УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ ФЕДЕРАЦИИ ПРОФСОЮЗОВ БЕЛАРУСИ
«МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ «МИТСО»

КИБЕРУГРОЗЫ КАК НОВЫЙ ВЫЗОВ ДЛЯ МЕЖДУНАРОДНОГО ГУМАНИТАРНОГО ПРАВА

Научное электронное издание

**СБОРНИК МАТЕРИАЛОВ
СТУДЕНЧЕСКОЙ НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ
(г. Минск, 27 мая 2022 г.)**

Минск
Международный университет «МИТСО»
2022

УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ ФЕДЕРАЦИИ ПРОФСОЮЗОВ БЕЛАРУСИ
«МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ «МИТСО»

Научное электронное издание

КИБЕРУГРОЗЫ КАК НОВЫЙ ВЫЗОВ ДЛЯ МЕЖДУНАРОДНОГО ГУМАНИТАРНОГО ПРАВА

СБОРНИК МАТЕРИАЛОВ
СТУДЕНЧЕСКОЙ НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ

(г. Минск, 27 мая 2022 г.)

Минск
Международный университет «МИТСО»
2022

УДК 341.1/.8
ББК 67.91
К38

Рекомендовано к опубликованию
Научно-методическим советом
Международного университета «МИТСО»
(протокол от 12.07.2022 № 7)

К38 **Киберугрозы как новый вызов для международного гуманитарного права** [Электронный ресурс] : сб. материалов студ. науч.-практ. конф., Минск, 27 мая 2022 г. / Междунар. ун-т «МИТСО» ; редкол.: О. М. Старовойтов [и др.] ; под общ. ред. О. М. Ленцевич. – Минск : Междунар. ун-т «МИТСО», 2022. – 120 с.

ISBN 978-985-497-397-5.

В настоящий сборник вошли работы студентов и школьников, выполненные в рамках комплекса мероприятий по международно-правовой тематике, проведенных кафедрой международного права Международного университета «МИТСО» в 2022 году при поддержке Белорусского Красного Креста. Это работы победителей конкурсов на лучшее эссе среди студентов вузов и выпускников школ, колледжей, гимназий, а также доклады студентов – участников научно-практической конференции «Киберугрозы как новый вызов для международного гуманитарного права». Предназначен для школьников старших классов, студентов и магистрантов, а также всех интересующихся международно-правовой тематикой.

Материалы публикуются в авторской редакции. Ответственность за достоверность информации, приведенных фактов и сведений несут авторы.

Научное электронное издание

КИБЕРУГРОЗЫ КАК НОВЫЙ ВЫЗОВ ДЛЯ МЕЖДУНАРОДНОГО ГУМАНИТАРНОГО ПРАВА
сборник материалов студенческой научно-практической конференции

Ответственный за выпуск *О. М. Ленцевич*
Подготовка оригинал-макета *Н. И. Рудович*

Минимальные системные требования:
браузеры Internet Explorer (версия не ниже 8),
Google Chrome, Mozilla Firefox (32- и 64-разрядная версия) и др.;
скорость подключения к информ.-коммуникат. сетям 1 Мбит/с;
доп. настройки к браузеру не требуются.

Учреждение образования Федерации профсоюзов Беларуси
«Международный университет «МИТСО».
Ул. Казинца, 21-3, 220099, Минск.
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий от 02.09.2014 № 1/423.

УДК 341. 1/.8
ББК 67.91

ISBN 978-985-497-397-5

СОДЕРЖАНИЕ

1. ПРИМЕНЕНИЕ НОРМ МЕЖДУНАРОДНОГО ГУМАНИТАРНОГО ПРАВА К КИБЕРНЕТИЧЕСКИМ СРЕДСТВАМ И МЕТОДАМ ВЕДЕНИЯ ВОЙНЫ

ИНФОРМАЦИОННАЯ ВОЙНА: НОВЫЙ ОБЛИК ВОЙНЫ

INFORMATIONAL WARFARE: THE NEW FACE OF THE WAR

Богуславская А. Р.
г. Минск,
Международный университет «МИТСО»,
студентка юридического факультета

Научный руководитель
Вежновец В. Н.
г. Минск,
Международный университет «МИТСО»,
профессор кафедры международного права,
кандидат юридических наук, доцент

Аннотация: В данной статье рассматриваются ключевые проблемы развития цифровых технологий и их дальнейшего использования для дестабилизации правопорядка и экономической состоятельности государств, для разжигания ненависти и провокации гражданских войн, а также проблемы регулирования информационной войны на современном этапе развития международно-правовых норм.

Ключевые слова: технологии, война, информационная война, дезинформация, информационное пространство, гибридная война.

Annotation: This article examines the key problems of the development of digital technologies and their further use to destabilize the rule of law and the economic viability of states, to incite hatred and provoke civil wars, as well as the problems of regulating information warfare in the modern development of international legal norms.

Keywords: technologies, warfare, informational warfare, disinformation, cyberspace, hybrid warfare.

Кто владеет информацией, тот владеет миром
Н. Ротшильд

В эпоху стремительного развития цифровых технологий информация – это не только знания и финансовое благополучие, но и опасное оружие в руках заинтересованных сторон, способное дестабилизировать внутригосударственный правопорядок, а также создать, как минимум, напряженную обстановку в отдельном регионе или мировом социуме в целом.

Дело в том, что «горячая» война обходится очень дорого, а гибридные методы воздействия являются отличной альтернативой, так как они достаточно

эффективны и не приводят к человеческим жертвам со стороны агрессора. Повсеместное неконтролируемое распространение «фейков» через Интернет, контролируемое извне, позволяет проникать практически в каждый дом. Между гражданами государств – жертвами информационной атаки создается атмосфера конфликта и безысходности, происходит активное манипулирование общественным мнением. Иная проблема происходит в тех случаях, когда Средствам массовой информации (далее – СМИ) удается дестабилизировать правопорядок, породить протестные действия со стороны населения, к экономическому спаду, к грубейшим нарушениям прав человека, таким как: право на достойный уровень жизни, образования, здравоохранения, культурные и иные права.

Следует отметить, что сам факт нарушения государством своих международных обязательств, закрепленных в Уставе ООН, и обязательств в области защиты прав человека путем использования пропаганды для нарушения стабильности политического режима другого государства или манипулирование мнением общественности будет расцениваться как нарушение обязательств, независимо от происхождения или характера этих нарушений [1]. Так, например, Устав ООН в статье 2 закрепляет принципы суверенного равенства всех членов Организации и воздержания от угрозы силой или ее применения против политической независимости, к наличию которой в информационной сфере будет прямо отсылать Таллинский Мануал и Проект статей об ответственности государств за международно-противоправные деяния [2; 3]. В свою очередь, ст. 19 и 20 Международного пакта о гражданских и политических правах, а также ст. 10 и 17 Европейской Конвенции по правам человека, закрепляют право человека на личное мнение и возможность беспрепятственно его придерживаться, а также запрет на пропаганду войны и ненависти в любом ее проявлении [4; 5]. Нарушение любого из этих принципов будет буквально расцениваться как нарушение государством своих международных обязательств перед международным сообществом и любой вовлеченной личностью.

В свою очередь, получатели информации становятся жертвами гибридной войны, проводимой с использованием средств массовой коммуникации. В Хельсинкском Заключительном акте 1975 года, который заложил основу Организации по безопасности и сотрудничеству в Европе, государства-участники обязались, среди прочего, поддерживать в отношениях друг с другом «атмосферу доверия и уважения между народами, отвечающую их обязанности воздерживаться от пропаганды агрессивных войн» против другого государства-участника [6], что прямо нарушается пропагандой, которую развивают государства и некоторые СМИ.

К примеру, в контексте Пакта о гражданских и политических правах, цензура ради политической целесообразности не может рассматриваться как демократический инструмент противодействия информационным воинам.

В этой связи следует обратить внимание на вопрос повышения эффективности противодействия современным вызовам и угрозам в информационном пространстве, включая борьбу с фейками и дезинформацией.

По нашему мнению, в мировом сообществе сейчас активно преобладают гибридные методы ведения войны, составной частью которых является

информационная война. Для того, чтобы этому противостоять, рассматривая СНГ как пример, следует по максимуму использовать потенциал интеграционных объединений, в которые входит Республика Беларусь и укрепить сотрудничество в области информационной безопасности, активнее продвигать СНГ, ОДКБ в социальных сетях, с целью действенного реагирования на фейки и информационные вбросы.

Следует отметить, что важным элементом индивидуального сопротивления пропаганде и дезинформации является выход из так называемого «информационного пузыря» или, другими словами, ситуации ограниченного доступа к информации, отличной от той, которая предоставляется алгоритмами, основанными на предыдущей активности пользователя, путем диверсификации источников информации и получения информации, отличной от предложенной с помощью алгоритмов, регулирующих социальные сети.

Каждый шаг развития информационных технологий делает географическое расстояние все менее существенным фактором. Учитывая растущую зависимость экономики и общества каждого государства от всемирной сети, каждому государству стоит пересмотреть спектр стратегических целей, которым на данный момент нужно уделить наибольшее внимание и финансирование на случай возникновения необходимости в обороне.

Помимо этого, международное право в данный момент не имеет четкого закрепления того, как будет трактоваться территория в области информационного пространства. Таллинское руководство по ведению кибервойны вводит определение того, что информационного пространство является неотделимым от понятия обычной суверенной территориальной прерогативы, однако нормы этого руководства не носят никакого обязательного характера для государств и иных субъектов международных отношений [2].

В заключение отметим, что в сфере информационной безопасности существуют пробелы в правовом регулировании на универсальном и локальном уровнях, что дает государствам полное право на практически безнаказанное вмешательство в дела других государств и подрыв их политического строя изнутри. На данном этапе развития международных отношений является большой проблемой привлечение государства к ответственности за действия СМИ и индивидов, распространяющих информацию, способную привести к нарушениям основных прав человека, началу гражданских войн и, в конечном счете, окончательной гибели государств. Такие проблемы необходимо решать на международном уровне путем принятия обязательных норм, которые государства должны будут соблюдать, вводить четкие рамки ответственности за действия в информационном пространстве как своего, так и других государств, и, наконец, разработать документы, которые бы вводили понятия «агрессия», «информационная война» и «нарушение прав человека в информационном пространстве» не отсылочным правом, которое регулирует все эти вопросы на данный момент, а универсальными документами для данной сферы, которые станут новой вехой развития международного мира и его поддержания со стороны всех государств.

Целесообразно также подумать над объединением потенциала аналитических центров государств-членов, к примеру, СНГ и ОДКБ, по формированию

сети данных структур для оказания содействия при подготовке концептуальных документов по актуальным вопросам международной безопасности.

Список цитированных источников

1. Charter of the United Nations [Electronic resource] // United Nations Human Rights. – Mode of access: https://treaties.un.org/doc/publication/ctc/uncharter.pdf. – Date of access: 05.05.2022.

2. Schmitt, M. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd ed.) [Electronic resource] / M. Schmitt // Cambridge. – Mode of access: https://www.cambridge.org/core/books/tallinn-manual-on-the-international-law-applicable-to-cyber-warfare/50C5BFF166A7FED75B4EA643AC677DAE. – Date of access: 03.05.2022.

3. Draft Articles on Responsibility of States for Internationally Wrongful Acts [Electronic resource] // International Law Commission. – Mode of access: https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf. – Date of access: 03.05.2022.

4. International Covenant on Civil and Political Rights [Electronic resource] // United Nations Human Rights. – Mode of access: https://www.ohchr.org/en/instruments-mechanisms/instruments/ international-covenant-civil-and-political-rights. – Date of access: 04.05.2022.

5. Convention for the Protection of Human Rights and Fundamental Freedoms [Electronic resource] // Council of Europe, 1950. – Mode of access: https://www.echr.coe.int/documents/convention_eng.pdf. – Date of access: 07.05.2022.

6. Final Act of Helsinki [Electronic resource] // Conference on Security and Co-operation in Europe (CSCE). – Mode of access: https://www.osce.org/files/f/documents/5/c/39501.pdf. – Date of access: 07.05.2022.

КВАЛИФИКАЦИЯ КИБЕРАТАК В СООТВЕТСТВИИ С НОРМАМИ JUS AD BELLUM И JUS IN BELLO

QUALIFICATION OF CYBER ATTACKS ACCORDING TO JUS AD BELLUM AND JUS IN BELLO REGULATIONS

Боярович В. И.
г. Минск,
Международный университет «МИТСО»,
студентка юридического факультета

Научный руководитель
Милашевская М. М.
г. Минск,
Международный университет «МИТСО»,
преподаватель кафедры международного права,
магистр юридических наук

Аннотация: В работе анализируются правовые основы для квалификации кибератак в соответствии с нормами jus ad bellum и jus in bello. Кроме того, автор дает определение понятиям «киберпространство», «кибероперация», «кибератака» и «кибероружие».

Ключевые слова: киберпространство, кибероперация, кибератака, кибероружие, право на самооборону, вооруженное нападение, применение и угроза применения силы.

Annotation: This scientific work analyzes the legal basis for the qualification of cyberattacks in accordance with the norms of jus ad bellum and jus in bello. In addition, the author defines the concepts of «cyberspace», «cyber operation», «cyberattack» and «cyberweapon».

Keywords: cyberspace, cyberoperation, cyberattack, cyberweapon, right to self-defense, armed attack, use and threat of use of force.

В современных реалиях киберпространство стало таким же возможным театром боевых действий наравне с вооруженными конфликтами в воздушном, морском, сухопутном пространствах. Информационные технологии потенциально могут использоваться для целей, несовместимых с поддержанием международного мира и безопасности, закрепленных в Уставе Организации Объединенных Наций (далее – Устав ООН). Дабы раскрыть тему исследования, необходимо дать определение таким понятиям, как «киберпространство», «кибероперация» и «кибератака». В соответствии с Таллинским руководством 2.0 по международному праву, применимым к кибернетическим войнам (далее – Таллинское руководство 2.0), киберпространство – это среда, созданная на базе физических (кинетических) и нефизических (некинетических) компонентов для хранения, изменения, обмена данными с использованием компьютерных сетей [1, с. 563]. Кибероперация – это использование компьютерных возможностей (кибервозможностей) для достижения целей в киберпространстве или через него [1, с. 563]. Согласно правилу 92, кибератака – это кибероперация, будь то наступательная или оборонительная с использованием компьютерных технологий, которая способна привести к ранениям и гибели людей или нанести ущерб и разрушить объекты инфраструктуры [1, с. 565]. Данные доктринальные дефиниции на текущий момент являются наиболее детальными и подходящими для проводимых исследований в рассматриваемой области в соответствии с нормами международного публичного и гуманитарного права.

Случаи реальной угрозы применения кибератак зафиксированы в различных странах мира. В 2003 году в Ираке был совершен взлом военной компьютерной системы и в последующем незадолго до вторжения иракские военные получили письма на электронную почту Министерства обороны Ирака с предупреждением, что против них готовится вооруженное нападение; в письме было упомянуто, что иракской стороне необходимо подготовить военную технику для обороны. В 2007 году в Эстонии была произведена серия кибератак на правительственные веб-сайты и базы данных, банковские и новостные системы и телерадиоканалы. Подвергнуты опасности городские системы жизнеобеспечения, т. е. критическая информационная инфраструктура. Примером служит использование вируса *Stuxnet* в 2010 году для того, чтобы вывести из строя центрифуги, которые использовались на ядерных объектах Ирана. Сопутствующим ущербом стали повреждения инфраструктуры ряда промышленных предприятий и замедление ядерной программы страны. Исходя из вышеупомянутых практических случаев, возникают следующие вопросы: возможно ли кибератаку квалифицировать в качестве нарушения запрета на применение или угрозы применения силы и имеют ли государства право на самооборону?

В некоторых случаях кибератаки могут являться прямым нарушением ст. 2 (4) Устава ООН [2], следуя из того, что кибератаки – это та «сила», которая может привести к потерям среди населения, нанести ущерб объектам и использоваться против территориальной неприкосновенности и политической независимости любого государства. Основываясь на консультативном заключении Международного Суда ООН о законности применения или угрозы применения ядерного оружия в вооруженных конфликтах, в § 39 указано, что применение ст. 2 и ст. 51 Устава ООН не поставлено в зависимости от конкретного вида оружия [3, с. 176].

Еще в 1961 году Я. Браунли предложил использовать два критерия для того, чтобы разрешать вопрос принадлежности определенного средства к оружию, а именно: способно ли данное устройство (инструмент) уничтожить человеческую жизнь или имущество и ассоциируется ли данное средство с вооруженными силами. Применение двух этих критериев позволило вывести то, что оружие с некинетическими свойствами: бактериологическое, биологическое, химическое может относиться к категории «оружие». Данные критерии также позволяют понять, что различные кибернетические средства возможно квалифицировать, как кибероружие. Таким образом, кибератаки, которые достигают определенного уровня эскалации и влекут соответствующие последствия, могут быть квалифицированы как напрямую нарушающие положения ст. 2 (4) Устава ООН [2].

Когда совершаются кибератаки против государства, естественным образом возникает вопрос о том, как защититься от подобных нападений и применима ли ст. 51 Устава ООН о неотъемлемом праве на индивидуальную и коллективную самооборону [2]. Говоря о киберпространстве проблемным аспектом, является квалификация кибератаки как «вооруженного нападения». Исходя из резолюций 13/73 и 13/68 Совета Безопасности ООН, принятых после террористических актов 11 сентября 2001 года, предоставляется возможным вывести то, что Совет Безопасности квалифицировал данную атаку в качестве вооруженного нападения в контексте ст. 51 Устава ООН [3, с. 170]. Благодаря данным резолюциям было дано определение того, что понятие вооруженности является достаточно широким. В современном мире стоит обращать внимание на те последствия, которые может повлечь использование того или иного средства, дабы беспрепятственно квалифицировать его как оружие. Заслуживает внимание определение, выработанное в Таллинском руководстве 2.0, кибероружие – это оружие, которое может быть а) направлено на конкретный военный объект или б) ограничено по критериям соразмерности, гуманности и необходимости, как того требует право вооруженных конфликтов, следовательно, они могут нанести удары по военным объектам и гражданским лицам, объектам [1, с. 573].

Международный Суд ООН в деле Никарагуа, не дав конкретного определения вооруженному нападению или применению силы, провел различие между этими двумя терминами и разработал концепцию «пробела» с использованием стандарта достаточных «масштабов и последствий», согласно которой только наиболее «жестокое» или «серьезное» применение силы будет рассмотрено как вооруженное нападение [4, с. 181]. Исходя из дела о нефтяных платформах, решение Международного суда ООН позволяет сделать выводы,

что в отдельных случаях одно нападение или серия нескольких кумулятивных нападений может быть растолкована как вооруженные нападения, подпадающие под статью 51 Устава ООН [4, с. 172].

Долгое время специалисты считали, что ст. 51 [2] касается таких субъектов международного права, как государства, дабы одна сторона могла легитимно воспользоваться правом на самооборону в соответствии с Уставом ООН. Вместе с тем вышеизложенные события 11 сентября 2001 г. на основании резолюций Совета Безопасности ООН позволяют сделать вывод о том, что вооруженное нападение может быть инициировано не только государством, но и негосударственными акторами [4, с. 187]. Однако Международный суд ООН настаивает на классической концепции, применимой к праву на коллективную или индивидуальную самооборону, но такие члены суда ООН, как Р. Хиггинс, П. Койманс и Т. Бургенталь указывают на то, что необходима смена правовой парадигмы и ограничительное толкование в современных реалиях не всегда применительно, так как вооруженное нападение, которое было совершено неправительственным актором, может рассматриваться в качестве дающего право на самооборону в исключительных случаях. Именно эти новаторские подходы являются оптимальными и применимыми в киберпространстве.

Квалифицируя киберугрозы в соответствии с нормами *jus ad bellum*, представляется возможным проанализировать применимость норм *jus in bello* в киберпространстве. Исходя из вышеупомянутых доказательственных примеров и детального анализа доктринальных дефиниций, реальной является угроза применения кибероружия в условиях вооруженных конфликтов. В Женевских конвенциях 1949 года и дополнительных протоколах к ним отсутствуют положения, регламентирующие рассматриваемую область. Исключительно ст. 36 Дополнительного протокола I закрепляет, что использование нового вида оружия не запрещено, если оно не противоречит существующим нормам международного права [5]. Однако все действующие нормы международного гуманитарного права (далее – МГП) должны применяться в киберпространстве до тех пор, пока мировое сообщество не придет к консенсусу и не проведет необходимую адаптацию всех международно-правовых актов к современным условиям, дабы обезопасить комбатантов и нонкомбатантов, защитить критическую информационную инфраструктуру и предотвратить дегуманизацию вооруженных конфликтов.

Подводя итоги исследования, необходимо отметить, что в настоящий момент требуется адаптация норм *jus ad bellum* и *jus in bello* к современным реалиям. Главной целью в ответ на современные вызовы является детальный юридический анализ, который создаст понимание в области правомерности тех или иных действий субъектов в киберпространстве, квалифицирует кибератаки как применение и угроза применения силы или как вооруженное нападение, предоставляющее право на самооборону в соответствии с Уставом ООН, регламентирует новые правовые дефиниции, основываясь на положения Таллинского руководства 2.0 и признает, что появилось новое пространство – киберпространство, а использование кибероружия в вооруженных конфликтах – это вопрос и проблема настоящего. Необходимы новые нормы, которые смогли бы предотвратить гуманитарные катастрофы и деятельность Генеральной

Ассамблеи ООН, инициативы Международного Комитета Красного Креста положат начало правовому сотрудничеству государств мира в разрешении новых проблем человечества в киберпространстве.

Список цитированных источников

1. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / M. N. Schmitt [et al.] ; M. N. Schmitt [ed.]. – Cambridge : Cambridge University Press, 2017. – P. 563–576.

2. Устав Организации Объединенных Наций [Электронный ресурс] : [подписан в г. Сан-Франциско 26.06.1945] // КонсультантПлюс. Россия / ЗАО «КонсультантПлюс». – М., 2022.

3. Действующее международное право: документы : в 2 т. / сост. Ю. М. Колосов, Э. С. Кривчикова. – М. : Международные отношения. Юрайт, 2007. – Т. 2. – С. 9–197.

4. Alston, P. Precedent In The World Court / P. Alston, E. Macdonald. – Oxford : Oxford Monographs in International Law, 2008. – 286 p.

5. International Humanitarian Law and Cyber Operations during Armed Conflicts [Electronic resource] // ICRC. – Mode of access: https://www.icrc.org/en/download/file/108983/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf. – Date of access: 12.05.2022.

ОПРЕДЕЛЕНИЕ ПРАВОВОГО СТАТУСА И КЛАССИФИКАЦИИ СУБЪЕКТОВ КИБЕРНЕТИЧЕСКОГО ПРОСТРАНСТВА В МЕЖДУНАРОДНОМ ГУМАНИТАРНОМ ПРАВЕ

DETERMINATION OF THE LEGAL STATUS AND CLASSIFICATION OF SUBJECTS OF CYBERNETIC SPACE IN INTERNATIONAL HUMANITARIAN LAW

Магунь В. Г.
г. Минск,
Международный университет «МИТСО»,
студент юридического факультета

Научный руководитель
Милашевская М. М.
г. Минск,
Международный университет «МИТСО»,
преподаватель кафедры международного права

Аннотация: В работе приведен анализ субъектов кибернетического пространства в дискурсе международного гуманитарного права и сделаны предложения по совершенствованию правового регулирования в данной области.

Ключевые слова: кибернетическое пространство, информационная война, информационный комбатант, информационная инфраструктура, комбатант в информационном пространстве, международное гуманитарное право, информация.

Annotation: The article analyzes the subjects of cybernetic space in the discourse of international humanitarian law and makes proposals for improving law regulation in this area.

Keywords: cybernetic space, information warfare, informational combatant, informational infrastructure, combatant in the informational space, international humanitarian law, information.

Среди всех отраслей международного права международное гуманитарное право имеет наибольшее число нюансов и проблем. Формальное правовое регулирование в данной области сформировалось к концу XIX века. Специфические условия общественных отношений в значительной степени усложняют правовое регулирование институтов, попадающих в условия вооруженного конфликта. В связи с этим препятствием международное гуманитарное право должно анализироваться намного тщательнее, постоянно совершенствоваться. В данный момент, одним из актуальных вопросов в области международного гуманитарного права является проблема кибернетических угроз и проблемы их правового урегулирования. Так, в рамках Международного Комитета Красного Креста в 2021 году прошел круглый стол на тему «Автономные системы вооружений и военное применение искусственного интеллекта», в 2013 году был опубликован журнал «Цифровые технологии и война». Специфическая природа международного гуманитарного права в совокупности с использованием кибернетических технологий представляет собой новую широкую область неурегулированных отношений. Процессы глобализации и всеобъемлющий характер развития кибернетических технологий осложняют регулирование этой области. Основным отличительным критерием новой области общественных отношений является форма и место осуществления деятельности – компьютерный код, цифровые единицы, информационное пространство или виртуальная реальность. Для развития новых областей правового регулирования необходимо сформировать основание. Отправной точкой, на наш взгляд, является определение критериев и особенностей квалификации субъектов кибернетического пространства.

Исследование субъектов кибернетического пространства требует разъяснения других терминов в данной области. Так, например, кибернетическое пространство составляет сферу деятельности, связанную с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающее воздействие на индивидуальное и общественное сознание, информационную инфраструктура и, собственно, информацию [1, с. 199]. Кибернетическое пространство, на наш взгляд, может представлять собой: с одной стороны, виртуальную реальность и информационные потоки, в которых действуют физические лица с определенной целью, с другой стороны, объекты информационной инфраструктуры, которые представляют собой совокупность технических средств и систем формирования, создания, преобразования, передачи, использования и хранения информации [1, с. 198]. В рамках исследования затронут вопрос информационной войны. Например, М. Либики полагает, что это: «…воздействие, направленное на манипулирование, искажения и опровержение информации» [3, с. 32]. В свою очередь, С. П. Расторгуев определяет информационную войну как: «…открытые

и скрытые целенаправленные информационные воздействия информационных систем друг на друга с целью получения определенного выигрыша в материальной сфере» [2, с. 16]. В данном исследовании второе определение информационной войны является более актуальным, так как анализ проводится в дискурсе международного гуманитарного права.

Вопрос определения информационного комбатанта является существенным. Так как определение в качестве действующего участника вооруженного конфликта, либо же действующего как частное лицо против государства, позволяет установить способ применения правовой квалификации совершенных действий. Ведь нанесение ущерба и уничтожение силы противника является задачей вооруженного конфликта для осуществления цели обретения преимущества над противником. Это означает, что в таких обстоятельствах лицо сможет избежать уголовной ответственности за совершенные деяния.

Отсутствие четкой квалификации может вызвать ряд проблем, в частности: возможно ли применение к такому комбатанту мер и способов воздействия, которые определены женевским или гаагским правом: «уничтожение военной силы противника», «взятие в плен». Следует дать такое определение и выявить меры воздействия, применимые к информационному либо кибернетическому комбатанту. Демонстрируется необходимость определения способов и методов ведения войны данными субъектами, так как специфика условий осуществления их деятельности отражает необходимость установления альтернативного либо дополнительного правового регулирования.

Одной из проблем международного гуманитарного права в кибернетическом пространстве является определение театра военных действий и часть объективной стороны условий совершения деяния. В этом аспекте можно выделить следующие понятия: глобальную сеть, базы данных, веб-пространство, которые не имеют видимых границ либо могут подразумевать все объекты кибернетики, распространяясь, таким образом, на все технические средства и живых существ, носящих или передающих информацию. Особенностью цифрового пространства является, в том числе, мгновенная коммуникация, нивелирование критерия расстояния и территориальных условностей. Зону военных действий практически невозможно определить, так как сервера, с которых могут действовать операторы кибернетической атаки, могут находиться в одном государстве, сигнал может перенаправляться через устройства для управления электронным адресом устройства на адрес другого государства, при этом след использования пополняется дополнительным адресом посредника, который осуществлял перенаправление адреса устройства пользователя. В результате к квалификации может привлекаться более чем одно государство. Вместе данные критерии делают невозможной правовую оценку либо квалификацию деяния. Из этого следует, что при квалификации деяний физических лиц в кибернетическом пространстве гражданство лица может стать вторичным признаком, не влияющим на квалификацию и последующую ответственность.

В этом же дискурсе возникает проблема атрибуции и установления ответственности государства. На наш взгляд, данная проблема может быть решена формированием института либо механизма, устанавливающего квалификацию независимых действий физических лиц либо поиска доказательств эффективного контроля и имеющего универсальную юрисдикцию.

Необходимо обозначить детальную характеристику комбатантов в кибернетическом пространстве. Учитывая особенности исследуемой области, к лицам, влияющим на информационные потоки, следует отнести индивидов, ведущих публичную идеологическую активность в информационном пространстве, мотивирующих на совершение определенных действий, формирование определенного повесткой собственной идеологии мнение в отношении противоборствующей стороны, как, например, политический лидер, блогер, радиоведущий, телеведущий. Далее, в данной области можно выделять лиц, действующих в информационных потоках в отношении противоборствующей стороны. Учитывая универсальный характер информационного пространства, нельзя недооценивать действия физических лиц противоборствующих сторон в отношении информационного правопорядка. Например, кибератаки, совершенные частными группами хакеров либо призывы к ненависти, разжигание межнациональной розни. В сущности, становится туманным как разграничение в такой среде комбатантов, так и квалификация соучастия, состава преступления либо определение его в рамки информационной, кибернетической войны. Здесь также сложно установить причастность и четко определить ответственных лиц, однако рациональным решением выглядит возможность применить аналогию права к составу общественного отношения, выражающего ответственность за некорректные публичные высказывания. В частности, заслуживают внимания «боты», автоматические объекты, действующие дистанционно на основе специальной программы, созданной злоумышленником и выполняющие определенные задачи в информационном пространстве под руководством «бота – пастуха», то есть лица, которое осуществляет настройку ботов [4, с. 553]. В данном случае стоит отметить, что боты являются средством ведения информационного противостояния, а непосредственным комбатантом является их оператор.

