Распространение и развитие Интернета стерло границы общения и распространения информации. В связи с массовым распространением компьютеров, мировое сообщество столкнулось с такими явлениями, как противоправная деятельность с использованием компьютера (и/или против компьютеров), а также преступная деятельность посредством сети Интернет. Многие ученые и специалисты разграничивают киберпреступность как правовую категорию и как социальное явление. Для первого характерно конкретное противоправное деяние с использованием компьютера, компьютерной сети или сети Интернет. Квалификация данных деяний в рамках киберпреступлений не вызывает сомнения и сложностей, так как здесь явно выражены признаки виртуального противоправного деяния, которые направлены на все сферы общественной жизни. Четкого разделения на конкретные виды киберпреступлений нет. Для привлечения к ответственности киберпреступника необходимо доказать его причастность к данному деянию. «Виртуальные следы» противоправного деяния легко скрыть ввиду легкости изменения и уничтожения компьютерной информации. Очень сложна, а порой и не возможна процедура оформления, изъятия данных доказательств. Данные факты затрудняют доказывание вины и причастности лица к виртуальному преступлению, тем самым способствуя увеличению процента нераскрытых преступлений. Киберпреступность и киберпреступления становятся актуальными угрозами в сфере безопасности человека, общества и государства. Они представляют реальную угрозу не только для отдельных государств, но и для всего мирового сообщества в целом.

Ключевые слова: киберпреступность; фишинг; кибербуллинг; интернет-группинг; секстинг; кибертерроризм; система противодействия.

Татьяна Владиславовна Плотникова, канд. юрид. наук, доцент,
кафедра специальной подготовки и обеспечения национальной
безопасности, ФГБОУ ВО «Тамбовский государственный университет
имени Г. Р. Державина», Тамбов, Россия;
plotnikova-tmb@mail.ru

Оксана Валерьевна Котельникова, канд. пед. наук, доцент,
кафедра специальной подготовки и обеспечения национальной
безопасности, ФГБОУ ВО «Тамбовский государственный университет
имени Г. Р. Державина», Тамбов, Россия;
cotelnikova.oksana@yandex.ru

ФЕНОМЕН КИБЕРПРЕСТУПНОСТИ В УСЛОВИЯХ XXI ВЕКА

На современном этапе развития общества невозможно представить нашу жизнь без умных помощников – компьютеров. За небольшой период времени компьютеризация завоевала все сферы жизни общества, что привело к тому, что в настоящее время компьютеры являются общественно важными инструментами трудовой деятельности, общения, развлечения

и т.д. Глобальная компьютеризация породила такие понятия, как информационно-коммуникационные сети, сеть Интернет и т.д.

С одной стороны, масштабное внедрение и использование компьютерной техники весьма облегчает жизнь как человеку, так и обществу. Электронные помощники делают всю основную монотонную работу, тем самым освобождая личности больше времени для собственного развития, отдыха и развлечений. Компьютеры делают нашу жизнь более безопасной. Распространение и развитие Интернета стерло границы общения и распространения информации. Благодаря «данному чуду техники» появилось множество новых профессий и сфер развлечений. Активная и массовая компьютеризация «подстегивает» прогресс, что выражается в огромных запросах развития науки и новых технологий для создания и развития все более мощных и совершенных электронно-вычислительных устройств. Развивается наукоемкое производство во многих странах, требуется большое число передовых специалистов.

С другой стороны, в связи с массовым распространением компьютеров, мировое сообщество столкнулось с такими явлениями, как противоправная деятельность с использованием компьютера (и(или) против компьютеров), а также данная деятельность посредством сети Интернет. Данные противоправные деяния получили название «киберпреступность». При этом тенденция данных преступных деяний с каждым годом все увеличивается [10].

