стрирование: теория и практика. - 2014. - Вып. 2. - Режим доступа: http://nbuv.gov.ua/UJRN/Patp_2014_2_3

6. Мунтян В. В. Государственные целевые программы как инструмент финансирования молодежной политики в Украине / В. Мунтян // Экономический вестник Запорожской государственной инженерной академии. - 2016. - Вып. 6 (2). - С. 127-131.

7. Полищук В. Стратегия молодежной политики в западноевропейских и восточноевропейских странах как основа поддержки детей и молодежи / В. Полищук // Научный вестник Ужгородского национального университета. Серия: Педагогика. Социальная работа. - 2013. - Вып. 26. - С. 157-159.

8. Сторожук Р. П. Зарубежный опыт реализации молодежной политики / Г. П. Сторожук. // Государственное строительство. - 2007. - № 1 (1). - Режим доступа: http://nbuv.gov.ua/UJRN/DeBu_2007_1%281%29__51.

9. Сторожук Р. П. Молодежная политика в Украине на пути к евроинтеграции / Г. П. Сторожук // Актуальные проблемы государственного управления: Сб. наук. трудов. ОРИГУ. Вып. 4 (24). - Одесса, 2005. - С. 170-178.

10. Сторожук Р.П. Государственная молодежная политика в контексте европейского выбора Украины: механизмы реализации: Автореф. дис. ... к. Гос. упр. / Г. П. Сторожук. - Одесса, 2007. - 23 с.

11. Стрюк М. И. Тенденции развития мобильности студентов и молодых ученых в европейском образовательно-научном пространстве / Н. И. Стрюк // Педагогика высшей и средней школы. - 2015. - Вып. 46. - С. 218-225.

12. Knight J. Crossborder Education: An Analytical Framework for Program and Provider Mobility / Jane Knight // Higher Education: Handbook of Theory and Research. Volume XXI / Edited by John C. Smart. - Dordrecht : Springer, 2006. - P. 345-395.

13. Knight J. Higher Education Crossing Borders / J. Knight // International Encyclopedia of Education. Third Edition / Editors-in-Chief Penelope Peterson, Eva Baker, Barry McGaw. - Oxford : Elsevier - Academic Press, 2010. - Volume 4. - P. 507-513

ИНФОРМАЦИЯ ОБ АВТОРЕ
Ярослав Николаевич БЕЛЯЕВ,
аспирант Национальной академии государственного управления при Президенте Украины, кафедра социальной и гуманитарной политики
Тел.: +380986992225
E-mail: 7770@i.ua

INFORMATION ABOUT THE AUTHOR
Yaroslav BELYAEV,
postgraduate student of the National Academy of Public Administration under the President of Ukraine, Department of Social and Humanitarian Policy
Phone: +380986992225
E-mail: 7770@i.ua

УДК: 343.9

# ИСТОРИКО-ПРАВОВЫЕ УСЛОВИЯ СТАНОВЛЕНИЯ КАТЕГОРИИ КИБЕРПРЕСТУПНОСТИ В МЕЖДУНАРОДНОМ И НАЦИОНАЛЬНОМ ПРАВЕ

**А. Ю. ДОВЖЕНКО,**
аспирант кафедры уголовного процесса Одесского государственного университета внутренних дел

В статье рассматриваются историко-правовые условия становления категории киберпреступности в международном и национальном праве. Прослеживаются истоки явления киберпреступности, её осознание в научно-правовой мысли и практике, а также этапы правового регулирования борьбы с киберпреступностью в национальных правовых системах и в международно-правовой системе. Делается вывод о том, что явление киберпреступности не является новым, однако длительное время оставалось скрытым за «традиционными» понятиями об имущественных преступлениях, преступлениях против личности и др. Потребность в выделении киберпреступности в отдельную категорию возникает с развитием электронных систем связи, которые породили транснациональный феномен киберпреступности.

***Ключевые слова**: киберпреступность, международная компьютерная преступность, правовое регулирование киберпреступности, борьба с киберпреступностью.*

## HISTORICAL AND LEGAL PRECONDITIONS FOR THE DEVELOPMENT OF THE CATEGORY OF CYBERCRIME IN THE INTERNATIONAL AND NATIONAL LAW

**A.Y. DOVZHENKO,**
PhD student of the Department of Criminal Procedure, Odessa State university of internal affairs

The article discusses the historical and legal conditions of the formation of the category of cybercrime in international and national law. It traces the origins of the phenomenon of cybercrime, its awareness in the scientific and legal thought and practice, as well as the stages of legal regulation of the fight against cybercrime in national legal systems and in the international legal system. It is concluded that the phenomenon of cybercrime is not new, but for a long time remained hidden behind the "traditional" concepts of property crimes, crimes against the person, etc. The need to separate cybercrime into a separate category arises with the development of electronic communication systems that gave rise to cybercrime.