Вышеуказанные лица действуют в рамках виртуальной реальности и информационных потоков, однако они не осуществляют влияния на информационную инфраструктуру и технические средства. Это означает, что комбатанты в информационном пространстве могут быть разделены на две категории: действующие в отношения общественного сознания и действующие в отношении информационной инфраструктуры. То есть лицо, которое осуществляет кибернетическую атаку в отношении противоборствующей стороны в целях получения военного преимущества, является «комбатантом в информационном пространстве». В свою очередь остальные участники информационных «поточных» войн являются «информационными комбатантами». Нельзя не упомянуть лиц, которые осуществляют нейтральную деятель-

ность, не принадлежат ни к одной из сторон, то есть являются некомбатантами информационного пространства или нейтральными пользователями.

Таким образом, усовершенствование правового регулирования и приведение международного гуманитарного права и областей информационного права в согласованную систему является острой надобностью современных вооруженных конфликтов. Переход практически всех существующих институтов из материальной формы в кибернетическое пространство и дальнейшую тенденцию по развитию этой области ставит невозможным вопрос о единой аналогии права по отношению ко всем возникающим отношениям. Отсутствие правового регулирования ставит под угрозу существование международного мира и безопасности и репутацию международного гуманитарного права, которое не способно своевременно ответить на возникающие вызовы и угрозы. На наш взгляд, в дискурсе международного гуманитарного права в кибернетическом пространстве можно выделить три категории участников: информационных комбатантов, комбатантов информационного пространства и некомбатантов информационного пространства или нейтральных пользователей. В дальнейшем, задача международного гуманитарного права лежит цифровизации права «Женевы», то есть в определении новых категорий, создании единых правовых актов для установления и квалификации действий лиц в кибернетическом пространстве и применения правового регулирования в новых специфических условиях ведения военных действий, а также формированию специальных институций либо механизмов по разрешению проблем и противоречий в различных сферах данной области отношений.

Список цитированных источников

1. Костенко, Н. И. Право международной информационной безопасности (становление, тенденции и проблемы развития) : монография / Н. И. Костенко. – М. : Юрлитинформ, 2019. – 464 с.

2. Расторгуев, С. П. Информационная война / С. П. Расторгуев. – М. : Радио и связь, 1999. – 416 с.

3. Libicki, Martin C. What Is Information Warfare? / Martin C., Libicki. – Washington : Center for Advanced Concepts and Technology Institute for National Strategic Studies, 1995. – 104 p.

4. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / M. N. Schmitt [at al.] M. N. Schmitt [ed.]. – Cambridge : Cambridge University Press, 2017. – 563 p.

ВЛИЯНИЕ КИБЕРАТАК (КИБЕРУГРОЗ) НА НЕОБХОДИМОСТЬ ИЗМЕНЕНИЯ ЖЕНЕВСКИХ КОНВЕНЦИЙ

THE IMPACT OF CYBER ATTACKS (CYBER THREATS) ON THE NEED TO CHANGE THE GENEVA CONVENTIONS

Неброева В. С.
г. Горки,
Белорусская государственная
сельскохозяйственная академия,
студентка факультета бизнеса и права

Научный руководитель
Куницкий И. И.
г. Горки,
Белорусская государственная
сельскохозяйственная академия,
старший преподаватель

Аннотация: В настоящей статье определена основная роль кибератак в жизни общества и как они влияют на общество в целом. Выявлена необходимость изменения Женевских конвенций в связи с киберпреступностью.

Ключевые слова: Женевская конвенция, международное гуманитарное право, мирное урегулирование конфликтов, вооруженные конфликты, кибератаки, киберпреступность.

Annotation: This article defines the main role of cyberattacks in the life of society and how they affect society as a whole. The necessity of changing the Geneva Conventions in connection with cybercrime has been identified.

Keywords: Geneva Convention, international humanitarian low, peaceful ways of conflicts, armed conflicts, cyberattack, cybercrime.

Сейчас в международном публичном праве практически невозможно разграничить нормы, направленные на ограничение методов ведения войны, и нормы, обеспечивающие защиту жертв войны. Такое положение сложилось после того, как из классической области применения права войны исчезло *jus ad bellum* (право на объявление войны), за исключением случаев признания войн правомерными. Эти две стороны – Гаагское право и Женевское право – преследуют одну и ту же цель. В настоящее время международное гуманитарное право можно обозначить как *jus in bello* (право войны), т. е. как регламентирующее поведение воюющих сторон во время вооруженного конфликта, а в более широком смысле и включающее в себя права и обязанности нейтральных сторон [1, с. 236].

Женевские конвенции составляют основу международного гуманитарного права – отрасли международного права, которая регулирует ведение вооруженных конфликтов и стремится ограничить их последствия. Они отстаи-

вают права тех, кто не участвует в военных действиях, военнопленных и других лиц, которые являются жертвами войны (вооруженного конфликта). Также конвенции призывают к предотвращению любых нарушений права. Они содержат в себе в некоторой степени суровые нормы за значительные нарушения.

Основная задача международного права в целом и Женевских конвенций в частности заключается в том, чтобы остановить агрессию в случае возникновения вооруженного конфликта. Женевские конвенции предполагают, что даже такая неуправляемая ситуация, как война, должна иметь свои рамки. Эти рамки прописаны и закреплены в международных соглашениях. Войны приносят с собой не только большую убыль населения. Помимо прочего, это еще и пытки, жестокое обращение, захват заложников, похищения людей, насилие физическое, психологическое и сексуальное. Все эти действия фактически запрещены Женевскими конвенциями и другими договорами международного права.

В 1949 году было принято четыре Женевские конвенции, а также дополнительные протоколы к ним. Первая Женевская конвенция защищает раненых и больных солдат в действующих армиях. В Конвенции 64 статьи, которые предусматривают защиту раненых и больных, а также медицинского и духовного персонала. В двух приложениях к Конвенции содержатся проект соглашения о санитарных зонах и форма удостоверения личности для медицинского и духовного персонала.

Вторая конвенция отстаивает права раненых, больных и лиц, потерпевших кораблекрушение, из состава вооруженных сил на море. Эта Конвенция заменила Гаагскую конвенцию 1907 года о применении принципов Женевской конвенции к морской войне.

Третья конвенция содержит положения об обращении с военнопленными. Эта конвенция заменила Конвенцию о военнопленных 1929 года. В ней 143 статьи, тогда как в Конвенции 1929 года было всего лишь 97.

Четвертая конвенция предоставляет защиту гражданскому населению во время войны. Женевские конвенции, принятые до 1949 года, касались только комбатантов, но не гражданских лиц. События Второй мировой войны показали, сколь катастрофичны последствия того, что не существует конвенции для защиты гражданских лиц во время войны. В Конвенции, принятой в 1949 году, учтен опыт Второй мировой войны. Конвенция состоит из 159 статей. В ней содержится короткий раздел, относящийся к общей защите населения от определенных последствий войны.

Эти четыре Женевские конвенции были объединены под названием «Женевские конвенции о защите жертв войны» и 12 августа 1949 г. приняты конференцией государств, созванной в Женеве по предложению Международного Комитета Красного Креста. К конвенциям приложено 11 рекомендаций конференции. Суммарное число статей четырех Женевских конвенций о защите жертв войны (без учета приложений) – 439 [2, с. 183].

Далее, в 1977 году к Женевским конвенциям о защите жертв войны 1949 года были приняты два Дополнительных протокола: Протокол I – о защите

жертв международных вооруженных конфликтов и Протокол II – о защите жертв вооруженных конфликтов немеждународного характера. Целью этих протоколов являлось внесение целесообразных уточнений и дополнений в нормы Женевских конвенций 1949 года [2, с. 185].

Но кроме положительного эффекта, в указанных международных актах существуют пробелы, которые постепенно восполняются, что позволяет им не терять актуальности в условиях современной войны. На сегодняшний день международными организациями рассматриваются вопросы возможности задержания людей по соображениям безопасности и новые международные нормы в отношении невоенных вооруженных конфликтов, которых становится в мире все больше [3].

Говоря о защите жертв войны, подразумевают обеспечение сторонами конфликта международно-правовой защиты для определенных категорий, то есть предоставление им такого статуса, который гарантировал бы гуманное обращение с ними и исключал насилие, издевательства, глумление над личностью и т. п.

XXI век, как и конец века XX, приносит новые реалии в военных действиях и правовом положении лиц, не участвующих в вооруженном конфликте в свете использования IT-технологий.

Мы сталкиваемся с ситуацией, когда гражданское население оказывается беззащитным перед угрозой террористических и хакерских атак. К тому же в современных военных столкновениях граница между мирным населением и агрессором часто бывает размыта.

Сейчас особое место в жизни общества занимает киберугроза, она представляет из себя незаконное проникновение или угрозу вредоносного проникновения в виртуальное пространство для достижения политических, социальных или иных целей. Киберугроза может воздействовать на информационное пространство компьютера, в котором находятся сведения, хранятся материалы физического или виртуального устройства. Атака, обычно, поражает носитель данных, специально предназначенный для их хранения, обработки и передачи личной информации пользователя. Киберугрозы исходят от хакеров, людей способных взламывать серверы и получать из них информацию незаконным путем [4].

На сегодняшний день кибератаки являются главной угрозой мировой финансовой системе, по своей опасности превосходя даже кредитные риски и риски ликвидности, ставшие причиной мирового финансового кризиса в 2008 году. Риски, за которыми сейчас следят чаще всего – это киберриски. Это то, что очень тщательно контролируется многими правительственными управлениями, включая ФРС и всеми крупными частными предприятиями [5].

Непосредственно в сфере международного гуманитарного права можно привести казус с Международным Комитетом Красного Креста (МККК), который обнаружил в 2022 году кибератаки на серверы МККК, где хранились данные служб Движения Красного Креста и Красного Полумесяца по восстановлению семейных связей. К серверам МККК, на которых размещались

персональные данные более чем 515 000 человек из разных стран мира, был получен несанкционированный доступ. Было установлено, что имела место кибератака с использованием новейших технологий – преступление, в результате которого была нарушена безопасность конфиденциальных данных гуманитарного характера. Хакеры воспользовались уязвимостью, которую не смогли обнаружить системы киберзащиты МККК, и, проникнув в их сеть, маскировались под зарегистрированных пользователей. Обнаружив взлом, МККК немедленно внесли изменения в ряд используемых ими процедур и инструментов [6].

В то же время такие изменения надо внести не только в технические нормы и регламенты, а и в нормы международного гуманитарного права (в частности, в 4-ю Женевскую Конвенцию, расширив рамки ее применения и распространить ее на «информационную войну», которая не всегда действует лишь в военное время).

Международное гуманитарное право может применяться в различных ситуациях, как международного вооруженного конфликта, так и вооруженного конфликта немеждународного характера. Следует отметить, что жертвы войны должны при всех обстоятельствах пользоваться защитой и гуманным обращением без какой бы то ни было дискриминации; лица из состава вооруженных сил воюющих сторон в случае их ранения или болезни пользуются особой защитой.

Анализируя нормы Женевских конвенций и реалии угрозы киберпреступности, которые несут в себе киберугрозы, исходящие от хакеров, являющихся высококвалифицированными специалистами, которые понимают тонкости работы программ ЭВМ и могут нанести неотвратимые последствия, на сегодняшний день, нам следует внести изменения и дополнения в соответствующие нормативные правовые акты – создать новую сферу правового регулирования – защиты информации граждан, организаций, международных межправительственных организаций и государств в киберпространстве.

Список цитированных источников

1. Бровка, Ю. П. Международное право. Особенная часть : учеб. пособие / Ю. П. Бровка [и др.] ; под ред. Ю. П. Бровки, Ю. А. Лепешкова, Л. В. Павловой. – Минск : Амалфея, 2011. – 688 с.

2. Ушаков, Н. А. Международное право : учеб. пособие / Н. А. Ушаков. – М. : Юристъ, 2000. – 304 с.

3. Международно-правовая защита прав человека в вооруженных конфликтах [Электронный ресурс] // United Nations Human Rights. – Режим доступа: https://www.ohchr.org/sites/default/files/Documents/Publications/HR_in_armed_conflict_RU.pdf. – Дата доступа: 08.05.2022.

4. Павлов, А. Страны с наибольшим и наименьшим риском киберпреступности [Электронный ресурс] / А. Павлов // SecurityLab.ru. – Режим доступа: https://www.securitylab.ru/analytics/528719.php. – Дата доступа: 10.05.2022.

5. Кибератаки – угроза номер один мировой финансовой системе [Электронный ресурс] // SecurityLab.ru. – Режим доступа: https://www.securitylab.ru/ news/518771. php. – Дата доступа: 10.05.2022.

6. Кибератака на МККК: наш анализ [Электронный ресурс] // МККК. – Режим доступа: https://www.icrc.org/ru/document/kiberataka-na-mkkk-nash-analiz. – Дата доступа: 12.05.2022.

ПРИМЕНЕНИЕ НОРМ МЕЖДУНАРОДНОГО ГУМАНИТАРНОГО ПРАВА К КИБЕРОПЕРАЦИЯМ ВО ВРЕМЯ ВООРУЖЕННЫХ КОНФЛИКТОВ

APPLICATION OF THE NORMS OF INTERNATIONAL HUMANITARIAN LAW TO CYBER OPERATIONS DURING ARMED CONFLICTS

Пасиницкий А. С.
г. Минск,
Международный университет «МИТСО»,
юридический факультет

Научный руководитель
Горбач Е. Н.
г. Минск,
Международный университет «МИТСО»,
старший преподаватель кафедры
международного права

Аннотация: В работе представлены отдельные аспекты применения норм международного гуманитарного права во время вооруженных конфликтов в киберпространстве, на основании которых был сделан вывод о необходимости разработки и принятия универсального понятийного аппарата, обновления и дополнения правовой базы, что позволит дать однозначный ответ о применении норм международного гуманитарного права к кибероперациям.

Ключевые слова: международное гуманитарное право, государство, киберпространство, нападение, кибероперация.

Annotation: The paper presents some aspects of the application of the norms of international humanitarian law during armed conflicts in cyberspace, on the basis of which it was concluded that it is necessary to develop and adopt a universal conceptual framework, update and supplement the legal framework, which will allow to give an unambiguous answer about the application of the norms of international humanitarian law to cyber operations.

Keywords: international humanitarian law, state, cyberspace, attack, cyber operation.

В современных условиях вопросы обеспечения информационной безопасности приобретают все большую актуальность. Это сопряжено в первую очередь с происходящей масштабной цифровизацией всех отраслей экономики, систем государственного управления и общественного жизнеобеспечения.

Не стала исключением и сфера военной деятельности государств. В настоящее время уровень развития военных информационных технологий позволяет говорить о возможности распространения военных действий на информационное пространство, или как его еще называют, киберпространство.

В связи с этим возрастает необходимость развития многостороннего сотрудничества по вопросам реагирования на современные угрозы и инциденты в киберпространстве, расследования подобных инцидентов и идентификации злоумышленников.

Как верно отмечено Н. Мельцером, киберпространство является «пятой сферой или пятым доменом ведения военных действий» после суши, моря, воздушного и космического пространств [1, с. 24]. Данное утверждение не может быть оспорено по той причине, что в силу уровня развития современных технологий киберпространство, в действительности, является потенциальным «театром» военных действий.

Конфликты в киберпространстве находят свое выражение в кибероперациях, выполнение которых происходит параллельно с осуществлением операций при помощи других средств и методов ведения войны. С одной стороны, кибероперации потенциально могут позволить сторонам в вооруженном конфликте достичь их военных целей, не причиняя вреда гражданским лицам и не нанося физического ущерба гражданской инфраструктуре. С другой стороны, недавние кибероперации, в большинстве своем не связанные с вооруженным конфликтом, показывают, что в настоящее время акторы, обладающие новейшими киберсредствами, способны помешать предоставлению основных услуг гражданскому населению. Посредством кибероперациий воюющие стороны могут проникнуть в систему и собрать, изъять, изменить, зашифровать или уничтожить данные, а также причинить непоправимый ущерб гражданской инфраструктуре и населению.

Нормы международного гуманитарного права, применяемые к кибероперациям во время вооруженного конфликта, ограничивают их таким же образом, как применение любого другого оружия, средств и методов ведения войны – и новых, и старых [2]. В юридической доктрине отсутствует единое понимание киберпространства, поскольку одни считают его новой сферой ведения войны, аналогичной воздуху, земле, морю и космическому пространству; другие же придерживаются мнения, что киберпространство – другой вид сферы ведения войны, поскольку оно создано человеком в отличие от перечисленных выше пространств, созданных природой.

Так, в статье 2 концепции Конвенции об обеспечении международной информационной безопасности, вынесенной Российской Федерацией в 2011 году на рассмотрение в Организацию Объединенных Наций, под информационным пространством понимается сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие, в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию [3, с. 3]. Аналогичное определение также закреплено в Соглашении между

Правительством Российской Федерации и Правительством Республики Беларусь [4]. Также заслуживает внимания определение, разработанное совместной группой российских и американских специалистов, которые отметили, что под киберпространством понимается электронная среда, в которой информация создается, передается, принимается, хранится, обрабатывается и уничтожается [5, с. 8].

С учетом вышеуказанного считаем, что под киберпространством необходимо понимать глобальную электронную среду, образованную физическими и нефизическими компонентами, включая комплекс технических и программных средств, в которой посредством использования компьютерных и мобильных сетей, включая глобальную информационно-коммуникационную сеть «Интернет», осуществляется формирование, передача, прием, хранение, обработка, модификация и уничтожение информации.

Принимая договоры в области международного гуманитарного права, государства стремятся регулировать конфликты в настоящем и в будущем. Государства включают в договоры по международному гуманитарному праву нормы, которые опережают разработку новых средств и методов ведения войны, предполагая, что вышеупомянутые нормы будут применимы и к ним. К примеру, в случае, если международное гуманитарное право применимо к будущим средствам и методам ведения войны, не было бы необходимости определять их законность в соответствии с существующими нормами международного гуманитарного права, как этого требует ст. 36 Дополнительного протокола I к Женевским конвенциям от 12.08.1949, касающихся защиты жертв международных вооруженных конфликтов от 8 июня 1977 г. (далее – Дополнительный протокол I). Этот вывод находит поддержку в Консультативном заключении Международного суда ООН относительно законности угрозы ядерным оружием или его применения, где Суд напомнил, что установленные принципы и нормы международного гуманитарного права, применимые в ситуации вооруженного конфликта, относятся «ко всем формам военных действий и всем видам оружия», включая оружие будущего [6].

Все больше государств и международных организаций подтверждают применимость норм международного гуманитарного права к кибероперациям во время вооруженных конфликтов, и надеются на обсуждение вопроса о том, как именно эти нормы применяются. Государства могут принимать решения о введении ограничений на кибероперации в дополнение к тем, которые можно найти в действующих положениях права, и могут разработать дополнительные нормы, в частности для усиления защиты гражданских лиц и гражданской инфраструктуры от последствий кибероперациий. Любые предполагаемые новые нормы должны взять за основу и укрепить существующую правовую базу, включая международное гуманитарное право. В случаях, не предусмотренных существующими нормами международного гуманитарного права, гражданские лица и комбатанты остаются под защитой так называемой оговорки Мартенса, то есть на них по-прежнему распространяется защита и действие принципов международного права, вытекающих из установившихся обычаев, принципов

гуманности и требований общественного сознания. Важно подчеркнуть, что подтверждение применимости норм международного гуманитарного права к кибероперациям во время вооруженного конфликта не легитимизирует кибервойну и не содействует милитаризации киберпространства. На самом деле, нормы международного гуманитарного права налагают некоторые ограничения на милитаризацию киберпространства, запрещая разрабатывать киберсредства военного назначения, которые нарушили бы нормы международного гуманитарного права [7, с. 313].

Согласно п. 1 ст. 49 Дополнительного Протокола I: «Нападения – это акты насилия в отношении противника, независимо от того, совершаются они при наступлении или при обороне и от того, на какой территории они совершаются» [8]. Толкование содержания понятия «вооруженное нападение» нашло свое отражение в пункте «g» ст. 3 решения Международного Суда ООН по делу Никарагуа против США 1986 года, где было установлено, что в вооруженное нападение, должна включаться не только акция регулярных вооруженных сил, осуществляемая через международную границу, но также «засылка государством или от имени государства вооруженных банд, групп, иррегулярных вооруженных формирований или наемников, которые осуществляют против другого государства вооруженные силовые действия, носящие столь значительный характер, что позволяет квалифицировать их как (помимо прочего) фактическое вооруженное нападение, осуществляемое регулярными вооруженными силами, «или его значительное участие в них» [9].

Следует отметить, что понятие «нападение» в соответствии с нормами международного гуманитарного права, определение которого дается согласно ст. 49 Дополнительного Протокола I, отличается от понятия «вооруженное нападение» по смыслу ст. 51 Устава ООН (являющаяся частью *jus ad bellum*), и его не следует путать с последним. Подтверждение того, что конкретная кибероперация или тип кибероперации представляет собой нападение согласно нормам международного гуманитарного права, не всегда означает, что эта кибероперация будет считаться вооруженным нападением в соответствии с Уставом ООН.

Если толковать понятие «нападение» как относящееся только к операциям, приводящим к гибели, ранениям и физическому ущербу, то кибероперация, которая направлена на нарушение работы электросети, банковской системы или системы связи, может не подпадать под действие основных норм международного гуманитарного права по защите гражданского населения и гражданских объектов. Поэтому вопрос о том, насколько широко или узко толкуется понятие «нападение» применительно к кибероперациям, представляется крайне важным в плане применимости этих норм и в плане защиты, которую они предоставляют гражданскому населению и гражданской инфраструктуре. Широко признается, что кибероперации, которые, как ожидается, приведут к гибели, ранениям или физическому ущербу, согласно нормам международного гуманитарного права, представляют собой нападения. В ноябре 2019 года в докладе Рабочей группы открытого состава по вопросу

о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности и группы правительственных экспертов по вопросу о поощрении ответственного поведения государств в киберпространстве в контексте международной безопасности указано, что сюда относятся и кибероперации, которые причиняют вред своими прогнозируемыми прямыми и «непрямыми» (косвенными) последствиями: например, когда пациенты, находящиеся в реанимационном отделении больницы, умирают, потому что больница осталась без электричества в результате кибератаки на электроэнергетическую систему [10]. Нападения, которые серьезно подрывают оказание основных услуг, не обязательно причиняя при этом физический ущерб, представляют собой одну из самых серьезных опасностей для гражданских лиц. Мнения расходятся, однако, относительно того, считать ли кибероперацию, приводящую к потере функциональности без причинения физического ущерба, нападением по определению международного гуманитарного права. Из этого следует, что появляется потенциальная возможность для обхода норм международного гуманитарного права. Такое чрезмерно ограничительное понимание понятия «нападение» с трудом согласуется с объектом и целью норм международного гуманитарного права, касающихся ведения военных действий. Поэтому чтобы обеспечить адекватную защиту гражданского населения от последствий кибероперaций, крайне важно, чтобы государства пришли к общему пониманию понятия «нападение».

Таким образом, сфера информационных технологий нуждается в однообразном правовом регулировании на международном уровне. На данном этапе развития информационных технологий, а также их использования для ведения военных действий государства по-разному толкуют, что включает в себя киберпространство, остаются вопросы с употреблением понятия «нападение» и т. д. Это разнообразие понятий и норм препятствует глобальному сотрудничеству, поскольку не единообразное понимание основных определений с исследуемой сфере обеспечивает неоднородные стандарты для того, чтобы деяние квалифицировалось как кибероперация. Чтобы преодолеть это препятствие в глобальной совместной стратегии кибербезопасности, необходимо предпринять следующие шаги:

– государства должны разработать и принять универсальный понятийный аппарат. Это гарантирует, что стандарты будут одинаковыми во внутреннем законодательстве каждой страны, присоединившейся к такому стандарту;

– государства должны определить, как следует толковать и применять нормы международного гуманитарного права в киберпространстве, поскольку государства, решающие разрабатывать или приобретать киберинструменты, должны использовать подобные инструменты в соответствии с нормами международного гуманитарного права;

– каждое государство должно определить международную совместную структуру кибербезопасности в качестве приоритетной области своей внешней политики;

– необходимо также приложить усилия для разработки универсально обязательного и практически осуществимого международного документа о применении киберинструментов во время вооруженных конфликтов.

Разрабатывая новые нормы для защиты гражданских лиц от последствий кибероперациий или с другими целями, необходимо взять за основу и укрепить существующую правовую базу, включая нормы международного гуманитарного права, обновить ее с учетом современных реалий и изменений. Поставить на повестку дня вопрос об обновлении и дополнении положений Женевских конвенций, их протоколов.

Список цитированных источников

1. Мельцер, Н. Непосредственное участие в военных действиях. Руководство по толкованию понятия в свете международного гуманитарного права / Н. Мельцер. – М. : МККК, 2017. – 74 с.

2. Международное гуманитарное право и вызовы современных вооруженных конфликтов [Электронный ресурс] : доклад 32-й Междунар. конф. Красного Креста и Красного Полумесяца, Женева, 8–10 дек. 2015 г. // МККК. – Режим доступа: https://www.icrc.org/ru/download/file/20891/mezhdunarodnoe_gumanitarnoe_pravo_i_vyzovy_sovremennyh_konfliktov.pdf. – Дата доступа: 24.04.2022.

3. Конвенция об обеспечении международной информационной безопасности (концепция) от 22.09.2011. – М. : МИД РФ, 2011. – 17 с.

4. Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности [Электронный ресурс] : [заключено 25 дек. 2013 г.] // ЭТАЛОН. Законодательство Респ. Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

5. Rauscher, K. F. The Russia – U. S. bilateral on cybersecurity: Critical terminology foundations / K. F. Rauscher, V. Yaschenko. – M. : MSU, 2011. – 48 p.

6. Консультативное заключение относительно законности угрозы ядерным оружием или его применения [Электронный ресурс] : заключение Междунар. Суда ООН, 8 июля 1996 г., № 95 // Adobe Acrobat. – Режим доступа: https:// international-review.icrc.org/sites/ default/files/reviews-pdf/2020-10/188.pdf. – Дата доступа: 24.04.2022.

7. Хенкертс, Ж-М. Обычное международное гуманитарное право / Ж-М. Хенкертс, Л. Досвальд-Бек. – М. : МККК, 2006. – Т. 1. – 874 с.

8. Дополнительный протокол I к Женевским конвенциям от 12.08.1949, касающимся защиты жертв международных вооруженных конфликтов, от 8 июня 1977 г. [Электронный ресурс] : [принят в г. Женеве 08.06.1977] // ООН. – Режим доступа: https://www.un.org/ru/humanitarian/law/geneva.shtml. – Дата доступа: 21.02.2014.

9. О военной и военизированной деятельности в Никарагуа и против Никарагуа [Электронный ресурс] : решение Междунар. Суда ООН, 27 июня 1986 г. – Режим доступа: https://legal.un.org/icjsummaries/documents/russian/st_leg_serf1. pdf. – Дата доступа: 25.04.2022.

10. Международное гуманитарное право и кибероперации во время вооруженных конфликтов : позиция Междунар. комитета Красного Креста, 2019 г. – Режим доступа: https://icrc_ihl_and_cyber_operations_during_armed_conflict_ru.pdf. – Дата доступа: 25.04.2022.

МЕЖДУНАРОДНО-ПРАВОВОЙ СТАТУС ВОЕННОПЛЕННЫХ

INTERNATIONAL LEGAL STATUS OF PRISONERS OF WAR

Стасевич П. В.
г. Минск,
Белорусский государственный
экономический университет,
студентка факультета права

Научный руководитель
Мазаник Е. Н.
г. Минск,
Белорусский государственный
экономический университет,
доцент кафедры международного
экономического права,
кандидат юридических наук, доцент

Аннотация: В работе исследуется международно-правовой статус военнопленных. Выявлены проблемы в международно-правовом регулировании относительно контроля за выполнением международных обязательств по соблюдению норм международного гуманитарного права государствами, содержащими военнопленных.

Ключевые слова: военнопленные, вооруженные конфликты, международное гуманитарное право, комбатант, гражданское население.

Annotation: The paper examines the international legal status of prisoners of war. The problems in the international legal regulation regarding the control over the implementation of international obligations to comply with the norms of international humanitarian law by States holding prisoners of war have been identified.

Keywords: prisoners of war, armed conflicts, international humanitarian law, combatant, civilian population.

К сожалению, сегодня тема вооруженных конфликтов не утратила своей актуальности. Несмотря на закрепление общепризнанных принципов международного права в Уставе Организации Объединенных Наций, принятом 26 июня 1945 г. в Сан-Франциско, до сих пор противоречия между государствами, а также нациями нередко разрешаются с применением военной силы.