Стоит отдельно отметить размах киберпреступности. На сегодняшний день многие международные эксперты утверждают, что число киберпреступлений устойчиво составляет 30 % от общего числа преступлений, совершаемых в мире, то есть каждое третье преступное деяние в мире совершается в виртуальном пространстве. Относительно Российской Федерации, по данным МВД РФ количество преступных деяний в IT-сфере составляет около 15 % от общего числа преступлений на 2019 год. При этом стоит также отметить, что на 2018 год данный показатель составлял всего лишь 9 % [7]. Исходя из данных показателей, можно сделать неутешительный вывод: число преступлений в виртуальном пространстве возрастает с довольно приличной динамикой – около 65 % за год.

Масштаб киберпреступности поистине завораживает. При этом данная угроза актуальна не только для России, но и для всего мирового сообщества. По статистике, каждую секунду в мире совершается около 18 попыток совершения противоправного деяния в IT-сфере, и около 40 % из них – удачные. По данным многих аналитических компаний около 2/3 пользователей Интернета хотя бы раз становились жертвами киберпреступников (в некоторых случаях жертва даже не подозревает о совершенном в ее отношении преступлении). Мировой ущерб от киберпреступлений исчисляется миллиардами. Только за 2018 год мировая экономика потеряла около 400 млрд долларов в связи с активной деятельностью киберпреступников [2].

Российская Федерация представляет собой актуальную территорию деятельности для виртуальных преступников. Появление и активное развитие киберпреступлений в рамках территорий РФ было зафиксировано в 2008 году. В настоящее время более 25 % от всего количества киберпреступлений приходится на нашу страну. Россия входит в рейтинг 10 самых

популярных стран для киберпреступников. Это показывает и официальная статистика. Так, в 2012 году было зарегистрировано 10 227 преступлений, в период с 2013 – 2016 данный показатель вырос в 3 раза (почти 22 тыс. в 2013 и около 66 тыс. преступлений в 2016), в 2017 было официально зафиксировано 90,5 тыс. киберпреступлений, 2018 году – 121 тыс. 247 преступлений, 2019 – около 300 тыс. [6]. Данные показатели, особенно за последний год, весьма красочно описывают активную тенденцию развития виртуальной преступности в нашей стране.

На сегодняшний момент вопрос понятия киберпреступления остается довольно спорным. Представители научного мира, а также специалисты в IT-сфере до сих пор не могут выработать единое и согласованное определение данного противоправного деяния. В общем, мы можем сказать, что это преступления, которые совершаются с помощью компьютерной системы или сети (Интернета), в рамках компьютерной системы или сети (Интернет), или против компьютерной системы или сети (Интернет). При этом для данных деяний характерно не только понимание компьютера, информационной сети (Интернет), данных как объекта преступления, но и деяния, где компьютер используется в качестве средства и орудия совершения преступления.

Многие ученые и специалисты также разграничивают киберпреступность как правовую категорию и как социальное явление. Для первого характерно конкретное противоправное деяние с использованием компьютера, компьютерной сети или сети Интернет. Квалификация данных деяний в рамках киберпреступлений не вызывает сомнения и сложностей, так как здесь явно выражены признаки виртуального противоправного деяния.

Более масштабно обстоит дело со вторым понятием киберпреступности как социальным явлением. Данное представление включает как все «прямо указывающие» преступные деяния в IT-сфере, так и косвенно выраженные деяния, которые носят характер «поддерживающих», «вспомогающих» осуществлению преступного деяния. Яркими примерами данной трактовки киберпреступлений являются общение между преступниками посредством виртуальных сообщений, писем, размещение криминально ориентированной информации на сайтах и т.д.

Данные преступления характеризуются анонимностью, максимальной скрытностью преступника. Как известно, в информационном пространстве довольно тяжело вычислить лицо, которое совершило противоправное деяние. Но сложность вычисления и формирование своеобразной «подушки безопасности» для преступника обеспечивают специальные средства и программы (анонимайзеры, использование интернет-кафе и т.д.)

