УДК 340.11:004

ОБ ОТДЕЛЬНЫХ АСПЕКТАХ ПРАВОВОГО РЕГУЛИРОВАНИЯ КИБЕРБЕЗОПАСНОСТИ УКРАИНЫ

Екатерина КАЛАЧЕНКОВА,
кандидат юридических наук, доцент,
доцент кафедры хозяйственного права
Донецкого национального университета имени Васыля Стуса

Елена ТИТОВА,
кандидат юридических наук, доцент,
доцент кафедры хозяйственного права
Донецкого национального университета имени Васыля Стуса

АННОТАЦИЯ

В статье проводится научно-теоретическое исследование, посвященное проблеме правового регулирования отношений в сфере обеспечения кибербезопасности Украины. Осуществляется анализ работ ученых и законодательной базы в указанной сфере. Проанализирована терминологическая составляющая обеспечения кибербезопасности с использованием технико-юридического инструментария, а именно языковых средств юридической техники. Указано на существующие недостатки терминологической базы с точки зрения средств юридической техники. Обоснована целесообразность уточнения понятий «информация об инциденте кибербезопасности», «кибербезопасность», «кибератака» в контексте совершенствования положений Закона Украины «Об основных мерах кибербезопасности Украины».

Ключевые слова: инцидент, жизненно важные интересы кибербезопасности, кибератака, киберугроза, правовое регулирование кибербезопасности, электронная коммуникационная сеть.

ABOUT SOME ASPECTS OF LEGAL REGULATION OF CYBER SECURITY OF UKRAINE

Katerina KALACHENKOVA,
Candidate of Law Sciences, Associate Professor,
Associate Professor at the Department of Commercial Law
of Vasyl' Stus Donetsk National University

Elena TITOVA,
Candidate of Law Sciences, Associate Professor,
Associate Professor at the Department of Commercial Law
of Vasyl' Stus Donetsk National University

SUMMARY

The article presents a scientific and theoretical study on the problems of legal regulation of relations in the field of cybersecurity of Ukraine. The analysis of researches of scientists and legislative base in this sphere is carried out. The article analyzes the terminological component of cybersecurity with the use of technical and legal tools, namely language means of legal technology. The existing shortcomings of the terminological base from the point of view of legal equipment are pointed out. The expediency of clarifying the concepts of "information about the incident of cybersecurity", "cybersecurity", "cyber-attack" in the context of improving the provisions of the Law of Ukraine "On basic measures of cybersecurity of Ukraine".

Key words: incident, vital interests of cybersecurity, cyber-attack, cyber threat, legal regulation of cybersecurity, electronic communication network.

Постановка проблемы. Кибербезопасность представляет собой стратегическую комплексную проблему любого государства, которая прежде всего касается экономики страны, особенно электронной промышленности, в том числе инфраструктуры электронных коммуникаций, технологий киберзащиты государственных информационных ресурсов, объектов критической информационной инфраструктуры [1, с. 14].

Украина занимает третью строчку рейтинга стран с наибольшим риском заражения через Интернет: 35,7% пользователей столкнулись с вебугрозами. Украина оказалась на девятой строчке рейтинга стран с наибольшим риском заражения мобильных устройств вредоносными программами (8,39%). Достаточно высок и риск столкновения с локальными угрозами (54,5%). К последним относятся объекты, которые проникли в компьютеры путем заражения файлов или съемных носителей, или сначала попали на компьютер не в открытом виде (например, программы в составе сложных инсталляторов, зашифрованные файлы и тому подобное). По указанному показателю страна занимает предпоследнюю строчку в топ-20 в мире, но первую в Европе [2, с. 33].

Актуальность темы исследования. За последнее время в Украине происходит как активное формирова-

ние законодательства о кибербезопасности, так и осуществление научных разработок соответствующей проблематики. Однако стремительное развитие отношений в указанной сфере, возрастающая роль информационный среды в жизни общества обуславливает необходимость повышения качества национального законодательства о кибербезопасности, уточнения направлений его дальнейшего развития. Вышеизложенное подтверждает актуальность избранной темы исследования.