***Keywords**: cybercrime, international computer crime, legal regulation of cybercrime, fight against cybercrime.*

Articolul discută condițiile istorice și legale ale formării categoriei de criminalitate cibernetică în dreptul internațional și național. El urmărește originea fenomenului infracționalității cibernetice, conștientizarea acestuia în gândirea și practica științifică și juridică, precum și etapele de reglementare juridică a luptei împotriva criminalității informatice în sistemele juridice naționale și în sistemul juridic internațional. Se concluzionează că fenomenul criminalității informatice nu este nou, dar a rămas mult timp ascuns în spatele conceptelor "tradiționale" ale crimelor de proprietate, crimelor împotriva persoanei etc. Nevoia de separare a criminalității cibernetice într-o categorie separată apare odată cu dezvoltarea sistemele de comunicații electronice care au dat naștere la criminalitatea informatică.

***Cuvinte-cheie**: criminalitatea informatică, criminalitatea informatică internațională, reglementarea legală a criminalității informatice, combaterea criminalității informatice.*

**Введение**. Преступность сопровождает человечество на протяжении всей его истории. Пожалуй, трудно назвать такую сферу существования, в которой невозможно совершить общественно опасное деяние, характеризуется как преступление. По опыту известно, что объектом преступного посягательства или его орудием может выступать любой предмет, объект, явление, которые могут иметь как материальную, так и нематериальную природу. Как писал один из основоположников науки криминалистики Н. С.Таганцев, «жизнь всех народов свидетельствует нам, что везде и всегда осуществлялись и осуществляются действия, которые по разным основаниям признаются недозволенными, но и вызывают определенные меры общества или государства, направленные против лиц, которые совершили действия, которые признаются преступными; всегда и везде существовали лица, которые более или менее упорно не подчиняются требованиям правового порядка» [9, с. 17]. Ключевой характеристикой деяния как преступления является его противоправность, следствием чего становится наказуемость. Н. А. Зелинская указывает, что действия преступления имеет неизбежным следствием уголовно-правовую репрессию [4, с. 271]. То есть, видимо деяние должно быть не только общественно опасным, но и быть уголовно запрещенным и тянуть за собой уголовное наказание, чтобы считаться преступлением и представлять собой объект исследования уголовно-правовых дисциплин, в частности криминалистики.

**Цель настоящей статьи состоит в том**, чтобы проследить историю становления понятия о киберпреступлении в международном праве. Для достижения этой цели используется исторический и сравнительно-правовой **метод**.

**Изложение основного материала**. С началом массового использования компьютеров и, в более широком смысле, различных электронно-вычислительных машин во всех сферах жизни, а также с развитием электронных сетей, в первую очередь сети Интернет, возникла и связанная с ними особая сфера общественно-опасной деятельности. Следует согласиться с П. Д. Биленчуком, Б. В. Романюком и В. С. Цымбалюком в том, что нельзя говорить о необычной новизне компьютерной преступности в криминалистической теории и практике. Киберпреступность была относительно малоизвестным явлением в современной науке уголовного права и криминалистики, однако в мировой практике его развитие продолжается уже более полувека. Она возникает одновременно с появлением компьютерной техники в 1940-х годах [5, с. 19].

Одновременно с возникновением угрозы компьютерной преступности, делаются первые попытки ее теоретического осмысления. Так, в 1958 году в Стенфордском исследовательском институте было подготовлено статистическое исследование по компьютерным преступлениям. К ним были отнесены повреждения и хищения компьютерного оборудования и информации; мошенничество или похищение средств, совершенные с помощью электронных устройств, несанкционированное использование компьютерных устройств и недозволенное применения машинного времени [3, с. 133]. Примечательно, что на этом первом этапе компьютерные преступления рассматривались исключительно как материальная угроза информации или экономическим или финансовым отношениям. Об угрозе компьютерным системам как таковым речь еще не шла.

О возникновении компьютерной преступности (киберпреступности) следует говорить с момента появления первых компьютерных устройств. И если в странах советского блока она не привлекала к себе внимания в связи с малой распространенностью электронных устройств, то в Западной Европе и США киберпреступность становится предметом исследования начиная, по меньшей мере, с 1970-х годов. В отличие от современности, в те времена еще не существовало большого рынка компьютеров, и эти компьютеры не были соединены в глобальную сеть. Однако, даже в примитивных, по сравнению с современными, сетях, возникают определенные преступные техники, которые в будущем стали основой киберпреступности.