Данные преступления отличаются своей мобильностью, то есть можно совершить преступление из любой точки земного шара, понадобится только компьютер и Интернет. А также стоит отметить, что преступник и жертва также могут находиться в абсолютно разных странах мира и между ними может существовать огромное расстояние.

Нестандартность киберпреступления также выступает отличительной чертой данного вида преступлений. Довольно сложно, а порой и невозможно, предугадать дальнейшие действия киберпреступника и развитие

событий. Также стоит отметить сложность мошеннических схем в виртуальном пространстве.

Возможность автоматизма киберпреступлений – своего рода «ноу-хау» в преступном мире. В данном признаке заложена возможность совершать преступления в виртуальном пространстве в автоматическом режиме. Например, хакер создает вредоносную программу, которая, в свою очередь, совершает киберпреступления (проникает на чужие компьютеры и отправляет личную информацию) без участия разработчика, то есть в автономном режиме [4, с. 46].

Киберпреступления в современном мире являются довольно перспективным вектором развития преступного мира. Данные противоправные деяния направлены практически на все сферы общественной жизни. Разновидность и масштабы данного вида преступлений постоянно растут. Стоит отметить, что четкого разделения на конкретные виды киберпреступлений нет. Из самых актуальных и повсеместных видов киберпреступлений мы можем выделить следующие.

Преступления, которые направлены против компьютерных систем и баз данных. Огромный перечень киберпреступлений можно отнести к данному виду – это и хакерские атаки, заражение интернет-вирусами и вредоносными программами и т.д. В качестве примера можно отметить постоянные взломы баз данных мобильных операторов с дальнейшим использованием полученной информации в различных целях (получение паспортных данных, рекламные рассылки, последующее использование в мошеннических целях и т.д.)

Преступления, связанные с получением экономической выгоды, например фишинг. Фишинг – самый распространенный вид мошенничества в Интернете. Главная цель данной «преступной махинации» – завладеть логином и паролем виртуальной учетной записи пользователя, и как следствие воспользоваться его личными данными в преступных целях (данные банковских карт, электронные кошельки, «очень личная информация» с перспективой вымогательства и т.д.). Как правило, данное преступное деяние совершается путем рассылки интернет-писем или сообщений в социальных сетях со ссылкой на поддельный сайт. На сайте преступники всеми способами пытаются заставить интернет-пользователя ввести данные своей учетной записи. Фишинговые направленные атаки стали называться так из-за того, что мошенники случайных жертв используют при этом мошенническую или поддельную электронную почту в качестве приманки. Многие ученые считают, что фишинг – одна из разновидностей социальной инженерии, основанная на незнании пользователями основ сетевой безопасности. Также многие аналитики утверждают, что около 70 % фишинговых атак успешны.

Посредством фишинговых рассылок происходят любые крупные утечки персональных данных в сети Интернет. Целью данного вида преступлений является незаконное получение конфиденциальной информации злоумышленниками.

Практикуется данный вид киберпреступлений весьма часто и масштабно, в том числе и в нашей стране. Так, в июле 2019 года была зафиксирована весьма масштабная фишинг-атака с применением вируса-

шифровальщика на менеджеров многих ТОПовых компаний России. По данным пресс-релиза крупнейшего игрока рынка IT-безопасности Group-IB за сутки было распространено более 1100 виртуальных сообщений с вирусом. Всего за 3-й квартал 2019 года было зафиксировано более 6,5 тыс. таких сообщений [9].

По данным исследования Qrator Labs, наиболее часто компании из финансового сектора сталкиваются с фишингом (30 %) и DDoS-атаками (26 %). 6 ноября 2018 года Kaspersky (ранее Лаборатория Касперского) сообщила, что ее решения заблокировали за 3-й квартал 2018 года более 137 миллионов попыток пользователей перейти на фишинговые страницы – это на 28 % больше, чем в предыдущем периоде. При этом свыше трети фишинговых атак (35 %) пришлось на организации финансовой категории: банки, платежные системы, интернет-магазины [5]. Все эти многочисленные поддельные страницы были созданы с одной целью – получить конфиденциальные данные пользователей, которые открыли бы злоумышленникам, помимо всего прочего, доступ к частным кошелькам и банковским счетам жертв.