В международном праве в зависимости от активности и характера действий сторон вооруженные конфликты представлены в трех основных ситуациях:

1) объявленная война;

2) применение силы агрессором, пользующимся подавляющим превосходством;

3) «вмешательство по приглашению» [1, с. 49].

В международном праве сложился принцип, в соответствии с которым все население государства делится на гражданское население и на участников вооруженных конфликтов. Гражданское население находится под охраной

международно-правовых норм, специально предназначенных для его защиты, в частности гражданские лица ни при каких обстоятельствах не могут быть объектом нападения, не могут быть захвачены противником, на них не может распространяться режим военного плена [1, с. 49].

Участники вооруженных конфликтов с учетом их степени участия в боевых действиях и характера выполняемых задач, делятся на две группы: 1) комбатанты, – те, кто сражается; 2) некомбатанты, – те, кто не сражается.

Комбатант – любое лицо (мужчина, женщина), входящее в состав вооруженных сил и имеющее право принимать непосредственно участие в военных действиях [2, с. 384]. К комбатантам относятся: личный состав регулярных вооруженных сил (кроме медицинского и духовного персонала); ополчение; добровольческие отряды, которые как входят, так и не входят в состав вооруженных сил. Личный состав организованных движений сопротивления и партизаны, члены экипажей торговых судов и самолетов, которые непосредственно участвуют в военных действиях, население, которое при приближении противника взялось за оружие – относятся к числу комбатантов, которые не входят в регулярный состав вооруженных сил.

К основным обязанностям комбатантов, закрепленным в международном праве, относятся:

1) отличать себя от гражданского населения, во время участия в военных действиях или при подготовке к ним в целях усиления защиты гражданского населения;

2) при проведении военных операций соблюдать равновесие между требованиями гуманности и военной необходимости.

Статус некомбатантов устанавливается для лиц, которые входят в состав вооруженных сил воюющих сторон или которые следуют за вооруженными силами, правомерно оказывают войскам всестороннюю помощь в выполнении поставленных боевых задач. Некомбатанты не имеют права принимать непосредственное участие в боевых действиях, имеющееся у них личное оружие может быть применено только в целях самообороны, а при попадании во власть противника, на них распространяется режим военного плена. В случае участия в боевых действиях они становятся комбатантами.

Таким образом, все участники вооруженного конфликта (комбатанты и некомбатанты), попадая во власть неприятеля, становятся военнопленными.

Военнопленные – все законные участники международных вооруженных конфликтов с момента, когда они попадут во власть неприятеля, и вплоть до их окончательного освобождения и репатриации:

1) комбатант противника – мужчина или женщина, которые попадают во власть со стороны противника в международном вооруженном конфликте (были захвачены или сдались в плен);

2) гражданские лица, которые следуют за вооруженными силами противника, например, военные корреспонденты, поставщики или личный состав рабочих команд, или служб, на которые возложено бытовое обслуживание вооруженных сил (последние должны иметь разрешение от воору-

женных сил, для подтверждения которого им выдается удостоверение личности) [2, с. 387]. Также, понятие «военнопленного» раскрывается через положения ст. 4 III Женевской конвенции «Об обращении с военнопленными» (Женева, 12.08.1949) (далее – Конвенция).

Статья 12 III Женевской конвенции устанавливает, что военнопленные находятся во власти неприятельской державы, но не отдельных лиц или воинских частей, взявших их в плен. Независимо от ответственности, которая может пасть на отдельных лиц, держащая в плену держава несет ответственность за обращение с военнопленными.

В соответствии со ст. 13 Конвенции, с военнопленными должны всегда обращаться гуманно, данный принцип является основополагающим в международно-правовом статусе военнопленных. Для получения каких-либо сведений к военнопленным не должны применяться пытки и различные меры принуждения со стороны государств, держащих их в плену (ст. 17 Конвенции). Ст. 13 содержит запрет на проведение различного вида опытов над военнопленными.

Международное гуманитарное право закрепляет запрет на осуществление дискриминации военнопленных по признакам расы, национальности, вероисповедания, политических убеждений. К женщинам оно предписывает относиться со всем полагающимся их полу уважением.

Женевской конвенцией предусмотрено наложение дисциплинарных взысканий во время вооруженных конфликтов. В период нахождения в плену государства-неприятеля должны уважать честь и достоинство женщин-военнопленных. Дисциплинарные взыскания, наложенные но военнопленных, не должны быть суровыми и опасными для жизни и здоровья военнопленных. Женщины-военнопленные не должны подвергаться жестокому обращению, когда отбывают дисциплинарное наказание. В этот период женщины-военнопленные должны находиться под надзором женского персонала и содержаться в помещениях отдельно от мужчин [3, с. 82].

В соответствии с Конвенцией, места, в которых военнопленные отбывают дисциплинарные наказания, должны отвечать требованиям гигиены. Наказанные пленные должны содержаться в чистоте. Каждый день они должны иметь возможность заниматься физическими упражнениями и гулять на воздухе не менее двух часов. Также одним из требований международного гуманитарного права является содержание военнопленных отдельно от осужденных. При отбытии дисциплинарных наказаний военнопленные не должны помещаться в тюрьмы, исправительные учреждения и т. д.

Часть III Конвенции закрепляет нормы, регулирующие работу военнопленных. Так, военнопленные могут привлекаться к работе, данный вопрос регламентируется международном гуманитарным правом. Они не привлекаются к работам, которые связаны с военной необходимостью и носят военный характер. Их рабочий день не превышает продолжительность рабочего дня мирного населения государства-неприятеля. Военнопленные обеспечиваются одеждой в соответствии с сезоном и рабочей одеждой, также им предоставляется во время рабочего дня час для отдыха и приема пищи. Также они получают заработную плату на свои нужды.

В соответствии с положениями ст. 26 Конвенции, находясь в плену, военнопленные имеют право на питание, которое должно быть достаточным для того, чтобы военнопленные не теряли в весе. Международно-правовой статус военнопленного затрагивает и такой аспект, как вероисповедание, который регулируют ст. 36, 37 Конвенции.

Неотъемлемым элементом международно-правового статуса военнопленного является право на медицинскую помощь. Так, данное право регулируется положениями Главы III Конвенции – Гигиена и медицинская помощь. На неприятельское государство ложится ответственность по обеспечению оказания медицинской помощи военнопленным. В ситуации наступления смерти военнопленного составляется заключение о его смерти. В заключении указывается причина смерти. Военнопленные должны быть погребены; это должна быть или индивидуальная могила или, если смертность массовая, – общая. Военнопленный должен быть захоронен таким образом, чтобы в дальнейшем родственники и близкие могли найти и посетить могилу [4, с. 67].

Проанализировав международно-правовой статус военнопленных, можно сделать следующие выводы. В Конвенции закреплены базовые элементы международно-правового статуса военнопленного, выработанные международным сообществом с учетом режима военного плена. В настоящее время остается открытым вопрос о добросовестном соблюдении воюющими сторонами рассмотренных выше положений Конвенции. Отсутствие механизма контроля за исполнением государствами, находящимися в военном конфликте, норм международного гуманитарного права, увеличивает возможность ухудшения содержания военнопленных в плену.

Представляется, что указанный механизм может быть разработан с учетом современных достижений науки и техники, к примеру, видеонаблюдение без нарушения личных прав военнопленных, с последующим предоставлением материалов, при необходимости, специально организованным для контроля органам в рамках международных организаций.

Несмотря на то, что Конвенцией охвачены различные аспекты международно-правового статуса военнопленных, в настоящее время необходимо учитывать влияние развития информационных технологий на его изменение. С учетом тех обстоятельств, что появились такие понятия, как «цифровые права», «цифровые услуги» и общей тенденции к цифровизации общественных отношений, представляется возможным полагать, что закрепление в Конвенции возможности использования цифровых средств связи для реализации отдельных прав военнопленных, привлечения к ранее не существующим видам работ, позволит усовершенствовать нормы, регулирующие права, обязанности и меры дисциплинарной ответственности военнопленных.

Список цитированных источников

1. Кремнев, П. П. Участники международных вооруженных конфликтов: еще раз о правовом статусе / П. П. Кремнев // Журнал Уральского гос. юрид. ун-та, Рос. юрид. журнал. – 2016. – № 5 (110). – С. 48–60.

2. Международное публичное право : учеб. пособие / Л. А. Васильева, О. А. Бакиновская. – Минск : ТетраСиситемс, 2010. – 576 с.

3. Бибарсова, Г. Ш. Особенности международно-правового статуса женщин-комбатантов / Г. Ш. Бибарсова // Организационно-правовое регулирование безопасности жизнедеятельности в современном мире : сб. материалов Междунар. науч.-практ. конф., Санкт-Петербург, 18–20 мая 2016 г. – СПб., 2016. – С. 80–82.

4. Гуторова, А. Н. Международно-правовое регулирование статуса военнопленных / А. Н. Гуторова // Права человека: история, теория, практика : сб. науч. ст. V Всерос. науч.-практ. конф., Курск, 4 нояб. 2016 г. – Курск, 2016. – С. 64–68.

ПРОБЛЕМА МЕЖДУНАРОДНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ ДЕЯТЕЛЬНОСТИ СМИ В ПЕРИОД ВООРУЖЕННЫХ КОНФЛИКТОВ

THE PROBLEM OF INTERNATIONAL LEGAL REGULATION OF MEDIA ACTIVITIES DURING ARMED CONFLICTS

Толстик М. А.
г. Минск,
Белорусский государственный
экономический университет,
студентка факультета права

Научный руководитель
Пехота Т. М.
г. Минск,
Белорусский государственный
экономический университет,
ассистент кафедры теории и истории права

Аннотация: В данной работе проанализирована проблема регулирования деятельности СМИ как инструмента воздействия на общественное сознание в период вооруженных конфликтов, а также приведен перечень мер рекомендательного характера для решения данной проблемы.

Ключевые слова: средства массовой информации, «четвертая ветвь власти», информационный ресурс, свобода получения информации, вооруженный конфликт, международное гуманитарное право.

Annotation: This paper analyzes the problem of regulating the activities of the media as a tool to influence public consciousness during armed conflicts, and also provides a list of recommendatory measures to solve this problem.

Keywords: mass media, «fourth branch of power», information resource, freedom of information, armed conflict, international humanitarian law.

Достижения науки и техники в информационной сфере кардинально изменили жизнь общества. Средства массовой информации (далее – СМИ) стали

основными источниками ее получения и оказывают значительное влияние на формирование общественного мнения. Это зависит от многих факторов: как подается информация, на какую целевую аудиторию она рассчитана, какие ресурсы при этом используются и др. В соответствии с п. 20 ст. 1 Закона Республики Беларусь «О средствах массовой информации», средство массовой информации – форма периодического распространения массовой информации с использованием печати, вещания теле- или радиопрограммы, глобальной компьютерной сети Интернет, а также сетевое издание как форма распространения массовой информации с использованием глобальной компьютерной сети Интернет [1]. Отметим, что на сегодняшний день наиболее распространенным источником получения информация является интернет, доступ к которому есть почти у каждого. Также отметим, что интернет имеет ряд преимуществ по сравнению с иными информационными ресурсами, и это увеличивает его востребованность, особенно среди более молодого поколения. В то же время, пожилые люди, профессиональная и иная деятельность которых не связана с использованием интернета, отдают предпочтение телевидению.

Значение СМИ в жизни общества и государства довольно велико. Многие ученые придерживаются мнения, что СМИ – это четвертая ветвь власти. Такая позиция кажется нам неоднозначной, поскольку одним из отличительных признаков какой-либо власти является наличие механизма открытого принуждения к совершению либо воздержанию от совершения определенных действий. СМИ в своей деятельности придерживаются принципа многообразия мнений, суть которого заключается в том, что различные мнения и взгляды должны свободно распространяться, и масс-медиа должны этому активно способствовать. Этот принцип, а также право на свободу слова и свободу получения информации в той или иной степени закрепляются во многих международно-правовых актах: Заключительном акте Совещания по безопасности и сотрудничеству в Европе (СБСЕ), подписанном 1 августа 1975 г. в Хельсинки; Международном пакте о гражданских и политических правах от 19 декабря 1966 г.; Конвенции о защите прав человека и основных свобод от 4 ноября 1950 г. и т. д. Но в международном праве отсутствуют документы, которые бы регулировали исключительно права и обязанности в сфере СМИ. Обратимся к Конвенции о защите прав человека и основных свобод, которая была подписана в Риме 4 ноября 1950 г. странами-участниками Совета Европы. Пункт 1 ст. 10 настоящей Конвенции гласит, что «каждый имеет право свободно выражать свое мнение». Далее, в этом же пункте, говорится о том, что государства могут «осуществлять лицензирование радиовещательных, телевизионных или кинематографических предприятий». В п. 2 настоящей статьи также упоминаются санкции, которые могут применяться в соответствии с национальными интересами и общественным порядком в государстве [2]. Таким образом, конвенция определяет лишь наиболее общее право человека, а механизм его правового регулирования каждое государство может установить самостоятельно.

Таким образом, деятельность СМИ эффективно урегулирована в рамках национального законодательства, но на международном уровне правовое положение участников этой сферы общественных отношений недостаточно определено и нуждается в конкретизации и издании специализированных актуальных документов.

Одна из самых важных функций СМИ, на наш взгляд, – это оказание определенного влияния на общественное мнение. В период вооруженных конфликтов психологическое воздействие на общество может привести к всевозможным последствиям, поэтому необходимо обратить особенное внимание на то, кто может нести в массы определенную информацию и какие цели он при этом преследует. Масс-медиа могут выступать в качестве миротворцев в определенном конфликте или, наоборот, спровоцировать агрессию. Поэтому важно, чтобы журналисты подавали объективную информацию, которая бы не была подвержена влиянию внешних факторов (известны случаи, когда СМИ становятся инструментом манипуляции общественным сознанием). Как было отмечено ранее, вооруженный конфликт – это серьезная проблема, отношение к которой у людей формируется в зависимости от того, как и какую информацию им преподносят. Можно выделить несколько принципов, на которых должна основываться деятельность СМИ в период вооруженных конфликтов:

1) своевременное предоставление актуальной информации;

2) объективная оценка происходящего, привлечение независимых экспертов;

3) учет целевой аудитории [3].

Таким образом, информация не должна искажаться, доводить ее до сведения людей необходимо вовремя и в соответствии с тем, для кого она предназначена.

Нам кажется рациональным урегулировать некоторые аспекты деятельности СМИ в рамках международного гуманитарного права.

Во-первых, они должны занимать нейтральную позицию, повлиять на которую невозможно ни со стороны государства, ни со стороны общественности. За попытку убедить или принудить какой-либо информационный ресурс сфальсифицировать информацию о вооруженном конфликте, в том числе фото- и видеоматериалы, должна быть установлена ответственность.

Во-вторых, деятельность масс-медиа в случае намеренной публикации недостоверной информации также должна быть урегулирована путем наложения санкций как на сам информационный ресурс, так и на лиц, ответственных за дезинформацию.

В-третьих, любая информация должна подтверждаться ссылками на какие-либо достоверные источники: должностных лиц и (или) их представителей, очевидцев, участников военных действий. Но в данном случае нельзя забывать об объективности информации, ответственность за которую также возлагается на журналиста.

Список цитированных источников

1. О средствах массовой информации [Электронный ресурс] : Закон Респ. Беларусь от 17 июля 2008 г. № 427-З : принят Палатой представителей 24 июня 2008 г. : одобр. Советом респ. 28 июня 2008 г. : в ред. Закона Респ. Беларусь от 24 мая 2021 г. ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

2. Европейская конвенция по правам человека [Электронный ресурс] // United Nations Human Rights. – Режим доступа: https://www.echr.coe.int/Documents/Convention_RUS.pdf. – Дата доступа: 03.05.2022.

3. Медовкина, Л. Ю. Влияние средств массовой информации на проведение вооруженных конфликтов [Электронный ресурс] / Л. Ю. Медовкина. // Научные ведомости. – 2009. – № 22. – Режим доступа: https://cyberleninka.ru/article/n/vliyanie-sredstv-massovoy-informatsii-na-provedenie-vooruzhennyh-konfliktov/viewer. – Дата доступа: 03.05.2022.

К ВОПРОСУ О ЗАЩИТЕ ГРАЖДАНСКОЙ ИНФРАСТРУКТУРЫ И ГРАЖДАНСКИХ ДАННЫХ В КИБЕРПРОСТРАНСТВЕ

ON THE PROTECTION OF CIVIL INFRASTRUCTURE AND CIVIL DATA IN CYBERSPACE

Чайкина А. В.
г. Минск,
Международный университет «МИТСО»,
студент юридического факультета

Сидьков Н. А.
г. Минск,
Международный университет «МИТСО»,
студент юридического факультета

Научный руководитель
Горбач Е. Н.
г. Минск,
Международный университет «МИТСО»,
старший преподаватель кафедры международного права

Аннотация: В работе представлены отдельные аспекты применения норм международного гуманитарного права в отношении гражданских данных и гражданской инфраструктуры в киберпространстве. В результате проведенного исследования авторы приходят к выводу о необходимости принятия нового международного акта для эффективного регулирования защиты гражданской инфраструктуры и гражданских данных во время вооруженного конфликта.

Ключевые слова: кибербезопасность, международное гуманитарное право, кибероперации, вооруженные конфликты, киберпространство, гражданские данные, Международный Комитет Красного Креста.

Annotation: The paper presents some aspects of the application of international humanitarian law to civil data and civil infrastructure in cyberspace. As a result of the study, the authors conclude that a new international legal instrument is needed to effectively regulate the protection of civil infrastructure and civil data during armed conflict.

Keywords: cybersecurity, international humanitarian law, cyber operations, armed conflicts, cyberspace, civilian data, International Committee of the Red Cross.

Актуальность исследования подтверждается стремительным развитием информационных технологий, которые могут быть использованы в ходе вооруженного конфликта и нанести серьезный вред гражданским объектам и гражданским данным. Использование кибероперaций во время вооруженного конфликта уже стало реальностью. Все больше государств имеют или развивают военный киберпотенциал, что позволяет с высокой долей вероятности предположить, что число таких операций будет расти и в итоге оказывать влияние на гражданское население [1]. Новые технологии вызывают и новые опасности, которые могут быть причиной серьезной обеспокоенности в самых различных областях, в частности, если они используются во время вооруженных конфликтов. Технологии разработки наступательных киберинструментов в настоящее времени вышли на такой уровень, который позволяет серьезно воздействовать на гражданскую инфраструктуру и наносить значительный ущерб гражданскому населению. Нужно отметить, что применение кибероружия до настоящего времени не приводило к катастрофическим гуманитарным последствиям, но это обстоятельство не снимает с повестки дня необходимость изучения и предотвращения подобных сценариев, принимая во внимание глобальный уровень современной инфраструктуры.

Во время работы над Таллинским руководством по международному праву, применимому к кибероперациям, стало очевидно, что эксперты во многом единодушны в отношении того, что международное гуманитарное право применяется в кибернетическом пространстве и что его основные нормы и принципы могут и должны применяться при осуществлении кибероперaций во время вооруженных конфликтов [2, с. 45].

Международный Комитет Красного Креста понимает «кибероперации во время вооруженных конфликтов» как операции против компьютерной системы или сети, или иного подключенного к сети устройства через поток данных, когда такие операции применяются в качестве средства или метода войны в контексте вооруженного конфликта [3, с. 915]. Совершенно очевидно, что, когда кибероперация осуществляется в контексте существующего вооруженного конфликта, ведущегося при помощи кинетических средств ко всем сторонам, применяются нормы международного гуманитарного права.

Военные операции в киберпространстве в состоянии нарушать функционирование важных гражданских инфраструктур. Сектор здравоохранения развивается в сторону все большей цифровизации и взаимосвязанности, что увеличивает его зависимость от цифровых технологий и возможных масштабов поражения в случае нападения. Необходимо отметить, что, часто явление цифровизации здравоохранения не сопровождается улучшением в сфере кибербезопасности [3, с. 912]. Поскольку сектор здравоохранения исключительно важен в любое время, но особенно во время вооруженных конфликтов и кризисов в области охраны здоровья, Международный Комитет Красного Креста призвал все государства уважать и предоставлять защиту медицинским службам и медицинским учреждениям от кибернападений любого рода как в мирное время, так и в ситуации конфликтов, и подтвердить свою приверженность международным нормам, которые запрещают такие действия [4, с. 337].

В свою очередь, чтобы защитить критически важную гражданскую инфраструктуру, которая зависит от киберпространства, важно обеспечить также защиту инфраструктуре самого киберпространства. Однако наблюдается проблема, заключающаяся во взаимосвязанности гражданских и военных сетей. Большинство военных сетей зависят от гражданской киберинфраструктуры, например, подводные оптоволоконные кабели, спутники, роутеры. Управление движением гражданского наземного, морского и воздушного транспорта все чаще использует навигационное оборудование, которое зависит от спутников глобальной навигационной спутниковой системы, таких как ГЛОНАСС, GPS и Galileo, которые могут использоваться и военными [5, с. 163]. Гражданские системы материально-технического снабжения и другие предприятия используют тот же самый Интернет и коммуникационные сети, по которым проходят и некоторые военные линии связи. За исключением отдельных сетей, которые конкретно предназначены для использования военными, практически невозможно провести различие между чисто гражданскими и чисто военными объектами киберинфраструктуры [6].

В соответствии с международным гуманитарным правом, нападения должны быть строго ограничены военными объектами. К военным объектам относятся только те, которые в силу своего характера, расположения, назначения или использования вносят эффективный вклад в военные действия и чье полное или частичное уничтожение, захват или нейтрализация при существующих в конкретный момент обстоятельствах дает явное военное преимущество. Все объекты, которые не являются военными объектами, являются гражданскими объектами в соответствии с международным гуманитарным правом и не могут становиться объектами нападения. В случае сомнения относительно того, не используется ли объект, который обычно используется с гражданскими целями, для внесения эффективного вклада в военные действия, следует предполагать, что этот объект остается под защитой в качестве гражданского объекта [7, с. 418].

Выяснить, когда гражданский объект становится военным объектом невозможно, если речь идет о киберпространстве или Интернете. Вместо этого воюющие стороны должны определить, какие компьютеры, узловые модули, маршрутизаторы или сети могли стать военным объектом. В таком случае необходимо проанализировать такие объекты по отдельности. Используемые средства и методы должны давать возможность направлять нападение на конкретные военные объекты, которые были идентифицированы и следует принять все возможные меры предосторожности, чтобы избежать или минимизировать опасность случайно воздействовать на оставшиеся гражданские объекты или части сети.

По сравнению с кинетическими военными операциями, кибероперации могут, в зависимости от обстоятельств, воздействовать, причиняя меньший ущерб или такой ущерб, который может быть легче возмещен или при котором может быть восстановлена ранее существовавшая ситуация. Это соображение особенно актуально в отношении объектов двойного использования: когда воюющая сторона пытается нейтрализовать командный пункт противника, расположенный в подземном бункере, отключив линию электроснабжения, которая одновременно поставляет энергию в гражданскую инфраструктуру. Кибероперация может позволить оператору удаленно определить, какие части сети отключить. Это могло бы дать возможность нападающей стороне достичь желаемого результата, избежав или по крайней мере минимизировав негативные последствия для энергоснабжения гражданских лиц [6].

Еще одним обсуждаемым вопросом, в контексте применения международного гуманитарного права к кибероперациям является то, пользуются ли гражданские данные такой же защитой, что и гражданские объекты. Международный Комитет Красного Креста относит к гражданским данным следующее – личные медицинские данные, данные органов социального обеспечения, налоговые сведения, банковские счета, файлы клиентов компаний и списки избирателей, которые крайне важны для функционирования большинства систем гражданской жизни [8]. Защита гражданских данных от кибероперациий во время вооруженных конфликтов становится все более важной, поскольку происходит активная цифровизация гражданской инфраструктуры. И, ожидается, что эта тенденция будет развиваться.

Нормы, предоставляющие защиту данным, принадлежащим определенным категориям объектов, пользующихся защитой согласно международному гуманитарному праву, подробно разработаны. Обязательства защищать и уважать медицинские объекты и операции по предоставлению гуманитарной помощи распространяются на медицинские данные и на данные гуманитарных организаций, которые важны для их операций. Аналогично, запрещается уничтожение данных или манипулирование данными, в целях приведения в непригодность объектов, необходимых для выживания гражданского населения, например, сооружения для снабжения питьевой водой [9, с. 264].

Вопрос о том, являются ли данные объектом международного гуманитарного права в операциях, которые не предназначены для того, чтобы причинить смерть или ранения лицу, или ущерб физическому объекту и не ожидается, что они станут их причиной, крайне важен. Выделяют два общих подхода.

В соответствии с первым подходом, данные являются объектом международного гуманитарного права. Считается, что операция, предназначенная для уничтожения данных, или которая собирается подвергнуть их манипулированию, или которая может вызвать такой эффект, будет нападением. Следовательно, она будет регулироваться нормами международного гуманитарного права, так как это будет уничтожение или повреждение объекта. Нормы международного гуманитарного права будут также применяться, если не ожидается, что такое уничтожение или манипулирование приведет к смерти, ранению лица, выведению из строя гражданской инфраструктуры. При этом операция, предназначенная для получения доступа к данным с целью шпионажа, не будет нападением и, следовательно, нормы международного гуманитарного права не применяются [7, с. 372].

Противоположный подход определяет, что операция, предназначенная для уничтожения данных или манипулирования ими, не приводит к смерти, ранению лица или повреждению гражданской инфраструктуры, не будет регулироваться нормами международного гуманитарного права. В соответствии с этим подходом, в защите гражданских данных, на которые не распространяются действия конкретного защитного режима, наблюдается пробел [10, с. 71].

Как подчеркнул Международный Комитет Красного Креста: «исключение важных данных гражданского характера из сферы защиты, предоставляемой международным гуманитарным правом гражданским объектам, привело бы к серьезному пробелу в защите» [3, с. 920].

Обобщая все вышесказанное, следует сделать вывод о том, что для предотвращения катастрофических гуманитарных последствий защита гражданской инфраструктуры и гражданских данных от кибератак должна занимать приоритетные позиции для государств. Однако, на данный момент нет единого мнения о том, как стоит предотвращать кибернападения. Полагаем, что для полноценной защиты от кибератак необходима разработка и принятие государствами единого международного акта, например, конвенции, с дальнейшим ее инкорпорированием в национальное законодательство государств с целью разработки компьютерной программы для превентивной защиты гражданских данных и объектов гражданской инфраструктуры. Это, в большей степени, поспособствует своевременной и эффективной защите, а также предотвратит разрушительные последствия кибератак на гражданскую инфраструктуру и гражданские данные в киберпространстве во время вооруженных конфликтов.

Список цитированных источников

1. Agence Nationale de la Sécurité des Système d'Information: Inform. System Defence and Security [Electronic resource] // ANSSI. – Mode of access: www.ssi.gouv.fr/uploads/IMG/pdf/20110215_Information_system_defence_and_security_France_s_strategy.pdf. – Date of access: 11.05.2022.

2. Schmitt, M. N. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / M. N. Schmitt. – Cambridge : Cambridge University Press & Assessment, 2017. – 265 p.

3. Brantly, A. F. The Cybersecurity of Health / A. F. Brantly // Council on Foreign Relations Blog. – 2020. – Vol. 8, iss. 5 – P. 890–952.

4. Akande, D. Call by Global Leaders: Work Together Now to Stop Cyberattacks on the Healthcare Sector / D. Akande // Humanitarian Law and Policy Blog. – 2020. – Vol. 11, iss. 2 – P. 324–350.

5. Greenberg, A. The Untold Story of NotPetya, the Most Devastating Cyberattack in History / A. Greenberg // Wired. – 2018. – Vol. 19, iss. 3 – P. 157–171.

6. Offensive Cyber and the People Who Do It – speech given to the Lowy Institute [Electronic resource] : Australian Signals Directorate // The Lowy Institute. – Sydney, 2019. – Mode of access: http://www.asd.gov.au/speeches/20190327-lowy-institute-offensive-cyber-operations.html. – Date of access: 11.05.2022.

7. Laurent, G. Twenty years later: international humanitarian law and the protection of civilians from consequences / G. Laurent, T. Rodenheuser, K. Derman // International Journal of the Red Cross. – 2021. – Vol. 913, № 13. – P. 367–427.

8. Дополнительный протокол I о защите жертв международных вооруженных конфликтов к Женевским конвенциям Международного Комитета Красного Креста [Электронный ресурс] : [заключен в г. Женеве 08.06.1977] // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

9. Boothby, W. H. The Law of Targeting / W. H. Boothby. – New York : Oxford : Oxford Univ. Press, 2012. – 384 p.

10. International humanitarian law and challenges of contemporary armed conflicts : report from the 32nd Intern. conf. of the Red Cross and Red Crescent, Geneva, 8–10 Dec. 2015 / Geneva. – Cambridge : Univ. of Cambridge, 2015. – 108 p.

2. АКТУАЛЬНЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КИБЕРПРОСТРАНСТВА В МЕЖДУНАРОДНОМ И НАЦИОНАЛЬНОМ ПРАВЕ

ИНФОРМАЦИОННЫЙ СУВЕРЕНИТЕТ КАК ФАКТОР ПОДДЕРЖАНИЯ ИНФОРМАЦИОННОГО ПОРЯДКА

INFORMATION SOVEREIGNTY: AS A FACTOR OF INFORMATION ORDER MAINTENANCE

Анциферова Э. Ю.
г. Минск,
Академия управления
при Президенте Республики Беларусь,
аспирант кафедры конституционного права

Научный руководитель
Бакун А. С.
г. Минск,
Белорусский государственный университет,
заместитель декана по учебно-воспитательной работе
юридического факультета
Белорусского государственного университета,
кандидат юридических наук, доцент

Аннотация: В работе детализируется и раскрывается содержание понятия «информационный суверенитет» в контексте информационной безопасности, а также выделяются его основные элементы. Делается вывод о том, что реализация информационного суверенитета является предпосылкой для формирования информационной безопасности в стране.
Ключевые слова: информатизация, информационное общество, информация, суверенитет, цифровой суверенитет, информационная безопасность.

Annotation: The article details and reveals the concept of an «information sovereign» expert on information security, as well as highlights its main elements. It is concluded that the implementation of information sovereignty is a prerequisite for the formation of information security in the country.
Keywords: informatization, information society, information, sovereignty, digital sovereignty, information security.

Современные исследования ученого сообщества характеризуются все большим вниманием к основополагающим понятиям, составляющим базовые теоретические категории современного общества. Информационный суверенитет выступает предметом исследования многих ученых, однако до сих пор не выработан единый подход к пониманию данного правового термина и анализу структурных элементов, что порождает проблемы в области понимания данного понятия.

Многие авторы рассматривали информационный суверенитет в контексте информационной безопасности государства. Д. В. Беленков и соавторы под информационным суверенитетом подразумевают «самостоятельность субъекта отношений в информационной сфере в проведении внутренней и внешней информационной политики и способность обеспечить безопасность собственного информационного пространства» [1]. Согласно мнению вышеназванных авторов, для формирования информационного суверенитета создается и реализовывается национальная информационная инфраструктура без определяющего вмешательства каких-либо иных субъектов, действующих за пределами национальной государственности, при включении ее в глобальную информационную среду с учетом интересов экономики, обеспечения информационной безопасности и защиты национального информационного пространства. В свою очередь Н. П. Ромашкина считает, что под информационным суверенитетом следует понимать «способность технологически и законодательно обеспечивать и защищать независимость государства и конституционные права граждан в информационном пространстве от внешних угроз, контролируя при этом происходящее в этом пространстве» [2, с. 16]. Так, перед государством стоит цель по контролю, предотвращению, а также техническому и законодательному обеспечению безопасности личности и государства от угроз, исходящих из международного виртуального пространства.

Достаточно узко понимает информационный суверенитет И. С. Ашманов, определяя его как «устойчивость государства к информационной войне в любых ее проявлениях» [3]. Представляется, что автор рассматривает информационный суверенитет лишь как инструмент ведения информационного противоборства, содействующий в предотвращении потенциальных угроз информационно-технического характера. При этом, электронный суверенитет понимается, как «защищенность от вирусов, атак, взломов, утечек, закладок, кражи данных, спама, выключения инфраструктуры ПО и устойчивость к электронным атакам» [3]. Акцентируя внимание на кибератаках виртуального пространства для достижения политических, социальных или иных целей, автор указывает на характеристики киберсуверенитета. Кибератаки воздействуют на информационное пространство компьютера, в котором находятся сведения, хранятся материалы физического или виртуального устройства. Атака поражает носитель данных, специально предназначенный для их хранения, обработки и передачи личной информации пользователя [4, с. 184]. Таким образом, по сути, данное определение является идентичным понятию информационного суверенитета.

Зарубежные авторы Дж. Обар (J. A. Obar) и А. Клемент (A. Clement) рассматривают суверенитет с позиции угрозы информационному пространству в части развития инфраструктуры для перенаправления потоков данных и вмешательства во внутренние дела независимого государства [5]. Частично придерживающийся мнения вышеназванных авторов Д. Л. Сивоволов, который рассматривает информационные угрозы как угрозы национальному суверенитету, при этом предлагая «расширить рамки понятия национальный суверенитет и включить в него информационный суверенитет» [6, с. 82]. Авторы указывают на обеспечение суверенитета при помощи защиты от угроз, а именно исключение неправомерного вмешательства во внутренние дела государства

и модификации информации с целью создания угрозы данному пространству. Так, для реализации информационной безопасности и суверенитета страны, необходимо сформулировать задачи, требующие безотлагательного решения.

Лаконичное мнение наблюдается у Е. Г. Зориной, которая считает, что информационный суверенитет состоит из технических и идеологических аспектов. Технический подразумевает собственные социальные сети, поисковики, национальное программное обеспечение, национальная электронная платежная система и т. д. Идеологический аспект указывает на наличие официальной идеологии или национальной идеи, высокого уровня популярной массовой культуры, развитой системы пропаганды, а также усовершенствованного законодательства в области информации [7, с. 346]. Таким образом, Е. Г. Зорина совмещает в идеологическом подходе информационно-психологическое и информационно-политическое направление, при этом полностью не указывает на истинно технический аспект, а именно наличие средств электронной инфраструктуры.

Более широкий перечень технических элементов информационного суверенитета вводит В. В. Бухарин, а именно: поисковая система, социальные сети, операционная система и программное обеспечение, микроэлектроника, сетевое оборудование, национальный сегмент сети Интернет, платежная система, собственные средства защиты, криптографические алгоритмы и протоколы, навигационная система [8, с. 79].

Необходимо отметить важный компонент информационного суверенитета, не фиксирующийся в мнениях другие авторов – наличие государственной операционной системы. В современных реалиях операционная система Windows, разработчиком которой является компания Microsoft, продолжает занимать лидирующее положение в сегменте персональных компьютеров. В государственных организациях часто применяется операционная система Astra Linux для информационных систем с конфиденциальной информацией, при этом информационное ядро и код являются разработкой Финляндии.

В связи с вышеизложенным можно сделать вывод о том, что реализация информационного суверенитета является предпосылкой для формирования информационной безопасности в стране. Существует необходимость создания четкой стратегии развития и обеспечения информационного суверенитета, а также структуризации общих интересов в сфере информатизации.

Список цитированных источников

1. Беленков, Д. В. Информационный суверенитет России и Европейского Союза, информационная политика и информационное противоборство: сущность и содержание [Электронный ресурс] / Д. В. Беленков, П. А. Гюлазян, Д. Э. Мазлумян // Международный студенческий научный вестник. – 2018. – № 5. – Режим доступа: https://eduherald.ru/ru/article/view?id=18949. – Дата доступа: 08.03.2022.

2. Ромашкина, Н. П. Информационный суверенитет в современную эпоху стратегического противоборства / Н. П. Ромашкина // Национальный исследовательский институт мировой экономики и международных отношений им. Е. М. Примакова РАН : Информационные войны. – 2019. – № 4 (52). – С. 14–19.

3. Ашманов, И. С. Информационный суверенитет [Электронный ресурс] / И. С. Ашманов // ЦВПИ. – Режим доступа: http://eurasian-defence.ru/sites/default/files/doc/ashmanov.pdf. – Дата доступа: 08.03.2022.

4. Massel, A. The current state of cyber security in Russia's energy systems and the proposed activities for situation improving / A. Massel, L. Massel // 6th International Conference on Liberalization and Modernization of Power Systems. Edited by Z. A. Styczynski and N. I. Voropai. – Saint Petersburg, 2015. – P. 183–189.

5. Obar, J. A. Internet Surveillance and Boomerang Routing: A Call for Canadian Network Sovereignty [Electronic resource] / J. A. Obar, A. Clement // SSRN. – Mode of access: https://papers.ssrn.com/abstract=2311792. – Date of access: 08.03.2022.

6. Сивоволов, Д. Л. Новые угрозы национальному суверенитету России в сфере информационной безопасности / Д. Л. Сивоволов // Социум и власть. – 2015. – № 6 (56). – С. 82–88.

7. Зорина, Е. Г. Информационный суверенитет современного государства и основные инструменты его обеспечения / Е. Г. Зорина // Изв. Сарат. ун-та. Нов. сер. Сер. Социология. Политология. – 2017. – Т. 17, вып. 3. – С. 345–348.

8. Бухарин, В. В. Компоненты цифрового суверенитета российской федерации как техническая основа информационной безопасности / В. В. Бухарин // Вестн. МГИМО ун-та. – 2016. – № 6 (51). – С. 76–91.

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ И ПОДХОДЫ К ИХ РЕШЕНИЮ

CURRENT PROBLEMS OF PERSONAL DATA PROTECTION AND APPROACHES TO THEIR SOLUTION

Бобкова Е. А.
г. Минск,
Белорусский государственный
экономический университет,
студентка факультета права

Научный руководитель
Пехота Т. М.
г. Минск,
Белорусский государственный
экономический университет,
ассистент кафедры теории и истории права

Аннотация: В исследуемой работе предоставлен подробный анализ проблемы кибербезопасности и пути решения данной проблемы, а также рассмотрены варианты предотвращения кибератак.

Ключевые слова: кибербезопасность, кибератака, персональные данные, информационная безопасность.

Annotation: The research work provides a detailed analysis of the problem of cybersecurity and ways to solve this problem, as well as options for preventing cyberattacks.

Keywords: cyber security, cyberattack, personal data, information security.

Вместе с созданием новых технологий развиваются и угрозы безопасности пользования разработанными нововведениями. Кибербезопасность является одной из основных проблем в современном мире. Кибератаки могут воздействовать на информационное пространство компьютера, в котором находятся персональные сведения, хранятся материалы физического или виртуального устройства. Все это приводит к тому, что расходы на информационную безопасность за последние десять лет вошли едва ли не в десятку самых крупных статей расходов большинства средних и крупных компаний по всему миру. Существуют различные виды кибератак, такие как фишинг, атаки программ-вымогателей, утечка данных, атаки «человек посередине» и многие другие. Все вышеперечисленные кибератаки в основном негативно воздействуют именно на людей, а не на системы.

Вышеупомянутые кибератаки напрямую влияют на жизнь людей. Утечка персональных данных предоставляет возможность «хакерам» через личную информацию людей, их электронную почту, номера телефонов с помощью различных манипуляций заполучить их денежные средства.

Одной из наиболее известных кибератак является взлом системы Uber в 2016 году. Система подверглась мощной хакерской атаке, в результате которой киберпреступники завладели личными данными 57 млн клиентов и водителей службы онлайн-такси. Злоумышленники украли имена, адреса электронной почты и номера телефонов 50 млн пассажиров Uber по всему миру, а также личную информацию о 7 млн водителей, в частности взломщики получили 600 тыс. номеров водительских удостоверений водителей из США. Представители службы такси заверили, что номера социального страхования, данные кредитных карт и другие данные хакерская атака не затронула [1].

Известны случаи, когда последствия кибератак затрагивали не только получение персональных данных, а также здоровье и жизнь человека. В 2015 году хакеры взломали сайт Ashley Madison, предназначенный для знакомств замужних женщин и женатых мужчин. В результате атаки произошла утечка данных 40 млн пользователей. Некоторым из них начали рассылать угрозы с требованием выкупа в $1 тыс. Под сильным давлением киберпреступников и эмоциональной нагрузкой, вызванной тревожностью за распространение личных данных, переписок, некоторые из пострадавших не смогли справиться с давлением; зафиксированы случаи самоубийства [2]. Еще один нашумевший инцидент произошел в сентябре 2020 года. Злоумышленники атаковали IT-систему университетской клиники в Дюссельдорфе. В результате 30 серверов и все подключенные устройства, в том числе аппараты жизнеобеспечения, на некоторое время вышли из строя [3].

Одной из основных проблем является проблема обнаружения кибератак. Заранее обезопасить себя от нападения «хакерами» с каждым годом становится все тяжелее. Считаем целесообразным предложить создание в Республике Беларусь систему аудита, предназначенную для защиты от кибератак, представляющую собой руководство по защите персональной информации, включая рекомендации по управлению персональными данными и предотвращению

утечки персональных данных. Данная система безопасности также должна включать в себя сертификацию. Это позволит людям уверенно выбирать компанию, которая находится под защитой от кибератак и не опасаться за свои персональные данные.

Можно провести аналогию с зарубежными странами. Например, в Великобритании разработан международный стандарт по информационной безопасности ISO/IEC 27001, который применим к организациям всех типов и размеров, включая государственные и частные компании, правительственные и некоммерческие организации. В нем содержатся рекомендации для организаций, отвечающих за обработку персональных данных в рамках системы менеджмента информационной безопасности.

Международно признанный стандарт ISO/IEC 27001 является надежной основой для управления и защиты своих информационных активов с тем, чтобы они оставались в безопасности. Преимущества стандарта ISO/IEC 27001 [4]:

– возможность выявления рисков и принятия мер по их оптимизации или устранению;

– гибкость адаптации инструментов к любым сферам деятельности;

– доверие со стороны заинтересованных лиц и клиентов благодаря защите их данных;

– соответствие стандартам гарантирует статус привилегированного поставщика.

Стандарт ISO/IEC 27001, в первую очередь, представляет собой анализ пробелов и недостатков, что позволит проверить, насколько организация близка к выполнению требований стандарта, выявить упущения и определить те сферы, которым следует уделить особое внимание. К тому же проводится предварительная оценка, позволяющая убедиться в том, что система менеджмента персональной информации организации работает эффективно в соответствии с требованиями стандарта. После устранения всех недостатков, найденных сотрудниками ISO/IEC 27001, организация проходит этап сертификации и ежегодно сотрудники стандарта будут проводить проверки для подтверждения соответствия требованиям стандарта.

В нынешнее время новых технологий люди все чаще подвергаются угрозам киберпреступников. В связи с развитием сети Интернет, созданием множества приложений все чаще люди оставляют свои персональные данные, не задумываясь о последствиях. Для того, чтобы обезопасить себя от нападения «хакеров», государство предлагает рекомендательные меры, а именно: не подключаться к общедоступным сетям Wi-Fi, создавать отдельную почту для приложений, социальных сетей, использовать всегда разные пароли, не предоставлять доступ к данным на телефоне и т. д. Однако перечисленных мер недостаточно, чтобы защитить персональную информацию. Поэтому внедрение системы аудита по защите персональных данных на основе опыта Великобритании будет способствовать безопасности таких данных, как финансовая информация, интеллектуальная собственность, персональные данные, сведения о сотрудниках или сведения, предоставленные третьими лицами. Это позволит снизить риски утечки информации и предотвратить различные кибератаки.

Список цитированных источников

1. Uber скрыла мощную кибератаку с кражей данных 57 млн клиентов и водителей [Электронный ресурс] // Технологии и медиа – 2017. – Режим доступа: https://www.rbc.ru/technology_and_media/22/11/2017/5a14c7f99a7947aff17f83c3. – Дата доступа: 02.05.2022.
2. Мэдисон, Э. «Самоубийства» из-за взлома сайта [Электронный ресурс] / Э. Мэдисон // Технологии. – 2015. – Режим доступа: https://www.bbc.com/news/technology-34044506. – Дата доступа: 02.05.2022.
3. Кибератаки могут убивать? [Электронный ресурс] // Десять самых громких кибератак XXI века. – 2021. – Режим доступа: https://trends.rbc.ru/trends/industry/600702d49a79473ad25c5b3e. – Дата доступа: 02.05.2022.
4. ISO/IEC 27001 – Менеджмент информационной безопасности [Электронный ресурс] // Bsi. – Режим доступа: https://www.bsigroup.com/ru-RU/ISO-IEC-27001. – Дата доступа: 02.05.2022.

ПРОБЛЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЭПОХУ ЦИФРОВЫХ ТЕХНОЛОГИЙ

THE PROBLEM OF DEFENCE PERSONAL DATA IN EPOCH OF INFORMATION TECHNOLOGIES

Гармаза Е. С.
г. Минск,
Военная академия Республики Беларусь,
курсант факультета внутренних войск

Научный руководитель
Леднёва А. С.
г. Минск,
Военная академия Республики Беларусь,
доцент цикла государственно-правовых дисциплин
кафедры юридических дисциплин,
кандидат исторических наук, доцент

Аннотация: Рассматриваются вопросы защиты персональных данных как фундаментального права человека на неприкосновенность частной жизни и их использования в качестве идентификации личности.

Ключевые слова: персональные данные, безопасность персональных данных, законодательство о защите персональных данных, ответственность за незаконные действия с персональными данными.

Annotation: The questions of data protection in the context of the fundamental human right to the personal privacy and its using as biometrics are examined.

Keywords: personal data, personal data security, personal data protection law, responsibility for illegal actions with personal data.

Развитие информационных технологий в наше время затрагивает все сферы деятельности человечества в мировой масштабе. Не стала исключением и информация о персональных данных. Персональные данные – это особый вид информации ограниченного распространения, составляющий основу практической реализации права на неприкосновенность частной жизни, закрепленного как в международных документах, так и в конституциях государств. Защита персональных данных необходима не только гражданам и обществу, но и властным структурам как неотъемлемое условие совершенствования их деятельности [1, с. 127].

Под информационной безопасностью обычно понимается состояние защищенности информационной среды общества, обеспечивающее ее формирование и развитие в интересах граждан, организаций и государства. А под информационными угрозами – различные факторы или совокупности отдельных факторов, создающие опасность нормальному функционированию информационной среды общества. Необходимо отметить, что осознание связи между состоянием информационной среды общества и возможностями достижения важнейших интересов человека и общества произошло относительно недавно. И тем не менее, многие государства мира, включая Республику Беларусь, уже разработали свои национальные доктрины в области информационной безопасности, а также концепции государственной политики по ее обеспечению [2].

Для развития нового типа отношений, взаимодействия государства и гражданского общества, основанных на широком использовании данных и цифровых технологий, необходимы организационные, материально-технические и нормативные предпосылки. Программа «Цифровая экономика», одобренная в Республике Беларусь, продвигает новейшие технологии по все сферы нашей жизни. Граждане хотят жить в благополучной среде, и цифровые услуги – это уже не только подача документов в электронном виде, но и онлайн-режим разрешения возникших проблем. Например, при работе с обращениями граждан, органы власти уходят от писем на бумажных носителях и переходят к платформам, на которых можно задать вопрос, высказать свое мнение, дать оценку работы служащего, получить обратную связь по своей проблеме. Но гражданин также должен быть уверен, что его личные данные не будут использованы в преступных целях.

Гражданские базы данных, как и военные – это национальное достояние. Государство должно обеспечить защиту личных данных своих граждан – информацию об их занятиях, и прочие «цифровые следы», представляющие интерес для уголовного мира, бизнес-структур, политических партий, общественной безопасности, международных отношений, военного дела. Как отмечают некоторые профессионалы, взломать или проникнуть сейчас можно в любую систему, вопрос лишь во времени и средствах. Если данные передаются сотруднику органа власти, банку или любой другой организации, оформляется согласие на обработку этих данных, и дальше ответственность за их сохранность несет данная организация. Если же человек сам выкладывает в общий доступ копии своих документов, личные сведения, то он должен осознавать и возможные последствия. Государство и в этом случае должно помогать людям

повышать общую компьютерную грамотность и обучать культуре информационной безопасности.

Еще до широкого развития интернет-технологий сбор сведений о жизни граждан был существенно ограничен, а в некоторых случаях и запрещен законом об оперативно-розыскной деятельности. Идея регулировать личные данные (иногда их называют большими данными) принадлежит президенту компании Info Watch Наталье Касперской. Законодательство, регулирующее работу с персональными данными граждан, позволяет различным структурам идентифицировать человека. Минимальный набор таких данных – это фамилия, имя и фотография. Но есть данные, обращение которых в интернете не регламентировано. Они разрознены по ресурсам или сервисам. Например, это информация о перемещениях, контактных, политических пристрастиях, уровне дохода, привычках, круге друзей, высказываниях в социальных сетях и так далее. Если эти данные интегрировать, что законом большинства государств в настоящее время не запрещено, можно будет узнать о конкретном человеке очень много. В интернете личные данные собирают, продают, сдают в аренду.

Такая совокупность личных данных может быть использована для различных целей. Стоит ли говорить, насколько возросла опасность «кражи личности» с развитием цифрового информационного пространства. Например, для подбора рекламы под конкретного человека, опознания пользователя с целью предложения ему товара, который он обсуждал, к примеру, в личной переписке. То есть личную информацию из глубин интернета используют разные компании и занимаются их продажей. Нужно выработать критерии для интернет-компаний, которые работают с персональными данными, и указать, в каких случаях они такие данные смогут продавать, а в каких – использовать только для своих целей. Также через норму закона необходимо прописать обязанность компаний предоставить справку пользователю обо всей собранной о нем информации, а также возможность заставить компанию эту информацию удалить. И ответственность за неудаление должна быть серьезной. Граждане должны быть уверены, что данные, содержащие номера счетов, информацию о здоровье или частной жизни, надежно защищены. Это предполагает необходимость точного определения, что для человека считается чувствительной информацией, и установления требований по контролю безопасности.

Еще один важный компонент цифровой политики личных данных – единая идентификация гражданина, которая будет проходить через все коммерческие и государственные сервисы. Здесь все более значительную роль начинает играть биометрическая идентификация. Идентификация и проверка личности всегда являлись частью повседневной жизни человека и имели целью установить неизвестное лицо на основе представленных им данных. До наступления электронной эры паспорта были необходимы, чтобы въехать в страну, а образцы подписей были обязательны при осуществлении банковских операций. Однако все эти методы требуют предоставления материального документа и до начала интернет-революции большинство операций осуществлялось в личном присутствии клиента.

Биометрия, то есть использование физических характеристик для проверки идентичности, не представляет из себя ничего принципиального нового. Система использования отпечатков пальцев для установления личности была разработана

более ста лет назад, хотя, конечно, еще не в цифровом формате. Сегодня эта технология используется для разблокировки айфонов и для входа в помещение, а, например, метод распознавания голоса позволяет подтвердить личность в течение 15 секунд, что гораздо быстрее, чем при помощи пароля.

Казалось бы, в эпоху, когда во главу угла ставится удобство, потребитель должен быть готов предоставить биометрические данные для ускорения операций. Но по-прежнему остается обеспокоенность тем, что биометрическая информация может быть похищена хакерами. Использование паролей, PIN-кодов и биометрических данных предполагает их передачу сторонним структурам, поэтому потребитель должен быть уверен, что эта информация будет храниться в безопасности. В чужих руках персональные данные могут быть использованы для свершения мошенничества, а с ростом утечек персональных данных мошенничества будут только множиться.

Для того, чтобы проверка личных данных была, с одной стороны, безопасна, а с другой, не вызывала негативных эмоций у пользователя, в России, например, разработан законопроект о цифровом профиле гражданина, который позволит аккумулировать данные о человеке, которые используются при предоставлении государственных услуг и сервисов. Как большая совокупность данных, цифровой профиль должен быть надежно защищен от утечек и злоупотреблений. Для этого разрабатываются правила идентификации и аутентификации. Прорабатывается механизм работы с так называемыми общедоступными данными [3].

Негативные моменты, связанные с недостаточной защитой персональных данных, выявилась в Беларуси в 2020 году, когда наблюдалась напряженная общественно-политическая обстановка. Через интернет произошел вброс персональных данных сотрудников силовых структур, военнослужащих, членов их семей и родственников. Этим воспользовались анархистски и радикально настроенные представители общества, незарегистрированные молодежные объединения, осуществляя экстремистские действия, представляющие угрозу жизни и здоровью людей.

Вопросы обеспечения общественной и личной безопасности граждан стали основой корректировки существующего законодательства. Генеральная прокуратура Республики Беларусь подготовила предложения по усилению ответственности за экстремистскую деятельность, в том числе предложено наказывать в уголовном порядке за незаконный сбор и распространение информации о частной жизни или персональных данных граждан, а также ввести повышенную ответственность за такие действия в отношении лица или его близких в связи с осуществлением служебной деятельности или выполнением общественного долга. Данные предложения нашли воплощение в поправках, внесенных в Уголовный кодекс Республики Беларусь. Подобные новации внедряются в законодательство целого ряда зарубежных государств.

Таким образом, в эпоху цифровых технологий обеспечение неприкосновенности частной жизни является одной из внутренних функций государства. Очевидно, что дальнейшая эволюция интернета приведет к очередному витку информационного проникновения в сферу персональных данных, но несмотря на очевидную сложность защитных технологий, ничего сверхъестественного

в них нет – по уровню развития они не опережают информационные технологии, а всего лишь следуют за ними.

Представляется, что для регулирования данного вида отношений между гражданами и государственными институтами, а также структурами бизнеса целесообразно создание отраслевой ассоциации, которая будет вырабатывать этические правила работы с такого рода информацией.

Список цитированных источников

1. Леднёва, А. С. Информационные технологии и цветные революции / А. С. Леднёва // Актуальные проблемы обеспечения общественной безопасности в Республике Беларусь: теория и практика : сб. материалов XXII Респ. науч.-практ. конф., Минск, 21 мая 2020 г. : в 2 ч. / Факультет внутр. войск УО «Военная академия Республики Беларусь» ; редкол.: В. А. Талалаев [и др.]. – Минск, 2020. – Ч. 2 : Правовое обеспечение выполнения задач внутренними войсками МВД Респ. Беларусь. – С. 126–129.

2. О Концепции информационной безопасности Республики Беларусь [Электронный ресурс] : постановление Совета Безопасности Респ. Беларусь, 18 марта 2019 г. № 1 // Нац. центр правовой информ. Респ. Беларусь ; КонсультантПлюс. Беларусь / ООО «ЮрСпектр». – Минск, 2022.

3. Личные данные доверят Роскомнадзору [Электронный ресурс] // Рос. газета. – 2020. – 28 июля. – Режим доступа: https://rg.ru. – Дата доступа: 03.05.2022.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА В СФЕРЕ КИБЕРОПАСНОСТИ

INFORMATION SECURITY AND PROTECTION IN THE FIELD OF CYBER DANGER

Касьянчик М. П.
г. Минск,
Институт пограничной службы Республики Беларусь,
курсант факультета подготовки офицерских кадров

Научный руководитель
Улитко С. А.
г. Минск,
Институт пограничной службы Республики Беларусь,
профессор кафедры идеологической работы,
кандидат педагогических наук, доцент

Аннотация: В представленных материалах акцентируется внимание на важной проблеме современности – информационной безопасности. Автор предлагает рассмотреть пути сохранения и защиты информации, а также ее важнейших элементов: системы и оборудования, предназначенных для использования, сбережения и передачи этой информации. Автор, будущий специалист по идеологической работе, формирует собственное мнение относительно того, как важно уметь защищать информацию на основе тех знаний и умений, которые развивают преподаватели ГУО «ИПС РБ».

Ключевые слова: информационная безопасность, киберопасность, кибербезопасность, конфиденциальность, целостность.

Annotation: The presented materials focus on an important problem of our time – information security. The author proposes to consider ways to preserve and protect information, as well as its most important elements: systems and equipment designed to use, store and transmit this information. The author, a future specialist in ideological work, forms his own opinion on how important it is to be able to protect information based on the knowledge and skills that teachers of the State Educational Institution «IPS RB» develop.

Keywords: information security, cyber danger, cybersecurity, confidentiality, integrity.

Прогресс нашего времени превратил информацию в продукт, который можно купить, продать, обменять. Нередко стоимость данных в несколько раз превышает цену всей технической системы, которая хранит и обрабатывает информацию.

Информационная безопасность– это сохранение и защита информации, а также ее важнейших элементов, в том числе системы и оборудование, предназначенные для использования, сбережения и передачи этой информации.

Информация считается защищенной, если соблюдаются два главных ее свойства:

Первое – целостность – предполагает обеспечение достоверности и корректного отображения охраняемых данных, независимо от того, какие системы безопасности и приемы защиты используются. Обработка данных не должна нарушаться, а люди, которые работают с защищаемыми файлами, не должны сталкиваться с проблемами, сбоями в работе программного обеспечения.

Второе – конфиденциальность – означает, что доступ к просмотру и редактированию данных предоставляется исключительно доверенным лицам.

Достаточно нарушить одно из свойств защищенной информации, чтобы использование системы стало бессмысленным.

Рассмотрим некоторые требования к защите информации.

Защита информационных ресурсов должна быть:

1. Постоянной. Киберпреступник в любой момент может попытаться обойти модули защиты данных, которые его интересуют.

2. Целевой. Информация должна защищаться в рамках определенной цели.

3. Плановой. Должна быть определенная структура действий и алгоритмов по защите информации.

4. Активной. Мероприятия для поддержки работы и совершенствования системы защиты должны проводиться регулярно.

5. Комплексной. Использование только отдельных модулей защиты или технических средств недопустимо. Необходимо применять все виды защиты в полной мере.

6. Универсальной. Средства защиты должны быть выбраны в соответствии с существующими в компании каналами утечки.

7. Надежной. Все приемы защиты должны надежно перекрывать возможные пути к охраняемой информации со стороны злоумышленника, независимо от формы представления данных.

Сегодня организации, ведомства сталкиваются с угрозами кибербезопасности и должны задумываться над безопасностью своих «продуктов», материалов, документов.

На практике основными причинами появления нарушений безопасности являются недостатки реализации механизмов защиты, недобросовестное несение службы со стороны личного состава, неправильное хранение документации или информации на флеш-носителях или же других накопителях, форс-мажорные обстоятельства и другие причины. Рассмотрим физические способы обеспечения информационной безопасности.

Физические меры защиты – это разного рода механические, электро- и электронно-механические устройства и сооружения, специально предназначенные для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам информационной системы и охраняемой информации. В перечень физических способов защиты информации входят:

– организация пропускного режима;

– организация учета, хранения, использования и уничтожения документов и носителей с конфиденциальной информацией;

– распределение реквизитов разграничения доступа;

– организация скрытого контроля за деятельностью пользователей и обслуживающего персонала информационной системы;

– мероприятия, осуществляемые при проектировании, разработке, ремонте и модификациях аппаратного и программного обеспечения [1, с. 56].

