УДК 343.9

И.А. Ефремова, А.Б. Смушкин, А.Г. Донченко, П.А. Матушкин

КИБЕРПРОСТРАНСТВО КАК НОВАЯ СРЕДА ПРЕСТУПНОСТИ

Комплексно исследуется кибернетическое пространство как новая среда преступности. Представлено иное видение дефиниции термина «кибернетическое пространство», выявлены особенности кибернетического пространства. Осуществлен анализ материального, информационного, социального, психологического аспектов кибернетического пространства, а также концепции киберпространства в криминалистике. Сформулировано авторское определение киберпреступности.
Ключевые слова: киберпреступность; киберпространство; киберсфера; кибербезопасность; защита информации

В последнее время активно ворвалась в правовое, информационное и социальное поле новая категория – киберпространство (виртуальное пространство, инцидентное компьютерное пространство и т.д.), которое стало новой средой для возникновения, существования и развития преступности (киберпреступности). С развитием информационно-телекоммуникационных технологий преступность в киберпространстве в последнее десятилетие стала одной из острейших проблем не только для Российского государства, но и для всего мирового сообщества. Все чаще и чаще преступные посягательства совершаются в новой среде – киберпространстве (например, хищения денежных средств с электронных счетов – фишинг). Можно отметить, что киберпреступность стала новой генерацией преступников, имеющей существенные отличия от «классических» преступников, вызванные именно спецификой киберпространства. Преступников, действующих в киберпространстве, в большинстве своем характеризует высокий интеллектуальный и образовательный уровень. Они раньше других (и уж точно раньше правоохранительных органов) берут на заметку новые концепции, связанные с постоянной трансформацией и изменением киберпространства: блокчейн, распределенное хранение информации, удаленная работа на ином устройстве с использованием своего только как «печатной машинки», даркнет с его специфическими характеристиками (тунельной маршрутизацией, «луковичным» принципом шифрования, анонимизацией пользователей и т.д.). Они используют новые методы совершения преступлений: фишинг, торговля «карженными» товарами, взлом аккаунтов и подмена личности владельца, DDOS-атаки и т.д. Преступность в сети также характеризуется специфическими особенностями, непосредственно связанными с киберпространством: трансграничность, возможность формирования преступных групп анонимно или из малознакомых лиц, геймификация совершения преступлений (многие рассматривают свою деятельность как игру, взлом защищенного сайта – как вызов)», дистанционность совершения «классических» преступлений (например, дистанционная торговля наркотиками), возможность автоматизации целых этапов совершения преступлений, возможность перехвата управления и использования в преступных целях частных и государственных устройств (что особо опасно становится с учетом расширения круга применения беспилотных и иных автоматизированных устройств), использование игровой среды (сетевых компьютерных игр) для преступной коммуникации, а также перемещения или легализации (отмывания) денежных средств, полученных преступным путем.

Преступления в киберпространстве оставляют специфическую следовую картину, о чем будет сказано дальше в нашем исследовании.

Специфичность киберпреступности связана в первую очередь с особенностями киберпространства как нового пространства совершения преступлений.

Однако, несмотря на то что преступность активным образом развивается в новой среде – в киберпространстве, среди научного сообщества нет единства во мнении относительно не только содержания новой среды преступности, но и самого ее наименования. Так, некоторые авторы используют оборот «виртуальное пространство» [1], другие – «киберпространство» [2–6], третьи – «информационная сфера» («среда») [7]. Имеются также компромиссные мнения, рассматривающие киберпространство и виртуальное пространство как тождественные понятия [8]. Однако, несмотря на схожесть данных терминов, они существенным образом разнятся. Виртуальная реальность представляет собой искусственную среду, совокупность ощущений человека, созданных посредством использования им различных технических, электронных устройств [9], в то время как кибернетическое пространство представляет собой обобщенное наименование упорядоченной в соответствии с определенными протоколами автоматизированной обработки информации системы программных средств и документальных файлов, расположенных в памяти электронных цифровых устройств или электронной цифровой информации, находящейся в процессе передачи любым доступным способом, либо информации, распределенной в компьютерной системе или сети.

Философы, социологи, криминалисты, специалисты в IT-технологиях, ученые и практики предлагают свои подходы применительно к своим целям и своим дисциплинам. Между тем данный феномен (киберпространство) продуцирует появление новой сетевой культуры, правосознания, а также новых видов правонарушений. С учетом специфики этого нового пространства в науке высказывались предложения о формировании новой комплексной дисциплины «киберология». «Киберология» должна быть именно комплексной дисциплиной, включающей знания психологии, философии, социологии, права, математики, физики и техники, связанных непосредственно с кибер-

нетическим пространством, а именно с его историей возникновения и развития, функционирования, обеспечением кибернетической безопасности [10. С. 85].

Некоторые авторы вообще считают киберпространство абстракцией. Подобное суждение высказывает Г.А. Атаманов [11]. Однако каким образом форма бытия реальных предметов может быть условной, абстрактной?

Впервые упомянул симбиоз кибернетики и пространства Уильям Гибсон в новелле «Сожжение Хром» (1982 г). Именно данный ученый впервые осмелился сделать предположение о взаимодействии (взаимовлиянии) компьютера и нервной системы его пользователя. Позднее Дж. Барлоу рассматривал два уровня киберпространства: первый уровень – уровень обмена информацией, которая происходит в форме программных кодов, порожденных непосредственно киберпространством; второй уровень – уровень виртуальной жизни, которая порождена в процессе обмена между аватарами (объекты, представляющие в виртуальном мире пользователей) информацией [12. С. 28].

Отсутствует единый подход среди правоприменителей не только отечественных, но и зарубежных. Так, Верховный Суд США в одном из решений указывал, что киберпространство представляет собой некий уникальный носитель, уникальность которого заключается в том, что он, не находясь на какой-либо определенной территории, доступен через информационно-телекоммуникационную сеть «Интернет» каждому в любой точке мира [13]. Такой подход не добавляет легкости пониманию содержания данного феномена.

В документах Пентагона, по данным И.М. Попова, киберпространство представляет собой находящийся внутри информационной среды глобальный домен, который состоит из сети информационно-технологических инфраструктур, включая информационно-телекоммуникационные сети, в частности информационно-телекоммуникационную сеть Интернет, компьютерные системы, встроенные процессоры и контроллеры [14]. Недостатком подобного подхода нам видится увеличение неопределенности при его использовании. Оборот «глобальный домен внутри информационной среды» подразумевает наличие в ней иных сущностей и объектов (доменов?) кроме киберпространства. «Контроллеры и процессоры» в контексте данного определения не имеют жесткой «привязки» к аппаратной или программной части компьютеров. Соответственно, не понятно, включается ли в данное определение аппаратная сторона – составные части компьютерного устройства. Неясно, что вообще понимается под информационной средой, частью которой является киберпространство (ноосфера? Совокупность любых информационных объектов?). Межу тем классический принцип логики – принцип Оккама – требует не умножать сущности без необходимости.

