УДК 342.95 (477)

ИСТОРИКО-ПРАВОВОЙ АНАЛИЗ РАЗВИТИЯ ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

Владислав БУХАРЕВ,
соискатель Университета современных знаний

АННОТАЦИЯ

В статье, на основе анализа научной литературы, а также положений международных и украинских нормативно-правовых актов, осуществлен историко-правовой анализ развития законодательства в сфере обеспечения кибербезопасности. Отмечается, что первым в истории законодательным актом, который урегулировал правонарушения в киберпространстве, был Закон «О борьбе с компьютерным мошенничеством и компьютерными злоупотреблениями», который был принят в 1986 году в Соединенных Штатах Америки. Обосновывается, что особенность генезиса законодательства о кибербезопасности – это его устойчивая взаимосвязь с эволюцией компьютерных технологий. Установлено, что основное развитие кибербезопасности осуществлялось в нормативной плоскости Европы, ведь основы этого института были заложены актами ЕС.

Ключевые слова: кибербезопасность, обеспечение кибербезопасности, нормативно-правовой акт, законодательство, историко-правовой анализ.

HISTORICAL AND LEGAL ANALYSIS OF THE DEVELOPMENT OF LEGISLATION IN THE SPHERE OF ENSURING CYBERSECURITY

Vladislav BUKHAREV,
Applicant of University of Modern Knowledge

SUMMARY

In the article, on the basis of analysis of scientific literature, as well as provisions of international and Ukrainian legal acts, a historical legal analysis of the development of legislation in the field of providing cybersecurity was carried out. It is noted that the first in the history of the legislative act, which resolved offenses in cyberspace, was the Law "On Combating Computer-Aided Fraud and Computer Abuse," which was adopted in 1986 in the United States of America. It is substantiated that the peculiarity of the genesis of cybersecurity legislation is its steady correlation with the evolution of computer technology. It was established that the main development of cybersecurity was carried out in the normative plane of Europe, because the foundations of this institution were laid down by the acts of the EU.

Key words: cybersecurity, cybersecurity, normative-legal act, legislation, historical-legal analysis.

Постановка проблемы. На современном этапе развития общества институт кибербезопасности является развитым правовым явлением, которое имеет нормативную основу. Однако становлению кибербезопасности предшествовал целый ряд событий, которые обусловили развитие ее юридического выражения в правовой системе государства. Понятием «кибербезопасность» описывается надлежащее состояние работы в сфере обработки информации путем использования вычислительной техники, другими словами, компьютеров. При этом электронные устройства сами по себе не представляют угрозы легальному статусу указанного выше института. Все меняется в тех случаях, когда речь идет не о самостоятельных компьютерных единицах, а о целой системе подобных устройств, с помощью которых осуществляется обмен информацией через мировую сеть. При таких условиях мы можем говорить о существовании нового информационного пространства (киберпространства), где реально имеют место ситуации фактического нарушения прав и свобод людей. В этом контексте кибербезопасность выступает в виде правового механизма обеспечения защиты прав и интересов людей в киберпространстве.

Актуальность темы исследования. Поэтому с целью более полного понимания института и его правовой природы необходимо проанализировать не только текущее нормативное состояние кибербезопасности на основе положений действующего законодательства, но и провести историко-правовое исследование ее появления и становления.

Состояние исследования. Отдельные аспекты развития института кибербезопасности рассматривали в своих научных трудах: Л.А. Макаренко, С.С. Скворцов, В.С. Стефанюк, А.Ю. Прокопенко, В.В. Марков, К.И. Шляпа, А.А. Миндюк, С.С. Алексеев, А.В. Логинов, Р.А. Стефанчук, А.И. Педешко, А.А. Тихомиров, А.Н. Кулиш, А.Н. Музычук, А.К. Тугарова, И.В. Европина и многие другие. Однако единого комплексного исследования, посвященного историко-правовому анализу развития законодательства в сфере обеспечения кибербезопасности, так и не было проведено.

