КОБЕЦ П. Н.
Доктор юридических наук, профессор, главный научный сотрудник Всероссийского научно-исследовательского института МВД России.
Эл. почта: pkobets37@rambler.ru

KOBETS P. N.
Doctor of law sciences, professor, chief researcher of the All-Russian Scientific Research Institute of the Ministry of Internal affairs of Russia.
E-mail: pkobets37@rambler.ru

КРАСНОВА К. А.
Кандидат юридических наук, доцент, ведущий научный сотрудник Всероссийского научно-исследовательского института МВД России.
Эл. почта: krasnova_vnii@mail.ru

KRASNOVA K. A.
Candidate of law sciences, Associate professor, leading researcher of the All-Russian Scientific Research Institute of the Ministry of Internal affairs of Russia.
E-mail: krasnova_vnii@mail.ru

ОБ ОБЩЕСТВЕННОЙ ОПАСНОСТИ КИБЕРСТАЛКИНГА И НЕОБХОДИМОСТИ ЕГО ПРЕДУПРЕЖДЕНИЯ

Аннотация. *Авторы подробно исследуют проблемы кибersталкинга и запугивания через информационно-телекоммуникационную сеть «Интернет». Новизна исследования заключается в том, что авторы анализируют общественную опасность кибersталкинга и разнообразные последствия посягательств на неприкосновенность частной жизни, выражающиеся в негативном воздействии на личность через Интернет. Сделан вывод о том, что сочетание технологических и социальных факторов поощряет людей к участию в подстрекательствах к насилию и преследованию других людей в сети «Интернет».*

Ключевые слова: *киберпреступность, кибersталкинг, кибербуллинг, организованная преступность, угроза национальной безопасности.*

ABOUT THE SOCIAL DANGER OF CYBERSTALKING AND THE NECESSITY OF ITS PREVENTION

Annotation. *The authors examine in detail the problems of cyberstalking and intimidation through the "Internet". The originality of the research is that the authors analyze the public danger of cyberstalking and various consequences of encroachments on privacy, expressed in negative impact on the person through the Internet. It is concluded that a combination of technological and social factors encourages people to participate in crimes or antisocial acts, such as incitement to violence and harassment of other people in the Internet.*

Keywords: *cybercrime, cyberstalking, cyberbullying, organized crime, threat to national security.*

За последние годы экспонентное развитие технологий, в особенности сети «Интернет», глубоко изменило способы, применяемые людьми для поиска и обмена информацией. Использование Интернета как средства коммуникации уже признано культурным феноменом, отражающим текущий эволюционный процесс [1, с. 40—50]. В условиях все большей доступности информационно-телекоммуникационной сети «Интернет» все чаще фиксируются случаи преследования людей с использованием информационно-коммуникационных технологий с целью вызвать раздражение, агрессию или беспокойство у людей, в том числе детей и подростков. Феномены кибербуллинга (от англ. cyber — «кибер» и bullying — запугивание) и киберсталкинга (от англ. cyber — «кибер» и stalking — тайное преследование, выслеживание) вот уже несколько лет являются предметом исследований, проводимых зарубежными криминологами, в частности, экспертами американского исследовательского центра кибербуллинга (The Cyberbullying Research Center).

При кибербуллинге используются сила или оказывается давление (прямо либо косвенно) в устной, письменной или физической форме или конклюдентно (путем демонстрации или иного использования фото-, видеоматериалов) в целях запугивания, угроз, травли, преследования или смущения при помощи Интернета или других технологий, к примеру, мобильных телефонов [2]. Домогательства, которые могут быть признаны кибербуллингом, как правило, связаны с применением разнообразных форм психического насилия: угроз убийством, угроз насильственных действий по отношению к жертве либо ее близким, угроз истребления имущества родных и близких, угроз распространения компрометирующих их сведений, аудио- и видеоматериалов либо иных сведений, разглашения которых пострадавшая сторона не желает, шантажа, клеветы, оскорблений, внушения и др. Подобные угрозы выражаются путем направления потерпевшему оскорбительных сообщений посредством электронной почты, через социальные сети и общедоступные мессенджеры. Кибербуллингу могут сопутствовать кража личных данных потерпевшего либо повреждение его оборудования для выхода в сеть «Интернет».

Киберсталкинг, в свою очередь, означает преследование какого-либо лица посредством сети «Интернет» и других информационно-телекоммуникационных сетей и электронных устройств. Киберсталкинг сопряжен со сбором информации о потерпевшем с помощью поисковых систем, привлечения внимания общественности к личности жертвы в негативном ключе и оскорблением жертвы посредством размещения в Интернете информации о ней через различные чаты, форумы, блоги, общедоступные мессенджеры и социальные сети. Все формы сталкинга включают в себя угрозы и имеют своей целью довести жертву до истощения от нервного перенапряжения.