В.А. Крайванова определяет киберпространство как «событийно-предметное пространство Интернета» [15]. Однако о каких предметах идет речь, она не уточняет. Подчеркивают значение сети Интернет и некоторые другие авторы. Так, А.В. Нестеров предлагает рассматривать термин «кибернетическое пространство», тождественный термину «интернет-пространство», который, как правило, используется для обозначения на определенной территории наличествующей национальной юрисдикции [16. С. 14].

Как сферу социальной деятельности, связанной с оборотом информации в информационно-телекоммуникационных сетях, в том числе в сети Интернет, определяет киберпространство И.М. Рассолов[17. С. 33]. Д.В. Грибанов, напротив, предлагает понимать под кибернетическим пространством не некую сферу социальной деятельности, а непосредственно совокупность общественных отношений, связанных с информацией, которая обрабатывается посредством ЭВМ [18].

И.М. Дзялошинский выделяет три концепции, три подхода к пониманию кибернетического пространства: во-первых, кибернетическое пространство – обычное пространство, имеющее место расположение и границы. Во-вторых, кибернетическое пространство представляет собой пространство информационных взаимодействий (в данном случае анализируемый термин тождествен терминам «информационное поле», «информационное пространство»). В-третьих, под кибернетическим пространством понимается совокупность социальных структур, которые между собой соединены информационными отношениями (отношениями, связанными с информацией (сбор, обработка и т.д.) посредством глобальных компьютерных сетей) [19].

Нам киберпространство представляется многоаспектной категорией, имеющей философское, социальное, психологическое, криминалистическое, уголовно-правовое, криминологическое и иные измерения. Между тем, как указывают большинство ученых, кибернетическое пространство необходимо рассматривать посредством комплексного подхода, где кибернетическое пространство представляет собой сложное явление, состоящее из системы элементов [2–4].

К особенностям киберпространства можно отнести дигитализацию, виртуализацию реальности, интерактивность, гиперссылку и функцию распространения [20. P. 45]. Дигитализация, или цифровизация всех сфер человеческой жизни, выражается в активной оцифровке всей аналоговой информации. Виртуализация реальности выражается в продуцировании новой реальности существования со своим этикетом, культурой, отсутствием границ, воспроизводством в кибермире отдельных социокультурных процессов реальности, а также проявлением своих собственных. Интерактивность приводит к тому, что пользователь становится активным участником построения киберпространства, внося в него новые знания и тексты, меняя старые и т.д. Это расширяет простор обмена знаниями и достижениями. Гиперссылки позволяют скреплять различные текстуальные и медиаположения вместо краткой отсылки к ним, формируя квазиединый продукт, потенциально имеющий все возможности для раскрытия именно того смысла, который хочет в него вложить автор, и включающий все необходимое для понимания всех смысловых слоев. Кроме того, в глобальном плане гиперссылки обеспечивают единство и взаимосвязь элементов интернета.

Функция распространения при этом означает, что при доступе поисковых систем к новой информации она становится доступной неограниченному кругу пользователей.

В криминалистическом аспекте категорию «киберпространство» можно рассматривать как инцидентное пространство электронных устройств. Спецификой этого пространства является информационное взаимодействие находящихся в нем объектов и действий пользователя, оставляющее в результате электронного следового контакта специфическую группу следов, именуемую виртуальными или электронно-цифровыми. Как отметил Е.П. Ищенко, особенностью данных следов является их многокомпонентный характер [21. С. 186].

В криминалистике концепция «киберпространство» прозвучала впервые в диссертации В.А. Мещерякова, в которую он включает не только системы автоматизированной обработки информации программных средств, но и объекты реального мира, помещения, в которых располагаются ЭВМ и их системы, непосредственно сами ЭВМ и т.д. [5. С. 44]. Похожего подхода придерживались и некоторые другие авторы [6].

Нам представляется, что в данном случае В.А. Мещеряков и другие производят смешение кибернетического и реального пространства. Неужели комната, пока в ней стоит компьютер, будет являться элементом киберпространства, а как только компьютер вынесли за порог – перестает? А во время прохождения дверного проема будет переходное состояние? То же самое можно сказать про технические комплексы обеспечения ее деятельности (системы связи, электропитания, заземления и т.п.). Неужели пока в электропитание, заземление, системы связи подключены к компьютеру, он – элемент киберпространства, а когда то же самое подключение произведено к факсимильному аппарату – нет. Важным вопросом в указанном контексте является также то, что современные смартфоны и планшетные устройства представляют собой те же компьютеры в миниатюре, с чуть другой основной направленностью специализации функций. Пользователь смартфона за день может находиться во множестве помещений.

Можно отметит, что В.А. Мещеряков, на наш взгляд, ошибочно при определении киберпространства, имеющего по определению, информационную структуру, во главу угла ставит именно материальные элементы.

Под кибернетическим пространством мы понимаем обобщенное наименование упорядоченной в соответствии с определенными протоколами автоматизированной обработки информации системы программных средств и документальных файлов, расположенных в памяти электронных цифровых устройств или электронной цифровой информации, находящейся в процессе передачи любым доступным способом, либо информации, распределенной в компьютерной системе или сети. При этом аппаратные средства, обеспечивающие существование киберпространства, нам представляются внешними по отношению к данной системе объектов. Однако и киберпространство, без расположенной в нем хотя бы базовой указывающей на определенные протоколы, используемые в данном объекте, тип файловой системы и т.д., нам представляется невозможным. Данная базовая информация может нести на себе следы входа в киберпространство, уничижения элементов в нем. Материальный аспект киберпространства подчеркивается различными авторами, однако мы остаемся на позиции того, что компьютерные, электронные, мультимедийные устройства являются не частью киберпространства, а лишь «ключами» к нему «порталами» входа. Социальный аспект киберпространства выражается в том, что это пространство социального коммуникационного взаимодействия индивидов, организации определенных целевых сообществ, сетевых взаимодействий, построения новых идентичностей.

Информационный аспект киберпространства наиболее показателен – киберпространство выражается в бесчисленных потоках цифровой информации. При этом информация в киберпространстве, с одной стороны, динамична и легкоизменима, например, изъятие или изменение определенной информации в киберпространтсве открытых источников при необходимости, для имеющих соответствующие возможности (властные, финансовые или технические) не представляет большой сложности, как и активная информационная атака, измененной информацией. Это несложно заметить по активному вмешательству в историю. Однако и скопировать, сохранить определенные информационные «артефакты», обнародовать их может любой, даже не самый опытный пользователь. Кроме того, любое вмешательство в информационный массив оставляет в материальных «ключах» к нему (компьютерных и иных устройствах) соответствующие электронные цифровые следы.