Именно поэтому **целью** статьи является историко-правовой анализ развития законодательства в сфере обеспечения кибербезопасности.

Изложение основного материала. Начиная рассмотрение основного материала представленного научного исследования, следует отметить, что первым в истории законодательным актом, который регулировал правонарушения в киберпространстве, был «The Computer Fraud and Abuse Act» (Закон о борьбе с компьютерным мошенничеством

и компьютерными злоупотреблениями), принят он в 1986 году в Соединенных Штатах Америки [1; 2, с. 146]. Данный акт, по сути, признавал проблему возможности совершения неправомерных действий в информационной сфере, что дало толчок к развитию института кибербезопасности. Закон закрепил ответственность за несанкционированное вмешательство в работу компьютерных систем или похищение информации из них. Кроме того, актом предусматривались санкции по отношению к лицам, которые совершают действия подобного характера.

Значительным вкладом в развитие института кибербезопасности стало принятие Советом Европы в 1989 году Рекомендации R (89) 9, в которой были закреплены: во-первых, четкий перечень действий, приобретающих признаки киберпреступлений; во-вторых, главные аспекты разработки и построения единой стратегии противодействия негативным действиям в киберпространстве [3]. Положения указанного акта фактически запустили механизм эволюции института безопасности в сфере использования компьютерных технологий с целью обмена данными. Развитие этого явления в последующие годы и до сегодняшнего дня проходило как на уровне международного права, так и национального, которое принималось под влиянием мирового законодательства.

Так, в 2000 году в Вене была принята Венская декларация о преступности и правосудии: ответы на вызовы XXI века (ООН). Конечно, этот документ не определял и не закреплял нормы относительно института кибербезопасности в том виде, в котором он существует сегодня. Однако на основе положений Декларации было принято решение разработать ориентированные на конкретные действия программные рекомендации по предупреждению преступлений, связанных с использованием компьютеров, и борьбы с ними. То есть уже в то время нарушения в сфере использования инновационных технологий характеризовались общественной опасностью, что позволило говорить о формировании киберпреступности. Декларация также возложила обязанность на всех государств – членов Организации Объединенных Наций (далее – ООН) работать в направлении укрепления их возможностей по предупреждению, расследованию и преследованию преступлений, связанных с использованием высоких технологий и компьютеров [4]. В том же году Европейским Союзом принимается Конвенция о взаимопомощи по уголовным делам между членами ЕС, в рамках которой были закреплены процессуальные особенности и новые механизмы взаимодействия между государствами по поводу противодействия киберправонарушениям [5].

Подытоживая изложенные выше факты, мы можем утверждать, что издание двух последних международных актов фактически заставило мировое сообщество взглянуть на явление кибербезопасности как на самостоятельный юридический институт, а не элемент системы того или иного механизма противодействия правонарушениям в сфере использования компьютерных технологий. В дальнейшем кибербезопасность будет определяться как отдельный правовой институт, в рамках которого осуществляется разработка стратегии преодоления антиобщественных действий в киберпространстве. Этот тезис подтверждается положениями Резолюции Генеральной Ассамблеи ООН о создании глобальной культуры кибербезопасности, принятой в 2002 году. В данном акте определяются ключевые пути создания глобальной культуры кибербезопасности, а также объясняются особые моменты механизма обеспечения этого института. Ключевым преимуществом Резолюции является то, что этот документ закрепил конкретные требования к субъектам кибербезопасности, которые последние должны неукоснительно выполнять, ведь от этого зависит реальное состояние правовой обеспеченности института [6].

Представленные в Резолюции требования вошли в положения Женевской декларации принципов построения информационного общества, принятой на Всемирном саммите по вопросам информационного общества 12 декабря 2003 года. В статье 35 части 5 главы Декларации указана необходимость формирования, развития и внедрения глобальной культуры кибербезопасности в сотрудничестве со всеми заинтересованными сторонами и компетентными международными организациями. Такие действия должны опираться на международное сотрудничество. В рамках глобальной культуры кибербезопасности важно повышать безопасность и обеспечивать защиту данных и неприкосновенности частной жизни, расширяя при этом доступ и масштаб торговых операций. Кроме того, необходимо принимать во внимание уровень социально-экономического развития каждой страны и учитывать связанные с ориентацией на развитие аспекты информационного общества [7].

