УДК 343:1

І.В. Владленова, канд. філос. наук, доцент, докторант кафедри теорії культури та філософії науки Харківського національного університету ім. В.Н.Каразіна

И.В. Владленова, канд. филос. наук, доцент, докторант кафедры теории культуры и философии науки Харьковского национального университета им. В.Н.Каразина

I.V. Vladlenova, PhD. Philosophy , Associate Professor, PhD of the Department of Culture and Philosophy of Science Kharkiv National University. V.N. Karazin

Е.А.Кальницький, канд. філос. наук, доцент, доцент кафедри філософії Національного університету «Юридична академія України імені Ярослава Мудрого»

Э.А. Кальницкий, канд. филос. наук, доцент, доцент кафедры философии Национального университета «Юридическая академия Украины имени Ярослава Мудрого»

Kalnytskyi E.A., PhD. Philosophy, Associate Professor, Department of Philosophy of the National University "Yaroslav the Wise Law Academy of Ukraine"

Cybercrime as a challenge to the Information Society

The main purpose of the paper is to study researches globalist aspect of nature of crimes in the sphere of computer information, study of the main areas of cybercrime and to make recommendations to the international community in combating such crimes by setting priorities for their development. The implementation of these goals requires the use of topical methods of knowledge, including general scientific and specially-cognitive character. Used philosophical approach contributes to a broad theoretical context for specific scientific developments, the development of effective organizational and legal measures aimed at improving the legal culture and legal consciousness. Computer crimes are not only contribute to the commission of criminal offenses, they are expanding the scope of criminal activity, functioning on a global scale. Cyber crime is now threatening not

only the national security of individual states, it threatens humanity at the international level.

Keywords: cyberspace, cybercrimes, globalization, information Society.

Кіберзлочинність як виклик інформаційному суспільству

Основні цілі дослідження статті полягають у з'ясуванні глобалістичного аспекту природи злочинів у сфері комп'ютерної інформації, вивченні основних напрямків кіберзлочинів і виробленню рекомендацій для міжнародного співтовариства у протидії таким злочинам шляхом виділення пріоритетних напрямів їх розвитку. Реалізація зазначених цілей передбачає використання актуальних методів пізнання, у тому числі як загальнонаукового так і спеціально-пізнавального характеру. Комп'ютерні злочини не тільки сприяють вчиненню кримінальних злочинів, вони розширюють сферу кримінальної діяльності, яка функціонує в глобальних масштабах. Філософський підхід може сприяти формуванню широкого теоретичного контексту для конкретних наукових розробок, виробленню ефективних організаційно-правових заходів, спрямованих на підвищення правової культури та правосвідомості.

Ключові слова: кіберпростір, кіберзлочини, глобалізація, інформаційне суспільство.

Киберпреступления как вызов информационному обществу

Современный этап развития общества характеризуется становлением информационного общества. Бурными темпами происходит развитие и внедрение средств связи, вычислительной техники, новых информационных технологий практически во все сферы человеческой деятельности. Все это приводит к формированию так называемого «кибернетического пространства»,

которое впитывает в себя не только общечеловеческие культурные ценности, но, и к сожалению, и все присущие обществу пороки. Это создает предпосылки к формированию различного рода преступлений.

В последние годы в средствах массовой информации широкое освещение получила проблема, связанная с киберпреступностью – новым социальным и уголовно-правовым негативным явлением. Компьютерные преступления не только способствуют совершению уголовных преступлений, они расширяют сферу криминальной деятельности, функционирующую в глобальных масштабах. Таким образом, киберпреступность сегодня представляет угрозу не только национальной безопасности отдельных государств, она угрожает человечеству на международном уровне. Задачи противодействия разных видов преступлений, освещаемых в их социально-философском, антропологическом измерениях, могут иметь ценность для конкретных отраслей права, криминологии, планирования правоохранительной деятельности. Анализ этих задач может помочь разработать основные способы эффективного решения важных социальных проблем по обеспечению безопасности, законности и правопорядка, борьбе с преступностью, защите прав и свобод человека. Философский подход может способствовать формированию широкого теоретического контекста для конкретных научных разработок, выработки эффективных организационно-правовых мер, направленных на повышение правовой культуры и правосознания.