Киберсталкинг может привести к тому, что киберобидчик — человек, который производит саму травлю, — станет представлять реальную угрозу для безопасности и благополучия жертвы. В частности, этот термином могут называться по-

пытки взрослых связаться с детьми и подростками через сеть «Интернет» [3, с. 101—104] с целью организации личной встречи и последующих действий, связанных с сексуальной эксплуатацией либо доведением до самоубийства [4, с. 78—84]. Эта форма кибербуллинга крайне опасна и может иметь самые серьезные последствия, поэтому при вскрытии таких фактов необходимо принимать все неотложные меры для их предотвращения.

Несмотря на то, что сталкинг и кибersталкинг внешне имеют общие черты, термины эти не являются синонимами, поэтому с ними надо обращаться соответственно. Авторы придерживаются той точки зрения, что кибersталкинг представляет собой новую форму девиантного поведения, поэтому его стоит отличать от офлайн-сталкинга (вне сети «Интернет»). Проведенное исследование показывает, что основное различие заключается в более разнообразной мотивации при кибersталкинге.

Кроме того, получил распространение корпоративный сталкинг, когда какое-то лицо, группа или организация преследует другое лицо, группу или организацию. В этом случае мотивами сталкинга выступают политическая или материальная выгода, недобросовестная конкуренция. Например, разногласия между различными конкурирующими компаниями могут быть связаны с использованием незаконных методов, взломом компьютеров, баз данных, электронной почты конкурента с последующим распространением через средства массовой информации данных, полученных противоправным путем.

Надо отметить, что сталкеры всегда вступают в какие-то отношения со своими жертвами. Из зафиксированных случаев использования сталкинга не было ни одного эпизода, когда бы сталкер не видел жертвы, хотя бы на фотографии, по телевидению или лично.

Современные кибersталкеры не ограничиваются географически небольшим районом и могут преследовать жертв в других странах с такой же легкостью, как будто бы она (жертва) живет в том же городе. Новейшие информационно-коммуникационные технологии позволяют кибersталкеру не только преследовать или угрожать другому лицу, но и подстрекать к таким действиям третью сторону, с которой он никогда не имел никаких отношений.

Стоит также отметить и то, что многие технологии, используемые кибersталкерами, были до недавнего времени невозможны. Кража идентичности, например, предполагает имитацию другого человека с тем, чтобы осуществлять различные действия, скажем, делать покупки онлайн мошенническим способом. Однако такие действия в условиях начала нового тысячелетия в России были невозможны, поскольку этой технологией пользовались едва ли несколько интернет-магазинов.

Особые опасения вызывает преследование в сети «Интернет» свидетелей преступлений и членов их семей [5, с. 38—41; 6, с. 192—194; 7, с. 30—33]. Особенно это касается свидетелей в уголовных процессах по делам об организованной преступности [8, с. 19—23]. Как показывает мировая практика, обеспечение безопасности лиц, включенных в программу защиты свидетелей, в киберпространстве становится все более актуальной проблемой [9, с. 76—94; 10, с. 57—62]. Одним

из вопросов, волнующих сотрудников программы защиты свидетелей, как в России, так и за рубежом, остается сохранение в тайне сведений о новом месте жительства свидетеля и членов его семьи, их новых именах, местах работы и учебы [11, с. 39—44; 12, с. 20—23; 13, с. 86—91; 14, с. 66—86; 15, с. 11—15].

Исследование кибersталкинга дает представление о том, что не все лица, занимающиеся такого рода противоправной деятельностью, имеют проблемы психиатрического характера [16, с. 103—108]. Более того, не все занимающиеся кибersталкингом нуждаются в психиатрической помощи. Достаточно подтверждений тому, что кибersталкинг является лишь инструментом для достижения какой-то вполне определенной цели. Иногда кибersталкинг используется для получения финансовой выгоды или для преодоления конкуренции. Некоторые организованные группы используют приемы, связанные с кибersталкингом, для преследования оппонентов. Например, организованные группы ненависти используют возможности сети «Интернет», чтобы распространять дезинформацию касательно расового превосходства и инспирировать насилие по отношению к другим людям или уничтожение их собственности [4, с. 75].