Защита информации представлена тремя этапами.

На первом этапе разрабатывается базовая модель системы, которая будет функционировать. Для этого необходимо проанализировать все виды данных, которые циркулируют в фирме и которые нужно защитить от посягательств со стороны третьих лиц. Целью может быть ознакомление, изменение, модификация или уничтожение данных.

На данном этапе важно понимать, что нарушители:

– незаконно используют данные (несанкционированный доступ);

– неконтролируемо распространяют информацию за пределы корпоративной сети. Утечка порой возникает из-за недочетов, слабых сторон технического канала системы безопасности;

– несознательные пользователи могут разглашать информацию, чтобы передать ее конкурентам или по неосторожности.

Второй этап включает разработку системы защиты. Это означает реализовать все выбранные способы, средства и направления защиты данных.

Система строится сразу по нескольким направлениям защиты, на нескольких уровнях, которые взаимодействуют друг с другом для обеспечения надежного контроля информации. Рассмотрим их.

Например, правовой уровень обеспечивает соответствие государственным стандартам в сфере защиты информации и включает авторское право, указы, патенты и должностные инструкции. Грамотно выстроенная система защиты не нарушает права пользователей и нормы обработки данных.

Организационный уровень позволяет создать регламент работы пользователей с конфиденциальной информацией, подобрать кадры, организовать работу с документацией и физическими носителями данных [2, с. 104].

Регламент работы пользователей с конфиденциальной информацией называют правилами разграничения доступа. Правила устанавливаются руководством совместно со службой безопасности.

Технический уровень условно разделяют на физический, аппаратный, программный и математический подуровни.

физический – создание преград вокруг защищаемого объекта: охранные системы, зашумление, укрепление;

аппаратный – установка технических средств: специальные компьютеры, системы контроля сотрудников, защиты серверов и корпоративных сетей;

программный – установка программной оболочки системы защиты, внедрение правила разграничения доступа и тестирование работы;

математический – внедрение криптографических и стенографических методов защиты данных для безопасной передачи по корпоративной или глобальной сети.

Третий, завершающий этап – это поддержка работоспособности системы, регулярный контроль и управление рисками. Важно, чтобы модуль защиты отличался гибкостью и позволял администратору безопасности быстро совершенствовать систему при обнаружении новых потенциальных угроз.

В настоящее время интернет и социальные сети стали неотъемлемой частью жизни большей части населения планеты, неизбежно меняется ландшафт не только каждодневной, событийной и внутренней, субъективной жизни человека, но и его профессиональной деятельности. Доступность интернета повлекла за собой почти неограниченный доступ пользователей к информации и к коммуникации друг с другом. А это значит, и неосторожное хранение важной переписки.

Так, например, в Государственном учреждении образования «Институт пограничной службы Республики Беларусь» изучается дисциплина «Защита информации», в рамках которой научным языком будущим офицерам-пограничникам объясняется феномен информационных войн, а также методы и способы защиты от их негативного влияния. Целью дисциплины является подготовка курсантов в вопросах защиты государственных секретов и служебной информации ограниченного распространения при решении задач

оперативно-служебной и иной деятельности, а также обеспечения специальной связью в подразделениях границы.

Задачами дисциплины являются:

– изучение основных руководящих документов, регламентирующих защиту государственных секретов и служебной информации ограниченного распространения, организацию документационного обеспечения в органах пограничной службы;

– привитие твердых практических навыков по защите государственных секретов при проведении секретных работ, обращении с секретными документами и изделиями, учете и хранении секретных и служебных документов в подразделениях границы, пограничного контроля;

– изучение основ технической защиты государственных секретов;

– повышения уровня теоретических знаний и практических навыков в вопросах защиты государственных секретов;

– воспитание у должностных лиц, допущенных к государственным секретам, чувства ответственности за доверенные им государственные секреты;

– выработка умений и навыков обращения с секретными документами и изделиями, организации скрытого управления в процессе управленческой деятельности в подразделениях органов пограничной службы.

Курсанты детально изучают основные категории политологии и идеологии, учатся понимать специфику формирования идеологии белорусского государства, анализируют явления политической жизни общества с позиции гражданственности и патриотизма, учатся анализировать и использовать в практической служебной деятельности служебный и боевой опыт действий подразделений границы, быть способными оценить влияние исторических и современных фактов на эффективное состояние оперативно-служебной деятельности.

И, конечно же, каждый из пограничников должен учиться самостоятельно противостоять негативным явлениям действительности: читать дополнительную литературу, смотреть аналитические передачи, общаться с компетентными людьми, стремиться быть дисциплинированными, ответственными пограничниками с ясной жизненной позицией, уметь проверять полученную информацию, по необходимости опровергать ее, приводя аргументы и доказательства, владеть методами убеждения, личного примера и др.

Список цитированных источников

1. Громов, Ю. Ю. Информационная безопасность и защита информации : учеб. пособие / Ю. Ю. Громов, В. О. Драчев, О. Г. Иванова. – Ст. Оскол : ТНТ, 2010. – 384 с.

2. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. – М. : ДМК, 2014. – 702 с.

КИБЕРУГРОЗЫ ДЛЯ АВТОРОВ МУЗЫКАЛЬНЫХ ПРОИЗВЕДЕНИЙ В XXI ВЕКЕ. ОНЛАЙН-ПИРАТСТВО

CYBER THREATS FOR AUTHORS OF MUSICAL COMPOSITIONS. ONLINE PIRACY

Коршок Д. И.
г. Витебск,
Витебский государственный университет
имени П. М. Машерова,
студент юридического факультета

Научный руководитель
Николичев Д. Н.
г. Витебск,
Витебский государственный университет
имени П. М. Машерова,
старший преподаватель кафедры
гражданского права и гражданского процесса

Аннотация: В работе рассмотрены проблемные аспекты защиты авторских прав, а также персональных данных пользователей нелицензионного программного обеспечения в условиях современных киберугроз.

Ключевые слова: авторское право, онлайн-пиратство, кибербезопасность, плагиат, нелицензионное программное обеспечение.

Annotation: The article discusses the problematic aspects of copyright protection, personal data of users using unlicensed software in the conditions of modern cyber threats.

Keywords: copyright, online piracy, cybersecurity, plagiarism, non-licensed software.

Музыка – неотъемлемая часть культуры, которая существовала на протяжении всей истории человечества, несмотря на политические режимы, формы правления, формы государственного устройства и другие исторические аспекты. Для каждого исторического периода характерна своя музыка, ведь ее пишут люди, которые проживают данное время, передают в ней свое восприятие мира. В зависимости от уровня развития общества, музыка создавалась разными способами. В самом начале это было повторение одних и тех же интонаций, которые передавались из поколения в поколение. С появлением письменности и музыкальной грамотности эти интонации перенеслись на бумагу в виде нот.

В наше время, с приходом электронно-вычислительной техники, все стало переходить в цифровой формат. Появились специальные программы-секвенсоры «DAW» (от англ. Digital Audio Workstation) – рабочие станции для цифровой обработки звука, а также огромное количество подключаемых модулей, расширяющих возможности секвенсора, называемых плагинами (от англ. Plug-in). Так как эти средства являются программами, которые находятся в цифровом формате, они могут представлять непосредственную

угрозу для тех, кто ими пользуется, а именно для композиторов, музыкантов-инструменталистов, диджеев и других авторов музыкальных произведений.

Несмотря на то, что производители данных программ стараются обеспечить кибербезопасность своим пользователям путем предоставления личных ключей-активаторов и прямых ссылок на продукцию, вероятность занести на свой рабочий компьютер вредоносный код – остается. Особенно это касается пользователей Российской Федерации, Республики Беларусь, Казахстана и других стран, в которых распространено онлайн-пиратство. Данный вид пиратства связан непосредственно со взломом платной продукции, копированием и распространением уже взломанной версии в массы совершенно бесплатно, тем самым нарушая авторские права создателей.

«Спрос» на данный вид пиратства возник на закате XX – начале XXI века. Он заключался в копировании и распространении кассет и дисков с зарубежными фильмами и музыкой. Со временем кассеты и диски устарели и пиратство перешло в онлайн-режим, в котором пользователи сети Интернет могли без проблем зайти на определенные сайты, такие как Rutracker, Bigtorrent, uTorrent и скачать совершенно бесплатную интересующую их информацию: фильмы, музыку и программы.

Данный вид пиратства популярен до сих пор, так как в ряде стран недостаточно высокий уровень доходов, чтобы обычные пользователи могли позволить тратить свои денежные средства на то, что можно получить бесплатно. По факту это превращает пользователей, которые скачали «пиратские версии» софта (сокр. от англ. Software – программа) – в воров, а создателей этого софта – оставляет без средств к существованию.

По статистике, предоставленной экспертами организации BSA (Business Software Alliance), доля «пиратского» программного обеспечения (далее – ПО) на Республику Беларусь составляет 82 %, на Украину – 80 %, на Казахстан – 74 %, на Российскую Федерацию – 62 %. Эти данные свидетельствую о том, что более половины всего ПО является не только нелицензионным, но и потенциально опасным. Эксперты BSA отметили, что использование «пиратского» ПО спровоцировало рост кибератак, которые сопряжены с финансовыми потерями [1].

В связи с этим в ряде стран были введены меры борьбы с пиратством. В Российской Федерации были внесены изменения в законодательство, а именно в 2013 году был принят Федеральный закон № 187 «О внесении изменений в законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях», который должен был защитить права авторов путем блокировки сайтов-распространителей «пиратского» ПО [2]. В Республике Беларусь была ужесточена ответственность за нарушение авторских прав, начиная административным взысканием в виде штрафа в размере от 10 до 30 базовых величин (на физическое лицо), заканчивая уголовной ответственностью в виде лишения свободы сроком до двух лет. Однако невысокую эффективность данных мер демонстрирует вышеприведенная статистика.

Кроме законодательных изменений, в целях противодействия пиратству и вредоносному ПО стали разрабатываться программы-антивирусы. Они должны препятствовать проникновению вредоносного ПО на компьютер, что в некотором роде должно обеспечить безопасность для хранящихся на нем данных. Популярными представителями таких программ-антивирусов являются: Dr.Web, Avast, Kaspersky, NOD32. Однако скачав антивирус, вы не становитесь на 100 % защищенными от кибератак и вирусов. Антивирусы существуют лишь как программы противодействия для уже созданных угроз, но не для новых.

Для авторов музыкальных произведений опасность представляют те самые аудио-секвенсоры, в которых создается музыка и наборы плагинов по обработке звука. Качая их со сторонних сайтов, существует риск занести на свой рабочий компьютер вредоносный код или программу. Для тех, кто использует свой компьютер как в рабочих, так и в личных целях, это чревато угрозой для конфиденциальной информации, начиная от утечки персональных данных, заканчивая их абсолютным уничтожением. Самой распространенной вредоносной программой являются «вирусы-вымогатели», которые требуют перевести на определенный счет крупную денежную сумму, в противном случае грозя удалить все данные с компьютера, включая саму систему.

Для авторов музыкальных произведений важно сохранить свою продукцию в высоком качестве, однако в случае занесения на компьютер вируса, он может повредить исходный код, что приведет к ухудшению качества продукта, либо к его полной нечитаемости, тем самым полностью аннулируя всю работу автора. Кроме того, существует риск, что к компьютеру будет получен удаленный доступ и злоумышленник сможет скачать еще не выпущенное музыкальное произведение и распространить его.

Из-за активного роста музыкальной индустрии и появления много-численных объектов авторского права в области музыки, участились право-нарушения в этой сфере, что повлекло за собой рост числа споров о защите авторских прав на музыкальные произведения. В Республике Беларусь по данным судебной коллегии по делам интеллектуальной собственности, общее количество споров, рассмотренных в период с 2017 по май 2021 г. составляет 653 дела, из них 578 дел, или 88,21 % – это споры в сфере авторских и смежных прав [3].

Авторские права нарушаются в Интернете чаще, чем какие-либо иные. Это обусловлено всеобщим интересом к музыкальным произведениям, а также тем, что Интернет представляет собой огромное поле деятельности для нарушителей, которых, ввиду удаленного доступа, проблематично отследить и, как следствие, привлечь к ответственности [4, с. 13].

В Республике Беларусь Закон «Об авторском праве и смежных правах» регламентирует порядок «работы» авторского права [5]. Однако самого понятия «музыкальное произведение» в национальном законодательстве не существует. Таким образом, музыкальные произведения как отдельные объекты авторского права являются уязвимыми. Несмотря на это, в республике существует Национальный центр интеллектуальной собственности, который регистрирует музыкальные произведения и устанавливает авторство.

За последние 10 лет Интернет сместил радио и телевидение с лидирующих позиций по проигрыванию музыкальных произведений, и очень многие, особенно начинающие музыканты, активно выкладывают свои «треки» на различные интернет-площадки или стриминговые сервисы. Яркими примерами таких стриминговых сервисов являются: «Spotify», «Apple Music», «VK Music», «Яндекс.Музыка». Они гарантируют полную безопасность авторских прав за денежное вознаграждение, выраженное в определенном проценте от суммы, образующейся в зависимости от количества прослушиваний. Фактически эти интернет-площадки заключают между собой и автором электронный лицензионный договор, в котором и фигурируют гарантии безопасности.

Также в Интернете существуют различные аудиостоки, которые представляют собой площадки для купли-продажи аудиоматериалов различных стилей и жанров. Примерами являются: «Audiojungle», «Pond5». Данные площадки тщательно подходят к безопасности загружаемых треков, а также одной из особенностей является аудио-водяной знак, который в обязательном порядке необходимо интегрировать в свое музыкальное произведения, с повторением через определенный временной интервал, как правило, каждые 10 секунд.

Евгений Касперский говорил, что безопасный компьютер – выключенный компьютер [6, с. 5]. Он подчеркивал, что большинство проблем с компьютером связано с их пользователями. В настоящее время невозможно находиться в состоянии полной кибербезопасности, всегда существует риск занести к себе на компьютер вредоносное ПО, даже установив антивирусные программы. Мы обмениваемся гигабайтами информации изо дня в день и никогда не знаем наверняка, представляет ли она опасность. Можно лишь минимизировать риски, скачивая лицензионную продукцию у официальных дилеров, не заходить на «подозрительные» сайты и обходить стороной «пиратскую» продукцию. Важно быть бдительными и осторожными.

Список цитированных источников

1. Global software survey // BSA. – 2018. – Vol. 1. – P. 10–11.

2. О внесении изменений в законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях [Электронный ресурс] : Федер. закон от 2 июля 2013 г. № 187-ФЗ : в ред. Федер. закона от 12.03.2014 // КонсультантПлюс. Россия / ЗАО «Консультант Плюс». – М., 2022.

3. Сведения о работе судебной коллегии по делам интеллектуальной собственности Верховного Суда Республики Беларусь [Электронный ресурс] // Верховный суд Респ. Беларусь. – Режим доступа: https://court.gov.by/ru/justice/press_office/c97e1ba948c041b1.html. – Дата доступа: 06.05.2022.

4. Алисова, Е. В. Актуальные проблемы защиты авторского права в сети Internet / Е. В. Алисова // Наука, образование и культура. – 2016. – № 7. – С. 12–16.

5. Об авторском праве и смежных правах [Электронный ресурс] : Закон Респ. Беларусь от 17 мая 2011 г. № 262-З : с изм. и доп. от 15 июня 2019 г. № 216-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

6. Касперский, Е. В. Компьютерное зловредство / Е. В. Касперский. – СПб. : Питер, 2007. – 207 с.

СПОСОБЫ БОРЬБЫ В ИНФОРМАЦИОННОЙ ВОЙНЕ

WAYS TO FIGHT IN THE INFORMATION WAR

Костенич Ю. В.
г. Минск,
Институт пограничной службы
Республики Беларусь,
курсант факультета подготовки
офицерских кадров

Научный руководитель
Улитко С. А.
г. Минск,
Институт пограничной службы
Республики Беларусь,
профессор кафедры идеологической работы,
кандидат педагогических наук, доцент

Аннотация: В представленных материалах акцентируется внимание на важной проблеме современности – информационной войне. Автор предлагает рассмотреть основные элементы информационной войны, а именно: физическое разрушение, психологические операции, дезинформация, электронные войны, прямые информационные атаки, меры безопасности. Автор, будущий специалист по идеологической работе, формирует собственное мнение относительно того, как важно уметь противодействовать информационным войнам на основе тех знаний и умений, которые развивают преподаватели ГУО «Институт пограничной службы Республики Беларусь».

Ключевые слова: информационная война, физическое разрушение, психологические операции, дезинформация, электронные войны, прямые информационные атаки, меры безопасности.

Annotation: The presented materials focus on an important problem of our time – the information war. The author proposes to consider the main elements of information warfare, namely: physical destruction, psychological operations, disinformation, electronic warfare, direct information attacks, security measures. The author, a future specialist in ideological work, forms his own opinion on how important it is to be able to counteract information wars on the basis of the knowledge and skills that the teachers of the State Educational Institution «IPS RB» develop.

Keywords: information warfare, physical destruction, psychological operations, disinformation, electronic warfare, direct information attacks, security measures.

Информационная война – это «открытые и скрытые целенаправленные информационные воздействия социальных, политических и других систем друг на друга с целью обеспечения информационного превосходства над противником и с целью нанесения идеологического ущерба. Она включает в себя ряд ключевых элементов. Основными ключевыми элементами являются: физическое разрушение, психологические операции, дезинформация, электронные войны, прямые информационные атаки, меры безопасности. Составной частью информационной войны может выступать физическое разрушение. Обычно оно имеет место быть в тех случаях, когда целью выступают элементы информационных систем. Информационная война носит преимущественно скрытый характер. Ее основным содержанием является ведение разведывательных и политико-психологических действий по отношению к противнику, а также осуществление мероприятий по собственной информационной безопасности. Информационная война представляет собой одну из форм борьбы между государствами. Если главными объектами воздействия при информационно-технической борьбе являются системы связи, телекоммуникационные системы и радиоэлектронные средства, то при информационно-психологической борьбе – психика политической элиты и населения противостоящих сторон, системы формирования общественного сознания, мнения, выработки и принятия решений [1, с. 14].

Цели информационной войны лежат в сфере психического отражения реальности, которое формируется на основе второй сигнальной системы враждующих сторон. Цель «разрушение неприятеля» в информационной войне достигается через организацию мероприятий, направленных на дезорганизацию государства как системы политического руководства и административного управления, дезорганизацию социальных систем и отношений, существующих между государственными и общественными институтами, социальными группами, гражданами. Государственная система вследствие таких мероприятий должна потерять легитимность и ресурс доверия со стороны собственных граждан, оказаться в роли изгоя в международных отношениях, утратить контроль над внутренними социальными процессами, а население – стать неспособным к самоорганизации. Таким образом, формируется основа для принятия внешнего управления. Последствия информационных войн страшны. От информационного влияния порой невозможно защититься, так как оно проникает во все сферы человеческой жизнедеятельности. Сущность информационной войны заключается в давлении на общество, в результате чего члены общества получают искаженное представление о действительности и не имеют возможности сделать правильные выводы и принять верные решения.

Информационная война используется в разных сферах, но ее цель всегда остается постоянной: повлиять на общественное мнение. Вести противодействие информационной войне бывает непросто, ведь манипуляции и пропаганда разрабатываются опытными специалистами. Чтобы не стать жертвой информационного влияния, следует рассматривать по интересующему вопросу мнения разных людей и задействовать разносторонние источники

информации. Защита от воздействия информационной войны сложнее, чем нападение. Общих технологий защиты нет, но используются такие варианты:

- игнорирование информационной войны;
- разоблачение технологии;
- активные действия в ответ;
- устранение причин информационной войны.

Связи с общественностью играют важную роль в жизни общества. Изначально созданные для информирования общественности о ключевых событиях в жизни страны и властных структур, они постепенно стали выполнять еще одну не менее важную функцию – воздействие на сознание своей аудитории с целью формирования определенного отношения к сообщаемым фактам, явлениям действительности. Это воздействие осуществлялось при помощи методов пропаганды и агитации, разрабатываемых на протяжении не одной тысячи лет. В скором времени связи с общественностью заняли важное место в жизни государств, а с развитием техники и технологии стали активно использоваться и на международном уровне с целью приобретения каких-либо преимуществ контролируемым им государством.

Однако сегодня влияние средств массовой информации (далее – СМИ) настолько велико, что мы сами становимся заложниками убеждений и мыслей, которые нам преподносят. Разжигание любой розни между людьми преступно со стороны тех, кто контролирует «четвертую власть», так как идет в противоречие с нормальным и стабильным развитием человечества, подталкивая нас к очередным конфликтам [2, с. 46].

Считаем, что современному человеку можно и нужно как можно больше рассказывать о вреде, которые приносят такие войны, а также научить его противостоять влиянию на свое сознание «извне».

На государственном уровне нужно создавать такие институты и принимать такие законы, которые будут направлены на защиту информационного и цифрового суверенитета нашего государства от атак других стран. Что касается общественности, то, по нашему мнению, мы должны добиваться создания СМИ «народного доверия», которые будут находиться под контролем не иностранных компаний, не государства и не частных лиц, а именно народа. Усилиями истинно гражданского общества будут проводиться частые инспекции таких СМИ, проверки их на надежность, а также участие самого гражданского общества в создании и распространении максимально правдивой информации хотя бы на местном уровне.

Так, например, на уровне образовательного учреждения ГУО «Институт пограничной службы Республики Беларусь», изучаются дисциплины «Основы военной политологии и геополитики. Теория политических систем», «Основы информационно-политической деятельности», «Современные идеологические концепции и доктрины», в рамках которых научным языком будущим офицерам объясняется феномен информационных войн, а также методы и способы защиты от их негативного влияния.

Курсанты детально изучают основные категории политологии и идеологии, учатся понимать специфику формирования идеологии белорусского государства, анализируют явления политической жизни общества с позиции гражданственности и патриотизма. Учатся анализировать и использовать в практической служебной деятельности служебный и боевой опыт действий подразделений границы, быть способными оценить влияние исторических и современных факторов на эффективное состояние оперативно-служебной деятельности.

И конечно же, каждый из нас должен самостоятельно противостоять негативным явлениям действительности: читать дополнительную литературу, смотреть аналитические передачи, общаться с компетентными людьми, стремиться быть дисциплинированным, ответственным пограничником с ясной жизненной позицией, уметь проверять полученную информацию, по необходимости опровергать ее, приводя аргументы и доказательства, владеть методами убеждения, личного примера и др.

Список цитированных источников

1. Завадский, И. И. Информационная война – что это такое? / И. И. Завадский // Конфидент. – 1996. – № 4. – С. 14–15.

2. Мигун, Д. А. Информационный экстремизм и информационная безопасность / Д. А. Мигун. – Минск : РИВШ, 2020. – 64 с.

К ВОПРОСУ КЛАССИФИКАЦИИ КИБЕРПРЕСТУПЛЕНИЙ В КИТАЙСКОЙ НАРОДНОЙ РЕСПУБЛИКЕ

ON THE ISSUE OF THE CYBERCRIMES CLASSIFICATION IN THE PEOPLE'S REPUBLIC OF CHINA

Малевский Н. А.
г. Минск,
Военная академия Республики Беларусь,
курсант факультета внутренних войск

Научный руководитель
Леднёва А. С.
г. Минск,
Военная академия Республики Беларусь,
доцент цикла государственно-правовых дисциплин
кафедры юридических дисциплин,
кандидат исторических наук, доцент

Аннотация: Рассматриваются наиболее распространенные виды киберпреступлений и меры уголовной ответственности за проникновение и вмешательство в работу информационных систем в КНР.

Ключевые слова: киберпреступление, противодействие, информационная безопасность, онлайн-мошенничество, кража виртуальных и реальных активов, кража аккаунтов, уголовная ответственность.

Annotation: The paper explores the most wide-spread forms of the cybercrimes and measures of criminal responsibility for penetrating and intervention in the work of informational systemsin the Republic of China.

Keywords: cybercrime, counteraction, information security, online-fraud, online-thefts, criminal responsibility.

Число Интернет-пользователей в современном Китае постоянно растет, причем с большой скоростью. Согласно информации, приведенной в опубликованном ЦРУ отчете World Factbook, уже 2008 году в КНР насчитывалось около 253 млн интернет-пользователей, что составляло 19 % населения страны [1, с. 34]. Наряду с удобством и большим объемом информации, которые обеспечивают цифровые технологии, китайские интернет-пользователи сталкиваются и с возросшим уровнем угроз киберпреступлений. В 2017 году в Управлении по коммуникациям провинции Хэнань сообщили, что в 2016 году 60 % Интернет-пользователей провинции, число которых составляет 79,6 млн человек, получили большое количество спама, а 58 % стали жертвами кражи аккаунта. Данные Network Hunt Platform (NHP), используемые Бюро общественной безопасности Пекина, свидетельствуют о том, что в 2016 году было получено 20623 заявлений об онлайн-мошенничествах, средний ущерб от которых составил 9471 юаней (приблизительно 1422 долл. США) [1, с. 34].

В конце 1990-х годов китайское правительство в ответ на рост киберпреступности стало разрабатывать и вводить новые законы и правила. В Уголовном кодекса Китайской Народной Республики в 1997 году появились новые статьи (286 и 287), предусматривающие наказание за компьютерные преступления. Тем не менее, незаконным было объявлено проникновение только в компьютерные системы, связанные с государственными учреждениями, оборонным ведомством, научными и технологическими организациями [2]. В 2009 и 2015 годах в ст. 285 было добавлено два новых раздела, которые расширяли список преступных деяний. 1 июня 2017 г. был принят «Закон о кибербезопасности» Китайской Народной Республики [3], который содержит гораздо больше положений, чем Уголовный кодекс, и уделяет большее внимание защите личной безопасности и целостности информационной инфраструктуры. «Закон о кибербезопасности» регламентирует сбор, хранение и обработку пользовательских данных, определяет обязанности всех сторон в обеспечении безопасности информационной инфраструктуры в контексте защиты национального «киберсуверенитета», то есть предприятий, финансовых учреждений и организаций, а также предусматривает наказание за их нарушение или невыполнение. В частности, «Закон о кибербезопасности» содержит определение «ключевой информации» и требует, чтобы вся ключевая

информация хранилась на серверах на территории Китая, а не за ее пределами. Организации, не соблюдающие это требование, подвергаются наказанию в виде приостановки деятельности, отзыва лицензии или денежного штрафа.

Подобно тому, что происходит на рынках США и Европы, нелегальный онлайн-рынок в Китае объединяет различные компоненты подпольной экономики, и такие, как логистика, операционная поддержка, торговля и коммуникации. Сегодня в условиях, когда группы, онлайн-форумы и чаты создают эффективные платформы для взаимодействия между людьми, преступники используют эти инструменты для создания подпольного рынка, где можно купить и продать нелегальные продукты и услуги, а также заключить незаконные трудовые соглашения. Предыдущие исследования выявили четыре производственно-сбытовые цепочки, существующие на нелегальном онлайн-рынке: кража реальных активов, кража виртуальных активов, взлом интернет-ресурсов и сервисов, хакерские технологии.

Кража реальных активов осуществляется, например, с помощью нелегального доступа к банковским или платежным онлайн-аккаунтам. Преступники похищают реальные активы, после чего их обналичивают. Типичная схема предусматривает два уровня – кражу и отмывание денег. Кража осуществляется с использованием различных приемов, таких как фишинг и/или внедрение вредоносного компьютерного программного обеспечения, например, троянов, чтобы получить информацию об аккаунте и учетные данные для входа. Отмывание денег осуществляется следующим способами: 1) средства переводятся на аккаунты преступника, часто зарегистрированные под фальшивыми именами, а их обналичивание производится через банкоматы, установленные в разных местах; 2) украденные активы используются для приобретения карточек магазинов или платежных карт, не позволяющих отследить информацию. Общие потери от краж реальных активов в Китае в 2016 году составили приблизительно 293 млрд долл. США.

Сетевые виртуальные активы. Вторая производственно-сбытовая цепочка связана с сетевыми виртуальными активами, такими как виртуальные валюты, оборудование и членство. За прошедшие полтора десятилетия китайский рынок онлайн-игр пережил стремительный рост, показав увеличение оборота от приблизительно 10 млн долл. США в 2001 году до примерно 27,3 млрд долл. в 2016 году. Большинство онлайн-игр предполагало систему виртуальных активов, таких как виртуальная валюта, виртуальные сокровища, оборудование и членство на сайте. Все это можно приобрести за реальные деньги или заработать за определенное время. Игроки сами быстро инициировали создание онлайн-рынка для торговли этими виртуальными активами.

Однако до 2008 году виртуальные активы в Китае оставались незащищенными. В этот период времени миллионы геймеров оставались беззащитными, а их виртуальные активы – уязвимыми, будучи легкой добычей для киберпреступников. Так же, как производственно-сбытовая цепочка кражи

реальных активов, производственно-сбытовая цепочка для виртуальных активов начиналась с получения информации об аккаунте и учетных данных для входа. После того, как аккаунт взламывался, преступники переводили находящиеся там активы на другой аккаунт или меняли пароль и настройки аккаунта для обеспечения контроля над ним. Захваченные виртуальные активы и/или аккаунты затем выставлялись на продажу на черном рынке. По имеющимся оценкам, убытки от этого вида преступной деятельности только в 2011 году достигли 1,42 млрд юаней (приблизительно 2134 млн долл. США), что составляет 3,18 % всего рынка онлайн-игр [1, с. 36].