Проблема киберпреступности в ее глобалистическом аспекте освещается следующими авторами: М. Бреннер, С. Гудман, Ф. Вильямс, Д. Деннинг, У. Зибер, Д. Льюис, М. Кабэй, Л. Шелли, Д. Шиндер и т.д. Среди отечественных исследователей назовем В.Д. Гавловского, В.С. Цимбалюк, С.Д.Бражника, С.Ю. Бытко, В.В. Воробьева, Д.А. Зыкова и т.д. Отметим, что изучение компьютерной преступности в рамках Уголовного кодекса Украины осложняется отсутствием четкого определения понятия «киберпреступление», а также «размытыми задачами» субъектов борьбы с киберпреступностью, распределения полномочий между ними и т.д. Также применение

традиционных для преступлений форм и методов борьбы, закрепленных в действующем законодательстве, не достаточно эффективно в условиях виртуального пространства.

Проблема киберпреступности усложняется также тем, что она связана с высокими технологиями, необходимостью в специалистах, имеющих правовое образование и обладающих достаточным уровнем информационной, компьютерной грамотности. Т.Л. Тропина выделяет несколько аспектов проблемы взаимосвязи преступности и информационных технологий:

– проблема детерминации роста преступности и ее глобализации информационной мегасредой и электронными средствами массовой коммуникации, а также проблема использования преступниками, преступными группами и сообществами достижений науки и техники (информационные технологии выступают как способ или средство совершения преступления, а также в качестве объекта посягательства);

– проблема правового регулирования процессов, связанных с преступным использованием компьютерных технологий;

– превентивные возможности глобальных информационных сетей и возможность использования информационных технологий правоохранительными органами [2].

Существует большое количество видов киберпреступлений, как правило, это кибератаки, обслуживание и создание вредоносных программ, несанкционированный доступ и перехват, незаконный сбор, хранение, изменение, раскрытие или распространение персональных данных, компьютерный абордаж, перехват информации, изменение компьютерных данных, компьютерное мошенничество, незаконное копирование и т.д.

Проблема киберпреступлений считается общемировой и требует концентрации усилий всех государств. Также борьба с киберпреступлениями должна подкрепляться определенными правовыми мерами, как-то: созданием специализированных правоохранительных, судебных органов; специальным обучением сотрудников правоохранительных и судебных органов власти;

согласованным набором правил и внедрением соответствующих средств для статистического анализа компьютерных преступлений и т.д.

Безусловно, киберпреступность является неизбежным недостатком информационного общества, в котором Интернет стал настоящей платформой для глобализации преступной деятельности, имеющей разрушительные физические и социальные последствия. Поэтому не только отдельные лица, но и различные международные организации, государства заинтересованы в обеспечении защиты от киберпреступлений. Более того, развитие и совершенствование информационных технологий расширяет возможности киберпреступлений, в том числе, и для совершения физических убийств, ибо в сфере здравоохранения, где многие устройства имеют выход в сеть, преступники, например, могут бесконтактно совершать убийства (Cyberhomicide), например, отключив кардиостимулятор или аппарат искусственной вентиляции легких, изменив предписанную дозировку лекарства. Безусловно, в будущем возрастет опасность мошенничеств, связанных с кредитными картами, возможными атаками на энергосистемы, обеспечивающих электроэнергией, военными объектами с системой управления беспилотными летательными аппаратами и т. д.

Большинство философов полагают, что отношения между государством и его гражданами должны опираться на моральную философию, поскольку уголовный закон должным образом направлен на определение «неправильного» с точки зрения морали [7;8]. Также необходимо опираться на философию действия и философию сознания, чтобы объяснять причину правонарушения.

Представители различных государств, в Женеве 10-12 декабря 2003 года на первом этапе Всемирной встречи на высшем уровне по вопросам информационного общества приняли Декларацию, в которой выделили положительные и отрицательные стороны развития информационного общества. Они определили, что информационно-коммуникационные технологии оказывают огромное влияние практически на все аспекты жизни. А потому их необходимо рассматривать как инструмент, а не как самоцель. При

благоприятных условиях эти технологии способны стать мощным инструментом повышения производительности, экономического роста, создания рабочих мест и трудоустройства, а также повышения качества жизни для всех. Они также могут содействовать ведению диалога между народами, странами и цивилизациями. Однако участники отметили и негативные тенденции, связанные с новыми возможностями для преступной деятельности [5].