Киберпреступники направляют свою фишинговую активность не только в целях массового распространения на неизвестных пользователей, но и на определенных лиц, небольшие социальные группы, выделяемые по профессиональному признаку. Чаще всего это менеджеры крупных компаний, банковские работники. Самый популярный путь индивидуально направленного преступного деяния осуществляется через электронную почту. Преступник, получив данные «ключевой» финансовой фигуры в определенной организации, начинает манипулировать финансовыми операциями, и как результат, денежными потоками в данной организации. Злоумышленник пытается вывести активы из фирмы, отдавая лжеразпоряжения и приказы от имени ключевого сотрудника, переводя их на свои поддельные счета.

Стоит также отметить, что не все специалисты в сфере IT-безопасности относятся к фишингу как к «серьезным» киберпреступлениям. По мнению Арона Хигби, фишинг стоит рассматривать как низкотехнологичную атаку. Согласно его массовым высказываниям и публикациям относительно преступников, их никогда не волнует, кто будет их целью, они используют большую сеть, на которую «ловят» как можно больше «рыбы». Создаются такие компании, как Spear Phishing, которые имеют основную цель – целенаправленное проникновение в одну организацию, посредством изучения имен и процессов внутри компании [8].

Если проанализировать масштабный, массовый фишинг и индивидуальные фишинговые атаки, то можно сделать заключение, что второй вид фишинговых атак является более сложным и спланированным. Как правило, при массовом фишинге используются уже готовые автоматизированные системы, которые могут осуществлять свою деятельность автономно. При индивидуальном фишинге злоумышленник подходит к процессу создания поддельной информации (сайтов, учетных записей) более целенаправленно и творчески. Он проводит довольно большую аналитическую работу, изучая все особенности и манеры жертвы, ее привычки и интересы. Затем вычисляет возможные «слабые места». Нередко для более эф-

фективной деятельности и увеличения положительной вероятности получения чужих данных преступник использует метод социального инжинеринга (использование нескольких видов киберпреступлений), доминирующим из которых выступает фишинг.

Специалисты в области IT-безопасности отмечают, что в условиях современного функционирования данных в сети Интернет большинство фишинговых ссылок и лжедокументов размещается на базе больших и популярных законных сайтах. Как правило, данные сайты имеют огромные архивы и довольно большой объем информации, в связи с чем сотрудники IT-безопасности данного сайта не успевают досконально обрабатывать всю поступающую и размещающуюся информацию на законном ресурсе. Преступников и их фишинговых детищ при таких условиях довольно сложно выявить и вовремя заблокировать.

Преступления против свобод и неприкосновенности личности. К данным понятиям можно отнести кибербуллинг, интернет-грумминг и секстинг. Основные жертвы данных преступлений – несовершеннолетние.

Кибербуллинг или интернет-травля – это осознанные и целенаправленные оскорбления, угрозы, компроматы в виртуальном пространстве, которые длятся в течение продолжительного периода времени. Данная травля осуществляется посредством электронных писем, социальных сетей, видеопорталов и т.д. Данное преступное деяние можно трактовать как вмешательство в личное пространство и ущемление свобод и достоинств личности. По данным исследования, проведенного корпорацией Mail.ru Group совместно с компанией Research Me, большинство российских интернет-пользователей (58 %) сталкивались с травлей в Интернете, в том числе с негативными комментариями в свой адрес. Самыми распространенными формами выражения агрессии респонденты назвали разовые комментарии, осуждение действий других людей и троллинг. Наиболее популярными поводами для травли в Интернете являются сексуальная ориентация, несоответствие стандартам красоты и онлайн-активность. Также выяснилось, что мужчины чаще подвергаются кибербуллингу, чем женщины (28 % против 21 %): первых травят за жизненные неудачи, вторых – за внешность. Тем не менее онлайн-агрессия не воспринимается россиянами как повод обратиться за помощью: 71 % жертв предпочли справляться с этой проблемой самостоятельно [1].