Состояние исследования. Проблеме научного осмысления правового обеспечения кибербезопасности посвящены работы таких исследователей, как И.В. Диордица, О.Д. Довгань, И.М. Доронин, Д.В. Дубов, Р.В. Лукьянчук, В.В. Петров, А.В. Шапка, В.П. Шеломенцев и другие. Однако отдельные аспекты обеспечения кибербезопасности в Украине все еще недостаточно освещены или требуют дополнительного исследования. Надлежащая эффективность мер по обеспечению кибербезопасности в значительной степени определяется уровнем правового регулирования в указанной сфере.

Целью и задачей статьи является научно-теоретическое обоснование вопросов обеспечения кибербезопасности в Украине, разработка теоретических и практических положений относительно повышения его результативности.

Изложение основного материала. Нормативную основу обеспечения кибербезопасности в Украине составляют: Конвенция Совета Европы о киберпреступности [3]; законы Украины «Об информации» [4], «О национальной безопасности Украины» [5], «О телекоммуникациях» [6], «О защите информации в информационно-телекоммуникационных системах» [7], «Об основных мерах обеспечения кибербезопасности Украины» [8]; указы Президента Украины «О решении Совета национальной безопасности и обороны Украины «О стратеги национальной безопасности Украины» от 6 мая 2015 г.» [9] и «О решении Совета национальной безопасности и обороны Украины от 27 января 2016 г. «О Стратегии кибербезопасности Украины» [10].

Стратегией кибербезопасности Украины поставлена задача создания соответствующей терминологической базы с целью обеспечения условий для безопасного функционирования киберпространства. И хотя сама Стратегия, по мнению исследователей, не сформировала основ стратегического управления в сфере кибербезопасности и не использует адекватных денотатов описания стратегических явлений [11, с. 14], в целом в Законе Украины «Об основных мерах обеспечения кибербезопасности Украины» (далее – Закон о кибербезопасности) [8] дается определение ключевых понятий в сфере кибербезопасности.

Эксперты главным образом положительно отзываются о принятии Закона о кибербезопасности как базового документа и в то же время отмечают наличие в нем целого ряда недоработок [12, с. 26]. Анализ упомянутого Закона показывает, что они есть и в терминологической базе. Термины и дефиниции необходимы для точного и определенного выражения воли законодателя. В законодательном тексте правовые дефиниции должны адекватно раскрывать содержание того или иного термина, определять его признаки, включать характеристики, данные в концентрированной и обобщающей форме [13, с. 178–179].

Следует согласиться, что законодательные дефиниции, включенные в тексты нормативно-правовых актов, имеют нормативный характер, являются видом юридических норм, выступают в связке с другими нормами, выполняя свои функции в составе нормативного блока, регулирующего те или иные общественные отношения [13, с. 125]. Соответственно, их изложение должно быть точным по сути и корректным по форме. Анализ содержащихся в Законе о кибербезопасности дефиниций свидетельствует о наличии определенных проблем, которые не только негативно сказываются на качестве Закона, но и могут повлиять на эффективность его реализации.

Отдельные понятия Закона о кибербезопасности являются недоработанными, изложены с нарушением логических связей между их смысловыми частями. Например, в ст. 1 Закона изложено понятие информации об инциденте кибербезопасности как сведения об обстоятельствах киберинцидента, в частности о том, какие объекты киберзащиты и при каких условиях подверглись кибератаке, какие из них успешно обнаружены, нейтрализованы, какие предотвращены, с помощью каких средств киберзащиты, в том числе с использованием каких индикаторов киберугроз. И если первая часть упомянутого определения является в целом корректной и понятной, то вторая не может не вызывать замечаний. Так, слова «из них успешно обнаружены», «нейтрализованы, предотвращены» при прямом прочтении относятся к понятию «объекты киберзащиты».

Понятно, что объекты киберзащиты в контексте указанного определения не могут быть «успешно обнаружены», «нейтрализованы», их невозможно «предотвратить». Применение подходов лингвистического толкования показывает, что слова «из них успешно обнаружены», «нейтрализованы, предотвращены» характеризуют именно киберинцидент, а не объекты киберзащиты. Небрежное изложение понятия «информация об инциденте кибербезопасности» в нормах законодательного акта не может не влиять отрицательно на качество законодательства о кибербезопасности, способность законодательства удовлетворять конкретные потребности правового регулирования.