Информационную составляющую киберпространства выделяет и Е.С. Шевченко (несмотря на подчеркивание аппаратной стороны), указывая на то, что кибернетическое пространство представляет собой область взаимодействия различного уровня систем [12. С. 37].

Кроме того, как мы уже отмечали ранее, кибернетическому пространству присущи виртуальные (электронно-цифровые) следы, которые отражают любые действия в кибернетическом пространстве [22. С. 43]. Данные следы авторами именуются по-разному – и цифровые, и электронные, и бинарные и электронно-цифровые [23–28]. Их исследование требует специфических рекомендаций, отраженных ранее в трудах многих авторов [29–32]. Казалось бы, выявление виртуальных следов в киберпространстве говорит о его сущности как специфического, но все же пространства, имеющего определенную протяженность. Это дает некоторым авторам возможность говорить о кибергеографии. При этом мерилом расстояния в кибергеографии будет либо время соединения между компьютерными устройствами, либо количество переходов по гиперссылкам [33, 34]. Однако прогресс в компьютерных технологиях неминуемо сокращает время соединений. Количество же переходов по ссылкам также вряд ли может быть мерилом киберрасстояния, поскольку переход на практически любой сайт боль-

шого интернета возможен через поисковую систему. Что же касается глубокого и теневого интернета, то их специфика требует специализированных программ или хаббов – шлюзов, прямой же переход по ссылкам из большого интернета в них невозможен. Представляется, что киберпространство имеет объем, но не имеет расстояний. Любой объект киберпространства занимает определенный информационный объем, но этот объем не снижает скорости перехода к другим объектам и значит, не может быть мерилом расстояния. Связь географии киберпространства с реальным миром может прослеживаться на уровне доменных имен первого уровня и IP-адресов. Однако это связь достаточно условна: российские пользователи могут создавать свои объекты в киберпространстве в доменах иных стран и наоборот; домен, выделенный СССР («.su»), заморожен, но уже созданные и не перенесенные в домен РФ («.ru» или «.рф») страницы продолжают функционировать, в отличие от СССР; существуют международные доменные зоны – .com, .net, .org, .edu и другие IP-адреса также могут носить динамический характер и не соответствовать конкретной точке земной поверхности.

Существование киберпространства обусловливается возможностью размещения в нем информации в определенной форме. Для этого необходимы программные средства («вспомогательная» информация), уже находившиеся на данном устройстве или «прошитые» в аппаратной части (CMOS, BIOS, средства, делящие пространство записи информации на кластеры, и т.д.). В криминалистических целях определение данной вспомогательной информации относится, скорее, к осмотру определенного материального носителя электронной информации и вряд ли может рассматриваться как осмотр киберпространства. Термин «осмотр киберпространства», по логике, должен иметь целью определение законов функционирования данного киберпространства (используемых протоколов и т.д.) и осмотр объектов в этом киберпространстве. При этом первый элемент существенного значения для следствия практически никогда не имеет, не устанавливается и не исследуется. Поэтому можно отметить, что как таковой осмотр киберпространства не производится, а имеет место осмотр электронного цифрового объекта в киберпространстве.

Задачами криминалистики на современном этапе формирования и освоения киберпространства нам представляются: дальнейшее криминалистическое исследование электронной цифровой информации, включая такие специфические формы ее хранения, как облачное и распределенное, разработка тактических аспектов производства следственных действий, направленных на обнаружение и изъятие доказательств в электронно-цифровом инцидентном пространстве, а также иного использования киберпространства в правоохранительных целях.

Относительно структуры киберпространства интересным представляется мнение М. Кастельса, выделяющего четыре материальных слоя пространства потоков [35. С. 386].

С точки зрения доступности киберпространство может быть разделено на большой интернет (основной интернет), глубокий интернет (часть интернета, не индексируемая поисковыми системами) и теневой интернет – даркнет (часть интернета, хоть и подключенная к общей сети, но не видимая без специальных программных средств). Кроме того, имеются корпоративные, государственные и региональные сети, а также сети, существующие параллельно Интернету: Fidonet, Usenet, Bitnet. Интернет можно рассматривать как связующее звено между ними.

Содержательно мы дифференцируем киберпространство на взаимопроникающие кластеры: развлекательный (включающий игровую, коммуникационную, текстовую, медийную и комбинированные части и др.); экономический; информационный; научно-образовательный; военный; криминальный.

Обязательным субъектом киберпространства является человек-пользователь. По крайней мере, пока не существуют саморазвивающиеся программы и искусственный интеллект, достигшие уровня самостоятельного, а не запрограммированного целеполагания. Любые аналитические, вредоносные или иные программы запускает человек, и итоговая цель их функционирования входит в орбиту его целей.

С психологической точки зрения специфика киберпространства выражается в изменении психологического содержания взаимосвязей: преступник – предмет преступления (потерпевший), которые превращаются во взаимосвязь: преступник – электронное устройство (сети) – потерпевший (предмет преступления) [12. С. 82]. Существенную роль играет и мнимая сетевая анонимность (когда общение происходит под вымышленными никнеймами), отстраненность, дистанцированность, возможность в любой момент прервать общение и добавить собеседника в черный список либо вообще заблокировать его, что приводит к «эффекту онлайн-дезингибиции» [36].

Следует отметить, что с социально-психологической точки зрения происходит активное взаимопроникновение киберпространства и реальности. Так, активно развиваются игры, имитирующие обычную жизнь (например, Second Life, Sims и другие многопользовательские ролевые игры). Социальные институты открывают свои филиалы в кибернетических мирах. Так, в виртуальном мире Second Life присутствуют Гарвард, Стэнфорд, университеты Хьюстона, Огайо, Нью-Йорка, вузы Ирландии, Нидерландов и Израиля [37–39]. Швеция, Эстония и ряд других стран открыли свои посольства в Second Life. В этой связи верно отмечает Р.М. Узденов, что информационно-телекоммуникационная сеть Интернет, компьютерные технологии стали неотъемлемой частью современного общества, создав новый его вид – виртуальное сообщество. Данное обстоятельство породило как позитивные, так и негативные процессы и явления [40]. Причиной или предметом преступлений в реальном мире становятся виртуальные взаимоотношения. В виртуальных играх и чатах для общения и в связи с ними совершается множество реальных преступлений: мошенничество при продажах виртуальных предметов, оскорбления, экстремистские высказывания. И мы перечислили только проблемы, касающиеся развлекательного сегмента киберпространства. Социальная сфера киберпространства также не является

прямым отражением реальности. Многими отмечается, что Сеть стимулирует появление новой ментальности, характерной для нарождающихся коммуникационных сообществ (интернет-сообществ) и опирающейся на объективные процессы расширения выбора во всех областях – от политики до стиля жизни, вытеснения иерархических организаций сетевыми, вытеснения представительной демократии демократией непосредственного участия, прямого гражданского действия или даже «облачной демократией» [41]. Киберпространство Сети становится местом появления и развития саморегулирующихся и самопреобразующихся социальных сообществ.