Взлом Интернет-ресурсов и сервисов. Третья производственно-сбытовая цепочка связана со злоупотреблениями в сфере Интернет-ресурсов и услуг. Китайское правительство вкладывает огромные средства в создание и совершенствование информационной инфраструктуры в таких социально значимых сферах, как общественная безопасность, транспорт, здравоохранение образование. Не обеспеченное достаточной защитой развитие критически важных объектов информационной инфраструктуры способствует деятельности киберпреступников, особенно при отсутствии регулирующего контроля над киберпространством. Довольно трудно получить общую картину последствий злоупотреблений в сфере Интернет-ресурсов и услуг, тем не менее, по существующей оценке, в 2011 году ущерб, нанесенный ботнетами, троянами, заражениями смартфонов, загрузками вредоносного программного обеспечения или взломом серверов, составил 1,88 млрд юаней (приблизительно 282 млн долл. США) [1, с. 37].

Хакерские технологии. Последняя цепочка представляет собой поставку различных продуктов и услуг, облегчающих совершение хакерских атак. Она служит своего рода двигателем для подпольной экономической онлайн-деятельности, поскольку обеспечивает техническую базу, такую как инструменты взлома и подготовка хакеров, для всех остальных производственно-сбытовых цепочек. Хакеры разрабатывают вредоносное программное обеспечение и распространяют его среди других киберпреступников. Кроме этого, они организуют обучение новых игроков, разрабатывая для них письменные инструкции, осуществляя групповые атаки и обеспечивая техническую поддержку.

Киберпреступники играют различные роли в производственно-сбытовых цепочках и входящих в них транзакциях. Например, хакера могут нанять для разработки вредоносного программного обеспечения и поставки его агенту, который затем продает его клиентам. Продукты и услуги, поставляемые хакером, потенциально способны помочь покупателям создать возможности для будущей киберпреступной деятельности.

В уголовном праве КНР различаются пять видов преступлений, связанных с компьютерами, в том числе незаконное проникновение, подчинение контролю и вывод из строя компьютерных систем, незаконное получение компьютерных

данных и намеренное создание или распространение вредоносных программ. Добавленные в 1997 году ст. 285 и 286 предусматривают ответственность за проникновение и вмешательство в работу государственных компьютерных систем и компьютерных систем, связанных с национальной обороной и научно-технологической сферой, а ст. 287 – за преступления, совершенные с использованием компьютера и сети Интернет, например, онлайн-мошенничество и онлайн-кражи. Благодаря быстрому развитию модели противодействия киберпреступности, в 2009 году ст. 285 была дополнена положениями о незаконном проникновении в другие типы компьютерных систем, не перечисленные в ее редакции 1997 года. В 2015 году ст. 285 вновь была расширена: в нее включили пункт об ответственности сетевых провайдеров, не обеспечивших безопасность сети, а также лиц, сознательно оказывающих техническую или материальную поддержку киберпреступникам.

Несмотря на то, что действующее законодательство охватывает широкий круг киберпреступной деятельности, остаются некоторые вопросы, связанные с правовым механизмом противодействия киберпреступности в Китае. Например, некоторые пункты ст. 286 содержат положения, толкование которых может вызвать затруднения и путаницу, в особенности потому, что во многих случаях современные киберпреступления начинаются с создания и распространения компьютерных вирусов, которые затем вызывают нарушения в работе системы, что, в свою очередь, ведет к потере информации и уничтожению приложений в зараженной системе.

Таким образом, киберпреступность в Китае как результат разнообразных враждебных действий становится источником серьезных проблем, которые угрожают государственному сектору, коммерческой деятельности, инновациям, экономическому росту, появлению новых услуг и продуктов. Китайское руководство понимает, что решение проблем кибербезопасности требует организованных коллективных усилий и предприняло меры по разработке национальной киберстратегии, важное место в которой отведено ужесточению правовой ответственности.

Список цитированных источников

1. Услуги по обеспечению кибербезопасности / Борьба с преступностью за рубежом. – 2019. – № 2. – С. 34–40.

2. Уголовный кодекс Китая / под ред. А. И. Коробеева, А. И. Чучаева, пер. с кит. Хуан Даосю. – М. : ООО «Юридическая фирма Контракт», 2017. – 256 с.

3. Закон о кибербезопасности КНР [Электронный ресурс] // ИМЭМО РАН. – Режим доступа: https://www.imemo.ru/news/events/text/knr-zakon-o-kiberbezopasnosti-prinyat – Дата доступа: 17.05.2022.

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

LEGAL SUPPORT OF CYBER SECURITY IN THE REPUBLIC OF BELARUS

Савченко Д. Г.
г. Гомель,
Гомельский государственный университет
имени Франциска Скорины,
студент юридического факультета

Научный руководитель
Копыткова Н. В.
г. Гомель,
Гомельский государственный университет
имени Франциска Скорины,
доцент кафедры гражданско-правовых дисциплин,
кандидат юридических наук, доцент

Аннотация: В работе рассматриваются аспекты обеспечения безопасности в сфере IT-пространства. Анализируется деятельность государственных органов по противодействию преступности в киберпространстве и нормы законодательства. Предлагаются меры по предотвращению угроз в области информационной безопасности.
Ключевые слова: национальная безопасность, информационная безопасность, информационное пространство, интернет, угроза.

Annotation: The paper discusses aspects of security in the IT-space. The activities of state bodies to combat crime in cyberspace and the norms of legislation are analyzed. Measures are proposed to prevent threats in the field of information security.
Keywords: national security, information security, information space, internet, threat.

В современном мире количество факторов риска постоянно возрастает. Военные конфликты, применение принудительных мер ограничительного характера, террористическая угроза являются современными вызовами национальной безопасности любого государства, и Республика Беларусь не является исключением. Напротив, исходя из своего геополитического статуса, она находится не только в центре Европы, но и событий, происходящих на ее территории, чем, в том числе обуславливается необходимость повышенной готовности к отражению угроз различного характера, способных причинить вред национальным интересам. Также следует обращать внимание на вероятность проникновения чуждой идеологии, нарушения норм и ценностных ориентиров изнутри государства, что носит наиболее опасный характер для национальной безопасности вследствие высокой латентности.

Информация всегда представляла особый интерес и ценность, как у потребителей, распространителей, так и у заказчиков. Исходя из того, что с проникновением IT-технологий практически на всех континентах и во всех

сферах жизни общества информация стала инструментом влияния на процессы, протекающие в том или ином обществе.

Используя социальные сети, мессенджеры, различные видеохостинги возможно оперативно оказывать массированное воздействие на массовое сознание путем распространения тех или иных данных, материалов фотосъемки, сопровождающихся уже готовыми умозаключениями в виде текстовых надписей, лишающих потребителя такой информации самостоятельного анализа ситуации, допущения сомнений в объективности представленной информации.

Как свидетельствуют данные глобального отчета Digital 2020, «на начало 2020 года более 4,5 миллиардов людей пользуются интернетом, а аудитория социальных сетей перевалила за отметку в 3,8 миллиарда. Почти 60 % мирового населения уже онлайн. Сегодня более 5,19 миллиардов человек пользуются мобильными телефонами. Среднестатистический пользователь проводит в интернете 6 часов 43 минуты каждый день. Если оставить около 8 часов в сутки на сон, это значит, что сейчас более 40 % времени бодрствования мы проводим в интернете» [1].

Согласно данным отчета по статистике интернета Global Digital 2022, «больше чем две трети (67,1 %) людей в мире сегодня пользуются мобильными телефонами, к началу 2022 года число уникальных пользователей мобильных достигло 5,31 миллиарда. Сначала прошлого года прирост составил 95 млн пользователей». В январе 2022 года во всем мире насчитывалось 4,62 млрд пользователей социальных сетей – 58,4 % от общей численности населения мира. Мировая аудитория соцсетей увеличилась больше чем на 10 %, так за 2021 год к социальным сетям присоединились 424 миллиона новых пользователей [2].

Можно с большой долей вероятности предположить, что в случае появления в интернет-пространстве какой-либо информации деструктивного характера, она будет воспринята значительной частью населения, в том числе и молодежью с не устоявшимися воззрениями и принципами, которые вместо того, чтобы строить будущее своей страны, будут его всячески тормозить или же вовсе – разрушать, а это в совокупности с факторами международной напряженности и кризиса является прямой угрозой национальным интересам и безопасности государства.

Исходя из положений Концепции национальной безопасности Республики Беларусь (далее – Концепции) можно заключить, что национальная безопасность является многосоставным понятием, включающим в себя, в том числе, и информационную безопасность. Согласно ст. 4 Концепции, под информационной безопасностью понимается «состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере» [3].

В связи с распространением информационных технологий и использованием сети Интернет в противоправных целях (наркобизнес, мошенничество, координация незаконных массовых мероприятий и т. п.), в Республике Беларусь создана сеть специализированных органов и подразделений, задействованных в сфере обеспечения информационной безопасности. В частности, этими вопросами занимается Управление «К» Министерства внутренних

дел Республики Беларусь, деятельность которого направлена на защиту интересов общества и государства от преступных и иных противоправных посягательств, осуществлямых посредством информационных технологий. Один из векторов деятельности Комитета государственной безопасности направлен на обеспечение национальной безопасности Республики Беларусь в научно-технологической и информационной сферах. При Президенте Республики Беларусь создан Оперативно-аналитический центр (ОАЦ), который осуществляет регулирование деятельности по обеспечению защиты информации, содержащей сведения, составляющие государственные секреты Республики Беларусь или иные сведения, охраняемые в соответствии с законодательством, от утечки по техническим каналам, несанкционированных и непреднамеренных воздействий. Координацию деятельности республиканских органов государственного управления, организаций в сферах научно-технической и инновационной деятельности, а также охраны прав на объекты интеллектуальной собственности осуществляет Государственный комитет по науке и технологиям. Совет Безопасности Республики Беларусь разрабатывает предложения по реформированию существующих или созданию новых органов, обеспечивающих безопасность личности, общества, определяет основные направления стратегии обеспечения национальной безопасности, организует эффективно функционирующую систему обеспечения безопасности страны.

Законодательство Республики Беларусь в сфере информатизации и защиты информации находится на достойном уровне и постоянно совершенствуется. Закон Республики Беларусь 2008 года «Об информации, информатизации и защите информации» регулирует отношения, возникающие при поиске, получении, передаче, сборе, обработке, накоплении, хранении, распространении, предоставлении и пользовании информацией. Указанным законом установлены правила по созданию и использованию информационных технологий, информационных систем и информационных сетей. Кроме того, закон устанавливает требования по организации и обеспечению защиты информации [4].

В целях совершенствования правового регулирования порядка взаимодействия операторов электросвязи с органами, осуществляющими оперативно-розыскную деятельность, Указом Президента Республики Беларусь в 2010 году утверждено Положение «О порядке взаимодействия операторов электросвязи с органами, осуществляющими оперативно-розыскную деятельность» [5]. Техническим регламентом Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» устанавливаются требования к средствам защиты информации в целях обеспечения национальной безопасности, а также предупреждения действий, вводящих в заблуждение потребителей относительно назначения и качества средств защиты информации [6]. Ряд приказов и постановлений принят Оперативно-аналитическим центром при Президенте Республики Беларусь, среди которых особое место занимает совместное Постановление ОАЦ и Министерства связи и информатизации Республики Беларусь 2015 года «Об утверждении положения о порядке ограничения доступа к информа-

ционным ресурсам (их составным частям), размещенным в глобальной компьютерной сети Интернет» [7].

Наличие достаточной законодательной базы и системы правоохранительных органов способствует снижению киберпреступлений в Беларуси. По заявлению заместителя председателя Следственного комитета Республики Беларусь А. Васильева, число киберпреступлений в Беларуси в прошлом году снизилось почти вдвое. «Если в 2020 году следователями возбуждено 25 571 уголовное дело, то в 2021 году – 15 503. Что касается цифровых показателей первого квартала 2022 года, то нами зарегистрировано вдвое меньше преступлений по ст. 212 (хищение путем модификации компьютерной информации) Уголовного кодекса – 2833. За аналогичный период 2021 года было установлено 5734 таких преступления» [8]. Однако, несмотря на эффективную работу правоохранительных органов, мошенники продолжают совершать хищения путем модификации компьютерной информации и несанкционированного доступа.

На наш взгляд, наибольшее внимание должно уделяться сфере общегосударственных информационных и телекоммуникационных систем. Это, прежде всего, информационные ресурсы, содержащие конфиденциальную информацию; автоматизированные системы управления, системы связи и др.

На современном этапе развития общества, когда возрастает объем информации и обеспечивается свободный доступ к информационным ресурсам, влияние информации на состояния национальной безопасности будет возрастать. В Республике Беларусь должны быть разработаны действенные меры по предотвращению угроз в области информационной безопасности.

В целях предотвращения наиболее негативных проявлений информационной агрессии необходимо усиленно заниматься патриотическим воспитанием молодого поколения в направлении формирования устойчивого желания отстаивать интересы государства, повышения уровня грамотности в сфере использования IT-технологий.

Существует необходимость повышения эффективности противодействия преступности в сфере интернет-пространства путем информирования общественности о данных фактах.

Список цитированных источников

1. Глобальная статистика интернета на 2020 год [Электронный ресурс] // WebCanape. – Режим доступа: https://www.web-canape.ru/business/internet-2020-globalnaya-statistika-i-trendy. – Дата доступа: 14.04.2022.

2. Вся статистика интернета и социальных сетей на 2022 год [Электронный ресурс] // WebCanape. – Режим доступа: https://www.web-canape.ru/business/statistika-interneta-i-socsetej-na-2022-god-cifry-i-trendy-v-mire-i-v-rossii. – Дата доступа: 19.04.2022.

3. Об утверждении Концепции национальной безопасности Республики Беларусь [Электронный ресурс] : Указ Президента Респ. Беларусь, 9 нояб. 2010 г., № 575 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

4. Об информации, информатизации и защите информации [Электронный ресурс] : Закон Респ. Беларусь от 10 нояб. 2008 г. № 455-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

5. Об утверждении Положения о порядке взаимодействия операторов электросвязи с органами, осуществляющими оперативно-розыскную деятельность [Электронный ресурс] : Указ Президента Респ. Беларусь в 2010 г. № 129 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

6. Об утверждении технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY) [Электронный ресурс] : постановление Совета Министров Респ. Беларусь, 15 мая 2013 г., № 375 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

7. Об утверждении положения о порядке ограничения доступа к информационным ресурсам (их составным частям), размещенным в глобальной компьютерной сети Интернет [Электронный ресурс] : постановление ОАЦ и Министерства связи и информатизации Респ. Беларусь, 19 фев. 2015 г., № 6/8 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

8. Число киберпреступлений снизилось почти вдвое. Зампред СК о тенденциях в области IT-преступлений [Электронный ресурс] // World News LLC. – Режим доступа: https://www.belta. by/society/view/chislo-kiberprestuplenij-snizilos-pochti-vdvoe-zampred-sk-o-tendentsijah-v-oblasti-it-prestuplenij-496880-2022. – Дата доступа: 20.04.2022.

ЗАКОНОДАТЕЛЬНОЕ РЕГУЛИРОВАНИЕ ЦИФРОВЫХ ПЛАТФОРМ КАК НАПРАВЛЕНИЕ ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

LEGAL DIGITAL PLATFORM REGULATION AS THE DIRECTION OF NATIONAL INFORMATION SECURITY

Сержантов Д. О.
г. Минск,
Военная академия Республики Беларусь,
курсант факультета внутренних войск

Научный руководитель
Леднёва А. С.
г. Минск,
Военная академия Республики Беларусь,
доцент цикла государственно-правовых дисциплин
кафедры юридических дисциплин,
кандидат исторических наук, доцент

Аннотация: Рассматривается развитие законодательства ряда иностранных государств по регулированию деятельности цифровых платформ и их ответственность за неисполнение установленных требований.

Ключевые слова: цифровая платформа, саморегулирование, законодательное регулирование, иностранные государства, информационная безопасность.

Annotation: The development of legislation in some foreign states of the digital platforms activities and its responsibility on non-observance of necessary demands are examined.

Keywords: digital platforms, self-regulation, legal regulation, foreign states, information security.

Сегодня инновационные технологии являются неотъемлемой частью нашей жизни. С одной стороны, они предоставляют человечеству значительные преимущества, но с другой – создают колоссальную уязвимость, так как в любой стране развитие и стабильное функционирование национальной экономики напрямую зависит от работы информационной структуры. В конце XXI в. киберугрозы приобрели уже стратегическое значение, и потому правовое обеспечение информационной безопасности приобретает государственную значимость. Представляется весьма актуальным проанализировать, как решаются эти вопросы в ряде государств мира.

Цифровая платформа – это основной создатель цифровой системы, она определяет правила игры, формирует добавленную стоимость, создает новые отношения и трансформирует старые. В этих условиях все чаще звучат слова о том, что мы столкнулись с новым феноменом – цифровыми государствами, наличие которых диктует новые требования к безопасности, к регулированию и к условиям существования всех традиционных институтов: государства, бизнеса, гражданского общества, отдельной личности.

Несмотря на то, что доходы международных цифровых платформ сопоставимы с бюджетами отдельных государств и что влияние таких платформ сопоставимо с влиянием властных структур, представляется маловероятной возможность признания их суверенитета как полноправных субъектов международного публичного права, потому что всегда за любой цифровой платформой стоит оператор (технологическая компания) – юридическое лицо, за которым, в свою очередь, стоят конкретные бенефициары цифрового бизнеса.

Цифровые платформы как бизнес создавались в период отсутствия каких-либо ограничений и требований к данной сфере деятельности и максимально извлекли свою выгоду из-за отсутствия границ сети интернет, позволяющего зарабатывать в одних странах и платить налоги в другой, оказывать влияние на экономику и политику одних государств, будучи резидентами других.

В результате национальные государства, традиционный бизнес и граждане столкнулись со следующими вызовами со стороны цифровых платформ: неравенство платформ и пользователя; уход платформ от юрисдикции государств; монополия платформ на рынке и цифровых услуг, и данных; сверхприбыли без налоговых обязательств.

В регулировании данного сегмента информационного пространства можно выделить два периода: первый датируется 2017 – 2019 гг.; второй – 2020 – 2021 гг.

Первый период характеризуется преобладанием саморегулирования и необязательного следования правилам в качестве основного подхода регулирования деятельности цифровых платформ в связи с отсутствием действенных механизмов принуждения иностранных цифровых платформ к выполнению установленных требований. 19 мая 2015 г. Европейской комиссией приняты Принципы улучшения саморегулирования и совместного регулирования [1]. Документ призван содействовать в странах Евросоюза открытости принятия решений в целях развития экономики для улучшения социальной сферы и защиты природы. 1 марта 2018 г. принимается более обстоятельный документ – «Рекомендации Европейской комиссии о мерах эффективного реагирования на нелегальный контент в сети интернет», в котором изложены оперативные меры саморегулирования с целью ускоренного обнаружения и удаления незаконного контента в сети интернет, укрепления сотрудничества между организациями и правоохранительными органами, а также повышения прозрачности данной деятельности и правовых гарантий для граждан [2].

В Великобритании с 2008 года было принято не менее 15 добровольных правил ведения деятельности интернет-платформами. Так, согласно отчету «Регулирование в цифровом мире», саморегулирование – важнейший элемент функционирования цифровой среды, особенно это касается платформ социальных сетей, публикующих авторский контент множества пользователей. Предполагалось учреждение национального независимого регулятора интернет-контента с широкими полномочиями, действующего на основании норм, установленных правительством, а также имеющего полномочия для наложения широкого спектра взысканий на компании-нарушители [3].

В Соединенных Штатах Америки рынок провайдеров интернет-услуг является самым крупным в мире. Но и здесь в первом десятилетии XXI в. государство воздерживалось от чрезмерного регулирования сферы онлайн-услуг. Поэтому саморегулирование компаний играло огромную роль в их функционировании. Крупные интернет-платформы, такие, как Facebook и Twitter, получали даже больше прав, благодаря своим условиям обслуживания и правилам пользования сервисом. Например, удаление недостоверной рекламы, выражений ненависти, публикаций с экстремизмом или сексуальной эксплуатацией людей или мошеннических объявлений не было нарушением Первой поправки в Конституцию США о свободе слова и осуществлялось на базе саморегулирования платформ. Интернет-провайдеры решали, что можно и что нельзя публиковать в сети интернет.

Второе десятилетие XXI в. отмечено началом перехода к государственному регулированию информационного пространства. Зарубежные государства, даже те, которые больше всех говорили о саморегулировании, начинают разрабатывать нормативные акты, которые устанавливают правовые требования к цифровым платформам в целях обеспечения интересов пользователей, государства, общества, национального бизнеса, осуществляя их

выполнение конкретными мерами принуждения (в том числе экономическими). 15 декабря 2020 г. Европейский союз принимает Закон о цифровых услугах, согласно которому все онлайн-посредники, предлагающие свои услуги на едином рынке, независимо от того, созданы они в ЕС или за его пределами, должны будут соблюдать новые правила. Особенно усиливается общественный надзор за онлайн-платформами, в частности, за платформами, охватывающими более 10 % населения ЕС.

В США Закон о правилах коммуникации [4] предписывает, что ни один поставщик или пользователь интерактивного компьютерного сервиса не должен рассматриваться как издатель или спикер любой информации, предоставленной другим поставщиком информационного контента. В соответствии с законом, американская компания, в отношении которой в иностранном государстве принято судебное решение, может получить приказ от американского суда, в котором говорится, что решение иностранного суда можно не выполнять.

Правительство Великобритании также предложило на рассмотрение и принятие комплексный законопроект, который заставит компании брать на себя ответственность за безопасность своих пользователей. Введение закона о безопасности в интернете (Online Safety Bill – OSB) [5] было спровоцировано смертью 14-летней Молли Рассел, покончившей с собой после просмотра онлайн-изображений членовредительства, и ее родители обвинили Instagram в том, что он частично виноват. Это заставило министров потребовать от компаний социальных сетей взять на себя больше ответственности за вредоносный онлайн-контент. Данный законопроект будет применяться к любым компаниям, которые предоставляют услуги пользователям из Великобритании и Австралии, независимо от того, где они находятся в мире. В частности, законопроект будет распространяться на социальные сети, платформы видеохостинги, мессенджеры, видеоигры, позволяющие взаимодействовать с другими игроками, и платформы электронной коммерции. Все компании, попадающие под действие законопроекта, должны будут предпринять соразмерные шаги для борьбы с незаконным контентом и деятельностью, а также для защиты детей от вредоносного контента.

На азиатском континенте, кроме Китая, который отношения в информационном пространстве жестко регулирует Уголовным кодексом, в Индии обязанности организаций и продавцов, вовлеченных в деятельность платформ электронной коммерции маркетплейс, были определены Законом об электронной коммерции 2019 и соответствующими подзаконными актами [6], а с 2021 года цифровые платформы обязаны раскрывать первоисточник противоправных постов по запросу регулятора или решению суда. В стране вводится трехуровневая система для урегулирования претензий к онлайн-платформам. Во-первых, администрацией соцсетей должен быть назначен представитель, имеющий индийское гражданство; во-вторых, рассмотрение претензий к цифровым площадкам, составление рекомендации для работы социальных сетей отнесено к полномочиям органа общественного контроля,

который может быть возглавлен бывшим судьей или другим авторитетным человеком. Третий уровень контроля закреплен за Министерством информации Индии.

В Турции на уровне закона цифровым платформам предписано оперативно удалять незаконный контент, а также открыть в стране официальные представительства и хранить данные пользователей на территории страны. При этом штрафы не рассматриваются как единственная санкция за данные нарушения. Невыполнение требований влечет за собой запрет рекламодателям размещать рекламу на платформах, нарушающих требования турецких законов. Кроме того, закон предполагает снижение трафика на 50 % после трех месяцев запрета рекламы и на 90 %, если не соблюдено обязательство в течение 30 дней после уменьшения пропускной способности на 50 %.

Список цитированных источников

1. Мхитарян, Ю. И. Государственная политика развития предпринимательства в сфере повышенного риска [Электронный ресурс] / Ю. И. Мхитарян // Электронный научный журнал «Век качества». – 2018. – № 4. – С. 7–22. – Режим доступа: http://www.agequal.ru/ pdf/2018/418001.pdf. – Дата доступа: 17.05.2022.
2. Шугуров, М. В. Правовая политика Европейского союза в сфере противодействия контрафакту в условиях Единого цифрового рынка [Электронный ресурс] / М. В. Шугуров // Международное право. – 2021. – № 4. – Режим доступа: https:// nbpublish.com/library_read_article.php?id=36846. – Дата доступа: 17.05.2022.
3. Ахмадзода, Н. С. Зарубежный опыт государственного регулирования в условиях цифровой экономики [Электронный ресурс] / Н. С. Ахмадзода // Мир экономики и управления. – 2021. – № 21 (1). – С. 104–118. – Режим доступа: https://doi.org/ 10.25205/2542-0429-2021-21-1-104-118. – Дата доступа: 17.05.2022.
4. Ляруш, В. Русскоязычные пациенты в США: модель коммуникации [Электронный ресурс] / В. Ляруш // Международные отношения. – 2009. – № 1. – Режим доступа: https://cyberleninka.ru/article/n/russkoyazychnye-patsienty-v-ssha-model-kommunikatsii-1. – Дата доступа: 17.05.2022.
5. Ромашкина, Н. П. Вооружения без контроля: современные угрозы международной информационной безопасности [Электронный ресурс] / Н. П. Ромашкина // ИМЭМО РАН. – 2018. – № 2 (55). – Режим доступа: https://cyberleninka.ru/article/ n/vooruzheniya-bez-kontrolya-sovremennye-ugrozy-mezhdunarodnoy-informatsionnoy-bezopasnosti – Дата доступа:17.05.2022.
6. Ерёмкин, М. А. Правовые аспекты регулирования налогообложения электронной коммерции: опыт Индии [Электронный ресурс] / М. А. Ерёмкин // Налоги и налогообложение. – 2019. – № 12. – Режим доступа: https://cyberleninka.ru/article/n/ pravovye-aspekty-regulirovaniya-nalogooblozheniya-elektronnoy-kommertsii-opyt-indii. – Дата доступа: 17.05.2022.

УНИФИКАЦИЯ ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ МЕЖДУНАРОДНЫХ КИБЕРПРЕСТУПЛЕНИЙ

UNIFICATION OF LEGISLATION IN THE FIELD OF INTERNATIONAL CYBERCRIME

Солодкая В. А.
г. Минск,
Белорусский государственный
экономический университет,
студентка факультета права

Научный руководитель
Пехота Т. М.
г. Минск,
Белорусский государственный
экономический университет,
ассистент кафедры теории и истории права

Аннотация: В данной работе проанализирована проблема отсутствия унифицированного международного законодательства в сфере киберпреступлений, а также приведен перечень мер рекомендательного характера для решения данной проблемы.

Ключевые слова: унификация, киберпреступность, кибербезопасность, убежища для киберпреступников, международные договоры, региональные правовые акты, национальные правовые акты.

Annotation: The article analyzes the problem of the lack of unified international legislation in the field of cybercrime, and provides a list of recommendatory measures to solve this problem.

Keywords: unification, cybercrime, cybersecurity, havens for cybercriminals, international treaties, regional legal acts, national legal acts.

Во время быстроразвивающегося информационного общества все чаще стал возникать вопрос о борьбе с киберпреступностью. Сегодня национальная безопасность государств в значительной степени зависит от обеспечения информационной безопасности. В современном мире все сферы жизнедеятельности находятся в прямой зависимости от работ вычислительных и информационных сетей, отчего те попадают в круг наиболее уязвимых. Очень важно понимать глобальный характер кибератак, т. к. на сегодняшний день они посягают не только на частные структуры, но и на государственные органы. Так, по данным международной службы по обеспечению безопасности от киберугроз Symantec Security, в мире каждую секунду подвергаются кибератаке 12 человек, а ежегодно в мире совершается около 556 млн киберпреступлений, ущерб от которых составляет более 100 млрд дол. США [1, с. 46].

Одной из наиболее актуальных проблем в области кибербезопасности является отсутствие унифицированного международного законодательства, которое позволило бы урегулировать данную сферу и сделало бы ее безопаснее. Сегодня национальное законодательство различных государств затрагивает

вопросы кибербезопасности. Однако существуют страны, где отсутствуют законы, регулирующие исследуемую сферу. В связи с этим появляется проблема: в таких государствах создаются безопасные убежища для кибер-преступников. Например, не представлялось возможным привлечь к уголовной ответственности гражданина Филиппин, создавшего вредоносную программу «LOVEBUG», т. к. на момент совершения преступления на Филиппинах отсутствовал закон о киберпреступности. Как видим, безопасные убежища для киберпреступников могут создаваться в случае, если законы о киберпреступности не соблюдаются должным образом, и/или если существуют расхождения в законодательстве разных стран в рассматриваемой области [2]. Исходя из данной проблемы, можно сделать вывод, что для ее решения необходимо эффективное международное сотрудничество и, как следствие, согласованность национального законодательства государств. В настоящее время различия по вопросам киберпреступности в национальном законодательстве большинства государств можно преодолеть путем унификации законов и усиления международного сотрудничества.