В США первые приговоры по уголовным делам по различным злоупотреблениям с компьютерной информацией были вынесены уже в 1960-х. Так, по делу Хэнкока суд штата Техас приговорил сотрудника страховой компании за преступные манипуляции с информацией из компьютерной базы данных, совершенные с корыстной целью. В деле Боттона лицо было осуждено за похищение коммерческой тайны с помощью копировальной машины [11]. В уголовных делах этого периода американские суды уделяли внимание преимущественно материальному ущербу, который был нанесен преступлением, а компьютерные средства рассматривались лишь как инструмент преступления, а не как самостоятельный элемент его состава. В 1960-1970-х годах компьютеры все еще не находили широкого потребления и использовались практически исключительно в учреждениях и на предприятиях, а также в научных учреждениях. Из-за высокой цены и малой распространённости, один и тот же компьютер обычно использовался многими лицами, что облегчало неразрешенный доступ к информации. Это, однако, не воспринималось как проблема, поскольку компьютеры не были соединены в единую систему, а, следовательно, доступ к ним все же был контролируемым.

Иной была ситуация с телекоммуникационными системами, в частности телефонными. Технические средства уже в то время позволяли вмешательства в их работу, в частности для перехвата сообщений, или для нелегального пользования. Слово «хакер», которое в дальнейшем стало использоваться для обозначения лиц, получающих неразрешенный доступ к компьютерным данным, возникло именно для обозначения телефонных «взломщиков». Впервые приговор по перехвату телефонных разговоров в США было вынесен в 1966 году по обвинению в мошенничестве [12]. В деле Турк федеральный суд отметил, что незаконное перехвата телефонного разговора может составлять преступление само по себе, независимо от его материального эффекта [13].

Осознание опасности компьютерных преступлений происходило не только в научной среде, но и в среде практиков. Так, Американская ассоциация адвокатов в 1979 году сформулировала такие признаки компьютерных преступлений как использование или попытка использования компьютера, вычислительной системы или сети с целью получения материальной выгоды, прикрываясь ложными предлогами, ложными обещаниями или притворяясь другим лицом, умышленные несанкционированные действия с целью повреждения, уничтожения или похищения компьютера, вычислительной системы или сети, а также умышленное нарушение связи между компьюте-

рами, вычислительными системами или сетями [8, с. 76].

Одновременно с первым осуждением появилось осознание необходимости криминализации общественно опасных посягательств, совершаемых с помощью электронной вычислительной техники. Такая криминализация в законодательстве отдельных государств проходила в четыре волны. Первая волна была связана с криминализацией посягательства на право на частную жизнь путем перехвата данных в электронно-коммуникационных сетях. В течение 1970-х и 1980-х годов соответствующие составы преступлений были введены в уголовное законодательство Австрии, Швеции, ФРГ, США, Франции, Дании, Норвегии, Израиля, Канады, Нидерландов, Португалии, Японии и других развитых стран. Вторая волна была связана с криминализацией корыстных манипуляций с электронной информацией, в частности похищения средств с банковских счетов. Такие положения в 1980-х годах появляются в законодательстве США, Соединенного Королевства, Дании, Канады, ФРГ и Австралии. Чуть позже наблюдалась третья волна криминализации (признание преступлениями посягательств на интеллектуальную собственность через электронные сети), а с конца 1980-х можно говорить о криминализации деяний, связанных с распространением запрещенной информации (такой как язык ненависти или порнография) через компьютерные сети [9]. Однако эти попытки были скорее ситуативными реакциями на проблему, чем системной борьбой с новым типом преступности.

Украина принимала и принимает участие в данной борьбе, хотя начала ее с заметным опозданием. Если в странах Западной Европы и Северной Америки законодательство по киберпреступлениям возникло еще в 1970-х-1980-х годах, то в Украине его становления приходится на период 1990-х-2000-х годов. Так, в 1994 году был принят Закон «О защите информации в информационно-телекоммуникационных системах», в котором было предоставлено понятие защиты информации и несанкционированного доступа к информации. В том же году были внесены изменения в действующий на тот момент Уголовного кодекса 1960 года, которыми был введен новый состав преступления: умышленное вмешательство в работу автоматизированных систем, что привело к искажению или уничтожению информации или носителей информации или распространение программных и технических средств, предназначенных для незаконного проникновения в автоматизированные системы и способных повлечь искажение или уничтожение информации или носителей информации.