Отдельный вопрос – правовое регулирование киберпространства (виртуального пространства, сетевого пространства и т.д.). Недостаточное правовое регулирование, в том числе уголовно-правовое, влечет появление новых форм преступного поведения, выходящего за рамки уголовного законодательства, которые позволяют виновным, действующим в виртуальном пространстве, извлекать преступную прибыль, причиняя вред гражданам, организациям и целым государствам. Отсутствие целенаправленного уголовно-правового воздействия приводит к появлению новых видов преступности. Использование информационного пространства в преступных целях способствует совершению преступлений посягающих на различные объекты уголовно-правовой охраны. Уголовно-правовая охрана киберпространства зачастую затрагивает разные сферы уголовно-правового противодействия.

В настоящее время международное сообщество выработало ряд международных документов, которые тем или иным образом затрагивают правовое регулирование киберпространства, киберпреступности, ее предупреждение и борьбу с ней [42].

В Бангкокской декларации «Взаимодействие и ответные меры: стратегические союзы в области предупреждения преступности и уголовного правосудия», принятой на 11-м Конгрессе ООН по предупреждению преступности и уголовному правосудию (Бангкок, Таиланд, 18–25 апреля 2005 г.), указывается на необходимость создания системы национальных мер и развития международного сотрудничества по противодействию киберпреступности. Европейская конвенция о преступности в сфере компьютерной информации (Будапешт, 23 ноября 2001 г.) справедливо обязывает государства совершенствовать законодательство в области криминализации неправомерного доступа к компьютерной системе; неправомерный перехват с использованием технических средств, не предназначенных для общего пользования компьютерных данных; умышленное неправомерное повреждение, удаление, ухудшение качества, изменение или блокирование компьютерных данных с причинением ущерба; умышленное создание неправомерно серьезных помех функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, ухудшения качества, изменения или блокирования компьютерных данных; подлог с использованием компьютерных технологий; мошенничество с использованием компьютерных технологий; деяния, связанные с порнографией несовершеннолетних, и другие деяния, связанные с незаконным использованием устройств.

Вопросами киберпреступности на международном и национальном уровне занимались различные ученые [43–53].

Термин «кибер» означает то, что относится к виртуальной реальности, к информационным, информационно-коммуникационным технологиям.

Анализ уголовно-правовой доктрины в рассматриваемой части позволяет констатировать, что в настоящее время в теории уголовного права принято использовать различные термины: «киберпреступность», «компьютерная преступность», «преступность в сфере компьютерной информации», «интернет-преступность», «преступность в сети Интернет», «информационная преступность», что является, несомненно, негативным явлением, ибо создает путаницу в терминологическом аппарате. По мнению некоторых авторов, термин «киберпреступность» шире терминологии «компьютерная преступность», поскольку связана с использованием компьютеров и информационных технологий и глобальных сетей [54]; большинство ученых эти понятия используют как синонимы. Термины «компьютерная преступность», «преступность в сфере компьютерной информации» несколько уже по своей смысловой нагрузке, чем термин «киберпреступность», суть которых сводиться к преступлениям, совершенным с помощью компьютера, компьютерных систем, а также иных средств доступа к киберпространству. Подобные суждения высказывают и зарубежные исследователи [55].

Киберпреступность представляет собой совокупность преступлений, которые совершаются не только с помощью компьютера или иных средств доступа к киберпространству (с помощью компьютера и иных средств доступа к киберпространству могут быть совершены и такие преступления, в которых компьютер был применен не по основному своему назначению, в частности, нанесение человеку удара компьютером), а непосредственно в киберпространстве. Компьютерные, электронные, мультимедийные устройства являются не частью киберпространства, а лишь «ключами» к нему, «порталами» входа.

Компьютерная преступность, преступность в сфере компьютерной информации, является лишь составной частью киберпреступности. Киберпреступность включает в себя не только преступления, посягающие на отношения, складывающиеся в сфере нормального оборота компьютерной информации, но и на иные охраняемые уголовным законом общественные отношения, непосредственно совершаемые в кибернетическом пространстве [56. С. 106]. Исходя из этого следует констатировать, что особенностью киберпреступности как самостоятельного виды преступности выступает место их совершения – кибернетическое пространство. Киберпреступность охватывает значительный круг преступлений, совершаемых в киберпространстве. Она может посягать на жизнь и здоровье человека и гражданина, его собственность, общественную безопасность и т.д. Ее появление связано с глобализацией информационных процессов и инте-

грацией преступности и кибернетического пространства, в связи с чем киберпреступность по своей сути является составной частью киберпространства и ее существование немыслимо без него (вне кибернетического пространства не может существовать кибернетическая преступность).

Термины «киберпреступность» и «интернет-преступность», «преступность в сети Интернет» также нельзя признать тождественными, ибо киберпространство составляют и иные информационно-телекоммуникационные сети (например, «FidoNet» либо частные локальные сети). В связи с этим интернет-преступность и преступность в сети Интернет, преступления, совершаемые с помощью информационно-коммуникационных технологий также являются частью киберпреступности. Таким образом, следует констатировать, что термин «киберпреступность» выступает наиболее общим термином по отношению к вышерассмотренным терминам.

Киберпреступность не стоит на месте, она постоянно развивается, изобретаются более изощренные способы совершения киберпреступлений, наносящие значительный ущерб государству, обществу и конкретной личности, который, по мнению ученых, в 2021 г. может составить 6 трлн долл. [57. С. 555], в связи с чем необходимо совершенствовать меры предупреждения и борьбы с киберпреступностью.

На основании вышеизложенного следует констатировать, что кибернетическое пространство представляет собой обобщенное наименование упорядоченной в соответствии с определенными протоколами автоматизированной обработки информации системы программных средств и документальных файлов, расположенных в памяти электронных цифровых устройств или электронной цифровой информации, находящейся в процессе передачи любым доступным способом, либо информации, распределенной в компьютерной системе или сети. Недостаточность правового регулирования кибернетического пространства влечет совершение преступлений, посягающих на различные общественные отношения, охраняемые действующим уголовным законодательством Российской Федерации, совершаемые в кибернетическом пространстве посредством компьютерных, электронных, мультимедийных устройств входа, именуемых киберпреступностью.