В последние годы наблюдается быстрое развитие компьютерных технологий, которые не только открывают широкие перспективы для развития науки и техники, но и создают благоприятную почву для формирования новых преступлений, быстротечность этого процесса затрудняет своевременный анализ происходящих в виртуальном пространстве преступлений. Не существует четкой дефиниции понятия «компьютерное преступление», «высокотехнологическое преступление» (киберпреступление). Киберпреступления, в самом широком смысле можно определить как преступления, связанные с использованием информационных технологий. Они отличаются возможностью использования информационно-коммуникационных сетей, циркуляцией нематериальных, виртуальных данных, а также независимостью от географических ограничений [6].

Информация в современном информационном обществе определяет силу и мощь государства, «оцифрованные» деньги преодолевают пространственные и временные трудности передвижения, интеллектуальные, не материальные продукты приобретают наибольшее значение. Этот процесс накопления «виртуальной» власти и капитала, протекающий в киберпространстве с невероятной скоростью, порождает новые виды преступлений. Киберпространство – это больше, чем прорыв в электронных средствах массовой информации, это область, в которой ментально существуют участники взаимодействия. Идеологический стереотип киберпространства содержит в себе три утопических доминанты: непримиримый гедонизм, эскапизм от повседневной реальности и традиционное мистическое желание

трансцендировать границы чувственного бытия. В рамках массовой культуры любую интерактивную развлекательную среду, генерируемую компьютерными технологиями, стихийно называют киберпространством. Киберпространство необходимо рассматривать в единстве технико-информационного, гуманитарного, социального содержания, в контексте современных тенденций развития информационных технологий и на пересечении различных философских концепций [1].

Киберпространство позволяет человеку проживать в «другом» мире. М. Федотов отмечает, что постепенно современный человек все в большей степени превращается в кибернавта – «сначала в приезжего, потом в жителя и, наконец, в полноценного гражданина совершенно другой страны, в которой иной язык, иные нравы и обычаи, иные законы. Собственно, это не одна страна, а некое неограниченное множество «стран», умещающихся в глобальном киберпространстве» [3].

Существует настоятельная необходимость в определении ответственности юридических лиц, установлении санкций, которые могут применяться к киберпреступлениям. Так как действия киберпреступников, как правило, не ограничены рамками одного государства, необходимо согласовать сотрудничество, направленное на борьбу с киберпреступлениями на международном уровне, чтобы обмениваться всей информацией, предназначенной для расширения сотрудничества.

Безусловно, регулирование виртуальных процессов информационного общества имеет решающее значение для его выживания и благополучия. Было бы ошибочным пытаться решать возникающие проблемы исключительно в области права. Сложность явления требует синтеза нескольких научных областей, начиная от философии, информатики до социологии и экономики.

Динамичность и вариабильность явления киберпреступности усложняет научную классификацию киберпреступлений, а также анализ и понимание этого явления в гуманитарном аспекте. Тем не менее, компьютерные преступления в целом можно разделить на две основные категории:

преступления, в которых компьютер является объектом нападения или преступления, в которых компьютер функционирует в качестве орудия преступления. Дальнейшая классификация киберпреступлений в криминологическом аспекте определяется с учетом типа используемых каналов, вида повреждений, характера совершенных действий и мотивов преступника: Cyber-service (обслуживание, повинность) – взлом в политических или личных целях, распространение вредоносного кода; Cyber-deception/theft (обман / кражи) – компьютерные мошенничества или пиратство, кражи личных данных, кредитных кражи электронных денег); Cyber-obscenity (непристойности, порнография) и Cyber- violence (насилие) – компьютерная атака, отказ в обслуживании, кибер-преследование.

В связи с угрожающим распространением и все более широкого профессионального использования широкополосного подключения к Интернету угрозы, которые представляют киберпреступления, увеличиваются.

