576/2712-7516_2022_11_7_559. EDN YOQRTU.
9. *Кучина Я. О.* Проблема экстраполяции элементов криминологической характеристики отдельных видов преступности в киберпространстве: общая характеристика кибersталкинга // Расследование преступлений: проблемы и пути их решения. 2020. № 3 (29). С. 47–51. EDN CAXCWU.
10. *Кобец П. Н., Краснова К. А.* Об общественной опасности кибersталкинга и необходимости его предупреждения // Вестник Восточно-Сибирского института МВД России. 2018. № 3 (86). С. 77–83. EDN YAAIQH.
11. *Солдатова Г. У., Рассказова Е. И., Чигарькова С. В.* Виды киберагрессии: опыт подростков и молодёжи // Национальный психологический журнал. 2020. Т. 2, № 2 (38). С. 3–20. DOI 10.11621/npj.2020.0201 EDN YJIBIE.
12. *Грязнова Е. В., Владимиров А. А., Соколова В. А.* Девиантное поведение молодёжи в виртуальной среде // Глобальный научный потенциал. 2022. № 9 (138). С. 36–38. EDN NINWZQ.
13. *Сулейменова Р. Д., Руденко В. В., Кышко М. Е.* Совершенствование аспектов информационной безопасности в условиях глобализации информационного пространства: кибersталкинг // Наукосфера. 2023. № 5-2. С. 317–323. EDN XBQYIS.
14. *Зипельмайер О.* Психосоциальное и психотерапевтическое консультирование женщин, пострадавших от сталкинга // Социальное обслуживание семей и детей: научно-методический сборник. 2020. № 19. С. 30–39. EDN WAFULZ.
15. *Батеева А. А.* Кибersталкинг как угроза психологическому благополучию личности в интернет-пространстве // Психология в системе социально-производственных отношений : сборник материалов III Международной научно-практической конференции (Красноярск, 17 апреля 2020 года). Красноярск : Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнева. 2020. С. 175–179. EDN UIEXOX.
16. *Kukul B.* Personal Data and Personal Safety: re-Examining the Limits of Public Data in the Context of Doxing // International Data Privacy Law. 2023. Vol. 13, № 3. P. 182–193. DOI 10.1093/idpl/ipad011. EDN BVJXBA.
17. The Privacy, Data Protection and Cybersecurity Law Review. Ninth edition. London : Law Business Research Ltd., 2022. 519 p. ISBN 978-1-80449-116-4.
18. *Nair T., Teo Y.-L.* Creating Women's «Safe Space» in Digital Life: Perspectives from Singapore. S. Rajaratnam School of International Studies, 2023. URL: http://www.jstor.org/stable/resrep53092 (дата обращения: 12.02.2024).
19. *Minocha L.* Cyber Stalking Prevention And Management // Shodhganga: a reservoir of Indian theses: сайт. URL: https://shodhganga.inflibnet.ac.in/handle/10603/368801 (дата обращения: 10.02.2024).
20. An Integrative Theory Addressing Cyberharassment in the Light of Technology-Based Opportunism / P. B. Lowry, J. Zhang, G. D. Moody [et al] // Journal of Management Information Systems. 2019. Vol. 36, № 4. P. 1142–1178. DOI 10.1080/07421222.2019.1661090.

21. To Intervene or Not to Intervene: Young Adults' Views on When and How to Intervene in Online Harassment / A. Davidovic, C. Talbot, C. Hamilton-Giachritsis, A. Joinson // Journal of Computer-Mediated Communication. 2023. Vol. 28, № 5. DOI 10.1093/jcmc/zmad027. EDN KOCPOU.
22. *Brookfield K., Fyson R., Goulden M.* Technology-Facilitated Domestic Abuse: An under-Recognised Safeguarding Issue? // The British Journal of Social Work. 2024. Vol. 54, № 1. P. 419–436. DOI 10.1093/bjsw/bcad206. EDN EKCDKS.
23. *Dhillon G., Smith K. J.* Defining Objectives for Preventing Cyberstalking // Journal of Business Ethics. 2019. Vol. 157. № 1. P. 137–158. DOI 10.1007/s10551-017-3697-x. EDN HTNZTH.

Сведения об авторе

Е. В. Ларина
кандидат социологических наук,
научный сотрудник
SPIN-код: 4048-6769

Статья поступила в редакцию 28.12.2024; одобрена после рецензирования 20.01.2025; принята к публикации 10.02.2025.