Число данных преступлений также растет. Согласно мониторинговому центру при Общественной палате РФ, в 2019 году порядка 500 эпизодов кибербуллинга.

Как показывает статистика, большинство жертв кибербуллинга – это подростки в возрасте от 12 до 17 лет.

Отдельно хотелось сказать о втором понятии – грумминге. *Интернет-грумминг* – это своеобразный подход взрослого человека к несовершеннолетним с сексуальными целями посредством Интернета. Можно сказать, что это виртуальное домогательство, совращение несовершеннолетних. Многие аналитики считают, что грумминг в условиях современного мира – это идеальное орудие для педофилов.

И последнее понятие, *секстинг* – пересылка информации интимного содержания посредством информационных технологий (фотографии, видео, сообщения и т.д.). Данное понятие появилось относительно недавно

в Новой Зеландии и связано с поступком 13-летней школьницы. Однако данное понятие в законодательствах многих государств попадает под уголовную ответственность, и рассматривается как синоним распространения детской порнографии.

Преступления, связанные с содержанием контента и нарушением авторских прав. Примерами данных противоправных деяний выступает распространение порнографии и незаконное распространение фильмов, музыки и т.д.

Кибертерроризм. Данное понятие возникло вследствие интеграции виртуального пространства с государством и основными сферами жизни общества. Под данным термином понимают преступные действия, направленные на дезорганизацию электронной, информационной системы общества, вследствие которых может быть причинен большой вред человеку, обществу и государству. Основная особенность данного вида киберпреступления – масштабность. Логично предположить, что главная цель данного противоправного деяния – нанести как можно больший вред человеку, чтобы показать авторитет или, как правило, воздействовать на решения органов власти. Красочным примером данного понятия может служить взлом системы NASA в 2015 году. Тогда произошла утечка важной информации, которая представляла государственную тайну и выражала национальный интерес.

Говоря о видах киберпреступлений, хотелось бы отдельно отметить ряд возможных интернет-угроз, которые тесно связаны и в определенном смысле раскрывают данное понятие. Большинство киберпреступлений направлены против виртуальных данных пользователей, а получить доступ к виртуальной среде возможно только посредством сети Интернет. Итак, среди основных угроз можно выделить:

- спам – так называемую вредоносную рекламу. Данная «рекламная информация» либо уже содержит шпионское программное обеспечение, либо переводит пользователей на сайт с вредоносной программой;

- фишинг – данное понятие раскрыто выше, однако хотелось бы отметить явное отличие фишинговых атак от спама. Спамы, как правило, рассылаются огромной группе пользователей, а фишинг имеет определенную целевую аудиторию;

- интернет-атаки – направленная деятельность злоумышленников на взлом компьютеров и кражи данных посредством сети Интернет. Хотелось бы отметить, что в последнее время стали популярны PDF-атаки; связана такая популярность с малозащищенностью и уязвимостью PDF-фалов;

- социальные сети – это очень актуальное и перспективное направление реализации киберпреступлений. На просторах социальных сетей распространяется огромное число вредоносных ссылок и программ;

- веб-приложения – это относительно новое направление интернет-угроз. Злоумышленники крадут целые базы данных пользователей через «поддельные» приложения;

- интернет-мошенничество – очень популярный вид реализации интернет-преступлений. Существует огромное число разнообразных схем от банальных до очень сложных (сюда можно отнести «лотереи», «подружка», «приглашение на работу», «ошибка», «нигерийская афера» и др.).