Можно выделить различные модели пресечения преступлений в киберпространстве, но все они будут так или иначе опираться на следующие компоненты: социальные нормы – рыночные отношения– правовые нормы-технические возможности. Они лежат в основе многослойной структуры управления, включающей заинтересованные стороны, структуры бизнеса и государства. Указанные слои управления выступают в качестве барьера для киберпреступности. Государство должно стоять в верхней части управления Интернетом как конечная регулирующая сила киберпространства. Внутренние функции государства (охранительная, экономическая, социальная, культурно-воспитательная, природоохранительная) и внешние функции, направленные на обеспечение существования государства в мировом обществе (защита государства от вооруженных нападений, поддержание международных политических отношений, экономических и культурных связей) полностью реализуют механизм социальных взаимодействия для реализации борьбы с киберперступностью.

В формировании политики и средств борьбы с проблемой киберпреступности необходимо избегать избыточного регулирования при сохранении открытости Интернета и защиты прав человека, как-то: право на частную жизнь и информационное самоопределение, свободу слова, информации и коммуникации. Кроме того, необходимо обратить внимание на предупреждение создания преступных технологий, которые имеют опасный потенциал.

Борьба с киберпреступностью является не только юридическим вопросом, но, напротив, затрагивает политические решения, которые простираются далеко за рамки закона. И эти решения должны быть сделаны путем открытого демократического участия всех участников информационного общества [4].

В наиболее опасной форме киберпреступность граничит с терроризмом, который направлен на национальную безопасность, жизненно важные инфраструктуры. Терроризм включает в себя действия, направленные на создание обстановки террора среди широкой общественности, группы лиц или конкретных людей. Террористические акты наносят тяжелый вред обществу, нарушая общественный порядок, вызывая массовый террор, физическое уничтожение и т.д. Кибертерроризм определяется как преднамеренное политически мотивированное нападение с помощью информации, компьютерных систем и программ, которые приводят к насилию. Такая кибератака может принимать различные формы: кибертеррорист может взломать компьютерные системы и нарушить внутреннее банковское дело, что пагубно повлияет на международные финансовые операции или ворваться в систему управления воздушным движением, что приведет к авиакатастрофе. Существует возможность взлома компьютеров фармацевтической компании, изменения формулы некоторых основных лекарств; нарушение давления в газопроводах и т.д.

И все же единого определения, закрепленного на законодательном уровне, пока не существует. Трудности в определении понятия

«кибертерроризм» связаны еще и с тем, что порой очень сложно отделить сам кибертерроризм от акций информационной войны и информационного оружия, от преступлений в сфере компьютерной информации. Дополнительные трудности могут возникнуть при попытке выявить специфику данной формы терроризма. Так, например, психологический и экономический аспекты кибертерроризма тесно переплетены, и невозможно однозначно определить, какой из них имеет большее значение. Эта неопределенность говорит об определенной новизне исследуемого явления.

В информационном пространстве существуют и используются различные приемы кибертерроризма:

– нанесение ущерба отдельным физическим элементам информационного пространства, например, разрушение сетей электропитания, наведение помех,

– использование специальных программ, стимулирующих разрушение аппаратных средств, а также биологических и химических средств для разрушения элементной базы и др.;

– кража или уничтожение информационного, программного и технического ресурсов, имеющих общественную значимость, путем преодоления систем защиты, внедрения вирусов, программных закладок и т. п.;

– воздействие на программное обеспечение и информацию с целью их искажения или модификации в информационных системах и системах управления;

– раскрытие и угроза опубликования или само опубликование закрытой информации о функционировании информационной инфраструктуры государства, общественно значимых и военных информационных систем, кодах шифрования, принципах работы систем шифрования, успешном опыте ведения информационного терроризма и др.;

– захват каналов СМИ с целью распространения дезинформации, слухов, демонстрации мощи террористической организации и объявления своих требований;

– уничтожение или активное подавление линий связи, неправильная адресация, искусственная перегрузка узлов коммутации;

– проведение информационных и психологических операций и др.

