УДК 342.9

СОСТОЯНИЕ АДМИНИСТРАТИВНО-ПРАВОВОГО ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ В УКРАИНЕ

Марина КОНДРАТЮК
аспирант кафедры кибербезопасности и информационного обеспечения
Одесского государственного университета внутренних дел

В статье освещены административно-правовые аспекты обеспечения кибербезопасности в Украине. Отмечено, что существующая административно-правовая система киберзащиты имеет разветвленный характер, в результате чего информационное пространство становится уязвимым к совершению преступлений. Представлены и проанализированы группы административно-правовых актов по обеспечению кибербезопасности в Украине: международные и национальные. Приведены виды правонарушений, связанных с компьютерами. Установлено, что, не смотря на то, что нормы Конституции являются нормами прямого действия, подлежащими безоговорочному выполнению, кибербезопасность в Украине в настоящее время пребывает не на высоком уровне. Раскрыты основные приоритеты обеспечения кибербезопасности и безопасности информационных ресурсов в Украине. Выделены правонарушения в сфере кибербезопасности, которые включены в украинское уголовное законодательство согласно Будапештской конвенции. Определены основные проблемы, существующие в административно-правовом обеспечении кибербезопасности в Украине. Предложены меры по совершенствованию административно-правового обеспечения кибербезопасности.

Ключевые слова: *информация, кибернетическое пространство, государство, кибернетизация, кибербезопасность, законодательство, административно-правовое обеспечение.*

CONDITION OF ADMINISTRATIVE AND LEGAL SECURITY OF CYBER SECURITY IN UKRAINE

Marina KONDRATYUK
Postgraduate Student of the Department of Cybersecurity and Information Support
of Odessa State University of Internal Affairs

The article deals with the administrative and legal aspects of cybersecurity in Ukraine. It is noted that the existing administrative and legal system of cyber defense has a branched character, as a result of which the information space becomes vulnerable to crime. Groups of administrative and legal acts on cybersecurity in Ukraine: international and national are presented and analyzed. The types of computer-related offenses are listed. Despite the fact that the norms of the Constitution are norms of direct action subject to unconditional enforcement, cybersecurity in Ukraine is currently not at a sufficiently high level. The main priorities of providing cybersecurity and security of information resources in Ukraine are revealed. Cyber security offenses have been identified and incorporated into Ukrainian criminal law under the Budapest Convention. The main problems that exist in the administrative and legal support of cybersecurity in Ukraine are identified. Measures to improve the administrative and legal support of cybersecurity have been proposed.

Keywords: *information, cyberspace, state, cybernetization, cybersecurity, legislation, administrative and legal support.*

ADMINISTRATIVE ŞI JURIDICE ALE SECURITĂŢII CYBERNETICE ÎN UCRAINA

Articolul tratează aspectele administrative şi legale ale securităţii cibernetice în Ucraina. Se observă că sistemul administrativ şi juridic existent de apărare cibernetică are un caracter ramificat, în urma căruia spaţiul informaţional devine vulnerabil la infracţiuni. Grupurile de acte administrative şi juridice privind securitatea cibernetică în Ucraina: internaţionale şi naţionale sunt prezentate şi analizate. Tipurile de infracţiuni legate de computer sunt enumerate. În ciuda faptului că normele Constituţiei sunt norme de acţiune directă, supuse aplicării necondiţionate, securitatea cibernetică în Ucraina nu se află în prezent la un nivel suficient de ridicat. Principalele priorităţi ale furnizării securităţii cibernetice şi securităţii resurselor informaţionale din Ucraina sunt dezvăluite. Infracţiunile de securitate cibernetică au fost identificate şi încorporate în dreptul penal ucrainean în temeiul Convenţiei de la Budapesta. Sunt identificate principalele probleme care există în sprijinul administrativ şi legal al securităţii cibernetice în Ucraina. Au fost propuse măsuri pentru îmbunătăţirea sprijinului administrativ şi legal al securităţii cibernetice.