Следует согласиться с исследователями, отмечающими, что сегодня без внимания часто остается тот факт, что качество нормативно-правового акта зависит от точности юридических формулировок, которые в нем находятся, от того, насколько они логически связаны и последовательны в единстве с другими правовыми предписаниями [14, с. 202].

Исходя из вышеизложенного, понятие информации об инциденте кибербезопасности целесообразно уточнить, указав что это «сведения об обстоятельствах киберинцидента, в частности о том, какие объекты киберзащиты и при каких условиях подверглись кибератаке, какие обстоятельства киберинцидента успешно обнаружены, нейтрализованы, предотвращены, а также сведения об использованных средствах киберзащиты и индикаторах киберугроз». Таким образом слова «из них успешно обнаружены», «нейтрализованы», «предотвращены» будут связаны со словами «обстоятельства киберинцидента», что позволит восстановить логику изложения соответствующей нормы закона.

При определении понятия кибернетической атаки (кибератаки) ученые использовали, как правило, отдельные ее признаки. В.П. Шеломенцев, обобщая научные подходы, определяет такие основные элементы характеристики кибернетической атаки: объект кибернетической атаки, способный воспринять целенаправленное воздействие кибернетического характера; сущность действий при кибератаке, их кибернетический аспект; средства кибератаки, способные сформировать влияние кибернетического характера; пространство (среда) кибератаки, в котором возможно осуществление влияния кибернетического характера [15].

В ст. 1 Закона о кибербезопасности кибератака определяется как направленные (умышленные) действия в киберпространстве, которые осуществляются с помощью средств электронных коммуникаций (включая информационно-коммуникационные технологии, программные, программно-аппаратные средства, другие технические и технологические средства и оборудования) и направлены на достижение одной или совокупности таких целей: нарушение конфиденциальности, целостности, доступности электронных информационных ресурсов, которые обрабатываются (передаются, хранятся) в коммуникационных и/или технологических системах, получение несанкционированного доступа к таким ресурсам; нарушение безопасности, устойчивого, надежного и штатного режима функционирования коммуникационных и/или технологических систем; использование коммуникационной системы, ее ресурсов и средств электронных коммуникаций для осуществления кибератак на другие объекты киберзащиты.

Таким образом, в упомянутом определении содержатся такие составляющие: указание на действия; перечисление средств кибератаки и цели кибератаки. Однако при этом в ряду перечисляемых целей кибератаки упоминается также «использование коммуникационной системы, ее ресурсов и средств электронных коммуникаций для осуществления кибератак на иные объекты киберзащиты». Такой подход сложно признать корректным. С одной стороны, результатом такого логико-семантического построения стало определение понятия кибератаки (выделено автором – *Е. К., Е. Т.*) через «использование коммуникационной системы, ее ресурсов и средств электронных коммуникаций для осуществления кибератак» (выделено автором – *Е. К., Е. Т.*), что фактически нарушает правило, согласно которому понятие не может определяться через себя самого. С другой стороны, последней из перечисленных целей кибератаки является «использование коммуникационной системы, ее ресурсов и средств электронных коммуникаций для осуществление кибератак на иные объекты киберзащиты» (выделено автором – *Е. К., Е. Т.*) в то время, как в предшествующем тексте определения нет четкого указания на объекты киберзащиты (или их перечисления), а в самом определении речь идет об объектах как о названных прямо объектами киберзащиты в ст. 2 Закона (например, коммуникационные системы), так и о таких, которые в конкретно установленном перечне объектов киберзащиты отсутствуют (электронные информационные ресурсы). Недостаточно корректным является также использование в одном определении понятия «коммуникационная система» и как объекта кибератаки, и как средства кибератаки без каких-либо дополнительных уточнений и оговорок.

Таким образом, понятие кибератаки, содержащееся в ст. 1 Закона о кибербезопасности, не соответствует таким требованиям, как полнозначность, определенность, системность, соразмерность, точность, логичность, устойчивость употребления терминов, и нуждается в дальнейшем уточнении.