Технологические факторы кибersталкинга поощряют людей к принятию участия в девиантных актах, поскольку они позволяют участвовать в них без страха перед уголовными или административными санкциями [17, с. 18—21]. Технологии дают как механизм, при помощи которого человек может действовать, так и необходимую защиту против уголовного или иного наказания. Современные информационно-коммуникационные технологии с каждым годом становятся все более доступными и легкими в применении. Более того, теперь практически любой человек может при помощи несложных технических приемов скрыть свою личность, действия и уничтожать любые доказательства противоправной активности в сети «Интернет». Доступность мощного недорогого программного обеспечения с шифратором также помогает отдельным лицам оставаться анонимными и скрывать свою деятельность. В частности, во многих расследованиях по делам о детской порнографии педофилы пользовались такими технологиями для того, чтобы скрыть свою деятельность [18, с. 180—186]. Дополнительную защиту кибersталкеры находят при использовании различных свободных программ для шифрования, которые дают пользователям доступ к наиболее мощным из имеющихся алгоритмов сокрытия следов активности в сети «Интернет». Например, существуют такие программы, которые стирают детали любого веб-сайта, на который заходил пользователь, файлы, которые он загружал, просматриваемые документы и т. д. При этом файлы стираются так, что не могут быть восстановлены никакими методами, применяемыми в судебной практике.

Следует отметить некоторые социальные факторы, которые способствуют формированию мотивации лица и подводят его к осуществлению антиобщественных или уголовно-наказуемых деяний при помощи сети «Интернет». Анонимность, которую допускает онлайн-коммуникация, создает растормаживающий эффект и приводит к девиантному поведению. При непосредственном общении индивиды, как правило, ограничены общественными нормами, которые управляют межлич-

ностным взаимодействием, непосредственным отрицательным подкреплением и видимыми последствиями неприемлемого поведения, в том числе возможными общественными санкциями. Используя возможности сети «Интернет», пользователи пребывают в относительной автономии и физической безопасности, сохраняя при взаимодействии дистанцию, зачастую не только не зная субъекта взаимодействия лично, но и не предвидя негативные последствия своего поведения — рискованного или потенциально причиняющего ущерб другому лицу. Следствием является агрессия, личное использование сомнительного контента (например, как порнографии) в сети «Интернет» [19, с. 62—68]. Логично предположить, что процесс, известный под названием «деиндивидуализация», может влиять на растормаживание, которое отмечается у многих пользователей Интернета. Деиндивидуализацию можно представить как такое состояние личности индивида, когда его самосознание сужено из-за принадлежности к группе. Человек может принимать участие в преступном деянии, если индивидуальная тождественность подавлена принадлежностью к группе. При таких обстоятельствах человек оказывается восприимчивым к ситуативным сигналам и может принимать участие в поведении, которое вне группового контекста не имело бы места. В крайних состояниях самосознание индивида под влиянием деиндивидуализации может привести его к поведению в форме «стада» не только в реальной жизни, но и в виртуальной [20, с. 10—14].

Рассматривая проблему того, как воспринимается личность и как она строится в киберпространстве, отметим, что индивиды могут создавать многочисленные киберличности, в основе которых лежат стратегические цели. Например, человек, работающий дома, может создать киберличность прагматичную и разумную для деловых отношений и киберличность более расслабленную и дружелюбную для общения с друзьями и семьей. Можно также создать асоциальную киберличность, например, расиста, которую индивид будет использовать в чатах с другими сторонниками расизма. Иными словами, личность преступника в киберпространстве не является статической характеристикой. Она реализуется в процессе онлайн коммуникации с собеседником, основываясь на контекстуальных чертах и ролях, принятых участниками диалога, которые находятся в данном контексте.

Криминологам хорошо известно, что преступное деяние характеризуют три почти всегда присутствующих элемента: возможный преступник, подходящая мишень (цель) и отсутствие того, кто способен удержать от совершения преступления. Существуют также три важные составляющие преступления: «реквизит» (например, инструменты), «камуфляж» (помогающий преступнику остаться незамеченным) и «аудитория», которую преступник желает поразить или напугать. Не требуется многих усилий, чтобы обнаружить все эти элементы в отношении противоправных деяний, совершаемых киберсталкерами. Например, мы уже упоминали о «реквизите» (в форме компьютерного оборудования, программного обеспечения и услуг) и «камуфляже» (в форме анонимных e-mail, шифрования и других технических приемов киберпреследования). Таким образом, сочетание технологических и социальных факторов поощряет людей к участию в преступлениях или

противоправных деяниях [21, с. 643].

В заключение хотелось бы отметить, что существует гораздо большее количество факторов, которые могут объяснить, почему некоторые индивиды участвуют в противоправном движении в сети «Интернет». Следует признать общественную опасность кибersталкинга и необходимость поиска оптимальных путей его предупреждения.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ

1. *Totaro S., Toffo E. & Scocco P.* (2016). Suicide prevention and the Internet, risks and opportunities: a narrative review. Suicidology Online, 7, 40—50. (In English).

2. 10 форм кибербуллинга [Электронный ресурс]. Режим доступа: http://stop-ugroza.ru/life/10-form-kiberbullinga-ot-kids-kaspersky-ru (дата обращения: 19.08.2018)..