Дороти Деннинг считает, что деятельность террористов в интернете можно классифицировать следующим образом: «активизм», «хакеризм» и «кибертерроризм». Активизм – это «легитимное» использование киберпространства для пропаганды своих идей, зарабатывания денег и привлечения новых членов. Хакеризм – это хакерские атаки, проводимые для выведения из строя отдельных компьютерных сетей или интернет-сайтов, получения доступа к секретной информации, хищения средств и т.д. Кибертерроризм – это компьютерные атаки, спланированные для нанесения максимального ущерба жизненно важным объектам информационной инфраструктуры [9]. Степень ущерба увеличивается от категории к категории, хотя увеличение степени ущерба не подразумевает увеличение политической эффективности. Хотя каждая категория обсуждается отдельно, четких границ между ними нет. Например, бомбардировка электронной почты одними может рассматриваться как хактивизм, а другими – как кибертеррористические действия. Также одно лицо может совершать одновременно весь спектр рассматриваемых действий: запускать вирусы, производить террористические действия, и в то же время собирать политическую информацию, создавать коалиции, координировать действия с другими лицами [2].

Террористы активно используют электронную почту для организации и координации атак. Многочисленные чаты и форумы, существующие в Интернете, идеально приспособлены для передачи зашифрованных посланий и приказов.

Ущерб от террористических действий в сетевой среде в основном связан:

– с человеческими жертвами или материальными потерями, вызванными деструктивным использованием элементов сетевой инфраструктуры;

– с возможными потерями (в том числе гибелью людей) от несанкционированного использования информации с высоким уровнем секретности или сетевой инфраструктуры управления в жизненно важных (критических) для государства сферах деятельности;

– с затратами на восстановление управляемости сети, вызванными действиями по ее разрушению или повреждению;

– с моральным ущербом как владельца сетевой инфраструктуры, так и собственного информационного ресурса;

– с другими возможными потерями от несанкционированного использования информации с высоким уровнем секретности.

Соответственно, кибертерроризм предоставляет целый ряд серьезных вызовов общественности.

Во-первых, в силу их внутреннего характера компьютерные атаки практически невозможно прогнозировать или проследить в реальном времени. Поэтому атака может начаться в любое время, в стране или за рубежом, и стоять за ней могут жаждущие острых ощущений юнцы, враждебно настроенные страны, преступники, шпионы и террористы; потребуются значительные ресурсы, чтобы с высокой степенью достоверности определить, кто несет за это ответственность. Технология, как представляется, не будет в состоянии в ближайшем будущем решить эту проблему.

Во-вторых, из-за сложности законов, действующих во всем мире, сбор доказательств в таких обстоятельствах, когда могли быть использованы Интернет или другие электронные средства, а также преследование по закону, поиск, захват и выдача отдельных лиц представляются проблематичными. Указанные проблемы актуализируют необходимость осмысления существующих и выработке новых международно-правовых механизмов борьбы с кибертерроризмом.

Можно констатировать, что угроза кибертерроризма в настоящее время является очень сложной и актуальной проблемой, причем она будет усиливаться по мере развития и распространения информационных технологий.

Таким образом, анализируя различные виды киберпреступлений и последствия, к которым они могут приводить, можно сделать следующие выводы:

– необходимо определить «новые» преступления против личности: онлайн преследования, притеснения, оскорбления чести и достоинства в чатах, на форумах и т.д., предотвращать угрозы, посягающие на безопасность жизни, здоровья, свободу, интересы семьи и безопасности несовершеннолетних в интернет-пространстве;

– разработать правовые аспекты регулирования и защиты авторских прав и интеллектуальной собственности в сети, пересмотреть существующие преступления против собственности, которые связаны с охраной и использованием нематериальных благ, определить новые преступления против собственности в условиях рыночных отношений и информационного общества;

– пересмотреть и определить детерминанты совершения конкретного преступления, которые, в свою очередь, могут быть использованы в процессе расследования и рассмотрения уголовного дела, а также при создании основ и методик индивидуальной профилактики, которые обуславливаются «проживанием» в виртуальном мире и зависимостью от интернета (проблема отчуждения, анонимности, киберсоциализация);

– типологизировать различные виды преступлений в сети, определить дефиниции понятий «киберпреступление», «киберпространство», «киберпреступник»;

– прогнозировать возможные опасности кибератак с целью их недопущения, проведение специального научного исследования конкретных перспектив развития киберпреступности на основе научных статистических, вероятностных, эмпирических, философских принципов;

– обратить внимание на угрозу терроризма, экстремизма, фашизма и т.д., которые реализуют потенциал информационных технологий;

– формировать общемировые стратегии борьбы с киберпреступностью, требующие концентрации усилий всех государств,

разработать межправительственные соглашения о сотрудничестве в сфере международной информационной безопасности;

– создать международно-правовую базу, определить согласованный набор правил и внедрить соответствующие средства для статистического анализа компьютерных преступлений и т.д.