Cuvinte-cheie: *informaţii, spaţiu cibernetic, stare, cibernetizare, securitate cibernetică, legislaţie, asistenţă administrativă şi legală.*

Постановка проблемы. На сегодняшний день одним из приоритетных направлений развития Украины является возникновение информационного общества. Меры по реализации данного шага предусматривают активное внедрение информационно-коммуникационных технологий, развитие кибернетического пространства. Опыт зарубежных стран свидетельствует о том, что переход части общественных отношений в кибернетическое пространство имеет ряд преимуществ. Они способствуют повышению прозрачности деятельности субъектов публичной власти, оперативности и эффективности их взаимодействия между собой и с представителями общественности, а также международным сообществом. Однако быстрое развитие информационных, информационно-телекоммуникационных средств, технологий, систем и сетей имеет негативные аспекты, в частности появление новой сферы для процветания преступной деятельности. На формирование преступности в данной сфере влияет целый ряд факторов: развитие компьютерных и информационно-коммуникационных технологий опережает развитие законодательства, регулирующего отношения в данной сфере; неограниченность государственными границами, что создает благоприятные условия для процветания транснациональной преступности; сложность выявления непосредственного субъекта преступной деятельности и доказательства его вины. Поэтому указанные и другие аспекты компьютеризации, кибернетизации значительной части общественной жизни заставляют нашу страну особое внимание уделять своей кибернетической безопасности.

Актуальность темы исследования. Повышение качества и эффективности организации, а также функционирования системы кибербезопасности возможно за счет совершенствования ее административно-правового обеспечения, которое предусматривает улучшение соответствующего законодательства и пересмотр системы субъектов, занимающихся данными вопросами. На протяжении последних лет в научной литературе все чаще поднимается вопрос о необходимости укрепления национальной кибербезопасности. Это вполне понятно, ведь с такими кибернетическими угрозами, которые есть сегодня, Украина раньше не сталкивалась, как результат – отсутствие необходимого опыта и неспособность эффективно противодействовать данным угрозам. Указанное обуславливает актуальность проведения комплексного изучения состояния административно-правового обеспечения кибернетической безопасности в Украине.

Состояние исследования. Вопросы административно-правового обеспечения кибербезопасности раскрыты в научных трудах А.А. Андрощука, В.М. Богуша, В.М. Бутузова, К.Ю. Галинской, С.В. Демедюка [], А.Л. Добржанской, Д.В. Дубова, А.Н. Клюева, Л.П. Коваленко, А.Н. Мельника, Ю.М. Онищенко, О.В. Орлова, А.В. Островой [21], В.В. Пахомова, А.В. Руденко, О.Ю. Синявской, М.В. Старинского, Ю.М. Супрунов, А.Л. Татузов, В.Б. Толубко, Ю. Шипилова [27], Є.В. Ющука. Однако, не смотря на наличие ряда научных работ, посвященных развитию кибернетического пространства, специальные комплексные исследования по определению состояния административно-правового обеспечения кибербезопасности в Украине, которые основаны на обновленном законодательстве в этой сфере, являются недостаточными.

Целью и задачей статьи является определение состояния и проблем административно-правового обеспечения кибербезопасности в Украине, а также путей его совершенствования.

Изложение основного материала. Процесс регулирования всех общественных отношений в государстве происходит в соответствии с требованиями нормативно-правовых актов, принятых в установленном законом порядке. Но законодательная база является лишь внешним выражением права и институтов, входящих в ее структуру, то есть, она предоставляет правовой системе государства материальный вид. Реальную же основу юридической отрасли составляют принципы, содержащиеся в положениях нормативно-правовых актов. В данном случае не является исключением и кибербезопасность, которая быстрыми темпами развивается в нашей стране. Указанный феномен является довольно широким правовым институтом. Его объектом выступают правоотношения в сфере обработки информации в кибернетическом пространстве. Не менее интересной выступает структура кибербезопасности, в состав которой входит система киберзащиты. Она представляет собой набор мер по обеспечению указанного выше правового института, который применяется для его стабильности и действенности. Однако систему обеспечения кибербезопасности можно рассматривать как правовое явление, что, в свою очередь, обусловливает наличие соответствующих правовых основ, на которых базируется ее действие. Современная нормативная база дает возможность выделить большое количество административно-правовых основ обеспечения института.