В Законе Украины «О телекоммуникациях», действующего с 2014 г., используется понятие «телекоммуникационная сеть», под которой понимается комплекс технических средств телекоммуникаций и сооружений, предназначенных для маршрутизации, коммутации, передачи и/или приема знаков, сигналов, письменного текста, изображений и звуков или сообщений любого рода по радио, проводным, оптическим или другим электромагнитным системам между конечным оборудованием. Также упомянутый Закон оперирует рядом связанных с таким определением понятий: «телекоммуникационная сеть общего пользования», «телекоммуникационная сеть доступа» и другие.

Подписание Соглашения об ассоциации между Украиной и ЕС внесло определенные коррективы в соответствующие терминологические основы, поскольку в Соглашении используется понятие «электронная коммуникационная сеть» (ст. 115). С учетом изложенного во всех известных сегодня проектах Закона об электронных коммуникациях предлагается использование понятия «электронная коммуникационная сеть». Таким образом, в перспективе понятие «телекоммуникационная сеть» в законодательстве Украины должно быть заменено понятием «электронная коммуникационная сеть». И в таком контексте подход, используемый в Законе о кибербезопасности, вызывает определенные замечания.

Так, в ст. 1 (п. п. 17, 21), ст. 8 (п. п. 2, 3, 4) Закона о кибербезопасности используются понятия «национальная телекоммуникационная сеть», «специальные телекоммуникационные системы (сети). Одновременно в ст. 1 (п. 21), ст. 2 (п. п. 1, 2), ст. 4 (п. п. 2, 4), ст. 8 (п. 2) используются понятия «системы электронных коммуникаций», «коммуникационные системы», «пользователи коммуникационных систем». Таким образом, законодатель для определения юридической сущности одного и того же явления использует разные понятия без указания, являются ли они идентичными или имеют какие-то сущностные различия. Это негативно сказывается на качестве самого Закона о кибербезопасности и затрудняет его эффективное применение. Поэтому целесообразно было бы осуществить унификацию терминологических подходов в Законе о кибербезопасности в контексте использования Соглашения об ассоциации именно термина «электронная коммуникационная сеть».

Центральным понятием Закона о кибербезопасности является непосредственно понятие «кибербезопасность». Кибербезопасность в ст. 1 Закона толкуется как защищенность жизненно важных интересов человека и гражданина, общества и государства при использовании киберпространства, при которой обеспечиваются устойчивое развитие информационного общества и цифровой коммуникационной среды, своевременное выявление, предотвращение и нейтрализация реальных и потенциальных угроз национальной

безопасности Украины в киберпространстве.

Указанный подход к понятию «кибербезопасность» уже был объектом критики в специальной литературе в связи с использованием термина «кибернетическое пространство», под которым понималась «среда, что возникает в результате функционирования на основе единых принципов и по общим правилам информационных (автоматизированных), телекоммуникационных и информационно-телекоммуникационных систем». Однако при этом неизбежно возникает вопрос об идентификации «жизненно важных интересов человека и гражданина, общества и государства» в такой среде. Как отмечают А.Д. Довгань и О.М. Доронин, в указанной среде не происходит и не могут в принципе происходить никакие общественные отношения между субъектами (человек, гражданин, общество, государство). Таким образом, неудачное определение термина «кибернетическая безопасность» логично приводит к не совсем правильному определению предмета указанного акта, его целей и, самое главное, к неправильному определению комплекса мероприятий по его внедрению [12, с. 15].

Анализируя понятие «кибербезопасность» (ст. 1 Закона о кибербезопасности), следует обратить внимание также на то, что круг субъектов, чьи интересы должны быть объектом защиты, исходя из его содержания, не совсем точно определенны. Речь идет о таких субъектах, как человек, гражданин, общество и государство. Однако при этом не упоминаются ни организации, ни субъекты хозяйствования, защищенность интересов которых также является неотъемлемым признаком кибербезопасности как определенного состояния защищенности. Субъекты хозяйствования упоминаются в отдельных статьях Закона о кибербезопасности, однако только в контексте осуществления ими компетенционных мероприятий по обеспечению кибербезопасности. Между тем без надлежащей защиты интересов субъектов хозяйствования реальное состояние кибербезопасности, как состояние защищенности, вряд ли возможно.

Так, например, общая оценка событий 27–29 июня 2017 г. показывает, что 70% украинских банков так или иначе пострадали от кибератак вируса «Petya». Видимым следствием таких атак стала остановка работы терминалов, платежных систем, отделений банков, а также ограниченный доступ к интернет-банкингу и международным переводам [16, с. 10)].