Фантазия киберпреступников не стоит на месте и поэтому появляется все больше новых мошеннических схем.

Говоря о большой популярности киберпреступлений, необходимо отметить тот факт, что многие преступления не то что не расследуются, они вообще не учитываются. Большое число преступлений вследствие многих причин (незначительный ущерб, нежелание жертвы обращаться к правоохранительным органам, невозможность выявления самого факта преступления и т.д.) так и остаются неизвестными и «сходят с рук» преступникам. Стоит подчеркнуть, что данная безнаказанность служит своего рода толчком для популярности киберпреступлений.

Как правило, киберпреступники или так называемые хакеры имеют очень высокий уровень теоретических и практических знаний, они своего рода «компьютерные гении» [3, с. 47]. У некоторых данный талант проявляется довольно в раннем возрасте. Например, известен случай, когда 14-летний подросток взломал сервер NASA для того, чтобы хранить там свои виртуальные данные.

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

Очевидно, что существует и юридическая проблема. Сюда мы можем отнести малорегламентированность или вовсе отсутствие регламентации со стороны нормативно-правовых актов. Суть данной проблемы заключается в отсутствии актуального законодательства, которое отвечало бы современным реалиям. Порой, не то что не регулируются уголовно-процессуальные действия со стороны государства, а вообще отсутствуют уголовная или иные виды ответственности за деяния в виртуальной сфере.

И еще одна немаловажная причина – отсутствие необходимых технических средств противодействия киберпреступлениям или техническая проблема. Порой техника преступников в разы превосходит технику правоохранительных органов. Данный факт показывает невозможность раскрытия некоторых преступлений в связи с некой отсталостью в «технологиях».

Таким образом, киберпреступность и киберпреступления становятся актуальными угрозами в сфере безопасности человека, общества и государства. Они представляют реальную угрозу не только для отдельных государств, но и для всего мирового сообщества в целом. Появившись сравнительно недавно, они с каждым днем набирают популярность и открывают новое огромное поле деятельности преступных кругов. Данная тенденция является опасной и может привести к непредсказуемым последствиям.

Список литературы

1. **Исследование** Mail.ru Group к 25-летию Рунета [Электронный ресурс]. URL: <https://corp.mail.ru/ru/press/releases/10391/> (дата обращения: 11.05.2020)
2. **Итоги** исследования: Киберпреступность в России и мире [Электронный ресурс]: URL: <https://rb.ru/news/itogi-issledovaniya-kiberprestupnost-v-rossii-i-mi/> (дата обращения: 11.05.2020)
3. **Карпова Д. Н.** Киберпреступность: глобальная проблема и ее решение // Власть. 2014. № 8. С. 46 – 50.
4. **Номоконов В. А., Тропинина Т. Л.** Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. № 1 (24). С. 45 – 55.
5. **Русские хакеры** переключились с российских банков на иностранные. Но эксперты ждут возобновления атак от молодого поколения [Электронный ресурс]: URL: <https://www.rbc.ru/finances/29/11/2019/5ddf8e0b9a7947adab57e61b> (дата обращения: 11.05.2020)
6. **Статистические данные** Генеральной Прокуратуры РФ [Электронный ресурс]: URL: <https://genproc.gov.ru/stat/data/1557476/> (дата обращения: 11.05.2020)
7. **Статистические данные** МВД РФ [Электронный ресурс]: URL: <https://мвд.рф/reports/item/18556721> (дата обращения: 11.05.2020)
8. **Типы** фишинговых атак и способы их выявления [Электронный ресурс]: URL: <https://www.osp.ru/winitpro/2019/03/13054903/> (дата обращения: 11.05.2020)
9. **Фишинг** [Электронный ресурс]. URL: [http://www.tadviser.ru/index.php/Статья:Фишинг_\(phishing\)](http://www.tadviser.ru/index.php/Статья:Фишинг_(phishing)) (дата обращения: 11.05.2020)
10. **Чекунов И. Г.** Киберпреступность: понятие, классификация, современные вызовы и угрозы // Молодые ученые. 2012. № 3. С. 178 – 186.