Следует отметить, что параллельно с развитием мирового законодательства правовой институт кибербезопасности также развивался на национальном уровне. Конечно, на начальном этапе становления Украины как независимого государства самого понятия «кибербезопасность» в нормативных документах страны фактически не существовало. Однако определенные основы института обеспечения информационной безопасности в различных сферах жизнедеятельности населения страны уже были имплементированы в национальное законодательство с учетом международно-правовых стандартов в этой области. Развитие правовых основ организации кибербезопасности в Украине нашло отражение в следующих нормативных актах, а именно: законах Украины: «О Концепции Национальной программы информатизации» от 4 февраля 1998 года, «О Национальной программе информатизации» от 2 октября 1992 года, «О защите информации в информационно-телекоммуникационной системе» от 5 июля 1994 года, «О научно-технической информации» от 25 июня 1993 года, «Об охране прав на топографии интегральных микросистем» от 5 ноября 1997 и др.

Соответствующие нормативные сдвиги в направлении развития системы обеспечения института кибербезопасности также прослеживаются на подзаконном уровне. В частности, в течение 2000–2001 годов Президентом Украины были изданы указы «О мерах по совершенствованию государственной информационной политики и обеспечения информационной безопасности Украины» и «О мерах развития национальной составляющей глобальной информационной сети Internet и обеспечения ши-

рокого доступа к этой сети в Украине». Положения данных актов определили вектор развития деятельности страны в сфере организации информационной безопасности, а также на нормативном уровне закрепили особенности использования инновационной в то время сети Internet и механизм ее государственной поддержки.

Наибольшим прорывом отечественного законодательства в сфере обеспечения кибербезопасности стала ратификация в 2005 году Конвенции о кибербезопасности, принятой Советом Европы. Согласно преамбуле, целью создания документа стала необходимость остановки действий, направленных против конфиденциальности, целостности и доступности компьютерных систем, сетей и компьютерных данных, а также злоупотребления такими системами, сетями и данными, путем установления уголовной ответственности за такое поведение, предоставления полномочий, достаточных для эффективной борьбы с такими уголовными преступлениями путем содействия их выявлению, расследованию и преследованию, как на внутригосударственном, так и на международном уровнях [8].

Последние годы характеризуются началом нового витка эволюции института кибербезопасности, который был существенно модифицирован нормами действующего законодательства. Переняв опыт зарубежных стран в сфере регулирования изучаемого явления, наша страна создала юридические основы его регулирования. Так, в 2016 году был издан Указ Президента, который ввел в действие решение Совета национальной безопасности и обороны Украины «О Стратегии кибербезопасности Украины». Инновационность данного акта заключается в том, что именно в его положениях впервые был использован термин «кибербезопасность».

Согласно общим положениям стратегии, стремительное развитие информационных технологий постепенно трансформирует мир. Открытое и свободное киберпространство расширяет свободу и возможности людей, обогащает общество, создает новый глобальный интерактивный рынок идей, исследований и инноваций, стимулирует ответственную и эффективную работу власти, а также активное привлечение граждан к управлению государством и решению вопросов местного значения, что обеспечивает публичность и прозрачность власти, способствует предотвращению коррупции. В то же время преимущества современного цифрового мира и развитие информационных технологий обусловили возникновение новых угроз национальной и международной безопасности. Наряду с инцидентами природного (непреднамеренного) происхождения растет количество и мощность кибератак, мотивированных интересами отдельных государств, групп и лиц [9]. Итак, стратегией четко определяется имеющаяся проблема нарушения прав и свобод граждан Украины в киберпространстве, в связи с чем возникает необходимость: во-первых, введения надлежащего механизма правового регулирования этой сферы, а во-вторых, обеспечения охраны общественного интереса от противоправных посягательств внутри нее.