В своей публикации «Трансформация кибербезопасности» ISACA отмечает, что «кибербезопасность охватывает все, что защищает организации и физические лица от умышленных атак, нарушений, инцидентов и их последствий. Кибербезопасность сосредотачивается на так называемых сложных направленных постоянных угрозах (APT), кибервойне и их влиянии на организации и людей» [17]. Таким образом, целесообразно в понятии кибербезпасности уточнить круг субъектов, чьи интересы должны быть объектом защиты.

В процессе дальнейшего совершенствования законодательства о кибербезопасности следует учитывать, что содержание в законе неточных, неясных, неоднозначных терминов, противоречий, законодательных ошибок служит основанием неадекватного его толкования, невнятного его понимания. Это, в частности, отражается на эффективности его применения. Если закон качественный, разработан с соблюдением правил юридической техники, содержит ясные и точные термины, то отпадает необходимость в его дополнительном разъяснении [18, с. 154].

Выводы. Основные дефиниции Закона о кибербезопасности должны получить грамотное и всестороннее раскрытие своего содержания, что является основой высокого качества закона, эффективности его применения и стабильности существования. В частности, нуждаются в уточнении такие понятия, как «кибербезопасность», «кибератака», «информация об инциденте кибербезопасности», в том числе с учетом изложенных в нашей статье замечаний.

Список использованной литературы:

1. Лук'янчук Р.В. Державне управління у сфері забезпечення кібербезпеки України: дис. … канд. юрид. наук: 25.00.01. Київ, 2017. 206 с.

2. Андрощук Г.О. Кібербезпека: тенденції у світі та Україні. Кібербезпека та інтелектуальна власність: проблеми правового забезпечення: матеріали міжнар. наук.-практ. конф. (Київ, 21 квітня 2017 р.). Київ, 2017. 146 с.

3. Конвенція про кіберзлочинність від 7 вересня 2005 р. № 2824-IV. Офіційний вісник України. 2007. № 65. Ст. 2535.

4. Про інформацію: Закон України від 2 жовтня 1992 р. № 2657-XII. Відомості Верховної Ради України. 1992. № 48. Ст. 650.

5. Про національну безпеку України: Закон України від 21 червня 2018 р. № 2469-VIII. Офіційний вісник України. 2018. № 55. Ст. 1903.

6. Про телекомунікації: Закон України від 18 листопада 2003 р. № 1280-IV. Відомості Верховної Ради України. 2004. № 12. Ст. 155.

7. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 5 липня 1994 р. № 80/94-ВР. Відомості Верховної Ради України. 1994. № 31. Ст. 286.

8. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. Відомості Верховної Ради. 2017. № 45. Ст. 403.

9. Про рішення Ради національної безпеки й оборони України від 6 травня 2015 р. «Про Стратегію національної безпеки України»: Указ Президента України від 26 травня 2015 р. № 287/2015. Офіційний вісник Президента України. 2015. № 13. Ст. 874.

10. Про рішення Ради національної безпеки й оборони України від 27 січня 2016 р. «Про Стратегію кібербезпеки України»: Указ Президента України від 15 березня 2016 р. Офіційний вісник Президента України. 2016. № 10. Ст. 198.

11. Діордіца І.В. Адміністративно-правове регулювання кібербезпеки України: автореф. дис. … докт. юрид. наук: 12.00.07. Запоріжжя, 2018. 29 с.

12. Довгань О.Д., Доронін І.М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія. Київ, 2017. 107 с.

13. Мамедов Э.Ф. Термины и дефиниции как средства юридической техники правотворчества: дисс. … канд. юрид. наук: 12.00.01. Иркутск, 2015. 184 с.

14. Легін Л.М. Поняття та критерії якості закону: проблеми визна-

чення. Проблеми законності. 2016. Вип. 132. С. 196–204.

15. Шеломенцев В.П. Поняття та сутність кібернетичної атаки. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2011. Вип. 25–26. С. 337–344. URL: http://nbuv.gov.ua/UJRN/boz_2011_25-26_39.