Сегодня ввиду прямой зависимости данных преступлений с вычислительными и информационными сетями, а также невозможности использования правовых инструментов, применяемых к правонарушениям в физическом мире, создать международный правовой акт, обеспечивающий кибербезопасность, представляется затруднительным. Большую роль в регулировании данного вопроса играют законодательные акты различных уровней, в особенности региональные. Так, национальные законы в области кибербезопасности зачастую содействуют международному сотрудничеству. Примером таких национальных законов может послужить Закон № 14 от 2014 года в Катаре, в котором предусматривается международное сотрудничество в сфере кибербезопасности.

Также большую роль играют региональные договоры в сфере кибербезопасности. К ним относятся:

– Соглашение о сотрудничестве в области обеспечения международной информационной безопасности, принятое Шанхайской организацией сотрудничества в 2010 году.

– Конвенция Африканского союза о кибербезопасности и защите персональных данных 2014 года.

– Конвенция Лиги арабских государств о борьбе с преступлениями в области информационных технологий, принятая Лигой арабских государств в 2010 году.

Однако наиболее значимым примером международных договоров в области защиты кибербезопасности является Конвенция Совета Европы о киберпреступлениях 2001 года. Основные задачи данной Конвенции: 1) гармонизация элементов внутреннего законодательства, касающихся правонарушений и соответствующих положений в сфере киберпреступлений; 2) установление полномочий и процедур, необходимых для расследования и судебного преследования за такие правонарушения, а также за другие правонарушения, совершенные при помощи компьютерных систем; для сбора доказательств по уголовным преступлениям в электронной форм; 3) разработка механизмов быстрого и эффективного международного сотрудничества [3].

Из этого следует, что существуют нормы различного уровня, регулирующие киберпреступность. Унификация изучаемых норм будет содействовать обеспечению международного сотрудничества в данной сфере, созданию условий для сбора и обмена доказательств о киберпреступности на международном уровне, исключит возможность создания убежищ для киберпреступников, а также возможность избежать наказания.

На основании вышеизложенного можно сделать вывод о необходимости принятия мер рекомендательного характера, которые бы поспособствовали усилению международной кибербезопасности. К данным мерам можно отнести:

– создание специализированных органов, деятельность которых была бы направленна на расследование международных киберпреступлений;

– меры, направленные на согласование норм различных государств в вопросах кибербезопасности (в особенности о расследовании и преследовании киберпреступлений);

– разработку различных методов сотрудничества в области обмена и путей сбора информации среди международных агентств в сфере расследований киберпроисшествий;

– создание в структуре Интерпола специального подразделения по борьбе с киберпреступностью.

Подводя итоги вышесказанного отметим, что на данный момент существуют международные договоры, региональные и национальные правовые акты, различающиеся по своему тематическому содержанию, географическому охвату и сфере применения. Данные различия создают трудности в преследовании киберпреступников, что приводит к безнаказанности в области киберпреступлений. Из этого следует необходимость развития совместных действий специалистов в сфере информационных технологий и ученых-юристов, которые будут направлены на борьбу с киберпреступностью и разработку унифицированного законодательства. Таким образом, с учетом всей опасности киберпреступлений и отсутствия международного акта, регулировавшего исследуемую сферу, можно резюмировать актуальность и необходимость унификации законодательства и международного сотрудничества в области кибербезопасности.

Список цитированных источников

1. Карпова, Д. Н. Киберпреступность: глобальная проблема и ее решение / Д. Н. Карпова // Власть. – 2015. – Т. 22, № 8. – С. 46–50.

2. Проект доклада УНП ООН «Всестороннее исследование проблемы киберпреступности» (2013) [Электронный ресурс] // UNODC. – Режим доступа: https://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME STUDY_210213.pdf. – Дата доступа: 01.05.2022.

3. Council of Europe, Convention on Cybercrime, European Treaty Series № 185 (Budapest, 23 November 2001) [Electronic resource] // Council of Europe. – Mode of access: http://conventions.coe.int/Treaty/en/Reports/Html/185.htm. – Date of access: 01.05.2022.

СОДЕРЖАНИЕ ПРАВА НА ПРИВАТНОСТЬ В ИНТЕРНЕТЕ

CONTENT OF THE RIGHT TO PRIVACY ON THE INTERNET

Терех Д. А.
г. Гродно,
Гродненский государственный университет
имени Я. Купалы, студент юридического факультета

Научный руководитель
Миськевич А. Ю.
г. Гродно,
Гродненский государственный
университет имени Я. Купалы,
старший преподаватель кафедры
теории и истории государства и права,
магистр юридических наук

Аннотация: В данной статье рассматривается тесная связь между правом на приватность и правом на неприкосновенность частной жизни. Также определено содержание права на приватность в сети Интернет.
Ключевые слова: приватность, право на неприкосновенность частной жизни, приватное пространство, информационная сфера.

Annotation: This article discusses the close relationship between the right to privacy and the right to privacy. The content of the right to privacy on the Internet is also defined.
Keywords: privacy, right to privacy, private space, information sphere.

Интернет и его общедоступность изменили привычные процессы в обществе. Появляются новые вопросы, требующие специфического правового регулирования. Нарушение права на приватность в Интернете – одна из наиболее актуальных тем. Исходная дилемма заключается в необходимости обеспечить, с одной стороны, права человека на приватность, свободу от слежки, свободное распространение информации, с другой стороны – защиту общественных и государственных интересов от угроз, связанных со злоупотреблениями этими правами.

Существует тесная связь между правом на приватность и правом на неприкосновенность частной жизни. Для того, чтобы разобраться, необходимо ознакомиться с содержанием данных прав.

Говоря о приватности, мы не имеем в виду просто сокрытие каких-либо фактов. Речь идет о праве на самоопределение, независимость и целостность. Если попытаться определить содержание приватности, то оно для каждого лица будет свое собственное. В информационной сфере круг данных, которое лицо пытается сделать недоступным для публики, всегда различен. Например, один человек не будет скрывать, что он ВИЧ инфицирован, может давать об этом интервью журналисту, а иной не сообщит об этом даже близким друзьям. Как следствие, границы приватности всегда индивидуальны.

Право человека на неприкосновенность его частной жизни в общем понимании представляет собой некоторую автономность индивида от вмешательства в его частную жизнь третьих лиц, включая государство, органы государственной власти и должностных лиц [1, с. 107].

Неприкосновенность частной жизни – одно из фундаментальных прав, которым наделен каждый гражданин. Его основное содержание составляет указание на определенную автономность любого человека от вмешательства со стороны третьих лиц, в том числе государства в лице его уполномоченных органов и должностных лиц, в его частную жизнь, которая, в свою очередь, должна обеспечиваться эффективной системой государственно-правовых средств и мер, нацеленных на охрану прав и свобод человека в области личной, семейной и интимной жизни, а также недопущение их нарушения.

Как видно из анализа содержания рассмотренных выше прав, данные права имеют идентичное содержание. Стоит отметить, что в русском языке понятие «приватность» идентично выражению «неприкосновенность частной и личной жизни». То есть, частная и личная жизнь – это и есть приватность.

По нашему мнению, приватность является более широким понятием, чем конфиденциальность, поскольку в его содержание включаются право на свободу от вторжения, право оставаться автономным и право управлять использованием информации о себе. Право индивида на конфиденциальность своих данных подразумевает лишь защиту персональных данных, чаще всего в виде защиты таких данных от неразрешенного раскрытия третьей стороне.

В интернете право на приватность включает в себя следующее:

Право на виртуальную личность. Каждый человек имеет право на виртуальную личность. Виртуальная человеческая личность (т. е. идентификация личности в информационных системах) неприкосновенна. Цифровые подписи, имена пользователей, пароли, PIN-коды не должны использоваться или изменяться другими лицам без согласия владельца. Тем не менее, право на виртуальную личность не должно быть использовано в ущерб другим.

Право на анонимность и использование шифрования. Каждый человек имеет право общаться анонимно в интернете. Каждый человек имеет право на использование технологии шифрования для обеспечения безопасного, частного и анонимного общения в интернете.

Свобода от слежки. Каждый индивид имеет право свободно общаться без произвольного наблюдения или перехвата информации, или угрозы наблюдения или перехвата информации.

Свобода от клеветы. Никто не должен подвергаться незаконным посягательствам на его честь и репутацию в интернете. Каждый человек имеет право на защиту от таких посягательств.

Право на приватность в Интернете –одно из самых значимых прав личности. В интернете право на приватность включает в себя право на виртуальную личность, право на анонимность и использование шифрования, свободу от слежки, свободу от клеветы.

По нашему мнению, несмотря на широкое использование понятие права на приватность, остается неосознанным. Для того, чтобы права человека были соблюдены в интернет-среде, все заинтересованные стороны должны осознать смысл таких прав, потребности и возможности их реализации в виртуальной среде и предпринять действия по их обеспечению [2, с. 45].

Вместе с тем, без реализации данного права на современном этапе едва ли возможно построение правового государства и нормальное функционирование общества. В век информационных технологий человек перестает чувствовать себя защищенным и становится объектом слежки, прослушивания и вмешательства в наиболее сокровенные сферы бытия, ранее недоступные никому, кроме самой личности.

Таким образом, можно сделать вывод о том, что наличие приватного пространства является предпосылкой безопасности, свободы и самоуважения. Право на приватность в Интернете требует правовой охраны и защиты, поскольку возможность легкого распространения информации создает дополнительные угрозы интересам человека. Нормальные отношения в обществе возможны только при условии уважения права на приватность.

Список цитированных источников

1. Янкин, А. Н. Международно-правовые средства защиты права на неприкосновенность частной жизни / А. Н. Янкин // Северо-Кавказский юрид. вестник. – 2017. – № 4. – С. 107–112.
2. Арешев, А. Г. Персональные данные в структуре информационных ресурсов: Основы правового регулирования / А. Г. Арешев, И. Л. Бачило, Л. А. Сергиенко ; отв. ред. д. ю. н., проф., засл. юрист РФ И. Л. Бачило. – Изд. 2-е, доп. и перераб. – М., 2006. – 217 с.

К ВОПРОСУ О МЕЖДУНАРОДНОМ ПРАВОВОМ РЕГУЛИРОВАНИИ БОРЬБЫ С КИБЕРУГРОЗОЙ

TO THE QUESTION OF THE INTERNATIONAL LEGAL REGULATION OF THE FIGHT AGAINST THE CYBERTHREAM

Филютич Д. А.
г. Брест,
Брестский государственный университет
имени А. С. Пушкина,
студент юридического факультета

Сливко О. Я.
г. Брест,
Брестский государственный университет
имени А. С. Пушкина,
старший преподаватель кафедры
теории и истории государства и права

Аннотация: В статье рассматриваются теоретические аспекты правового регулирова-ния международной борьбы с угрозами в сфере информационной безопасности. Исследованы нормативные акты и деятельность универсальных и региональных организаций.

Ключевые слова: киберугроза, информационная безопасность, международные акты.

Annotation: The article deals with the theoretical aspects of the legal regulation of the international fight against threats in the field of information security. The regulations and activities of universal and regional organizations were examined.

Keywords: cyber threat, information security, international acts.

Киберугроза является целенаправленным проникновением в виртуальное пространство. Как правило, оно незаконное и направлено на достижение противоправных финансовых, политических, духовных, идеологических и других целей.

Киберугроза может воздействовать на информационное пространство общества и государства. Но изначально кибератака направлена на конкретное техническое устройство, в котором находятся персональные данные и сведения виртуального или физического устройства. Атака, в основном, поражает носитель данных, специально предназначенный для их хранения, обработки и передачи личной информации пользователя.

Злоумышленники приникают в серверы и получают из них информацию незаконным путем. Исторически сложилось так, что компьютерный злоумышленник-«хакер» является высококвалифицированным специалистом, который понимает все тонкости работы программ компьютера.

Интенсивное распространение киберугрозы угрожает не только государственной, но и международной безопасности.

На протяжении последних десятилетий в международных отношениях был принят ряд нормативных актов для борьбы с киберугрозами. Различные международные организации универсального и регионального характера приняли ряд конвенций.

В первую очередь стоит отметить, что в рамках Совета Европы в 2001 году подписана Конвенция о компьютерных преступлениях № 185, цель которой заключается в кодификации национальных законодательств в сфере привлечения киберпреступников к уголовной ответственности. Также данный договор обязывает оказывать взаимную помощь при расследовании данных видов преступлений.

В 2009 году заключено Межправительственное соглашение членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. Члены данного соглашения установили руководящие принципы в международном сотрудничестве. Кроме того, определены направления сотрудничества.

В 2011 году на сессии Генеральной Ассамблеи ООН Российской Федерацией, Китаем, Таджикистаном и Узбекистаном предложен проект «Правил поведения в области обеспечения международной информационной безопасности». Данный документ предусматривал нормы, которые обязывают государства сотрудничать в борьбе с преступной или террористической деятельности с использованием информационно-коммуникативных технологий (далее – ИКТ), и сдерживать любые распространения информации в сфере террористического, экстремистского и сепаратистского характера.

В 2013 году Организация по безопасности и сотрудничеству в Европе приняла так называемые «меры по укреплению доверия в области кибербезопасности». Эти меры необходимы для повышения эффективности межгосударственного обмена в различных форматах, включая рабочие совещания, семинары и круглые столы. Основной целью принятия этих мер является создание механизма, который позволит государствам сокращать риски возникновения конфликтов в результате использования ИКТ. Такая деятельность должна быть направлена на предотвращение конфликтов в результате использования ИКТ и на обеспечение использования ИКТ в мирных целях.

Практически все региональные и универсальные международные организации и форумы в той или иной степени рассматривают проблемы киберзащиты, а также обнаружения и пресечения киберпреступности.

В настоящее время не существует единого многостороннего соглашения по борьбе с международной киберугрозой. Как отмечает М. Вильданов, создаваемые международные договоры не будут ограничивать наступательный киберпотенциал в сфере воздействия на гражданскую инфраструктуру. Международный документ должен обеспечить соответствие ответа на кибератаку исходя из ее масштаба, продолжительности и потенциальной угрозы для гражданских объектов [1]. Данный подход, конечно, потребует выработки в той или иной мере режима верификации.

Ключевыми субъектами международного сотрудничества в области информационной безопасности являются США, Россия, Китай, Великобритания, Франция, Германия. Эти страны обладают наибольшим потенциалом в сфере кибервоздействия на инфраструктуру.

На национальном уровне государства предпринимают различные меры для борьбы с киберугрозой. США, реализуя свой государственный суверенитет, регулируют вопросы обеспечения не только кибербезопасности своей страны, но и единства глобального киберпространства. Однако, многие государства не обладают возможностью реализации своего верховенства в вопросах национальной кибербезопасности.

Политика США строится на праве на превентивные, упреждающие удары по предупреждению кибератак. Действия, в результате которых под угрозой оказываются объекты компьютерной информации или военные системы управления, расцениваются как действия военного характера. Последствия от таких противоправных действий по силе равны.

В рамках НАТО страны Европы выражают озабоченность относительно информационных угроз экономике, безопасности и территориальной целостности. Поэтому главные задачи по обеспечению кибербезопасности стран НАТО выражаются в следующих аспектах:

– распространение принципов коллективной безопасности на информационно-телекоммуникационную сферу. Кибератаки против личностной информации индивида приравниваются к военному нападению;

– отнесение киберпространства к категории среды ведения боевых действий наряду с космосом, воздухом, морем и сушей;

– Ориентация на повышение оборонного потенциала компьютерных программ с интеграцией возможностей взаимодействовать между государствами-членами блока;

– совместные действия в киберпространстве [1].

Сотрудничество на двустороннем уровне по вопросам информационной безопасности реализуется между государствами, обладающими значительными киберпотенциалами. Кроме того, эти страны, как правило, воспринимают друг друга как угрозу или же наоборот, объединяются против общей угрозы. Режимы двустороннего взаимодействия также находятся в состоянии имплементации. Как правило, они ориентированы на формирование доверия и предсказуемости в отношениях между государствами.

Наиболее значимые меры в международных отношениях по укреплению доверия в киберпространстве разработаны в рамках ООН. Вопрос информационной безопасности был внесен в повестку дня ООН в 1998 году. А в 1999 году была принята резолюция Генеральной Ассамблеи ООН 53/70 «Достижения в сфере информации и коммуникации в контексте международной безопасности». С тех пор Генеральный секретарь ежегодно представляет Генеральной Ассамблее доклад, содержащий позиции государств-членов ООН по данной теме.

В целях выработки основ правового режима обеспечения кибербезопасности в рамках ООН сформированы три группы правительственных экспертов (ГПЭ) по достижениям в сфере информатизации и телекоммуникации в контексте международной безопасности. Первый успешно представленный ГПЭ доклад был представлен в 2010 году.

Принятые меры укрепления доверия в области кибербезопасности были расширены на заседаниях ГПЭ в 2013 и 2016 годах. Достигнут определенный консенсус относительно необходимости применения и адаптации существующих норм международного права.

В целом меры укрепления доверия в киберпространстве, предлагаемые ООН, можно свести к следующему:

– разработка дополнительных механизмов и процессов по вопросам защиты информационной инфраструктуры от киберугроз;

– разработка единых словарей терминов и определений в сфере информационной безопасности;

– создание государственных органов, ответственных за межгосударственные контакты по обмену информацией в рамках информационно-компьютерных технологий для осуществления национальной безопасности;

– обмен информацией и кооперация в расследовании киберпреступлений;

– организация совместных мероприятий обучения и подготовки персонала в сфере информационной безопасности.

Таким образом, защита общегосударственной инфраструктуры от киберугроз остается глобальной проблемой, требующей международно-правового регулирования и создания режима информационной безопасности.

Международное сотрудничество в данной сфере ведется в основном на региональном и двустороннем уровне. С учетом сложившихся тенденций актуальность международно-правовых аспектов применения информационных технологий в эпоху кибервойн будет только возрастать. Международные нормы являются важной основой стабильности в киберпространстве и защиты инфраструктуры.

Список цитированных источников

1. Вильданов, М. Международно-правовые аспекты защиты инфраструктуры государств от киберугроз [Электронный ресурс] / М. Вильданов // Factmil.com. – Режим доступа: http://factmil.com/publ/soderzhanie. – Дата доступа: 04.05.2022.

К ВОПРОСУ О МЕХАНИЗМЕ СОТРУДНИЧЕСТВА ГОСУДАРСТВ В БОРЬБЕ С КИБЕРПРЕСТУПНОСТЬЮ

TO THE QUESTION OF THE MECHANISM OF COOPERATION OF STATES IN THE FIGHT AGAINST CYBERCRIME

Аль-Хшали Висам Шакир Хуссейн
Россия, г. Челябинск,
Южно-Уральский государственный университет,
магистрант Юридического института

Научный руководитель
Русман Г. С.
Россия, г. Челябинск,
Южно-Уральский государственный университет,
заведующий кафедрой уголовного процесса,
криминалистики и судебной экспертизы,
кандидат юридических наук, доцент

Аннотация: В работе изучен вопрос организации механизма взаимодействия государств в борьбе с киберпреступностью на международном уровне. Акцент сделан на нормах международного права, регламентирующих вопросы межгосударственного взаимодействия при выявлении кибератак, их предупреждению, расследованию и непосредственно борьбе с киберпреступностью. В статье указаны организации, созданные международным сообществом с целью борьбы с киберпреступностью.

Ключевые слова: международное сотрудничество, международное право, национальное право, киберпреступность, противодействие киберпреступности.

Annotation: This article examines the issue of organizing a mechanism for interaction between states in the fight against cybercrime at the international level. The focus is on international law governing interstate cooperation in detecting and combating cybercrime. The article identifies organizations created by the international community to combat cybercrime.

Keywords: international cooperation, international law, national law, cybercrime, combating cybercrime.

Цифровизация и компьютеризация не только улучшают жизнедеятельность общества и государства, но и являются причиной развития киберпреступности. Актуальность изучения киберпреступности и способов борьбы с ней продиктована временем, развитием технологий и вовлеченностью буквального каждого человека на планете в цифровой мир.

Уникальность киберпреступлений заключается в том, что они могут быть совершены без непосредственного контакта преступника с источником информации, в условиях удаленности. Другой особенностью киберпреступлений является высокий уровень латентности, ввиду чего скоординированный механизм сотрудничества государств становится важной задачей мирового сообщества.

Изучение различных подходов к пониманию киберпреступности позволяет отметить, что в общем смысле киберпреступность представляет собой вмешательство в информационное пространство как граждан, чья персональная информация является предметом защиты государства, так и государства, нарушая нормальное функционирование государственных органов [1, с. 313].

Современная реальность такова, что на международной арене нет государства, которое было бы полностью защищено от кибератак. Однако утечка государственной информации не просто подрывает нормальное функционирование государственных органов, но и может быть использована против такого государства на международной арене, стать причиной международных конфликтов, подорвать суверенитет государства и ослабить его позиции не только как участника внешней политики, но и как субъекта, защищающего свою целостность различными средствами [2, с. 371].

В такой ситуации защита цифровой информации и развитие цифровых технологий, призванных защитить важные данные и обеспечить нормальное функционирование общества и государства, являются приоритетом деятельности международного сообщества.

Важным шагом мирового сообщества в борьбе с киберпреступностью явилось создание специализированных органов – Интерпола, Европола, Евроюста. Однако, учитывая специфику обеспечения информационной безопасности и особенности правовой системы каждого государства, координация деятельности государств в данном вопросе затруднена. Поэтому указанные выше организации, признавая суверенитет каждого участника мирового сообщества, в числе своих целей ставят не только непосредственную защиту информации государства, но и создание вспомогательных органов, которые призваны исключить возникновение дисбаланса и дестабилизации работы государственных органов.

Деятельность государств в борьбе с киберпреступностью в первую очередь основывается на принципе непротиворечия положениям Европейской Конвенции о защите прав человека и основных свобод, принятой в 1950 году, и призвана расширять права, ей предоставленные [3, с. 28].

Несмотря на то, сколько государств задействовано в решении вопроса противодействия киберпреступности, всеобщая согласованность не просле-

живается, поскольку национальное правовое регулирование препятствует согласованности в части признания того или иного деяния преступным и уголовно наказуемым [4, с. 332].

В связи с этим, ведущие в вопросе противодействия киберпреступности международные организации предпринимают действия, направленные на отражение в своих резолюциях особенностей права всех государств.

К примеру, Евросоюз в целях преодоления несогласованности уголовных норм государств разработал Директиву об электронной торговле и Директиву о сохранении личных данных, в т. ч. Поправку к Рамочному решению о борьбе с терроризмом, что позволяет законодательству отдельных стран реализовывать положения международного права.

Также Евросоюз разработал инструменты, позволяющие странам-участницам внедрять в свою национальную правовую систему положения о борьбе с киберпреступностью, актуальные для международного права. Важнейшим инструментом является Конвенция о киберпреступности, которая включает в себя не только нормы материального уголовного права, но и положения о международном сотрудничестве. В 2007 году к данной Конвенции была представлена Конвенция о защите детей, которая признала преступной деятельностью обмен детской порнографией и получение доступа к таким данным посредством коммуникационных технологий.

В 2013 году в Гааге открыт центр по борьбе с киберпреступностью. В 2015 году Интерпол инициировал создание и открытие Международного центра по борьбе с киберпреступностью в Сингапуре с целью выявления, анализа и предотвращения киберугроз и преступлений в сфере информационных технологий.

В 2015 году участники Шанхайской организации сотрудничества предложили на рассмотрение Генеральной Ассамблеи ООН проект Международного кодекса поведения в области информационной безопасности, призванный определить и закрепить права и обязанности государств в области противодействия киберпреступности. В результате рассмотрения указанного проекта Генеральная Ассамблея ООН в 2018 году приняла резолюцию «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности».

В 2021 году в Российской Федерации издано Постановление об одобрении Соглашения о сотрудничестве стран СНГ в области кибербезопасности. Указанное Соглашение было утверждено советом глав государств СНГ на конференции в Душанбе в 2018 году. Оно указывает на создание правовых механизмов, которые позволяют эффективно взаимодействовать компетентным органам с другими странами в вопросах предупреждения, пресечения, расследования и раскрытия киберпреступлений.

В 2021 году Президент Российской Федерации издал Указ «об утверждении основ государственной политики Российской Федерации в области международной информационной безопасности» [5]. Указ содержит сведения

о стратегическом планировании международной информационной безопасности, определяет ведущие угрозы в данной области, цели и задачи политики Российской Федерации в вопросе сотрудничества с мировым сообществом.

Указанные акты, принятые международными организациями и государствами в рамках своей внутренней политики, не являются исчерпывающими и охватывающими все особенности борьбы с киберпреступностью [6, с. 58].

Одной из проблем совершенствования международного сотрудничества и правовой регламентации в данной области является то, что киберпреступность развивается с той же скоростью, что и цифровое пространство, к которому подключено множество человек на планете и большинство государственных органов. Соответственно, международное сообщество должно выработать не только механизм эффективного сотрудничества, но и механизм, позволяющий максимально быстро реагировать на все новшества, которые становятся доступны киберпреступникам.

В целом на пути к гармонизации сотрудничества стран в борьбе с киберпреступностью, следует выделить ряд проблем:

– несоответствие норм национального права нормам международного права, регулирующего борьбу с киберпреступностью;

– несвоевременное реагирование мирового сообщества и отдельных государств на изменения методов, средств и способов совершения киберпреступлений, что существенно снижает эффективность расследований;

– высокая латентность совершаемых киберпреступлений;

– разобщенность в трактовке понятий и содержаний киберпреступлений, квалификации таких действий как преступлений в законодательствах различных стран и пр.

Таким образом, взаимодействие государств в сфере борьбы с киберпреступлениями требует обобщения правовых норм различных государств при регламентации действий сторон в процессе использования средств в борьбе с киберпреступлениями и максимальной имплементации норм в национальные правовые системы, что позволит мировому сообществу максимально слаженно выстраивать методы борьбы с киберпреступлениями.

Список цитированных источников

1. Романовский, Г. Б. Проблемы противодействия терроризму в современном мире : в 2 т. / Г. Б. Романовский, О. В. Безрукова // Национальная безопасность в современной России: стратегия противодействия экстремизму и терроризму и перспективы преодоления глобальных проблем : материалы Всерос. науч. конф., 2016. – С. 310–318.

2. Якимова, Е. М. Международное сотрудничество в борьбе с киберпреступностью / Е. М. Якимова, С. В. Нарутто // Всерос. криминолог. журнал. – 2016. – Т. 10, № 2. – С. 369–378.

3. Климова, Е. А. Правовые основы полицейского и судебного сотрудничества по уголовным делам в праве Европейского союза : дис. … канд. юрид. наук : 12.00.09 / Е. А. Климова. – М. : МГИМО, 2011. – 193 с.

4. Сабадаш, В. П. Специальные подразделения и организации по борьбе с Интернет-мошенничеством в различных государствах мира / В. П. Сабадаш // Библиотека криминалиста. – 2013. – № 5 (10). – С. 328–338.

5. Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности : Указ Президента Рос. Федерации, 12 апр. 2021 г., № 213 // Собрание законодательства Рос. Федерации. – 2021. – № 16. – Ч. I. – Ст. 2746.

6. Химченко, И. А. Информационное общество: правовые проблемы в условиях глобализации : дис. ... канд. юрид. наук : 12.00.13 / И. А. Химченко. – М., 2014. – 174 с.

ПЕРСПЕКТИВЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

PROSPECTS FOR LEGAL REGULATION OF THE STATE POLICY IN THE FIELD OF ENSURING CYBER SECURITY

Шеметова Д. А.
г. Минск,
Белорусский государственный
экономический университет,
студентка факультета права

Научный руководитель
Пехота Т. М.
г. Минск,
Белорусский государственный
экономический университет,
ассистент кафедры теории и истории права

Аннотация: В ходе данной работы произведен анализ государственной политики в области обеспечения кибербезопасности, выявлены проблемы государственной политики в данной области, а также выработаны пути решения выявленных проблем.

Ключевые слова: кибербезопасность, кибертерроризм, атака на информацию, киберпреступность, киберугрозы.

Annotation: In the course of this work, an analysis of the state policy in the field of cybersecurity was made, the problems of state policy in this area were identified, and ways to solve the identified problems were developed.

Keywords: cyber security, cyber terrorism, attackon information, cyber crime, cyber threats.

Прогресс информационно-коммуникационных технологий, повлекший многообразие информационных процессов и развитие информационных отношений, обусловил необходимость обеспечения информационной безопасности государства, так называемой кибербезопасности. Под кибербезопасностью в общем смысле понимается совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных.

Одной из насущных проблем в международном сообществе выступает кибертерроризм. В. А. Голубев под ним понимает преднамеренную атаку на информацию, обрабатываемую компьютером, компьютерную систему или сеть, которая создает опасность для жизни и здоровья людей или наступления других тяжких последствий, если такие действия были совершены с целью нарушения общественной безопасности, запугивания населения или провокации военного конфликта [1].

Глобальной проблемой кибертерроризма является то, что он представляет собой информационное оружие, основывающееся на современных информационных технологиях, программном обеспечении компьютерных сетей и систем.

Несмотря на все разговоры о мире и гуманизме, в области обеспечения так называемой кибербезопасности, современное общество и государства периодически подвергаются различного рода киберугрозам. Так, по статистике, которая приводится в исследовании компании Positive Technologies, количество кибератак в 2020 году, по сравнению с 2019 годом, увеличилось на 51 %, а в 2021 году прирост кибератак увеличился на 1,2 %. Тем не менее, наиболее интересными отраслями, по мнению злоумышленников, явились государственные и медицинские учреждения, а также промышленные предприятия [2].