Несмотря на целесообразность и приоритетность принятой Стратегии, информативность этого подзаконного нормативного акта довольно низкая. В частности, в его положениях довольно часто термины «киберзащита» и «кибербезопасность» отождествляются, что не позволяет понять все аспекты уникальности данного института. Кроме этого, весомый недостаток заключается в отсутствии в положениях Стратегии дефиниций таких понятий, как «киберпространство», «киберпреступления», «киберугроза» и других. Иными словами, нормативный акт создает механизм обеспечения института, сущность которого реально остается непонятной. С другой стороны, Стратегия показывает венец развития института кибербезопасности, эволюция которого осуществлялась на протяжении большого отрезка времени.

В свою очередь, недостатки указанного нормативного акта фактически были устранены новым Законом Украины «Об основных принципах обеспечения кибербезопасности в Украине». Его главной целью является определение правовых и организационных основ государственной политики, направленной на защиту жизненно важных интересов человека и гражданина, общества и государства в киберпространстве, основных принципов и направлений обеспечения кибербезопасности Украины [10]. Кроме стратегически важной цели, данный нормативный документ характеризуется рядом других особенностей: во-первых, закон фактически легализует все понятия с приставкой «кибер-», которые до сих пор существовали преимущественно в научных работах ученых или положениях международных нормативно-правовых актов; во-вторых, этот нормативный документ на законодательном уровне закрепляет принципы, основные направления обеспечения и объекты кибербезопасности Украины; в-третьих, Закон уточняет понятие субъектов механизма обеспечения кибербезопасности, а также более детально представляет их полномочия в этой сфере.

Выводы. Итак, проведя историко-правовой анализ развития и становления правового института кибербезопасности, нами было рассмотрено большое количество нормативных актов как международного, так и национального права. Это позволило выделить главную особенность генезиса изучаемого явления – его устойчивую взаимосвязь с эволюцией компьютерных технологий. Вопрос обеспечения кибербезопасности приобрел особое значение из-за повышения уровня обмена информацией между различными субъектами с помощью инновационных технологий и сети Internet. Основное развитие кибербезопасности осуществлялось в нормативной плоскости Европы, ведь основы этого института были заложены актами ЕС. На уровне национального законодательства институт начал развиваться в начале XXI века. Его становлению предшествовало принятие целого ряда законодательных актов, которые прямо не устанавливали правовой статус кибербезопасности, не говоря о механизме ее обеспечения. Крупнейшим шагом к имплементации в правовую систему Украины исследуемого института стала ратификация Конвенции Совета Европы о киберпреступности в 2005 году. Этот документ определил ключевые типы правонарушений, которые совершаются в киберпространстве, а также процедурные особенности международного сотрудничества в борьбе с ними.

Список использованной литературы:

1. Marshall J.H., Balle M.W. Office of Legal Education Executive Office for United States Attorneys. 2010. 213 p.

2. Буяджа С.А. Генезис правового регулювання боротьби з кіберзлочинністю у світі. Науковий вісник Ужгородського національного університету. 2014. Вип. 29. Ч. 2. Том 4/2. С. 145–149.

3. Computer-related crime. Recommendation no. R. (89) 9 on computer-related crime and final report of the European Committee on Crime Problems. Strasbourg. – Council of Europe, Pub. And Documentation Service. Croton – N.Y. : Manhattan Pub. Co., 1990. 114 p.

4. Віденська декларація про злочинність та правосуддя: відповіді на виклики XXI століття: Міжнародний документ, декларація від 17.04.2000 р. URL: http://zakon3.rada.gov.ua/laws/show/995_443

5. Конвенція про взаємодопомогу в кримінальних справах між державами-членами Європейського Союзу: Міжнародний документ, конвенція від 29.05.2000 р. URL: http://zakon5.rada.gov.ua/laws/show/994_238/page

6. Мосьондз С.О. Адміністративно-правова охорона сфери науки в Україні: концептуальне бачення. Науково-аналітичний журнал «Митна справа». 2012. № 5 (83). Ч. 2. Книга 2. С. 102–107.