В Украине существующая административно-правовая система киберзащиты имеет разветвленный характер, в результате чего информационное пространство становится уязвимым к совершению преступлений. Прежде чем перейти к анализу национального законодательства в сфере защиты информации, следует отметить, что за годы независимости Украины вопрос кибернетической и информационной безопасности развивался по остаточному принципу. Разработка нормативно-правовых документов по регулированию этой сферы происходила бессистемно. Они часто базировались на устаревших советских нормах и вступали в противоречие друг с другом. В результате возникло угнетающее состояние в системе кибернетической безопасности и информационно-коммуникационных технологий вообще. Ученый В.В. Бухарєв утверждает, что правовые основы обеспечения кибербезопасности – это весь массив руководящих идей, принципов и положений, закрепленных в нормативно-правовых актах различной юридической силы, определяющих механизм правового регулирования обеспечения кибербезопасности [18, с. 70].

Стоит отметить, что административно-правовые акты в данной сфере можно разделить на две группы: международные (Конвенция Совета Европы «О киберпреступности»; Директива NIS) и национальные (Конституция Украины и соответствующие нормативно-правовые акты, регулирующие вопросы в этой сфере; нормативно-правовые акты органов исполнительной власти; нормативно-правовые акты специальных субъектов обеспечения кибербезопасности [20; 22]. Так, Конвенция Совета Европы «О киберпреступности», известная как Будапештская конвенция, является единственным юридически обязательным международным документом по этому вопросу. В ней указано, что это первое международное соглашение, которое связано с преступлениями, совершенными через Интернет и другие компьютерные сети (нарушение авторских прав, связанное с компьютерным мошенничеством; детская порнография; нарушение сетевой безопасности) [27]. Проанализировав нормы Конвенции, можно сделать вывод, что основные функции, которые касаются обеспечения информационной безопасности, противодействия и совершения киберпреступлений, реализуются правовой системой каждого из государств-участников отдельно. Наличие недостатков в законодательстве является их внутренними проблемами. С нашей точки зрения, значительным преимуществом ратификации Конвенции выступает такой вид международного сотрудничества государств-участниц, как экстрадиция – общие принципы взаимной помощи с целью расследования уголовных преступлений.

В 2016 году Европейским парламентом принята первая часть единого для ЕС законодательства о кибербезопасности – Директива NIS. Так как Украина не входит в ЕС, Директива NIS не является обязывающей, однако она служит руководством в вопросах надлежащей практики. Некоторые из положений были добровольно внедрены в украинское законодательство, другие остаются без внимания. Директиву NIS саму по себе можно использовать как источник для совершенствования украинского внутреннего законодательства. Официальную дорожную карту внедрения Директивы NIS в украинское законодательство можно разработать в рамках механизма, установленного Соглашением об ассоциации между Украиной и Европейским Союзом. Сейчас в Верховной Раде Украины зарегистрирован законопроект, который, среди прочего, направлен на гармонизацию законодательства Украины с правом Европейского Союза, в частности с Директивой NIS (анализ законопроекта приводится в разделе «Законодательный уровень» Закона о кибербезопасности) [27]. Государственная служба специальной связи и защиты информации (ГСССЗИ) пытается внедрить требования Директивы NIS в законопроекты, которые готовит эта служба. Однако ее представители признали, что при разработке комплексных законов о кибербезопасности, которые будут отвечать требованиям Директивы NIS, крайне важна международная помощь [19].

Главным нормативным документом, Конституцией Украины [1], предусмотрено, что защита суверенитета и территориальной целостности страны, обеспечение ее экономической и информационной безопасности выступают главными задачами государства, делом всего украинского народа. С нашей точки зрения, несмотря на то, что нормы Конституции являются нормами прямого действия, подлежащими безоговорочному выполнению, кибербезопасность в Украине в настоящее время пребывает на не достаточно высоком уровне. Информационные отношения по обеспечению кибернетической безопасности в государстве урегулированы действующим законодательством, Законами Украины № 2657-XII [6], № 2230-XII [5], 18.02.1992 №2135-XII [4], № 3475-IV [10], № 2939-VI [11], № 81/94-ВР [7], № 1932-XII [3], № 1280-IV [9], №851-IV [8], №2163-VIII [12]; Указами Президента № 287/2015 [13], № 32/2017, решением Сове-

та национальной безопасности и обороны Украины от 29.12.2016 «Об угрозах кибербезопасности государства и неотложных мерах по их нейтрализации» [14]; отдельными положениями Уголовного кодекса Украины [2], отдельными Постановлениями и Распоряжениями Кабинета Министров (Постановление Кабинета Министров Украины от 14.05.2015 №303 «Некоторые вопросы организации межведомственного обмена информацией в Национальной системе конфиденциальной связи» [15]; Распоряжение Кабинета Министров Украины от 6.12.2017 № 1009 «Об одобрении Концепции создания государственной системы защиты критической инфраструктуры» [17]).