16. Павловська А.М. Халімон З.В. Кібербезпека у банківському секторі: чи допоможе IT-outsourcing? Юридична газета. 2018. № 10 (612). С. 10–11.

17. Элементы для создания глобальной культуры кибербезопасности: Резолюция Генеральной Ассамблеи ООН от 20 декабря 2002 г. № 57/239. URL: http://zakon3.rada.gov.ua/laws/show/995_b42.

18. Холикзода А.Г. Критерии качества закона: общетеоретическое исследование: дисс. … канд. юрид. наук: 12.00.01. Душанбе, 2018. 190 с.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Калаченкова Екатерина Александровна – кандидат юридических наук, доцент, доцент кафедры хозяйственного права Донецкого национального университета имени Васыля Стуса

Титова Елена Витальевна – кандидат юридических наук, доцент, доцент кафедры хозяйственного права Донецкого национального университета имени Васыля Стуса

INFORMATION ABOUT THE AUTHORS

Kalachenkova Ekaterina Aleksandrovna – Candidate of Law Sciences, Associate Professor, Associate Professor at the Department of Commercial Law of Vasyl' Stus Donetsk National University

kalachenkova.e.a@gmail.com

Titova Elena Vitalyevna – Candidate of Law Sciences, Associate Professor, Associate Professor at the Department of Commercial Law of Vasyl' Stus Donetsk National University

andromeda2015@ukr.net

УДК 351/354:004(477)

ЭЛЕКТРОННОЕ УПРАВЛЕНИЕ В КОНТЕКСТЕ УСТОЙЧИВОГО РАЗВИТИЯ

Евгения КАЛИШЕНКО,
аспирант кафедры административного и финансового права Национального университета биоресурсов и природопользования Украины; ведущий юрисконсульт Государственного предприятия «Украинский институт интеллектуальной собственности»

АННОТАЦИЯ

Статья посвящена исследованию электронного управления в контексте устойчивого развития. Система Организации Объединенных Наций неразрывно связывает электронное управление с устойчивым развитием и призывает страны к более эффективному задействованию потенциала информационно-коммуникационных технологий для содействия достижению согласованных на международном уровне целей в области устойчивого развития. Благодаря инновациям и развитию электронного управления, государственно-административные органы во всем мире могут стать более эффективными, предоставлять более качественные услуги и отвечать требованиям прозрачности и подотчетности. В статье анализируются международные документы Организации Объединенных Наций, а также национальные нормативно-правовые документы в области электронного управления.

Ключевые слова: электронное управление, электронное правительство, электронные услуги, информационно-коммуникационные технологии, устойчивое развитие, Организация Объединенных Наций, Цели Устойчивого Развития.

ELECTRONIC GOVERNANCE IN THE CONTEXT OF SUSTAINABLE DEVELOPMENT

Evgeniya KALISHENKO,
Postgraduate Student at the Department of Administrative and Financial Law of the National University of Life and Environmental Sciences of Ukraine; Leading Lawyer at the State Enterprise "Ukrainian Intellectual Property Institute"

SUMMARY

The article is devoted to the study of e-governance in the context of sustainable development. The United Nations system inextricably links e-governance (e-government) with sustainable development and calls on countries to better engage the potential of information and communication technologies to help achieve internationally agreed sustainable development goals. Through innovation and e-government, public administrations around the world can be more efficient, provide better services and respond to demands for transparency and accountability. The article analyzes the international documents of the United Nations, as well as national regulatory documents in the field of e-governance.

Key words: electronic governance (e-governance), electronic government (e-government), electronic services (e-services), information and communication technologies, sustainable development, United Nations, Sustainable Development Goals.

Постановка проблемы. Процессы, которые получили название «электронное управление», имеют место практически во всех странах. При этом вокруг понятия «электронное управление» ведутся постоянные дискуссии, и оно остается неоднозначным. Многозначность определений обусловлена тем, что ученые акцентируют внимание на разных аспектах и принципах функционирования электронного управления.

Однако и ученые, и правительственные должностные лица, межправительственные учреждения, организации гражданского общества, частный сектор и граждане в целом связывают появление такого понятия, как «электронное управление», «электронное правительство» с масштабным, глубинным и динамичным проникновением информационно-коммуникационных технологий в государственный сектор,