Осознанию законодателем, органами государственной власти и специалистами опасности, которую несет киберпреступность, способствовало так называемое «винницкое дело», которое имела место в 1998 году. Преступник, используя систему электронных платежей, незаконно перевел на счет банка в Латвии больше 80000000 гривен. Однако, из-за отсутствия надлежащего правового регулирования в уголовном законе, этот случай не был отнесен к категории киберпреступлений и рассматривался как обычное мошенничество. Таким образом, нужно констатировать, что в 1990-х годах Украина находилась на более раннем этапе того пути, который прошли западные страны, и продолжала рассматривать киберпреступность как разновидность обычной преступности.

Вместе с тем, компьютерная преступность приобретает широкое распространение и системный характер уже в 1980-х годах, причем страдали от нее именно развитые страны, которые становились все более зависимыми от компьютерных сетей во всех сферах деятельности. В США появляются первые преступные группировки, которые специализировались на киберпреступности. Возникают первые компьютерные вирусы, которые были способны наносить вред компьютерным системам даже без прямого участия человека [2, с. 2]. Важно то, что компьютерные преступления немедленно стали интернациональными. Отдельные хакеры и группы хакеров действовали вне государственных границ. Так что и реагирования на новый тип преступности должно было носить международный характер.

На совершенно новый уровень проблема киберпреступности вышла с развитием глобальных компьютерных сетей. Как известно, первой такой сетью стал расположенный в США ARPANet, объединявший электронно-вычислительные машины крупных исследовательских центров. Поскольку доступ к самим компьютерам был строго ограничен, и они предназначались исключительно для официальной переписки и передачи данных в системе практически отсутствовали механизмы защиты от внешних вмешательств. Это стало своеобразным признаком компьютерных сетей, в 1980-е и 1990-е они проникали во все более широкий круг общественных отношений, от политических и финансовых до личных. С появлением современной сетевой архитектуры и сети Интернет, угроза от преступного влияния на нее стала глобальной, ведь ограничить доступ к сети невозможно даже теоретически, так же как проблематична полная изоляция от нее компьютерных устройств. Эта глобальность означала, что и угроза киберпреступности стала глобальной и могла быть преодолена только скоординированными усилиями государств.

С. А. Буяджи выделяет четыре этапа развития международного сотрудничества в борьбе с киберпреступностью:

1) Этап зарождения (1986 год - 1989 год), на котором принимались первые национальные законы по борьбе с киберпреступностью;

2) Этап систематизации уголовного законодательства отдельных стран по борьбе с киберпреступностью (1989 - 2000 год);

3) Этап консолидации европейского сообщества для борьбы с киберпреступностью (2000 год - 2001 год);

4) Современный этап правового регулирования борьбы с киберпреступностью (2001 год - наши дни) [1, с. 5].

Примечательно, что до второй половины 1990-х годов киберпреступления рассматривались исключительно как такие, которые совершаются с личными материальными целями. Однако, во второй их половине возникает целый пласт преступлений, направленных против государственной и международной безопасности. В частности, оказалось, что Интернет-среда предлагает многочисленные возможности для террористической деятельности, и создает у потенциальных террористов ощущение безнаказанности. Показательна первое дело о теракте с использованием Интернета, случилось в США в 1998 году. Был задержан 12-летний хакер, который, с группой других подростков, спланировал слом системы контроля плотины. Открытие дамбы потенциально могло привести к затоплению двух городов с населением более миллио-

на человек. Учитывая малолетство и «хулиганский» характер преступления, наказание для виновных было условным, однако само дело продемонстрировало страшную угрозу уязвимости компьютерных систем жизнеобеспечения современной цивилизации.

Во второй половине 1990-х годов Интернет превращается во «вторую реальность», что становится не просто отражением реальности первой, но и способен на нее активно влиять. Все значительные события в мире получили свое отражение в виртуальном пространстве. Появляется такое явление как кибервойны (первой такой войной считается война НАТО против Югославии), возникает экономическая кииберпреступность (к примеру, коммерческие проникновения в компьютерные системы предприятий с целью получения информации или прекращения их работы).

В качестве ответа на все эти вызовы делаются первые попытки международно-правового регулирования борьбы с киберпреступностью. В 2000 году принимается Конвенция Организации Объединенных Наций (ООН) против транснациональной организованной преступности. В ней использован термин «транснациональные организованные преступления, совершаемые с использованием компьютеров, телекоммуникационных сетей и других видов современной технологии» [6].