Административно-правовые основы обеспечения кибербезопасности нашего государства также нашли свое проявление в Законе Украины «Об основных принципах обеспечения кибербезопасности Украины». В качестве примера можно привести п.6 ст. 7 указанного закона, где закреплена приоритетность мер обеспечения кибербезопасности. Сущность этого принципа обеспечения кибербезопасности заключается в том, что меры закреплены именно в нормах административного законодательства, ведь они осуществляются государственными органами и используются в целях предупреждения правонарушений в той или иной сфере и недопущения совершения правонарушений в будущем [12]. Кроме того, в рамках системы обеспечения кибербезопасности административно-правовое регулирование приобретает более широкое понимание. На основании вышеуказанного, необходимо констатировать, что принятие единого комплексного нормативного акта, который бы регулировал отношения кибербезопасности на национальном уровне, является крайне важным и необходимым для нашего государства в настоящее время. Однако, на наш взгляд, Закон Украины «Об основных принципах обеспечения кибербезопасности Украины» очень сильно расширяет полномочия государственных органов власти, тем самым позволяя им вмешиваться в осуществление деятельности субъектами хозяйствования.

Соответствующие меры в сфере киберзащиты используются и в правоохранительной сфере Украины. В декабре 2011 был создан Департамент по борьбе с киберпреступностью МВД Украины, а в начале 2012 были образованы соответствующие территориальные подразделения. Новым этапом в противостоянии с киберпреступностью в Украине стало создание 13 октября 2015 киберполиции как структурного подразделения Национальной полиции [16]. В Украине также существует подразделение, в компетенцию которого входит противодействие киберпреступности – это Департамент контрразведывательной защиты интересов государства в сфере информационной безопасности. Также следует обратить внимание на Национальный координационный центр кибербезопасности – рабочий орган Совета национальной безопасности и обороны Украины. Центр обязан обеспечивать координацию деятельности субъектов национальной безопасности и обороны Украины во время реализации Стратегии кибербезопасности Украины, повышать эффективность системы государственного управления в процессе формирования и реализации государственной политики в сфере кибербезопасности [23].

Значительным шагом в обеспечении кибербезопасности стало подписание в 2019 году Меморандума о взаимодействии и сотрудничестве в сфере кибербезопасности и киберзащиты между Центром киберзащиты Национального банка Украины и Государственным центром киберзащиты (Государственная служба специальной связи и защиты информации). Такое сотрудничество направлено на предотвращение, выявление, эффективное реагирование на противодействие актуальным киберугрозам, повышение уровня информационной безопасности и ситуационной осведомленности в сфере кибербезопасности и киберзащиты [19]. Однако, на наш взгляд, формирование и реализация перечисленных действий в данной сфере требует доработок.

Поэтому с целью решения указанных проблем на государственном уровне были предложены и реализованы следующие меры:

1. Кабинетом министров Украины разработан проект Закона Украины «Про внесение изменений в Закон Украины «Об основах национальной безопасности Украины», в котором учтены вопросы кибербезопасности [22]. Данный документ является результатом работы специалистов силовых структур (СБУ, МВД, Минобороны), цель которого – сформировать основы государственной политики в сфере обеспечения кибербезопасности Украины; 2. Кабинетом министров Украины разработан Проект Закона о внесении изменений в некоторые законы Украины относительно усиления ответственности за совершенные правонарушения в сфере информационной безопасности и борьбы с киберпреступностью. В проекте закона содержатся изменения, которые предлагается внести в Кодекс Украины об административных правонарушениях и законы Украины «Об оперативно-розыскной деятель-

