DOI 10.20310/2587-9340-2018-2-8-96-107
УДК 004.056+343.98

КИБЕРПРЕСТУПНОСТЬ КАК УГРОЗА МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ

В.В. Харин, Т.В. Плотникова
Тамбовский государственный университет им. Г.Р. Державина
392000, Российская Федерация, г. Тамбов, ул. Интернациональная, 33
E-mail: vadimka.va@mail.ru, plotnikova-tmb@mail.ru

Аннотация. С появлением первого компьютера жизнь человека изменилась навсегда. Виртуальное пространство стало составной частью нашей жизни. Однако и преступность эволюционировала, появился новый специфический вид – киберпреступность. В данном исследовании рассмотрены особенности нового вида преступлений. Показаны история первых преступных деяний, формирование понятия киберпреступности и ее последующее развитие. Несмотря на стремительную популярность среди криминальных кругов, в науке нет четко определенного и общепринятого понятия киберпреступления. Данные деяния характеризуются весьма специфичными признаками. Это подталкивает рассматривать киберпреступления как не совсем стандартные преступления. Показана классификация и основные угрозы, порождаемые данными преступными деяниями. Рассмотрено законодательство России и зарубежных стран. В России, как и в некоторых зарубежных странах, основной уклон делается на закреплении ответственности за данное деяние в Уголовном кодексе. При этом стоит отметить, что государства довольно быстро реагируют на появление новых угроз и стараются сформировать актуальное законодательство. Выявлены и обоснованы проблемы раскрытия киберпреступлений. Данные преступления являются весьма актуальными угрозами в сфере безопасности человека, общества и государства. Киберпреступность представляет собой угрозу не только национального и регионального масштаба, но и грозит международной безопасности.

Ключевые слова: киберпреступность; кибертерроризм; виртуальное пространство; информационная безопасность

В 1941 г. в США был создан первый компьютер. Это изобретение, которому на то время не уделялось столь важное и огромное внимание, стало проводником в огромный и непредсказуемый мир виртуальной информации. Мы живем в условиях, где инновации и информационные технологии играют ведущую роль в жизни общества. Невозможно

представить жизнь современного человека без виртуального пространства. Процессы глобализации, бурное развитие компьютерных технологий, всеобщая интеграция повлекли за собой возникновение современного информационного общества. Цивилизованное государство и общество не могут существовать без параллельной виртуальной реальности. В цифровой реальности находится огромное количество личной и служебной информации, документации, денежных средств, активов. Она представляет собой своеобразную огромную базу по обмену информацией, развлечений, работы и т. д.

Однако данный виртуальный мир хранит и свои «сюрпризы». В условиях информатизации и глобальной компьютеризации произошли весомые изменения во всех сферах жизни общества. Не обошел данный процесс изменения и преступную среду, а именно: появилась новая форма преступлений – преступления в сфере информационных технологий, или киберпреступления.

Данный термин впервые появился в середине 70-х гг. XX века в США, именно в это время были совершены первые преступления с использованием информационных технологий. В 1973 г. кассир местного банка в Нью-Йорке использовал компьютер, чтобы украсть более 2 млн долларов. Причем совершил он данное противоправное деяние совершенно простым способом – перевел сумму на свой личный счет. Само официальное понятие, а также основные признаки киберпреступления были сформулированы лишь в 1974 г. на Конференции Американской ассоциации адвокатов [1]. Позже, только в 1986 г., был принят первый нормативно-правовой документ противодействия киберпреступлениям – «Закон о мошенничестве с использованием компьютеров».

Несмотря на это, до сих пор нет четко определенного и общепринятого понятия данного преступления. Обобщенно мы можем сказать, что киберпреступления – это преступления, которые совершаются в так называемом виртуальном пространстве. В состав данного понятия включены преступления, которые совершаются с помощью компьютерной системы или Сети (Интернета), в рамках компьютерной системы или Сети (Интернет), или против компьютерной системы или Сети (Интернет). Киберпреступность – это довольно обширное понятие. К данному виду противоправных деяний мы можем отнести и преступления, где компьютер, информационная сеть (Интернет), данные и т. д. – являются объектом, и преступления, где компьютеры используются как средство и орудие. К этому же понятию многие ученые относят и действия в информационном пространстве для поддержания условий

преступной общности, группы, например, использование электронной почты для коммуникации, обмен криминальным опытом и специальными познаниями.

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.

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[1].

Преступления, которые направлены против компьютерных систем и баз данных. Огромный перечень киберпреступлений можно

[1] Юридический интернет-журнал «Первый юрист». URL: https://urist.one/dolzhnostnye-prestupleniya/kiberprestupnost/kiberprestuplenie.html (дата обращения: 18.06.2018).

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 рассылок 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. Многие ученные 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.