ЛИТЕРАТУРА

1. Ищенко Е.П. О некоторых подходах к выявлению и расследованию преступлений, совершаемых в виртуальном пространстве // Использование современных информационных технологий в правоохранительной деятельности и региональные проблемы информационной безопасности : сб. материалов науч.-практ. конф. Калининград, 2006. Вып. VII. С. 214–226.
2. Степанов-Егиянц В.Г. Преступления в сфере безопасности обращения компьютерной информации: сравнительный анализ: дис. ... канд. юрид. наук. М., 2005. 168 с.
3. Дзялошинский И.М. Права человека в киберпространтсве // Право знать: история, теория, практика. 2003. № 11–12. С. 5–8.
4. Головин С.Н., Андреев, А.Г. Безопасность в киберпространстве, или России необходим информационный кодекс // Закон и право. 2003. № 11. С. 7–10.
5. Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации : дис. … д-ра юрид. наук. Воронеж, 2001. 386 с.
6. Шевченко Е.С., Михайлюченко Н.Н. Киберпространство как элемент обстановки совершения преступлений // Академический юридический журнал. 2015. № 2. С. 52–59.
7. Яковец Е.Н. Правовые основы обеспечения информационной безопасности Российской Федерации : учеб. пособие. М. : Юрлитинформ, 2014. 406 с.
8. Рассолов И.М.. Право и Интернет. Теоретические проблемы. 2-е изд., доп. М. : Норма, 2009. 384 с.
9. Добринская Д.Е. Киберпространство: территория современной жизни // Вестник Московского университета. Серия 18. Социология и политология. 2018. Т. 24, № 1. С. 52–70.
10. Тонконогов А.В., Стельмах А.П. «Киберология» как научная дисциплина // Социально-гуманитарные знания. 2013. № 1. С. 85–96.
11. Атаманов Г.А. Комментарий к проекту Концепции Стратегии кибербезопасности Российской Федерации, размещенному на сайте Совета Федерации. URL: http://council.gov.ru/press-center/discussions/38324/
12. Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений : автореф. дис. … канд. юрид. наук. М., 2016. 22 с.
13. Darrel C. Menthe. Jurisdiction in Cyberspace: A Theory of International Spaces // Michigan Telecommunications & Technology Law Review. 1998. Vol. 4, is. 1. P. 69–103.
14. Попов И.М. Взгляд на действия в киберпространстве под военным углом зрения // Digital Russia. URL: http://d-russia.ru/vojna-v-kiberprostranstve-uroki-i-vyvody-dlya-rossii.html
15. Крайванова В.А. Киберпространство : курс лекций. Барнаул : Изд-во АлтГТУ, 2011. 110 с.
16. Нестеров А.В. Интернет-поле VS киберпространства // Вопросы безопасности. 2015. № 4. С. 13–27.
17. Рассолов И.М. Киберпространство и позитивное право // Политика и общество. 2009. № 2. С. 33–37.
18. Грибанов Д.В. Правовое регулирование кибернетического пространства как совокупности информационных отношений : дис. ... канд. юрид. наук. Екатеринбург, 2003. 227 с.
19. Дзялошинский И.М. Особенности коммуникативного поведения в киберпространстве // Проблемы воздействия языка и мышления. М. : Интеллект-центр, 2010. С. 16–41.
20. Lister M. New media: a critical introduction. London : Routledge, 2003.
21. Ищенко Е.П. Киберпреступность: криминалистический аспект проблемы // Библиотека криминалиста. 2013. № 5 (10). С. 181–192.
22. Смушкин А.Б. Виртуальные следы в криминалистике // Законность. 2012. № 8. С. 43–45.
23. Ищенко Е.П. Криминалистика: главные направления развития // Сибирские уголовно-процессуальные и криминалистические чтения. 2012. № 1. С. 201–209.
24. Иванов В.Ю. К вопросу о классификации электронно-цифровых следов // Национальная безопасность / nota bene. 2020. № 3. С. 64–71.
25. Абрамова А.А. Значение виртуальных следов в расследовании финансирования терроризма // Общество: политика, экономика, право. 2017. № 4. С. 85–87.
26. Мещеряков В.А. «Виртуальные следы» под «Скальпелем Оккама» // Информационная безопасность регионов. 2009. № 1. С. 28–33.
27. Агибалов В.Ю. Виртуальные следы в криминалистике и уголовном процессе. М. : Юрлитинформ, 2012. 152 с.
28. Милашев В.А. Проблемы тактики поиска, фиксации и изъятия следов при неправомерном доступе к компьютерной информации в сетях ЭВМ : автореф. дис. ... канд. юрид. наук. М., 2004. 21 с.