ности», «О Службе безопасности Украины», «О контрразведывательной деятельности», «Об основах национальной безопасности Украины» и «О разведывательных органах Украины». Основная цель проекта Закона заключается в повышении способности служб безопасности и разведки противостоять киберугрозам. Однако полномочия, необходимые для отслеживания и расследования киберпреступлений, также следует предоставить правоохранительным органам, связанным с уголовной юстицией. Все мероприятия должны отвечать Уголовному процессуальному кодексу и условиям, а также упреждающим мерам, предусмотренным им, даже не смотря на то, что расследовать предстоит именно киберпреступление. Необходимо четко разграничить меры, направленные на защиту национальной безопасности, и меры уголовной юстиции. В случае сбора информации во время деятельности службы национальной безопасности или разведки необходимо установить четкие правила, может ли такая информация служить доказательством в уголовном производстве, а если да – то при каких условиях [22]. В проекте Закона введено новое определение кибернетической безопасности (кибербезопасности). Стоит провести комплексный обзор обсуждаемых проектов законов, поскольку они предлагают внести схожие изменения в законы, которые часто дублируют друг друга. 3. Предложены концептуальные подходы к комплексному пересмотру законодательства Украины, которое касается вопросов национальной обороны.

В результате нами выделены основные проблемы, которые существуют в административно-правовом обеспечении кибербезопасности в Украине:

1. Отсутствие в Украине единой государственной системы противодействия киберпреступности и единого нормативного документа, который бы четко обозначил основные понятия, а также определил зоны ответственности государственных структур в сфере кибербезопасности.

2. Отсутствие положения о критической инфраструктуре (КИ). Отсутствует единая национальная система защиты КИ, а регуляторные правила по защите КИ недостаточны и непоследовательны, в частности не хватает специального закона о КИ и ее защите. Существующее постановление Кабинета Министров Украины относительно процедуры формирования перечня информационно-телекоммуникационных систем государственных объектов КИ было принято в 2016 году, до принятия Закона о кибербезопасности, поэтому противоречит ему. Правительство не смогло принять новые нормативные акты в предусмотренный Законом о кибербезопасности срок, который истек в августе 2018 года. При этом отсутствуют общие критерии и методология отнесения объектов к КИ, а также процедура аттестации и категоризации КИ. В результате перечень объектов КИ до сих пор не утвержден, и положения Закона о кибербезопасности по защите КИ остаются декларативными.

3. Устарелость и несистематизированность правовых актов по вопросам национальной безопасности. Они содержат много несогласований, не учитывают особенности угроз нового вида, в том числе влияние «гибридной» агрессии.

4. Отсутствие координации государственных структур в сфере кибербезопасности.

5. Наличие бюджетных рамок, которые ограничивают способность правительства платить конкурентоспособные зарплаты для привлечения и удержания нужных специалистов в области кибербезопасности. В докладе MITRE освещены проблемы низких зарплат, которые правительство платит сотрудникам – специалистам в сфере ИТ и кибербезопасности; уровень этих зарплат гораздо ниже по сравнению с частным сектором. Многие украинские стейкхолдеры согласны, что это является ограничительным фактором. Возможности правительства ограничены из-за правовых требований, которые следует изменить, чтобы агентства могли содержать и мотивировать специалистов в сфере ИТ и кибербезопасности. Кроме того, низкие зарплаты повышают риск инсайдерских атак и сами по себе создают уязвимость в плане кибербезопасности. Кроме того, одна из проблем в сфере киберзащиты состоит в том, что Украина до сих пор является уязвима к киберугрозам, и не в последнюю очередь из-за очень широкого транслирования иностранных программных продуктов и использования материально-технической базы иностранного производителя [21, с. 98].

Поэтому нами определены меры по совершенствованию административно-правового обеспечения кибербезопасности:

1. *Принятие всеохватывающего закона о кибербезопасности.* Закон «Об основных принципах обеспечения кибербезопасности Украины» 2017 года является дорожной картой для будущих нормативных актов. Учитывая украинскую правовую систему и практику, стране необходимо принять всеохватывающий закон о кибербезопасности, который будет регулировать полный спектр вопросов кибербезопасности и отвечать международным стандартам. Принимая во внимание сложность темы, с

нашей точки зрения, разработка такого закона требует консультаций с разными стейкхолдерами и привлечения к его написанию экспертов из разных сфер, включая представителей агентств по кибербезопасности.