В 2001 году был принят основополагающий международный документ - Конвенция о киберпреступности, определивший понятие киберпреступности, терминологию, которая к ней применяется, а также обязанность государств по криминализации соответствующих деяний. Украина ратифицировала Конвенцию в 2005 году. Определение киберпреступности в Конвенции не предоставляется, однако из положений следует, что к киберпреступлений отнесены, по меньшей мере, незаконный доступ, нелегальный перехват компьютерных данных, вмешательство в компьютерные данные, вмешательство в компьютерные системы, злоупотребления компьютерными устройствами, подделка, связанная с компьютерами, мошенничество, связанное с компьютерами, правонарушения, связанные с детской порнографией, правонарушения, связанные с нарушением авторских и смежных прав [7]. С принятием Конвенции можно говорить о начале глобальной комплексной борьбы против киберпреступности.

**Выводы**. Понятие киберпреступности не зародилось на пустом месте. С возникновением новой сферы общественного бытия (киберсферы), возникла и связанная с ней противоправная деятельность. Несколько десятилетий потребовались для осознания специфического характера киберпреступлений, который позволил бы выделит их в отдельную группу. Такое осознание произошло с появлением транснациональной киберпреступности с использованием компьютерных сетей. Начиная приблизительно с 2000 года, можно говорить о возникновении комплексного международно-правового регулирования борьбы с киберпреступностью.

**Список использованных источников**


1. Буяджи С. А. Правове регулювання боротьби з кіберзлочинністю: теоретико-правовий аспект. Дис…канд. юрид. наук. 12.00.01. Київ, 2018. 203 с.
2. Дзюндзюк Б. В., Дзюндзюк В. Б. Поява і розвиток кіберзлочинності. *Державне будівництво*, 2013. № 1. С. 1-12.
3. Європіна І. В. Види протиправних діянь у сфері новітніх інформаційних технологій. *Вісник Академії адвокатури України*. 2010. Число 3. С. 129-136.
4. Зелінська Н. А. Поняття «міжнародний злочин» в історико-правовому ракурсі. *Актуальні проблеми політики*. 2007. № 4. С. 271-277.
5. Комп'ютерна злочинність: Навчальний посібник. За ред. П. Д. Біленчук, Б. В. Романюк, В. С. Цимбалюк та ін. Київ: Атіка, 2012. – 240 с.
6. Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності. Прийнята резолюцією 55/25 Генеральної Асамблеї від 15 листопада 2000 року. URL: https://zakon.rada.gov.ua/laws/show/995_789. (Дата звернення: 12.10.2018).
7. Конвенція про кіберзлочинність від 23.11.2001. URL: https://zakon.rada.gov.ua/laws/show/994_575. (Дата звернення: 12.10.2018).
8. Пушкаренко, П. І. Кіберзлочинність як новітній феномен тіньової економіки. *Проблеми і перспективи розвитку банківської системи України : зб. наук. праць* / Державний вищий навчальний заклад «Українська академія банківської справи Національного банку України». Суми, 2006. Т. 17. С. 75-82.
9. Таганцев Н. С. Русское уголовное право. Лекции. Часть общая. В 2 т. Т. 1. Москва: Наука, 1994, 380 с.
10. Goodman M. D., Brenner S. W. The Emerging Consensus on Criminal Conduct in Cyberspace. URL: https://uclajolt.com/home/Articles/2002/03_020625_goodmanbrenner.pdf (Дата звернення: 11.10.2018).
11. Li J. X. Cyber Crime and Legal Countermeasures: A Historical Analysis. *International Journal of Criminal Justice Sciences*. 2017. Vol. 12. P. 196-207.
12. United States v. Hoffa 367 F.2d 698 (7th Cir. 1966). URL: https://casetext.com/case/united-states-v-hoffa-15 (Дата звернення: 11.10.2018).
13. United States v. Turk 526 F.2d 654 (5th Cir. 1976). URL: https://casetext.com/case/united-states-v-turk (Дата звернення: 11.10.2018).



ИНФОРМАЦИЯ ОБ АВТОРЕ
Алексей Юрьевич ДОВЖЕНКО,
аспирант кафедры уголовного процесса Одесского государственного университета внутренних дел

INFORMATION ABOUT THE AUTHOR
Aleksey Yrevich DOVZHENKO,
postgraduate Student, Department of Criminal Procedure, Odessa State University of Internal Affairs
7358180@gmail.com


Culegere şi paginare computerizată. Bun de tipar 14.05.2019. Formatul 60x84-1/8. Tipar ofset.
Coli tipar conv. 11,75. Imprimat la „Tipocart Print" SRL, mun. Chişinău.