Original article
DOI: 10.19181/snsp.2025.13.1.8

CYBERSTALKING AS A MODERN THREAT TO PUBLIC SECURITY: COUNTERMEASURES IN RUSSIA AND ABROAD

Elena Viktorovna Larina
Institute of Sociology of FSTAS RAS,
Moscow, Russia,
elena_shulgina@inbox.ru,
ORCID 0000-0002-4928-4388

For citation: Larina E. V. Cyberstalking as a modern threat to public security: countermeasures in Russia and abroad. *Sociologicheskaja nauka i social'naja praktika.* 2025;13(1):170–189. (In Russ.). DOI 10.19181/snsp.2025.13.1.8.

Abstract. Information and telecommunication technologies in the modern world are becoming an important part of social reality, permeating all spheres of society. This trend in addition to unconditional progress in various sectors of life, also leads to the emergence of new challenges and threats, including the spread of various forms of cyberdeviance that pose a danger to the individual and society. The relevance of the problem under consideration is provided by statistics from Russian law enforcement agencies on the multiple increase in crimes in the field of computer information, published information from one of the leading companies in the field of information security on the number of victims of stalking on the Internet in different countries, as well as an increase in the number of identified applications aimed at stalking in virtual space. This article is devoted to the analysis of the phenomenon of cyberstalking, which is one of the most aggressive forms of manifestation of deviant behavior

on the Internet, as well as to research of measures to counteract the problem under study used in various countries of the world. The methodological basis of the conducted research was the collection, systematization and analysis of materials of original scientific works in the field of the studied problems using specialized information search systems. A review of statistical data and legislative acts aimed at countering various manifestations of harassment have been also carried out. In particular, an analytical review was made of the current strategies for protecting the security of the population in the digital environment in countries such as the USA, Great Britain, Germany, Singapore, India, China, Japan, etc. The status of cyberstalking in the Russian Federation, as well as the existing countermeasures against it, was considered. Statistical data on the number of victims of cyberstalking, as well as their age and gender distribution are presented. Some characteristics of the persons carrying out the persecution and the means by which they usually act are indicated. An overview of the key elements of current strategies for protecting public safety in the digital environment in Europe, Asia and the United States is provided. The most widely used mechanisms for combating aggression in the network are identified which are part of the cybercrime counteraction system in most of the countries under consideration which may indicate a high level of their effectiveness. Such mechanisms include the criminalization of various forms of harassment in the virtual space, monitoring the degree of cybersecurity of users, constantly increasing the level of public awareness of existing risks on the Internet, specialized educational campaigns, providing free assistance to victims of harassment, etc. Based on the above, it was concluded that it is advisable to use the most effective measures to counter cyberstalking operating abroad to protect the Russian population in the virtual space.

Keywords: cyberstalking, persecution, aggression, virtual space, victim, security, countermeasures

REFERENCES

1. Ilyichev I. E., Bogmatsera E. V. Public safety and security of society: the relationship of concepts. *Problems of Law Enforcement=Problemy pravoohranitel'noj deyatel'nosti*. 2018;(1):11–19. (In Russ.).
2. Beck U. Risk Society. Towards another modernity. Translated from German by V. Sedelnik, N. Fedorova; Last words by A. Filippov. Moscow: Progress-Tradiciya; 2000. 384 p. (In Russ.). ISBN 5-89826-059-5.
3. Gilinsky Ya. I. Essays on criminology. St. Petersburg: Alef-Press; 2015. 140 p. (In Russ.).
4. Vershinina I. A., Lyadova A. V. Data in the digital world: new opportunities or additional risks? *Bulletin of the Peoples' Friendship University of Russia=Vestnik Rossijskogo universiteta druzhby narodov.* Series: Sociology. 2020;20(4):977–984. (In Russ.). DOI 10.22363/2313-2272-2020-20-4-977-984.
5. Karpova D. N., Proskurina A. S. Socio-technical turn in the study of digitalization of society. *Power=Vlast'*. 2020;28(1):97–105. (In Russ.). DOI 10.31171/vlast.v28i1.7048.
6. Komlev Yu. Yu. Crime: trends and challenges on the threshold of a new technological revolution. *Bulletin of VEGU=Vestnik VEGU*. 2017;4(90):67–75. (In Russ.).
7. Komlev Yu. Yu. From the digitalization of society to cybercrime, cyberdeviance and the development of digital deviantology. *Russian Deviantological Journal=Rossiyskiy deviantologicheskiy zhurnal.* 2022;2(1):17–26. (In Russ.). DOI 10.35750/2713-0622-2022-1-17-26.
8. Ivanova E. S., Evdokimova A. N. Cybersecurity as a basis for ensuring the national security of the country. *Journal of Applied Research=Zhurnal prikladnykh issledovaniy*. 2022;(11):559–563. (In Russ.). DOI 10.47576/2712-7516_2022_11_7_559.