Преступления против свобод и неприкосновенности личности. К данным понятиям можно отнести кибербуллинг, интернет-груминг и секстинг. Основные жертвы данных преступлений – это 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. Как показывает статистика, большинство жертв кибербуллинга – это подростки в возрасте от 12 до 17 лет. Отдельно хотелось бы сказать о втором понятии, о груминге. Интернет-груминг – это своеобразный подход взрослого человека к несовершеннолетним с сексуальными целями посредством Интернета. Можно сказать, что это виртуальное домогательство, совращение несовершеннолетних. Многие аналитики считают, что груминг в условиях современного мира – это идеальное орудие для педофилов. И последнее понятие – секстинг – пересылка информации интимного со-

держания посредством информационных технологий (фотографии, видеосообщения 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 выступают распространение порнографии и незаконное распространение фильмов, музыки и т. д.

Кибертерроризм. Данное понятие возникло вследствие очень сильной 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 г. 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 направлено против виртуальных данных пользователей, а получить доступ к виртуальной среде возможно только посредством сети Интернет. Итак, среди основных угроз можно выделить следующие[2].

Спам – так называемая вредоносная реклама. Данная «рекламная информация» либо уже содержит шпионское ПО, либо переводит пользователей на сайт с вредоносной программой.

Фишинг – данное понятие раскрыто выше, однако хотелось бы отметить явное отличие фишинговых атак от спамов. Спамы, как правило, рассылаются огромной группе пользователей, а фишинг имеет оп-

[2] Интернет портал «Центр обучения IT». URL: http://sys-team-admin.ru/stati/bezopasnost/170-kiberprestupnost-ponyatie-vidy-i-metody-zashchity.html (дата обращения: 18.06.2018).

ределенную целевую аудиторию, которой и рассылаются вредоносные сообщения.

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 количество 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 количество 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.

Тенденция роста данных преступлений очень высока. По статистике, каждую секунду в мире совершается около 18 киберпреступлений, то есть около полутора миллионов преступлений в день, и этот показатель постепенно растет. 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).

Количество киберпреступлений постоянно растет. На территории Российской Федерации за 2010 г. было зафиксировано 7974 преступления данного вида. В 2012 г. – 10227 киберпреступлений. В период с 2013 по 2016 г. количество зафиксированных преступлений увеличилось с 10 до 66 тысяч. А на протяжении 2017 г. было выявлено и зафиксировано 90688 преступлений. Как мы видим, темп роста киберпреступлений нарастает с каждым годом. Также следует учитывать тот факт, что данная статистика официальная. А как известно, огромное количество киберпреступлений не фиксируется или вовсе умалчивается. Мы можем предположить, что количество и темп нарастают намного быстрее, чем показывает официальная статистика.

Представленные данные являются лишь статистикой по России. Трудно представить размер преступной деятельности в данном направлении по всему миру. Особенно стоит отметить размер ущерба, который составляет около 110 млрд долларов в год. Основываясь на представленных данных и показателях, мы можем сделать вывод, что киберпреступления являются весьма опасной угрозой для безопасности государственной и международной стабильности.

Довольно интересно будет посмотреть противодействия преступлениям в виртуальном пространстве со стороны государства в форме законодательства. По данным нормативно-правовых актов можно раскрыть характер и степень противодействия нарастающей международной угрозе.

Итак, страна, возглавляющая рейтинг по количеству киберпреступлений, – Соединенные Штаты Америки. США – одно из первых государств, которое обратило внимание на киберугрозы. Стоит отметить, что здесь в 1986 г. был принят первый закон – Закон о компьютерном мошенничестве и злоупотреблениях с их использованием (Computer fraud and abuse act (CFAA)) [2]. Данный вид преступлений нашел свое отражение и в документе, являющимся основным для обеспечения национальной безопасности государства – Стратегии национальной безопасности (2017 г.). В связи с особенностью территориального устройства и политическим режимом отдельные особенности киберпреступлений нашли свое отражение в федеральных законах и законах отдельных штатов. Также стоит отметить, что в 2018 г. была обновлена Стратегия кибербезопасности США, разработанная и принятая в далеком 2003 г.

Говоря о Европе, хотелось бы отметить нормативно-правовой акт, который поддержали 46 государств мира (и 23 ратифицировали) – это Конвенция Совета Европы о киберпреступности, вступившая в силу 1 ноября 2004 г. Эта конвенция представляет собой набор основных принципов для любой страны, разрабатывающей всеобъемлющее национальное законодательство по киберпреступности, а также рамки для международного сотрудничества между странами-участницами в сфере киберпреступлений. Можно сказать, что это своего рода шаблон для законодательства отдельных стран в информационной сфере.