29. Неупокоева И.А., Шеховцова Л.С., Кочерова Л.А. Осмотр места происшествия как информационная основа расследования преступления // Закон и право. 2018. № 6. С. 136–139.
30. Семенов А.Ю. «Некоторые аспекты выявления, изъятия и исследования следов, возникающих при совершении преступлений в сфере компьютерной информации» // Сибирский юридический вестник. 2004. № 1. С. 53–55.
31. Земцова С.И., Суров О.А., Галушин П.В. Организационно-тактические аспекты производства осмотра компьютера при расследовании преступлений, связанных с незаконным оборотом «дизайнерских» наркотиков, совершаемых с использованием Интернет-магазинов // Вестник Сибирского юридического института МВД России. 2016. № 3 (24). С. 18–25.
32. Поляков В.В., Слободян С.М. Анализ высокотехнологичных способов неправомерного удаленного доступа к компьютерной информации // Известия Томского политехнического университета. Инжиниринг георесурсов. 2007. № 1. С. 212–216.
33. Романенко М.А. Следственный осмотр по делам о преступных нарушениях авторских прав в сфере программного обеспечения // Вестник Омского университета. Серия: Право. 2008. № 1. С. 171–175.
34. Хуторной С.Н. Киберпространство и реальный мир // Вестник Московского государственного областного университета. Серия: Философские науки. 2011. № 2. С. 67–71.
35. Кастельс М. Информационная эпоха: экономика, общество и культура. М. : Гос. ун-т Высшая школа экономики, 2000. 606 с.
36. Suler J. The Psychology of Cyberspace. Rider University, 2000.
37. Войскунский А.Е. Поведение в киберпространстве: психологические принципы // Человек. 2016. № 1. С. 36–49.
38. Lagorio Ch. The Ultimate Distance Learning // The New York Times. 2007.
39. Lamont I. Harvard's Virtual Education Experiment in Second Life // Computerworld. 2007.
40. Texas A&M Chemist Experiments with Potential of Online Learning. Texas A&M University College of Science, 2013.
41. Узденов Р.М. Новые границы киберпреступности // Всероссийский криминологический журнал. 2016. № 4. С. 649–655.
42. Якимова Е.М., Нарутто С.В. Международное сотрудничество в борьбе с киберпреступностью // Всероссийский криминологический журнал. 2016. № 2. С. 369–376.
43. Руденко В.Н. Прямая демократия: модели правления, конституционно-правовые институты / отв. ред. А.Н. Кокотов, М.И. Кукушкин. Екатеринбург : УрО РАН, 2003. 476 с.
44. Суходолов А.П., Колпакова Л.А., Спасенников Б.А. Проблемы противодействия преступности в сфере цифровой экономики // Всероссийский криминологический журнал. 2017. № 2. С. 258–267.
45. Denning D.E. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy // Nautilus Institute for Security and Sustainable Development. URL: https://nautilus.org/global-problem-solving/activism-hacktivism-and-cyberterrorism-the-internet-as-a-tool-for-influencing-foreign-policy-2/
46. Pollitt M. Cyberterrorism. Fact or Fancy? // Proceedings of the 20th National Information Systems Security Conference. Washington, 1997.
47. Williams P. Organized Crime and Cybercrime: Synergies, Trends and Responses // The Computer Crime Research Center. URL: http://www.crime-research.org/library/Cybercrime.htm
48. Shelley L. Organized Crime, Terrorism and Cybercrime // Security Sector Reform: Institutions, Society and Good Governance. Baden-Baden, 2003.
49. Weimann G. Special Report 116: www.terror.net How Modern Terrorism Uses the Internet. URL: https://www.files.ethz.ch/isn/39096/2004_march_sr116.pdf
50. Winterfeld S., Andress J. The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice. Syngress, 2012. 170 p.
51. Мирошников Б.Н. Борьба с киберпреступлениями – одна из составляющих информационной безопасности Российской Федерации // The Computer Crime Research Center. URL: http://www.crime-research.ru/articles/Mirosh1
52. Ушаков С.И. Преступления в сфере обращения компьютерной информации (Теория, законодательство, практика) : дис. ... канд. юрид. наук. Ростов н/Д, 2000. 176 с.
53. Пучков Д.С. Особенности уголовно-правового регулирования применения кибертехнологий в зарубежных странах // Вестник краснодарского университета МВД России. 2018. № 4 (42). С. 21–25.
54. Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология вчера, сегодня, завтра. 2012. № 1 (24). С. 45–55.
55. Brenner S.W., Goodman M.D. The emerging consensus on criminal conduct in cyberspace // International Journal of Law and Information Technology. 2002. Vol. 10, is. 2. P. 139–223.
56. Простосердов М.А. Проблемы квалификации компьютерных преступлений // Российское правосудие. 2012. № 6 (74). С. 106–110.
57. Суходолов А.П., Антонян Е.А., Рукинов М.В., Шамрин М.Ю., Спасенникова М.Г. Блокчейн в цифровой криминологии: постановка проблемы // Всероссийский криминологический журнал. 2019. № 4. С. 555–563.

Статья представлена научной редакцией «Право» 30 августа 2021 г.

Cyberspace as a New Crime Environment

Vestnik Tomskogo gosudarstvennogo universiteta – Tomsk State University Journal, 2021, 472, 248–256.
DOI: 10.17223/15617793/472/29

Irina A. Efremova, Saratov State Law Academy (Saratov, Russian Federation). E-mail: efremova005@yandex.ru
Aleksandr B. Smuskin, Saratov State Law Academy (Saratov, Russian Federation). E-mail: skif32@ya.ru
Aleksandr G. Donchenko, Saratov State Law Academy (Saratov, Russian Federation). E-mail: donchenko.a.g@yandex.ru
Pavel A. Matushkin, Saratov State Law Academy (Saratov, Russian Federation). E-mail: foxbox003@gmail.com
Keywords: cybercrime; crime in Internet; cyberspace; cybersphere; cybersecurity; information protection.

The aim of the study is to analyze the cybernetic space as a new environment of crime and to develop a definition apparatus based on it. The material of the study was: international acts, the current legislation of the Russian Federation, scientific literature. The methodology is based on the dialectical method of cognition. In addition, the authors used general (analysis and synthesis, logical, system-structural methods) and specific (formal-legal) scientific methods of cognition. The authors note that, in the Russian legal literature, there is no single position regarding the definition of the cybernetic space and the unambiguity of its interpretation. Various approaches to the definition of the term "cybernetic space" are considered. Another vision of the term is presented. The authors state that the "virtual reality" and the cybernetic space are distanced; the cybernetic space is a multidimensional category that has philosophical, social, psychological, criminalistic, criminal-legal, criminological, and other dimensions. The features of the cybernetic space (digitalization, virtualization of reality, interactivity, hyperlink and distribution function) are revealed. The authors analyze the material, informational, social, and psychological aspects of the cybernetic space, as well as the concept of cyberspace in criminalistics; identify the tasks of criminalistics at the present stage of the cybernetic space's formation and development; formulate the definition of the cybercrime; determine the correlation of cyberspace with other related categories. The authors conclude that the

cybernetic space is a generalized name for a system of software tools and documentary files arranged in accordance with certain protocols of automated information processing, located in the memory of electronic digital devices or electronic digital information in the process of transmission in any available way, or information distributed in a computer system or network. The lack of a legal regulation of the cybernetic space entails cybercrimes – crimes, infringing on various social relations protected by the current criminal legislation of the Russian Federation, committed in the cybernetic space through computer, electronic, multimedia input devices.