– в основу изучения киберпреступлений использовать принципы и идеи философии, разработать концептуальный аппарат, необходимый для точного и подробного описания и обсуждения моральных взаимоотношений людей в сети.

Список использованных источников

1. Вылков Р.И. Киберпространство как социокультурный феномен автореф. дис. на соискание науч. степеня канд. филос. наук : спец. 09.00.01 «Онтология и теория познания» / Р.И. Вылков. – Екатеринбург, 2009. – 151 с.
2. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы [Электронный ресурс] / Тропина Т.Л. – Режим доступа: http://www.crime.vl.ru/index.php?p=3626&more=1.
3. Федотова М. «Киберпространство и его обитатели: государство, общество, человек»: Доклад «14-е Потсдамские встречи, организованные Германо-российским форумом 18.06.2012» [Электронный ресурс] / Федотова М. –Режим доступа: http://www.president-sovet.ru/chairman/speech/2537/.
4. Broumas A. Tackling Crime in Cyberspace : A Strictly Legal Issue?/ Broumas A. http://www.lawandtech.eu/tag/CoE-Cybercrime-Convention.html.
5. Declaration of Principles Building the Information Society: a global challenge in the new Millennium [Электронный ресурс]. – Режим доступа: http://www.itu.int/wsis/docs/geneva/official/dop.html.
6. Fight against cybercrime [Электронный ресурс]. – Режим доступа: http://europa.eu/legislation_summaries/justice_freedom_security.htm.

7. Moore M. S. Act and Crime : The Theory of Action and Its Implications for Criminal Law (Clarendon Law Series) /. Moore M. S. – Oxford : Oxford University Press, 1993 – 432 p.

8. Tadros V. Criminal Responsibility / Tadros V. . – Oxford : Oxford University Press, 2005. – 408 p.

Spisok literetury ta dgerel

1. Valkov, RI Cyberspace quasi sociocultural Author phaenomenon. dis. in scientificis indagator. Ph.D. gradus liber. Philosophiae. scientia speciali. 09.00.01 'Ontology et theoriam scientiae' / RI Valkov. - Ekaterinburg, MMIX. - CLI p.

2. Tropina TL Kiberpestupnost: conceptus a civitate, poenalibus remediis adversus omnia [electronic resource] / TL Tropina - Modum aditus: http://www.crime.vl.ru/index.php?p=3626&more=1.

3. Fedotov SUM «cyberspace et habitatores ejus: in statu societatis populi» fama «14th Potestampium adunationibus Forum Latin-Russian 18.06.2012» [electronic resource] / M. Fedotov-access modum: http://www .president-sovet.ru/chairman/speech/2537 /.

4. Broumas A. Tackling Crime in Cyberspace : A Strictly Legal Issue?/ Broumas A. http://www.lawandtech.eu/tag/CoE-Cybercrime-Convention.html.

5. Declaration of Principles Building the Information Society: a global challenge in the new Millennium [Электронный ресурс]. – Режим доступа: http://www.itu.int/wsis/docs/geneva/official/dop.html.

6. Fight against cybercrime [Электронный ресурс]. – Режим доступа: http://europa.eu/legislation_summaries/justice_freedom_security.htm.

7. Moore M. S. Act and Crime : The Theory of Action and Its Implications for Criminal Law (Clarendon Law Series) /. Moore M. S. – Oxford : Oxford University Press, 1993 – 432 p.

8. Tadros V. Criminal Responsibility / Tadros V. . – Oxford : Oxford University Press, 2005. – 408 p.

9. Dorothy E. Denning. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. http://www.crime.vl.ru/docs/stats/stat_92.htm