В Великобритании существует свой нормативно-правовой акт – Акт о компьютерных злоупотреблениях. Данный документ был принят еще в 1990 г., и со временем в него вносились небольшие изменения, отражающие развитие общественных отношений в данной сфере. Раз-

меры наказания за совершение преступления в компьютерной сфере – штраф, или лишение свободы на срок от 6 месяцев до 5 лет.

В Голландии борьба с киберпреступностью ведется путем введения новых статей в действующий Уголовный кодекс. Был создан целый государственный орган, основным направлением которого является формирование законодательной базы противодействия киберпреступлениям – это Консультативный комитет по компьютерным преступлениям. Как один из примеров деятельности данного органа можно отметить принятие в 1993 г. «Закона о компьютерных преступлениях», дополняющий УК Голландии новыми составами. Функционирует данный комитет и в настоящее время.

В Германии также основное законодательное противодействие реализуется через Уголовный кодекс. В данной стране встал вопрос о закреплении уголовной ответственности за преступления в сфере компьютерной информации в УК уже в 1986 г. (по данным статистики, в 1987 г. было зарегистрировано 3355 таких преступлений. Первые изменения были внесены уже 1 августа 1987 г. При этом в УК Германии не существует специальной главы, посвященной киберпреступлениям, нормы, содержащие ответственность за преступления в сфере компьютерной информации, рассредоточены по разделам Особенной части Кодекса.

Рассматривая законодательство против киберпреступлений в Российской Федерации, мы должны, в первую очередь, обратить свое внимание на Стратегию Национальной Безопасности РФ. Прямого указания на киберпреступность, как угрозу для национальной безопасности, в Стратегии нет. Однако указания (предпосылки) на данный вид преступлений находятся в статьях 21 и 22, они также указаны в стратегических национальных приоритетах – Государственной и общественной безопасности (статьи 43 и 47).

Своего рода логическим продолжением Стратегии Национальной Безопасности РФ является Доктрина информационной безопасности РФ (ИБ), которая была принята 5 декабря 2016 г. Данная доктрина необходима для формирования государственной политики и выработки совершенствования системы обеспечения информационной безопасности. В документе определены следующие основные угрозы и характеристики состояния ИБ: возрастают масштабы компьютерной преступности, прежде всего в кредитно-финансовой сфере; методы, способы и средства совершения компьютерных преступлений становятся все

изощреннее; повышается сложность и количество скоординированных компьютерных атак.

Говоря об Уголовном кодексе Российской Федерации, следует отметить, что в его составе киберпреступления выделены в отдельную главу – главу 28 «Преступления в сфере компьютерной информации». Данная глава состоит из 4 статей: неправомерный доступ к компьютерной информации (статья 272 УК РФ); создание вредоносных программ (статья 273 УК РФ); нарушение правил хранения компьютерной информации (статья 274 УК РФ); воздействие на критическую информационную инфраструктуру Российской Федерации (статья 274.1 УК РФ). Помимо этого, мы можем квалифицировать киберпреступления и по обычным статьям, таким, как клевета (статья 128.1 УК РФ); нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (статья 138 УК РФ); нарушение авторских и смежных прав (статья 146 УК РФ); незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (статья 183 УК РФ).

Рассматривая законодательную базу стран мира и России, мы можем сделать вывод, что государства максимально быстро реагируют на новые угрозы и стараются сформировать соответствующее законодательство, отвечающее современным реалиям. Однако почему при таких условиях популярность киберпреступности растет, а процесс раскрытия данных преступлений становится все сложнее?

Отвечая на данный вопрос, мы должны, в первую очередь, отразить тот факт, что многие преступления не то что не расследуются, они вообще не учитываются. Большое количество 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 также подчеркнуть, что данная безнаказанность служит своего рода толчком для популярности киберпреступлений.

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

Третья проблема 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 данных доказательств. Данные факты затрудняют доказывание вины и причастности лица к виртуальному преступлению, тем самым способствуя увеличению процента нераскрытых преступлений.

Следующая причина выражена в юридических проблемах. 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 отсутствует 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 превосходит технику правоохранительных органов. Данный факт показывает невозможность раскрытия некоторых преступлений в связи с некой отсталостью в «технологиях» [1].

Таким образом, мы можем сделать вывод, что киберпреступность и киберпреступления становятся весьма 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 относительно недавно, они с каждым днем набирают популярность и открывают новое огромное поле деятельности преступных кругов. Данная тенденция является весьма опасной и может привести к непредсказуемым последствиям.

Список литературы

1. *Айков Д., Сейгер К., Фонсторх У.* Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями. М.: Мир, 1999. 351 с.
2. *Фролов М.Д.* Уголовная ответственность за мошенничество в сфере компьютерной информации по законодательству стран Северной и Южной Америки, Океании, Азии и Африки // Административное и муниципальное право. 2015. № 11 (95). С. 1164-1168. DOI 10.7256/1999-2807.2015.11.16911.