9. Kuchina Ya. O. The problem of extrapolating elements of criminological characteristics of individual types of crime in cyberspace: general characteristics of cyberstalking. *Crime Investigation: Problems and Solutions=Rassledovaniye prestupleniy: problemy i puti ikh resheniya*. 2020;(3):47–51. (In Russ.).
10. Kobets P. N., Krasnova K. A. On the public danger of cyberstalking and the need to prevent it. *Bulletin of the East Siberian Institute of the Ministry of Internal Affairs of Russia=Vestnik Vostochno-Sibirskogo instituta MVD Rossii*. 2018;(3):77–83. (In Russ.).
11. Soldatova G. U., Rasskazova E. I., Chigarkova S. V. Types of cyber aggression: experience of adolescents and youth. *National Journal of Psychology=Natsional'nyy psikhologicheskiy zhurnal*. 2020;2(2):3–20. (In Russ.). DOI 10.11621/npj.2020.0201.
12. Gryaznova E. V., Vladimirov A. A., Sokolova V. A. Deviant behavior of young people in a virtual environment. *Global Scientific Potential=Global'nyy nauchnyy potentsial*. 2022;(9):36–38. (In Russ.).
13. Suleymenova R. D., Rudenko V. V., Kyshko M. Ye. Improving aspects of information security in the context of globalization of the information space: cyberstalking. *Scienceosphere=Naukosfera*, 2023;(5-2):317–323. (In Russ.).
14. Zipel'mayyer O. Psychosocial and psychotherapeutic counseling of women victims of stalking. *Social Services for Families and Children: Scientific and Methodological Collection=Social'noe obsluzhivanie semej i detej: nauchno-metodicheskij sbornik*. 2020;(19):30–39. (In Russ.).
15. Bateyeva A. A. Cyberstalking as a threat to psychological well-being of an individual in the Internet space. In: Psychology in the system of social and industrial relations: collection of materials of the III international scientific and practical conference, Krasnoyarsk, April 17, 2020. Krasnoyarsk: Sibirskij gosudarstvenny'j universitet nauki i texnologij imeni akademika M. F. Reshetneva; 2020. P. 175–179. (In Russ.).
16. Kukul B. Personal data and personal safety: re-examining the limits of public data in the context of doxing. *International Data Privacy Law*. 2023;13(3):182–193. DOI 10.1093/idpl/ipad011.
17. The privacy, data protection and cybersecurity law review. Ninth edition. London: Law Business Research Ltd., 2022. 519 p.
18. Nair T., Teo Y.-L. Creating women's "safe space" in digital life: perspectives from Singapore. S. Rajaratnam School of International Studies, 2023. Available at: http://www.jstor.org/stable/resrep53092 (accessed: 12.02.2024).
19. Minocha L. Cyber stalking prevention and management. Shodhganga: a reservoir of Indian theses: webcite. Available at: https://shodhganga.inflibnet.ac.in/handle/10603/368801 (accessed: 10.02.2024).
20. Lowry P. B., Zhang J., Moody G. D., Chatterjee S., Wang Ch., Wu T. Proposing an integrative theory to address the sociotechnical nature of cyberharassment in light of technology-based opportunism. *Journal of Management Information Systems*. 2019;36(4):1142–1178.
21. Davidovic A., Talbot C., Hamilton-Giachritsis C., Joinson A. To intervene or not to intervene: young adults' views on when and how to intervene in online harassment. *Journal of Computer-Mediated Communication*. 2023;28(5). DOI 10.1093/jcmc/zmad027.
22. Brookfield K., Fyson R., Goulden M. Technology-facilitated domestic abuse: an under-recognised safeguarding issue? *The British Journal of Social Work*. 2024;54(1):419–436. DOI 10.1093/bjsw/bcad206.
23. Dhillon G., Smith K. J. Defining objectives for preventing cyberstalking. *Journal of Business Ethics*. 2019;157(1):137–158. DOI 10.1007/s10551-017-3697-x.

Information about the Author

E. V. Larina
Candidate of Sociology,
Researcher

The article was submitted 28.12.2024; approved after reviewing 20.01.2025; accepted for publication 10.02.2025.