REFERENCES

1. Ishchenko, E.P. (2006) O nekotorykh podkhodakh k vyyavleniyu i rassledovaniyu prestupleniy, sovershaemykh v virtual'nom prostranstve [On some approaches to the identification and investigation of crimes committed in the virtual space]. In: *Ispol'zovanie sovremennykh informatsionnykh tekhnologiy v pravookhranitel'noy deyatel'nosti i regional'nye problemy informatsionnoy bezopasnosti* [The Use of Modern Information Technologies in Law Enforcement and Regional Problems of Information Security]. Vol. 7. Kaliningrad: [s.n.]. pp. 214–226.
2. Stepanov-Egiyants, V.G. (2005) *Prestupleniya v sfere bezopasnosti obrashcheniya komp'yuternoy informatsii: sravnitel'nyy analiz* [Crimes in the sphere of security of computer information circulation: comparative analysis]. Law Cand. Diss. Moscow.
3. Dzyaloshinskiy, I.M. (2003) Prava cheloveka v kiberprostrantsve [Human rights in cyberspace]. *Pravo znat': istoriya, teoriya, praktika*. 11–12. pp. 5–8.
4. Golovin, S.N. & Andreev, A.G. (2003) Bezopasnost' v kiberprostranstve, ili Rossii neobkhodim informatsionnyy kodeks [Security in cyberspace, or Russia needs an information code]. *Zakon i pravo*. 11. pp. 7–10.
5. Meshcheryakov, V.A. (2001) *Osnovy metodiki rassledovaniya prestupleniy v sfere komp'yuternoy informatsii* [Fundamentals of methods of investigation of crimes in the field of computer information]. Law Dr. Diss. Voronezh.
6. Shevchenko, E.S. & Mikhaylyuchenko, N.N. (2015) Kiberprostranstvo kak element obstanovki sovershenia prestupleniy [Cyberspace as an element of the crime scene]. *Akademicheskiy yuridicheskiy zhurnal*. 2. pp. 52–59.
7. Yakovets, E.N. (2014) *Pravovye osnovy obespecheniya informatsionnoy bezopasnosti Rossiyskoy Federatsii* [Legal Bases of Ensuring Information Security of the Russian Federation]. Moscow: Yurlitinform.
8. Rassolov, I.M. (2009) *Pravo i Internet. Teoreticheskie problemy* [Law and the Internet. Theoretical problems]. 2nd ed. Moscow: Norma.
9. Dobrinskaya, D.E. (2018) Cyberspace: territory of contemporary life. *Vestnik Moskovskogo universiteta. Seriya 18. Sotsiologiya i politologiya – Moscow State University Bulletin. Series 18. Sociology and Political Science*. 1(24). pp. 52–70. (In Russian).
10. Tonkonogov, A.V. & Stel'makh, A.P. (2013) "Cyberologia" as a scientific discipline. *Sotsial'no-gumanitarnye znaniya*. 1. pp. 85–96. (In Russian).
11. Atamanov, G.A. (2014) *Kommentariy k proektu Kontseptsii Strategii kiberbezopasnosti Rossiyskoy Federatsii, razmeshchennomu na sayte Soveta Federatsii* [Commentary on the draft Concept of the Cybersecurity Strategy of the Russian Federation, posted on the website of the Federation Council]. [Online] Available from: http://council.gov.ru/press-center/discussions/38324.
12. Shevchenko, E.S. (2016) *Taktika proizvodstva sledstvennykh deystviy pri rassledovanii kiberprestupleniy* [Tactics of investigative actions in the investigation of cybercrimes]. Abstract of Law Cand. Diss. Moscow.
13. Darrel, S. (1998) Menthe. Jurisdiction in Cyberspace: A Theory of International Spaces. *Michigan Telecommunications & Technology Law Review*. 1(4). pp. 69–103.
14. Popov, I.M. (2013) Vzglyad na deystviya v kiberprostranstve pod voennym uglom zreniya [A look at actions in cyberspace from a military point of view]. *Digital Russia*. [Online] Available from: http://d-russia.ru/vojna-v-kiberprostranstve-uroki-i-vyvody-dlya-rossii.html.
15. Krayvanova, V.A. (2011) *Kiberprostranstvo* [Cyberspace]. Barnaul: Altai State Technical University.
16. Nesterov, A.V. (2015) Internet-pole VS kiberprostranstva [Internet field VS cyberspace]. *Voprosy bezopasnosti – Security Issues*. 4. pp. 13–27. (In Russian). DOI: 10.7256/2409-7543.2015.4.16743
17. Rassolov, I.M. (2009) Kiberprostranstvo i pozitivnoe pravo [Cyberspace and positive law]. *Politika i obshchestvo*. 2. pp. 33–37.
18. Gribanov, D.V. (2003) *Pravovoe regulirovanie kiberneticheskogo prostranstva kak sovokupnosti informatsionnykh otnosheniy* [Legal regulation of cybernetic space as a set of information relations]. Law Cand. Diss. Yekaterinburg.
19. Dzyaloshinskiy, I.M. (2010) Osobennosti kommunikativnogo povedeniya v kiberprostranstve [Features of communicative behavior in cyberspace]. In: *Problemy vozdeystviya yazyka i myshleniya* [Problems of the Impact of Language and Thinking]. Moscow: Intellekt-tsentr. pp. 16–41.
20. Lister, M. (2003) *New Media: A critical introduction*. London: Routledge.
21. Ishchenko, E.P. (2013) Cybercrime: a forensic aspect of the problem. *Biblioteka kriminalista*. 5 (10). pp. 181–192. (In Russian).
22. Smushkin, A.B. (2012) Virtual traces in criminalistics. *Zakonnost'*. 8. pp. 43–45. In Russian).
23. Ishchenko, E.P. (2012) Kriminalistika: glavnye napravleniya razvitiya. *Sibirskie ugolovno-protsessual'nye i kriminalisticheskie chteniya – Siberian Criminal Procedure and Criminalistic Readings*. 1. pp. 201–209. (In Russian).
24. Ivanov, V.Yu. (2020) To the question on classification of digital footprint. *Natsional'naya bezopasnost' / nota bene – National Security / Nota Bene*. 3. pp. 64–71. (In Russian). DOI: 10.7256/2454-0668.2020.3.33308
25. Abramova, A.A. (2017) The value of virtual traces in the investigation of the terrorism financing. *Obshchestvo: politika, ekonomika, pravo – Society: Politics, Economics, Law*. 4. pp. 85–87. (In Russian). DOI: 10.24158/pep.2017.4.21
26. Meshcheryakov, V.A. (2009) "Virtual'nye sledy" pod "Skal'pelem Okkama" ["Virtual traces" under "Occam's Razor"]. *Informatsionnaya bezopasnost' regionov*. 1. pp. 28–33.
27. Agibalov, V.Yu. (2012) *Virtual'nye sledy v kriminalistike i ugolovnom protsesse* [Virtual Traces in Criminalistics and Criminal Procedure]. Moscow: Yurlitinform.
28. Milashev, V.A. (2004) *Problemy taktiki poiska, fiksatsii i iz'yatiya sledov pri nepravomernom dostupe k komp'yuternoy informatsii v setyakh EVM* [Problems of tactics of search, fixation and removal of traces in case of unauthorized access to computer information in computer networks]. Abstract of Law Cand. Diss. Moscow.
29. Neupokoeva, I.A., Shekhovtsova, L.S. & Kocherova, L.A. (2018) Inspection of the scene as an information basis investigation of crimes. *Zakon i pravo*. 6. pp. 136–139. (In Russian). DOI: 10.24411/2073-3313-2018-10036
30. Semenov, A.Yu. (2004) Nekotorye aspekty vyyavleniya, iz"yatiya i issledovaniya sledov, voznikayushchikh pri sovershenii prestupleniy v sfere komp'yuternoy informatsii [Some aspects of identification, seizure and investigation of traces arising from the commission of crimes in the field of computer information]. *Sibirskiy yuridicheskiy vestnik – Siberian Law Herald*. 1. pp. 53–55.
31. Zemtsova, S.I., Surov, O.A. & Galushin, P.V. (2016) Organizational and tactical aspects of computer examination procedure in investigation of crimes involving illegal trafficking in designer drugs and committed by using on-line stores. *Vestnik Sibirskogo yuridicheskogo instituta MVD Rossii – Vestnik of Siberian Law Institute of the MIA of Russia*. 3 (24). pp. 18–25. (In Russian).
32. Polyakov, V.V. & Slobodyan, S.M. (2007) Analysis of high-tech methods of illegal remote computer data access. *Izvestiya Tomskogo politekhnicheskogo universiteta. Inzhiniring georesursov – Bulletin of the Tomsk Polytechnic University. Geo Assets Engineering*. 1. pp. 212–216. (In Russian).
33. Romanenko, M.A. (2008) Sledstvennyy osmotr po delam o prestupnykh narusheniyakh avtorskikh prav v sfere programmnogo obespecheniya [Investigative examination in cases of criminal copyright violations in the field of software]. *Vestnik Omskogo universiteta. Seriya: Pravo – Herald of Omsk University. Series Law*. 1. pp. 171–175.