3. *Вехов В.Б.* Компьютерные преступления: способы совершения и раскрытия / под ред. Б.П. Смагоринского. М.: Право и закон, 1996. 182 с.

Поступила в редакцию 23.07.2018 г.
Отрецензирована 24.08.2018 г.
Принята в печать 04.10.2018 г.
Конфликт интересов отсутствует.

Информация об авторах
Харин Вадим Витальевич – контролер Управления безопасности. Тамбовский государственный университет им. Г.Р. Державина, г. Тамбов, Российская Федерация. E-mail:vadimka.va@mail.ru
Плотникова Татьяна Владиславовна – кандидат юридических наук, доцент, доцент кафедры специальной подготовки и обеспечения национальной безопасности, зам. директора института права и национальной безопасности по инновационно-производственной работе. Тамбовский государственный университет им. Г.Р. Державина, г. Тамбов, Российская Федерация. E-mail: plotnikova-tmb@mail.ru

Для цитирования
Харин В.В., Плотникова Т.В. Киберпреступность как угроза международной безопасности // Актуальные проблемы государства и права. 2018. Т. 2. № 8. С. 96-107. DOI 10.20310/2587-9340-2018-2-8-96-107.

DOI 10.20310/2587-9340-2018-2-8-96-107

CYBERCRIME AS A THREAT TO INTERNATIONAL SECURITY

V.V. Harin, T.V. Plotnikova
Tambov State University named after G.R. Derzhavin
33 Internatsionalnaya St., Tambov 392000, Russian Federation
E-mail: vadimka.va@mail.ru, plotnikova-tmb@mail.ru

Abstract. With the advent of the first computer, human life changed forever. Virtual space has become an integral part of our lives. However, crime has evolved, a new specific species has emerged called cybercrime. In this study, we consider the features of a new type of crime. The history of the first criminal acts, the formation of the concept of cybercrime and its subsequent development are shown. Despite the rapid popularity among criminal circles, there is no clearly defined and generally accepted concept of cybercrime in science. These acts are characterized by very specific features. This encourages considering cybercrimes as not quite the standard of a crime. The classification and the main threats generated by these criminal acts are shown. The legislation of Russia and foreign countries is considered. In Russia, as in some foreign countries, the main focus is on fixing the responsibility for this

act in the Criminal Code. At the same time, it should be noted that the states react rather quickly to the emergence of new threats and try to form relevant legislation. Identified and justified the problem of disclosure of cybercrime. These crimes are very relevant threats to human security, society and the state. Cybercrime is not only a national and regional threat, but also a threat to international security.

Keywords: cybercrime; cyber terrorism; cyberspace; information security

References

1. Aykov D., Seyger K., Fonstorkh U. *Komp'yuternyye prestupleniya. Rukovodstvo po bor'be s komp'yuternymi prestupleniyami* [Computer Crimes. Guidelines for Combating Computer Crimes]. Moscow, Mir Publ., 1999, 351 p. (In Russian).
2. Frolov M.D. Ugolovnaya otvetstvennost' za moshennichestvo v sfere komp'yuternoy informatsii po zakonodatel'stvu stran Severnoy i Yuzhnoy Ameriki, Okeanii, Azii i Afriki [Criminal liability for computer fraud in the legislation of the countries of North and South America, Oceania, Asia and Africa]. *Administrativnoye i munitsipal'noye pravo – Administrative and Municipal Law*, 2015, no. 11 (95), pp. 1164-1168. DOI 10.7256/1999-2807.2015.11.16911. (In Russian).
3. Vekhov V.B. *Komp'yuternyye prestupleniya: sposoby sovershenia i raskrytiya* [Computer Crimes: Commission and Disclosure Methods]. Moscow, Pravo i zakon Publ., 1996, 182 p. (In Russian).

Received 23 July 2018
Reviewed 24 August 2018
Accepted for press 4 October 2018
There is no conflict of interests.

Information about the authors

Harin Vadim Vitalyevich – Security Management Controller. Tambov State University named after G.R. Derzhavin, Tambov, Russian Federation. E-mail: vadimka.va@mail.ru
Plotnikova Tatyana Vladislavovna – Candidate of Jurisprudence, Associate Professor, Associate Professor of Special Training and National Security Department, Deputy Director of the Institute of Law and National Security for Innovation and Production Work. Tambov State University named after G.R. Derzhavin, Tambov, Russian Federation. E-mail: plotnikova-tmb@mail.ru

For citation

Harin V.V., Plotnikova T.V. Kiberprestupnost' kak ugroza mezhdunarodnoy bezopasnosti [Cybercrime as a threat to international security]. *Aktual'nye problemy gosudarstva i prava – Current Issues of the State and Law*, 2018, vol. 2, no. 8, pp. 96-107. DOI 10.20310/2587-9340-2018-2-8-96-107. (In Russian, Abstr. in Engl.).