2. *Анализ правовой базы кибербезопасности в соответствии с Директивой NIS.* Украине следует провести полный анализ первичного и вторичного законодательства, идентифицировать нормы, которые противоречат Директиве NIS, и предложить поправки в соответствии с рекомендациями, предложенными на основе такого анализа. Украинские власти не способны разрабатывать соответствующие законопроекты в соответствии с требованиями Директивы NIS, поэтому им нужна международная поддержка.

3. *Создание тезауруса терминологии кибербезопасности и его легитимизация в текстах вышеуказанных законов.* Законы, регулирующие вопросы кибербезопасности, были приняты в разные времена, и в них использована разная терминология. Это значительно усложняет процесс реализации этих законов. Чтобы обеспечить общее понимание кибербезопасности, нужен всеохватывающий анализ терминологии и гармонизация национального законодательства.

4. *Гармонизация законодательства по единому виденью круга субъектов, на которых возлагается обязательства обеспечения национальной безопасности, в том числе кибернетической безопасности.*

5. *Внесение поправок в законодательство о правоохранительных органах, ответственных за защиту кибербезопасности от киберпреступлений и кибертерроризма.* Украинские стейкхолдеры в сфере кибербезопасности по-разному видят роль и полномочия агентств по кибербезопасности и процесс предоставления таких полномочий. Поскольку Закон о кибербезопасности предоставил значительные полномочия СБУ и ГССССЗИ, многие представители частного сектора жаловались на то, что это было сделано в Законе о кибербезопасности, а не путем внесения поправок в законы о СБУ и ГССССЗИ. При этом в СБУ и ГССССЗИ возник спор о нехватке полномочий и ресурсов, чтобы работать эффективно. Украине стоит извлечь пользу из тщательного анализа и консультаций по разграничению полномочий между правоохранительными органами, отвечающими за защиту кибербезопасности.

6. *Разработка Стратегии кибербезопасности на период 2020–2025 годов и Стратегического плана.* ГССССЗИ считает, что нынешняя Стратегия кибербезопасности действует в период 2016–2020 годов, поскольку она была принята в соответствии со Стратегией национальной безопасности Украины, срок действия которого истекает в 2020 году. Самое время обновить стратегию и разработать стратегический план на будущее.

7. *Внесение в действующие нормативно-правовые документы положений о роли и месте научных учреждений, высших учебных заведений для подготовки специалистов в сфере кибербезопасности.*

8. *Формирование кибернетической безопасной политики на научной основе.*

Выводы. Таким образом, нами определено состояние административно-правового обеспечения кибербезопасности в Украине. Несмотря на то, что нормы Конституции являются нормами прямого действия, подлежащими безоговорочному выполнению, кибербезопасность в настоящее время пребывает на не достаточно высоком уровне. В стране существующая административно-правовая система киберзащиты имеет разветвленный характер, в результате чего информационное пространство становится уязвимым к совершению преступлений. Разработка и реализация большого количества нормативно-правовых документов в сфере кибербезопасности привела к тому, что в Украине отсутствует единая государственная система противодействия киберпреступности и единого акта, который бы четко обозначил основные понятия, а также определил зоны ответственности государственных структур в сфере кибербезопасности.

Список использованной литературы

1. Конституция Украины от 28.06.1996. URL: http://zakon3.rada.gov.ua/laws/show/254 (дата обращения: 04.02.2020).

2. Уголовный кодекс Украины от 05.04.2001 № 2341-III. URL: http://zakon3.rada.gov.ua/laws/show/2341-14 (дата обращения: 04.02.2020).

3. Закон Украины «Об обороне Украины» от 06.12.1991 № 1932-XII. URL: http://zakon5.rada.gov.ua/laws/show/1932-12 (дата обращения: 04.02.2020).

4. Закон Украины «Об оперативно-розыскной работе» от 18.02.1992 №2135-XII. URL: https://zakon.rada.gov.ua/laws/show/2135-12 (дата обращения: 06.02.2020).

5. Закон Украины «О службе безопасности Украины» от 25.03.1992 № 2230-XII. URL: https://zakon.rada.gov.ua/laws/show/2229-12 (дата обращения: 06.02.2020).

6. Закон Украины «Об информации» от 02.10.1992 №2657-XII. URL: http://zakon3.rada.gov.ua/laws/show/2657-12 (дата обращения: 04.02.2020).