3. *Жестеров П. В.* Криминологические меры предупреждения преступлений против несовершеннолетних: проблемы реализации в России // Вестн. С.-Петерб. юрид. акад. 2017. № 1 (34). С. 101—104.

4. *Краснова К. А., Ережипалиев Д. И.* Противодействие кибербуллициду как средство предупреждения суицидов несовершеннолетних // Юристъ-Правоведъ. 2017. № 3 (82). С. 78—84.

5. *Краснова К. А.* Правовые и организационные основы предупреждения преступлений против участников уголовного судопроизводства органами внутренних дел // Рос. следователь. 2015. № 22. С. 38—41.

6. *Лозовицкая Г. П., Краснова К. А., Дьяченко Н. Н.* Состояние обеспечения применения мер государственной защиты в отношении потерпевших, свидетелей и иных участников уголовного судопроизводства // Пробелы в рос. законодательстве. 2010. № 4. С. 192—194.

7. *Кобец П. Н., Краснова К. А.* О проблеме возмещения вреда потерпевшему на стадии предварительного расследования // Уголовное судопроизводство. 2009. № 4. С. 30—33.

8. *Краснова К. А., Агапов П. В.* Психологическое воздействие и его значение в оперативно-розыскной деятельности по делам об организованной преступности // Юрид. психология. 2014. С. 19—23.

9. *Кобец П. Н., Краснова К. А.* Проблемы возмещения вреда потерпевшему на стадии предварительного расследования // Адвокатская практика. 2009. № 6. С. 76—94.

10. *Ивлиева Н. В., Краснова К. А., Николаева Е. С.* Проблемы, возникающие при отмене мер безопасности, применяемых в отношении защищаемых лиц // Научный портал МВД России. 2015. № 3 (31). С. 57—62.

11. *Краснова К. А.* Правовые основы защиты свидетелей в Европейском Союзе // Адвокатская практика. 2016. № 1. С. 39—44.

12. *Краснова К. А.* Институциональные основы защиты свидетелей в Европейском Союзе // Междунар. уголовн. право и междунар. юст. 2014. № 1. С. 20—23.

13. *Кобец П. Н., Краснова К. А.* Об опыте организации программ защиты свидетелей в Европейском Союзе // Юрид. наука. 2015. № 1. С. 86—91.

14. *Краснова К. А.* Защита свидетелей в государствах-членах ЕС // Междунар. право. 2015. № 4. С. 66—86.

15. *Краснова К. А.* Международно-правовые гарантии обеспечения безопасности потерпевших и свидетелей в Европейском Союзе // Междунар. правовой курьер. 2014. № 6. С. 11—15.

16. *Кобец П. Н.* Рассмотрение актуальных правовых аспектов использования методов прикладной психологии в следственной практике правоохранительных органов Российской Федерации на занятиях со студентами юридических факультетов // Психолого-педагогическое обеспечение учебно-воспитательного процесса в вузе и пути его совершенствования: матер. межвуз. науч.-практ. конф. 22 июня 2005 г. / Под ред. д-ра экон. наук, проф. *Е. В. Волкова*. М.: Изд-во МИП, 2005. С. 103—108.

17. *Кобец П. Н.* Основные факторы, способствующие совершению преступлений экстремистской направленности со стороны религиозных тоталитарных сект, действующих в России // Рос. следователь. 2007. № 22. С. 18—21.

18. *Кобец П. Н.* Опыт и проблемы предупреждения транснациональной организованной преступности в сфере высоких технологий // Россия и АТР: проблемы безопасности, миграции и преступности: матер. междунар. науч.-практ. конф. Владивосток: Изд-во Дальневост. ун-та, 2007. С. 180—186.

19. *Кобец П. Н.* О факторах, детерминирующих преступность в условиях чрезвычайных ситуаций // Актуальные проблемы уголовного права и криминологии, уголовного процесса и криминалистики, уголовно-исполнительного права, преподавания учебных дисциплин криминологического цикла: матер. междунар. науч.-практ. конф., посв. 20-летию образования юрид. ф-та (19—20 мая 2014 г.) / отв. ред. *Г. И. Цепляева*. Петрозаводск: Изд-во ПетрГУ, 2014. С. 62—68.

20. *Кобец П. Н.* Использование психологических методов организации памяти потерпевших, свидетелей и подозреваемых в следственной практике правоохранительных органов Российской Федерации и зарубежных стран // Юрид. психология. 2009. № 6. С. 10—14.

21. *Краснова К. А.* Уголовно-правовые меры борьбы с кибербуллицидом несовершеннолетних // Уголовное право: стратегия развития в XXI веке: матер. XV междунар. науч.-практ. конф. (25—26 янв. 2018 г.). М.: РГ-Пресс, 2018. С. 640—643.