34. Khutornoy, S.N. (2011) Cyberspace and virtual reality. *Vestnik Moskovskogo gosudarstvennogo oblastnogo universiteta. Seriya: Filosofskie nauki – Bulletin MSRU. Series: Philosophy*. 2. pp. 67–71. (In Russian).
35. Castells, M. (2000) *Informatsionnaya epokha: ekonomika, obshchestvo i kul'tura* [The Information Age: Economy, society and culture]. Translated from English by O.I. Sharatan. Moscow: Higher School of Economics.
36. Suler, J. (2000) *The Psychology of Cyberspace*. Rider University.
37. Voyskunskiy, A.E. (2016) Behavior in a cyberspace: some psychological principles. *Chelovek – Human Being*. 1. pp. 36–49. (In Russian).
38. Lagorio, Ch. (2007) The Ultimate Distance Learning. *The New York Times*. 7 January.
39. Lamont, I. (2007) Harvard's Virtual Education Experiment in Second Life. *Computerworld*. 21 May.
40. Texas A&M Chemist Experiments with Potential of Online Learning. Texas A&M University College of Science, 2013.
41. Uzdenov, R.M. (2016) New frontiers of cybercrime. *Vserossiyskiy kriminologicheskiy zhurnal – Russian Journal of Criminology*. 4 (10). pp. 649–655. (In Russian). DOI: 10.17150/2500-4255.2016.10(4).649-655
42. Yakimova, E.M. & Narutto, S.V. (2016) International cooperation in cybercrime counteraction. *Vserossiyskiy kriminologicheskiy zhurnal – Russian Journal of Criminology*. 2 (10). pp. 369–376. (In Russian). DOI: 10.17150/1996-7756.2016.10(2).369-378
43. Rudenko, V.N. (2003) *Pryamaya demokratiya: modeli pravleniya, konstitutsionno-pravovye instituty* [Direct Democracy: Models of government, constitutional and legal institutions]. Yekaterinburg: UB RAS.
44. Sukhodolov, A.P., Kolpakova, L.A. & Spasennikov, B.A. (2017) Issues of counteracting crimes in the sphere of digital economy. *Vserossiyskiy kriminologicheskiy zhurnal – Russian Journal of Criminology*. 2 (11). pp. 258–267. (In Russian). DOI: 10.17150/2500-4255.2017.11(2).258-267
45. Denning, D.E. (1999) Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. *Nautilus Institute for Security and Sustainable Development*. [Online] Available from: https://nautilus.org/global-problem-solving/activism-hacktivism-and-cyberterrorism-the-internet-as-a-tool-for-influencing-foreign-policy-2.
46. Pollitt, M. (1997) [Cyberterrorism. Fact or Fancy?] *Proceedings of the 20th National Information Systems Security Conference*. Baltimore. 7–10 October 1997. Washington: [s.n.].
47. Williams, P. (n.d.) Organized Crime and Cybercrime: Synergies, Trends and Responses. *The Computer Crime Research Center*. [Online] Available from: http://www.crime-research.org/library/Cybercrime.htm.
48. Shelley, L. (2003) Organized Crime, Terrorism and Cybercrime. In: Bryden, A. & Fluri, P. (eds) *Security Sector Reform: Institutions, Society and Good Governance*. Baden-Baden: Nomos Verlarsgesellschaft.
49. Weimann, G. (2004) www.terror.net. How Modern Terrorism Uses the Internet. *Special Report 116*. [Online] Available from: https://www.files.ethz.ch/isn/39096/2004_march_sr116.pdf.
50. Winterfeld, S. & Andress, J. (2012) *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice*. Syngress.
51. Miroshnikov, B.N. (2003) Bor'ba s kiberprestupleniyami – odna iz sostavlyayushchikh informatsionnoy bezopasnosti Rossiyskoy Federatsii [The fight against cybercrime is one of the components of information security of the Russian Federation]. *The Computer Crime Research Center*. [Online] Available from: http://www.crime-research.ru/articles/Mirosh1.
52. Ushakov, S.I. (2000) *Prestupleniya v sfere obrashcheniya komp'yuternoy informatsii (Teoriya, zakonodatel'stvo, praktika)* [Crimes in the sphere of circulation of computer information (Theory, legislation, practice)]. Law Cand. Diss. Rostov-on-Don.
53. Puchkov, D.S. (2018) Features of the criminal law regulation of the implementation of cyber technologies in the countries of the world. *Vestnik krasnodarskogo universiteta MVD Rossii*. 4 (42). pp. 21–25. (In Russian).
54. Nomokonov, V.A. & Tropina, T.L. (2012) Kiberprestupnost' kak novaya kriminal'naya ugroza [Cybercrime as a new criminal threat]. *Kriminologiya vchera, segodnya, zavtra*. 1 (24). pp. 45–55.
55. Brenner, S.W. & Goodman, M.D. (2002) The emerging consensus on criminal conduct in cyberspace. *International Journal of Law and Information Technology*. 2 (10). pp. 139–223.
56. Prostoserdov, M.A. (2012) Problems of classification of computer crimes. *Rossiyskoe pravosudie*. 6 (74). pp. 106–110. (In Russian).
57. Sukhodolov, A.P. et al. (2019) Blockchain in digital criminology: problem statement *Vserossiyskiy kriminologicheskiy zhurnal – Russian Journal of Criminology*. 4. pp. 555–563. (In Russian). DOI: 10.17150/2500-4255.2019.13(4).555-563

Received: 30 August 2021