References

1. **Available at:** <https://corp.mail.ru/ru/press/releases/10391/> (accessed 11 May 2020).
2. **Available at:** <https://rb.ru/news/itogi-issledovaniya-kiberprestupnost-v-rossii-i-mi/> (accessed 11 May 2020).
3. **Karpova D.N.** [Cybercrime: a global problem and its solution], *Vlast'* [Power], 2014, no. 8, pp. 46-50. (In Russ.).
4. **Nomokonov V.A., Tropinina T.L.** [Cybercrime as a new criminal threat], *Kriminologiya: vchera, segodnya, zavtra* [Criminology: yesterday, today, tomorrow], 2012, no. 1 (24), pp. 45-55. (In Russ.).
5. **Available at:** <https://www.rbc.ru/finances/29/11/2019/5ddf8e0b9a7947adab57e61b> (accessed 11 May 2020)
6. **Available at:** <https://genproc.gov.ru/stat/data/1557476/> (accessed 11 May 2020)
7. **Available at:** <https://мвд.рф/reports/item/18556721> (accessed 11 May 2020)
8. **Available at:** <https://www.osp.ru/winitpro/2019/03/13054903/> (accessed 11 May 2020)
9. **Available at:** [http://www.tadviser.ru/index.php/Статья:Fishing_\(phishing\)](http://www.tadviser.ru/index.php/Статья:Fishing_(phishing)) (accessed 11 May 2020)
10. **Chekunov I.G.** [Cybercrime: concept, classification, modern challenges and threats], *Molodyye uchenyye* [Young scientists], 2012, no. 3, pp. 178-186. (In Russ.).

The Phenomenon of Cybercrime in the 21st Century

T. V. Plotnikova, *Cand. of Legal Sci., Associate Professor,
Department of Special Training and National Security,
Derzhavin Tambov State University, Tambov, Russia;
plotnikova-tmb@mail.ru*

O. V. Kotelnikova, *Cand. of Ped. Sci., Associate Professor,
Department of Special Training and National Security,
Derzhavin Tambov State University, Tambov, Russia;
cotelnikova.oksana@yandex.ru*

The spread and development of the "Internet" has erased the boundaries of communication and the dissemination of information. With the massive spread of computers, the world community is faced with such phenomena as illegal activities using a computer (and / or against computers), as well as this activity through the Internet. Many scientists and experts distinguish between cybercrime as a legal category and as a social phenomenon. The first is characterized by a specific unlawful act using a computer, computer network or the Internet. The qualification of these acts within the framework of cybercrime is not in doubt and complexity, because here are clearly expressed signs of a virtual illegal act. These illegal acts are aimed at all spheres of public life. There is no clear division into specific types of cybercrime. For cybercriminal prosecution, it is necessary to prove their involvement in this illegal act. The "virtual traces" of an illegal act are easy to hide due to the ease of changing and destroying computer information. A procedure for processing and seizing evidence is quite complicated, and sometimes impossible. These facts make it difficult to prove the guilt and involvement of a person in a virtual crime, thereby contributing to an increase in the percentage of unsolved crimes. Cybercrime has become a threat to security of man, society and the government. It poses a real threat not only to individual states, but also to the entire world community as a whole.

Keywords: cybercrime; phishing; cyberbullying; internet grooming; sexting; cyber terrorism; counteraction system.

© Т. В. Плотникова, 2020

© О. В. Котельникова, 2020

Статья поступила в редакцию 14.05.2020

При цитировании использовать:

Плотникова Т. В., Котельникова О. В. Феномен киберпреступности в условиях XXI века // *Право: история и современность*. 2020. № 3(12). С. 141 – 150. doi: 10.17277/pravo.2020.03.pp.141-150