7. Закон Украины «О защите информации в информационно-телекоммуникационных системах» от 05.07.94 №81/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-

%D0%B2%D1%80 (дата обращения: 04.02.2020).

8. Закон Украины «Об электронных документах и электронном документообороте» от 22.05.2003 №851-IV. URL: https://zakon.rada.gov.ua/laws/show/851-15 (дата обращения: 05.02.2020).

9. Закон Украины «О телекоммуникациях» от 18.11.2003 №1280-IV. URL: https://zakon.rada.gov.ua/laws/show/1280-15 (дата обращения: 05.02.2020).

10.Закон Украины «О государственной службе специальной связи и защиты информации Украины» от 23.02.2006 № 3475-IV. URL: http://zakon3.rada.gov.ua/laws/show/3475-15 (дата обращения: 04.02.2020).

11.Закон Украины «О доступе к публичной информации» от 13.01.2011 № 2939-VI. URL: http://zakon5.rada.gov.ua/laws/show/2939-17 (дата обращения: 04.02.2020).

12.Закон Украины «Об основных принципах обеспечения кибербезопасности Украины» от 05.10.2017 №2163-VIII URL: http://search.ligazakon.ua/l_doc2.nsf/link1/T172163.html (дата обращения: 04.02.2020).

13.Указ Президента «О решении Совета национальной безопасности и обороны Украины «О Стратегии национальной безопасности Украины» от 26. 05.2015 №287/2015.

14.Указ Президента о решении Совета национальной безопасности и обороны Украины от 29 декабря 2016 года «Об угрозах кибербезопасности государства и неотложных мерах по их нейтрализации» от 13.02.2017 № 32/2017.

15.Постановление Кабинета Министров Украины «Некоторые вопросы организации межведомственного обмена информацией в Национальной системе конфиденциальной связи» от 14.05.2015 №303.

16.Постановление Кабинета Министров «Об образовании территориального органа Национальной полиции» от 13.10.2015 №831. URL: http://zakon3.rada.gov.ua/laws/show/831- 2015-% D0% BF (дата обращения: 04.02.2020).

17.Распоряжение Кабинета Министров Украины «Об одобрении Концепции создания государственной системы защиты критической инфраструктуры» от 6.12.2017 №1009.

18.Бухарев В.В. Административно-правовые основы обеспечения кибербезопасности Украины: дис… канд. юридических наук. Специальность: 2.00.07 - административное право и процесс; финансовое право, информационное право, Сумы, 2018. 221 с.

19.Государственная служба специальной связи и защиты информации URL: http://www.dsszzi.gov.ua/dsszzi/control/ru/index (дата обращения: 03.02.2020).

20.Демедюк С.В. Административно-правовое регулирование отношений в сфере обеспечения кибербезопасности в Украине. *Южно-украинский правовой журнал.* 2015. № 3. С. 119–123.

21.Островой А.В. Формирование государственной политики обеспечения кибернетической безопасности в Украине : дис. канд. наук. специальность : государственное управление. Мариуполь, 2019. 239 с.

22.Отчет по Украине «О действующем законодательстве и проекты законов, которые дополняют различные вопросы, связанные с киберпреступностью и электронными доказательствами, а также вносят изменения в них» от 3.12.2016. URL: https://rm.coe.int/16806f3743 (дата обращения: 03.02.2020).

23.Шипилова Ю. Правовая база украинской кибербезопасности: общий обзор и анализ. URL: https: //ifesukraine.org/wp-content/uploads/2019/10/IFES-Ukraine-Ukrainian-Cybersecurity-Legal-Framework-Overview-and-Analysis-2019-10 -07-Ukr.pdf (дата обращения: 05.02.2020).

ИНФОРМАЦИЯ ОБ АВТОРЕ
КОНДРАТЮК
Марина Владимировна,
аспирант кафедры
кибербезопасности и
информационного обеспечения
Одесского государственного
университета внутренних дел;

INFORMATION ABOUT THE AUTHOR
KONDRATYUK
Marina Vladimirovna,
Postgraduate Student of the Department of Cybersecurity and Information Support of Odessa State University of Internal Affairs;
e7x54h8i@gmail.com