7. Декларація принципів «Побудова інформаційного суспільства – глобальне завдання у новому тисячолітті»: Міжнародний документ, декларація від 12.12.2003 р. URL: http://zakon3.rada.gov.ua/laws/show/995_c57

8. Конвенція про кіберзлочинність: міжнародний документ, конвенція від 23.11.2001 р. Офіційний вісник України. 2007. № 65. С. 107.

9. Про Стратегію кібербезпеки України: Указ від 15.03.2016 р. № 96/2016. Офіційний вісник України. 2016. № 23. С. 69.

10. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. http://zakon2.rada.gov.ua/laws/show/2163-19

ИНФОРМАЦИЯ ОБ АВТОРЕ

Бухарев Владислав Викторович – соискатель Университета современных знаний

INFORMATION ABOUT THE AUTHOR

Bukharev Vladislav Viktorovich – Applicant of University of Modern Knowledge

stanislav2107@mail.ru

УДК 343.97

СОВРЕМЕННЫЙ НАУЧНЫЙ ПОТЕНЦИАЛ ИССЛЕДОВАНИЯ КРИМИНАЛИЗАЦИИ ЛИЧНОСТИ

Марина ВАЛУЙСКАЯ,
кандидат юридических наук,
доцент кафедры криминологии и уголовно-исполнительного права
Национального юридического университета имени Ярослава Мудрого

АННОТАЦИЯ

В статье рассматривается состояние исследований криминализации личности. На сегодняшний день криминология располагает лишь фрагментарными сведениями о личности преступника и, как правило, в статике – на момент совершения преступления. Криминализация личности, т.е. процесс приобретения ею криминогенных свойств, практически не исследуется. Поэтому криминология не располагает сведениями, позволяющими приостановить процесс криминализации на тех стадиях, когда ее степень не достигла качественно нового уровня – общественной опасности.

Проанализированы современные факторы криминализации, а также обстоятельства, которые необходимо учитывать при исследовании криминализации личности. Предлагается использовать современный научный потенциал по составлению компьютерных программ для определения степени криминогенности личности с целью предупреждения совершения ею преступлений.

Ключевые слова: личность преступника, криминализация личности, предупреждение преступности, факторы криминализации личности, социализация личности преступника, криминологические тесты, цифровые технологии.

MODERN SCIENTIFIC POTENTIAL OF RESEARCH OF CRIMINALIZATION OF PERSONALITY

Marina VALUYSKAYA,
Candidate of Law Sciences, Associate Professor at the
Department of Criminology and Criminal Executive Law of Yaroslav Mudryi National Law University

SUMMARY

The article studies the state of research of the criminalization of personality. Now criminology has only fragmentary information about the personality of a criminal and as a rule given in statics - at the moment of crime. Criminalization of personality, i.e. the process of acquiring its criminogenic characteristics is practically not being investigated. Therefore, criminology does not have the information that allows suspending the process of criminalization at those stages when its degree has not reached yet a qualitatively new level – public danger.

The article analyzes the modern factors of criminalization, as well as the circumstances that must be considered in the study of the criminalization of personality. It proposes to use modern scientific resources for the compilation of computer programs to determine the degree of criminalization of a person in order to prevent from crimes commitment.

Key words: personality of a criminal, criminalization of a person, crime prevention, factors of criminalization of a person, socialization of the person of a criminal, criminological tests, digital technologies.

Постановка проблемы. Проблема предупреждения преступности – главная задача криминологической науки. Для ее решения криминологи исследуют преступность как социальное явление, отдельные преступления (виды преступлений) как частные случаи проявления преступности, личность преступника, факторы преступности. Как правило, характеристика личности преступника присутствует в криминологических исследованиях, посвященных отдельным видам пре-