Стоит добавить, что одним из способов проявления кибертерроризма является политически мотивированная атака на информацию. Она заключается в непосредственном управлении социумом с помощью превентивного устрашения. Без сомнений, что политическая система любого государства непосредственно связана с информацией, ее производством и распространением. На сегодняшний момент большинство государств в целях повышения эффективности государственных услуг используют при реализации государственного управления систему «электронного правительства», которое базируется на элементах электронного документооборота, системе автоматизации управления государством и других информационных элементах. В рамках функционирования электронного правительства также предусматривается переход от бумажного взаимодействия органов власти к электронному взаимодействию посредством специализированного класса программного обеспечения. Для решения этой задачи организуется защищенная «электронная транспортная (почтовая) система» – информационно-коммуникационная система (далее – ИКС) с общей «системой обмена информации» на базе глобальных вычислительных систем, обеспечивающая эффективный и безопасный информационный обмен между органами власти.

Однако, при реализации политики в области обеспечения кибербезопасности можно выделить некоторые проблемы международного права в сфере осуществления кибербезопасности. Например, к ним можно отнести, прежде всего, несоответствие условий, при которых кибератаки были бы невозможными. Большое значение имеет наблюдение показателей кибербезопасности. Тем не менее, важное место занимает выявление технических устройств, программ, представляющих опасность деятельности ИКС.

Меры по решению вышеперечисленных проблем могут быть следующими.

Во-первых, необходимо создать условия, при которых киберпреступность, киберугрозы, а также кибератаки будут невозможны в осуществлении. Создание таких условий должно осуществляться субъектами обеспечения кибербезопасности посредством целенаправленной деятельности по противодействию киберугрозам.

Во-вторых, целесообразно сформировать систему мониторинга показателей и характеристик кибербезопасности, а также обеспечить возможность составления прогнозных показателей по кибератакам, с целью отслеживания статистики проводимой политики.

В-третьих, необходимо обеспечить приоритет предупредительных мер при реализации политики в области кибербезопасности. В частности, следует выработать направления международной политики по выявлению технических устройств и программ, представляющих опасность для нормального функционирования ИКС, с целью предотвращения возможных кибератак.

Таким образом, для решения наиболее важных проблем международной политики в области обеспечения кибербезопасности и противодействия кибертерроризму, в первую очередь, следует обеспечить приоритет предупредительных мер при реализации политики в области кибербезопасности, которые существенно снизят риск проявления киберпреступности.

Список цитированных источников

1. Голубев, В. А. Кибертерроризм: понятие, проблемы противодействия [Электронный ресурс] / В. А. Голубев // ТУСУР. – Режим доступа: https://journal.tusur.ru/ru/arhiv/1-1-2010/kiberterrorizm-ponyatie-problemy-protivodeystviya. – Дата доступа: 21.04.2022.

2. Актуальные киберугрозы: итоги 2021 года [Электронный ресурс] // Positive technologies. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021. – Дата доступа: 02.05.2022.

ИНФОРМАЦИОННЫЕ СЕТИ КАК ИСТОЧНИК РАДИКАЛИЗАЦИИ МОЛОДЕЖИ

INTERNET AS THE SOURCE OF THE YOUTH RADICALISATION

Щерблюк Н. В.
г. Минск,
Военная академия Республики Беларусь,
курсант факультета внутренних войск

Научный руководитель
Леднёва А. С.
г. Минск,
Военная академия Республики Беларусь,
доцент цикла государственно-правовых дисциплин
кафедры юридических дисциплин,
кандидат исторических наук, доцент

Аннотация: Рассматриваются проявления экстремизма среди молодежи, пути вовлечения ее в противоправные деяния и меры противодействия этому явлению.
Ключевые слова: молодежная среда, экстремизм, интернет, противодействие, информационная безопасность.

Annotation: Manifestations of the extremism among young people, ways of her involving into illegal actions and measures of countering this occurrences are examined.
Keywords: youth environment, extremism, Internet, counteraction, information security.

Молодежь в любой стране выступает в роли важного ресурса в обществе. В то же время она в силу незначительного жизненного опыта легко поддается деструктивному информационно-психологическому воздействию. В настоящее время в ряде государств мира не прекращаются войны, вооруженные конфликты, влекущие изменения в экономической, политической и идеологической сферах. Нехватка продовольствия, воды, бедствия климатического и экологического характера вынуждают людей покидать родину, вливаться в мощную миграционную волну. В таких экстремальных условиях старая система человеческих ценностей разрушается, а новая еще не сформирована. Социальные волнения и материальное неблагополучие служат благодатной почвой для появления радикальных групп агрессивной ориентации, которые пропагандируют идеи национальной, расовой и религиозной вражды. Большинство из них – молодежь в возрасте от 14 до 30 лет. Ученые социологи отмечают оформление такого нового социального феномена, как молодежный экстремизм, получивший особое распространение в XXI в. Например, в России на 2022 год на учете числятся 450 молодежных экстремистских организаций, объединяющих более 20 тыс. человек. Из этих группировок 147 провозглашают себя «скинхедами», 72 – являются футбольными фанатами, 31 – исповедует идеи российского национального единства, 18 – называются реперами и 8 – членами

национал-большевистской партии [1, с. 129]. По странам молодежная группа, потенциально политически настроенная, в структуре населения составляет: в Африке – 19 %, Латинской Америке – 17 %, в Азии – 16 %, Океании – 15 %, Северной Америке – 14 %, Европе – 11 % [2, с. 22].

Появлению неформальных, противозаконных молодежных объединений способствует и Интернет, возможности которого в формировании у молодежи асоциальных установок, противоправного поведения безграничны. Информационные интервенции обладают стремительностью, всеохватностью, вездесущностью, придавая обратной связи автоматический характер. Это свойство Интернета еще более усиливается в социальных сетях, которые дают возможность одновременного общения не только двух, но и многих, одновременно вступающих в контакт, людей. Такое свойство социальных сетей способствовало организации протестов, движений, акций неповиновения, убийств, других насильственных деяний в виде разрушающей и сметающей на своем пути волны, с которой властям было трудно, а порой невозможно справиться.

Сущностью совершения общественно опасных инцидентов террористической и экстремистской направленности является радикализация. В самом общем виде под радикализацией понимается процесс перехода от ненасильственных форм выражения неприятия тех или иных форм жизни или идей к насильственным действиям. Интернет выступает также одним из основных способов вербовки новых членов. Имеет место и феномен «самовербовки», т. е. идеология интернет-пользователей изменяется под влиянием пропаганды, переводя пользователей в члены экстремистских и террористических организаций. Такие известные социальные медиа-платформы, как Facebook, Twitter, Telegram, YouTube и т. д., благодаря особенным способностям интерфейса, являются уникальным средством коммуникации. Необыкновенность таких социальных сетей в том, что, развиваясь и совершенствуясь, мобильные технологии могут в режиме реального времени рассказать о резонансном событии, прежде чем это будет объявлено в официальных СМИ.

Веб сам по себе – не основание или причина радикализации, а фактор, который содействует переходу человека к совершению насильственных действий. На сегодня веб дозволяет творить не только профессиональные веб-сайты, которые редактируются журналистами-специалистами, а также и непрофессиональные самостоятельные веб-ресурсы, содержание которых регулируют рядовые интернет-пользователи. Надо отметить, что экстремистские и террористические группы отлично используют информационные сети для вовлечения молодежи по всему миру в противоправную деятельность. Политика краудсорсинга (поиск и использование способностей, опыта пользователей социальными сетями для продвижения идеологии ИГИЛ и совершения терактов), направленная на быстрый поиск сторонников джихадистов среди читателей сайтов, журналов и твитов ИГИЛ (организация запрещена в Российской Федерации и Республике Беларусь), серьезно обеспокоила правительство западных стран и США. Оказалось, что любой молодой человек, как в Европе, так и в других странах, мог стать и мишенью для ИГИЛ, и мог осуществить теракт. Так и случилось, например, в штатах Калифорния

и Орландо в 2015 году, когда теракты были совершены американцами, которые никогда не посещали арабские страны, но были почитателями виртуальной информации об ИГИЛ – этой первой в истории террористической организации, которая и в настоящее время проводит масштабную и эффективную информационную войну в сети Интернет.

Другой пример. В феврале 2019 года в социальных сетях Палестинской Газы начались экономические протесты под лозунгом «Мы хотим жить», которые были инициированы через сети радикалами, именовавшими себя «медийными неполитическими активистами СМИ», объединенными в неизвестную «Группу 11 марта». Несмотря на заявленную «неполитизированность», через телеграмм-каналы и местные чаты прошла агрессивная агитация против правящего в этой части палестинского государства движения ХАМАС. Следствием такой организованной активности стали самые с 2007 года масштабные выступления.

Радикалы принимают идею о том, что насилие нужно для продвижения к цели и пропагандируют готовность перехода к насилию через сети. По разным оценкам, в социальной сети Twitter в среднем генерируются 350 000 твитов за минуту и около 500 млн твитов в день, а медиа-платформа Facebook остается крупнейшей интернет-платформой с 500 млн активных пользователей.

Многие террористические государства, особенно исламистской направленности, придерживаются теории-утопии процветающего государства, которое основывается на религии, экономике, экспансии, природе, справедливости, социальной жизни. Среди этих тем главными являются религия, экономика и экспансия. Посредством манипуляций в социальных сетях формируется представление об организации, например, Исламского правительства, как о действенной правительственной системе с процветающей экономикой и социальной обеспеченностью. Также утверждается, что Исламское правительство является отражением правильного ислама. Такой образ подкрепляется видеоклипами и фотоизображениями в социальных сетях, демонстрирующими людей, вместе практикующих религиозную деятельность, такую, как молитва и пост.

Еще одним пользующимся популярностью методом создания положительного вида экстремистского государства, кроме публикаций в социальных сетях медиа-контента, является переписка с возможными новобранцами в онлайн-чатах. В таковой переписке у адресата формируется образ идеального исламского (надо понимать – террористического) государства, человеку обещают наилучшую жизнь, месячные пособия, безвозмездное продовольственное обеспечение и медсервис – только приезжай и вставай в ряды слуг Аллаха. Но те, кому удалось вернуться домой после пребывания на Востоке, на территории подконтрольной ИГИЛ, сознаются, что исламское правительство, которое они для себя представляли, кардинально отличается от действительности.

Информационный экстремизм использует слабую социальную приспособленность молодежи для того, чтоб сделать ее своим средством, своим орудием в решении определенных задач. Экстремизм подавляет, иногда в насильственной и грубой форме, личность человека, поскольку его сознание и ум для

информационного экстремизма является лишним. Они ему не необходимы. Информационный экстремизм – это разработка использования фальшивых сведений для того, чтобы сделать из человека послушный механизм, который можно запрограммировать на исполнение нужных разрушительных деяний. Конкретно в этом и состоит опасность информационного экстремизма, который, вроде бы исподволь, ненавязчиво устремляется привить юному человеку образ идей и идеи, которые являются деструктивными и ориентированы на разрушение сообщества и страны. При всем этом информационный экстремизм делает это методично, исподволь подводя к деструктивным идеям.

Неконтролируемый интернет – это также вброс непроверенных сведений, неверных посылок, которые выдаются как честные и на базе которых человеку предлагается прийти к выводу, который неутешителен для имеющегося сообщества и страны. Потому информационный экстремизм следует рассматривать и как изощренную форму экстремизма, в борьбе с которой можно и необходимо применять более совершенные способы и подготовленные средства.

Информационный радикализм нацелен на то, чтобы перевернуть сознание юного человека. Идеологи знают, как подготовить молодежь, чтобы потом передать ее в руки эгоистично настроенным политикам. Потому задачей страны и сообщества на сегодня является выявление всех направлений виртуального экстремизма для того, чтобы обозначить в нем те болевые точки, воздействуя на которые можно организовать противодействие. Главным средством такой борьбы является приведение доводов, изобличающих ересь, фейки, на которых основано психологическое влияние на ценностные установки молодежи, ведение постоянного мониторинга настроений студентов вузов, средних специальных учебных заведений и школ с целью выявления случаев распространения экстремистских идей.

При всем этом нужно также учесть политическую неустойчивость молодежной среды, на которую рассчитан и информационный экстремизм, те трудности, которые вызывает социализация у юных людей. Решение проблемы лежит в совместных действиях и усилиях родителей, правоохранительных органов, образовательных учреждений, органов местного самоуправления. Целесообразно разработать специальные программы, препятствующие доступу к тем сайтам, которые пропагандируют насилие, жестокость, неповиновение и конфронтацию.

Список цитированных источников

1. Батюкова, В. Е. К вопросу о противодействии молодежному экстремизму в России / В. Е. Батюкова // Право. Юридические науки. – 2022. – № 2. – С. 129–131.

2. Фитуни, Л. Моделирование протестных технологий в системе медиакоммуникационной зависимости / Л. Фитуни // Азия и Африка. – 2019. – № 12. – С. 22–29.

КОНКУРСЫ ЭССЕ

Победители конкурса эссе учащихся 11-х классов общеобразовательных школ, гимназий и обучающихся средних специальных учреждений образования *«1000 слов О КИБЕРБЕЗОПАСНОСТИ в условиях вооруженных конфликтов»*

Гран-при

Генюш Полина Викторовна
ГУО «Нарочская средняя школа № 2
Мядельского района Минской области»

1000 СЛОВ О КИБЕРБЕЗОПАСНОСТИ В УСЛОВИЯХ ВООРУЖЕННЫХ КОНФЛИКТОВ

В настоящее время крайне актуальной является тема кибербезопасности в условиях вооруженных конфликтов. Война – это продолжение политики в ином виде. Современные военные конфликты решаются не только на поле боя. С развитием мировой политики и различных технологий, в том числе информационных, войны принимают все новые облики.

«Глобальная цифровизация затронула все сферы, и вооруженные конфликты – не исключение», – выразил свою точку зрения об интеграции информационных технологий в нынешнем обществе Петер Маурер, Президент Международного Комитета Красного Креста. Я не могу не согласиться с данным высказыванием. Более того, хочу лично от себя добавить, что в условиях вооруженных конфликтов особо важную роль играет сохранение устойчивой кибербезопасности.

Кибербезопасность – это совокупность процессов и технологий, методов и практик, используемых для защиты и охраны компьютеров, сетей, серверов, приложений, а также персональных и организационных данных, носителями которых они являются.

Прежде чем определить главные правила компьютерной безопасности в вооруженных конфликтах, следует выявить, какие встречаются киберугрозы и в чем заключается их влияние на общественную жизнь.

В мирное время от стандартных киберугроз, таких как киберпреступление, кибератака и кибертерроризм, страдает немыслимое количество людей. По статистике сайта belta.by, в нашей стране число жертв киберпреступлений неутомимо растет: по сравнению с 2015 годом оно увеличилось в 10 раз и составило 25 тысяч человек в 2020 году.

В условиях военных конфликтов существует реальная возможность нанесения вреда посредством кибероперациий не только на военные объекты,

но и на гражданские, несмотря на запрет подобных действий Международным Гуманитарным Правом (далее – МГП). Также компьютерная атака, в отличие от «живой», позволяет скрыть источник нападения и присвоить его другому лицу. В вооруженный период среди хакеров и интернет-мошенников все чаще используются фишинг (от англ. fishing – выуживание), шпионское ПО и атаки Man-in-the-Middle (их также называют «человек посередине» или «посредник»), с помощью которых злоумышленники получают доступ к личной информации с целью вымогательства и шантажа государственных или гражданских лиц, использования их денежных средств и накоплений. Тем самым киберпреступники наводят панику среди людей, подрывают доверие к органам власти и общественным организациям и провоцируют формирование военных противоречий в киберпространстве.

Также во время вооруженных конфликтов огромное значение приобретает информационная война. Множество СМИ освещают происходящие события, делают их достоянием всего мира. В условиях войны в информационном поле с обеих сторон конфликта появляются недостоверные, непроверенные материалы, которые выдаются за правду. Существуют и наблюдатели, нейтрально настроенные или выступающие за одно из конфликтующих государств. Наблюдатели также могут распространять недостоверные сведения, умышленно или нет. Иногда бывает очень сложно определить, является информация достоверной или же это так называемый «фейк».

В этом потоке информации важно критически мыслить и не поддаваться эмоциональному воздействию. Грамотная пропаганда может внедрить в наше мировоззрение ложную картину о происходящем.

Поэтому важно знать и соблюдать правила поведения в киберпространстве. Прежде всего, нужно проверить информацию, сверив ее с другими источниками. В первую очередь следует читать только официальные и проверенные источники, а не сомнительные телеграмм-каналы и посты в соцсетях. Однако необходимо помнить, что в условиях военного времени даже надежные медиа и официальные лица могут ошибаться. Поэтому, прочитав важную новость, необходимо дождаться ее опровержения или подтверждения. Если речь идет о страницах в соцсетях, то нужно обращать внимание на то, верифицирован ли аккаунт.

Хорошими средствами защиты личной или коммерческой информации являются также использование надежных паролей и пин-кодов, установка антивирусных программ, обновление программного обеспечения и операционной системы, удостоверенность в легитимности и правомерности сайта и/или лица, подключение только к проверенным и защищенным сетям Wi-Fi.

Элементарные правила неизменны для военной и без военной ситуаций, так как являются основой для безопасного использования технологий и сети Интернет. Однако стоит всегда понимать, что в рамках военного конфликта большую роль играет государство и его стремление к снижению потерь. Каждое государство несет ответственность за субъектов, проводящих кибероперации; совершает их в соответствии с установленными международными

правовыми нормами; старается минимизировать ущерб инфраструктуре и человеческие потери, принимает меры по защите граждан.

Кибербезопасность как мера предосторожности для современного человека стала практически неотъемлемой частью жизни как в мирное, так и в военное время. Я думаю, что знание базовых правил безопасности во многом поможет нам обеспечить сохранность и защищенность своей персональной информации и работоспособность устройств. Но при этом надо не забывать о банальной гуманности. Важно не только не попасться на крючок, но и не закинуть удочку самому. Любой агрессивный поступок влечет за собой такую же агрессию, дезинформация и фейки формируют предубеждения и могут привести к физическому насилию.

Безусловно, киберпреступления стали на уровне с обычными преступлениями в условиях вооруженных конфликтов. Поэтому каждому необходимо помнить, как обезопасить себя и других от возможного виртуального нападения.

Диплом 1-й степени

Войтович Елизавета Игоревна
ГУО «Гимназия № 2 г. Бреста»

КИБЕРАТАКИ СЛОВНО СТИХИЙНЫЕ БЕДСТВИЯ

Кибератаки словно стихийные бедствия: невозможно предотвратить обрушение урагана на город, но, безусловно, можно к нему подготовиться.

Сейчас трудно встретить человека, не имеющего смартфона в кармане, компьютера дома, банковской карточки в кошельке. Предприятия уже давным-давно перешли от толстых журналов и папок к электронным таблицам и базам данных, а работать можно почти из любой точки земного шара.

Информатизация общества, внедрение информационно-коммуникационных технологий практически во все сферы жизни сильно сказывается не только на персональном комфорте современного человека, но и влечет за собой ряд негативных последствий, главное из которых – получение лишь видимой свободы и беспрепятственного доступа к информационным технологиям, на деле же в таких условиях гораздо легче «диктовать» свои убеждения и управлять одновременно большим количеством людей. Кроме того, имея перед собой такое разнообразие девайсов, возрастает риск стать жертвой разного рода киберпреступлений.

Если вопрос безопасности является насущным для простого человека, то несложно догадаться, что безопасность целого государства в значительной степени зависит от возможностей реализовывать политические, экономические и социальные функции в виртуальном пространстве.

Киберпространство является такой же средой для ведения боевых действий, как и земля, море и воздушно-космическое пространство. Очевидно, что агрессия в киберпространстве в корне отличается от того, что мы привыкли видеть в кино и СМИ; это совершенно новая отрасль военного дела.

С развитием информационно-коммуникационных технологий военнослужащие непрерывно обучаются искусству ведения «кибервойны», потому встает ряд вопросов:

- Уместно ли вообще употреблять термин «кибервойна», говоря о противостояниях в кибер- и/или информационном пространстве?
- Какой должна быть «новая армия», способная защищать государство не только на реальном поле боя, где свистят пули и гремят взрывы, но и сидя перед мониторами?
- Какие меры стоит предпринять государствам для обеспечения полной защиты автоматизированных систем органов военного и государственного управления?

Лейтмотивом звучит тема новизны проблемы кибербезопасности, поэтому соответствующая терминология еще не была принята, однако стоит обратить внимание на то, что часто под киберпространством подразумевают лишь Интернет, упуская из виду сегменты киберпространства, изолированные от Интернета: автоматизированные системы управления промышленных предприятий, закрытые военные сети и т. д.

Очевидно, что целью агрессора в «кибервойне» является уничтожение или выведение из строя систем управления противника. Каким образом? Можно нанести ядерный или артиллерийский удар по пунктам управления и узлам связи, применить десантно-диверсионные силы, но здравый смысл подсказывает, что данные действия не являются кибернетическими. А вот вирусы, DDOS-атаки, уничтожение баз данных, нарушение хранимого контента и т. д. могут приводить как к полному, так и частичному выходу из строя элементов автоматизированных систем управления, следовательно – к нарушению выполняемых ими функций, а иногда и к их полному параличу.

Однако о подобного рода действиях ничего не сказано в Статье 3 Резолюции Генеральной Ассамблеи ООН3314 (XXIX)«*Определение агрессии*», где по пунктам расписано, какие действия квалифицируются в качестве акта агрессии.

Существует проблема анонимности: до тех пор, пока государство не идентифицирует автора агрессии, оно не может предпринимать против него какие-либо действия, в том числе военные.

Немаловажный фактор – неравенство стран в развитии информационно-коммуникационных технологий. Это делает высокоразвитые страны, например, США, более уязвимыми к различного рода кибервоздействиям, но они не могут реализовать подобного вида агрессию к странам, чья армия не столь зависима от информационно-коммуникационных технологий в военной сфере. В результате понятие войны не может адекватно описывать подобное противоборство, так как становится нерелевантным для одной из его сторон.

«Кибервойна» – публицистический термин, который используют невежественные в военном отношении люди, пытаясь напугать друг друга. Война подразумевает такую разновидность вооруженного противоборства, в процессе которого государства-участники вынуждены максимально напрягать и использовать большую часть имеющихся в их распоряжении ресурсов для достижения поставленных военно-политических целей, а действия в киберпространстве – лишь часть полномасштабного противостояния.

Тем не менее, для реализации противодействия в киберпространстве появляется потребность в создании «киберподразделений», новых перспективных видов и родов войск. Целью воздействия вовсе не обязательно является перехват управления, вмешательство в алгоритмы, нарушение функционирования целевой киберсистемы, или причинение ущерба. Воздействие может производиться, например, на гражданские частные системы с целью их мобилизации.

Конечно, делать ставку только на данный вид вооружения безрассудно, потому как даже самого выдающегося программиста может легко обезвредить не самый выдающийся солдат с автоматом. С другой стороны, в странах, где боевые информационные системы не столь развиты, существуют банковские и другие государственные системы, которыми массово пользуются граждане. Нарушение их работы повлечет за собой волнения в обществе и позволит достигнуть политических целей войны.

Наиболее удачным вариантом для государства будет иметь помимо классического вооружения подразделения, занимающиеся обороной страны в киберпространстве.

В нашей стране была создана «IT-рота», где проходят срочную службу программисты. Их технические навыки и творческий потенциал используются в интересах Министерства обороны, а вместо традиционного армейского быта, солдаты занимаются разработкой программного обеспечения.

Немаловажный факт – киберпространство не статично. Недостаточно единожды взломать сеть, так как постоянно возникают новые локальные сети, а еще чаще меняется конфигурация действующих сетей: добавляются новые сегменты, совершенствуется и/или заменяется программное обеспечение, поэтому мониторить сети военнослужащим требуется постоянно.

В современных условиях, в целях эффективного отражения угроз кибербезопасности, автоматизированные системы органов военного и государственного управления должны совершенствоваться, должна повышаться степень их автоматизации и компьютеризации. Актуальным для государства является обеспечение кибербезопасности как в мирное, так и в военное время.

Надежная киберзащита подразумевает использование совокупности подсистем: подсистемы защиты, обеспечивающей компьютерную и информационную безопасность систем связи; подсистемы обнаружения; подсистемы реагирования. Тем не менее, защита государства должна производиться с помощью единой динамичной интеллектуальной системы, ее параметры

должны адаптироваться и меняться под воздействием внешних и внутренних кибератак на протяжении всего ее существования.

Такая система должна не только своевременно обнаруживать новые киберугрозы и кибератаки, но и автоматически настраивать оптимальный режим работы в зависимости от степени угрозы. Важной функцией является способность наносить удар на системы управления противника, а также способность к дезинформации противоборствующей стороны об истинных свойствах и параметрах автоматизированной системы управления и ее системы кибербезопасности.

Создание эффективной системы кибербезопасности государства предусматривает полную реализацию комплексного подхода в обеспечении информационной безопасности объектов автоматизированных систем управления, заключающегося в рациональном сочетании следующих составляющих: защита от утечки по техническим каналам и противодействие техническим средствам разведки, применение аппаратно-программных средств защиты информации, разработки и реализация комплекса организационно-технических мер.

Функционирование всех вышеперечисленных систем должно быть регламентировано соответствующими документами и правовыми актами.

Не даром в народе говорят: «Предупрежден – значит вооружен». Даже не будучи под угрозой нападения, власти и ведомства должны обеспечить безопасность не только важнейших стратегических объектов, но и, пожалуй, в первую очередь, своих граждан. Ведь благополучие страны – есть благополучие, комфорт и уверенность в счастливом будущем живущих в ней людей.

Диплом 2-й степени

Волкова Виктория Александровна
ГУО «Озерецкая детский сад – средняя школа
Глубокского района»

КИБЕРБЕЗОПАСНОСТЬ В УСЛОВИЯХ ВООРУЖЕННЫХ КОНФЛИКТОВ

Кибербезопасность – это совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных. Целью кибератак является получение доступа к конфиденциальной информации, ее изменение или уничтожение, вымогательство денег у пользователей или нарушение нормального бизнес-процесса [1].

Сложно переоценить важность кибербезопасности в современном мире. Она необходима, потому что меры, принимаемые в рамках обеспечения

кибербезопасности, призваны защитить от хищения и последующего использования в злых умыслах конфиденциальных данных, личной медицинской информации, интеллектуальной собственности, государственных и отраслевых информационных систем – всего, что хранится и работает с использованием информационных технологий [2].

Кибербезопасность находит применение в самых разных областях, от сферы бизнеса до мобильных технологий. В этом направлении можно выделить несколько основных категорий. Это безопасность сетей, приложений, информации, операционная безопасность, аварийное восстановление и непрерывность бизнеса, повышение осведомленности.

Кибербезопасность борется с тремя видами угроз.

Киберпреступление – действия, организованные одним или несколькими злоумышленниками с целью атаковать систему, чтобы нарушить ее работу или извлечь финансовую выгоду.

Кибератака – действия, нацеленные на сбор информации, в основном политического характера.

Кибертерроризм – действия, направленные на дестабилизацию электронных систем с целью вызвать страх или панику [3].

В современных вооруженных конфликтах также используются кибероперации, что влечет за собой потенциальные гуманитарные последствия. Международное гуманитарное право ограничивает применение кибероружия во время вооруженного конфликта так же, как любого другого оружия. Любое применение государствами силы регулируется Уставом Организации Объединенных Наций и соответствующими нормами обычного международного права. Международные споры должны разрешаться мирными средствами во всех областях, в том числе в киберпространстве.

Кибероперации могут подорвать работу жизненно важных объектов гражданской инфраструктуры и помешать предоставлению основных услуг населению. В ситуации вооруженного конфликта объекты гражданской инфраструктуры защищены от кибератак существующими принципами и нормами международного гуманитарного права. Особая защита предоставляется больницам и объектам, необходимым для выживания гражданского населения [4].

Во время вооруженных конфликтов запрещено применение киберсредств, которые распространяются неизбирательно и при этом наносят неизбирательный ущерб. С технической точки зрения, некоторые киберинструменты можно проектировать и использовать таким образом, чтобы они направлялись против конкретных целей и наносили вред конкретным объектам, а не распространялись неизбирательно или причиняли неизбирательный ущерб. Однако в киберпространстве все взаимосвязано, поэтому любой объект, подключенный к интернету, может подвергнуться нападению из любой точки мира; кибератака на одну систему может иметь последствия для многих других [4].

Все большее число стран развивает военный киберпотенциал. Технологии в разработке наступательных киберсредств шагнули далеко вперед. Во время

вооруженного конфликта кибероперации ведутся в поддержку операций с применением кинетического оружия или параллельно с ними.

Посредством кибероперациий воюющие стороны могут проникнуть в систему и собрать, изъять, изменить, зашифровать или уничтожить данные. Также возможно использовать взломанную компьютерную систему для запуска и изменения процессов, которые она контролирует, или для иного манипулирования этими процессами. Работа производств, объектов инфраструктуры и линий связи, транспортной, правительственной или финансовой системы может быть подорвана, изменена.

В последние годы кибератаки обнажили уязвимость систем жизнеобеспечения. Кибероперации сопряжены с риском эскалации ситуации, которая повлечет за собой соответствующие гуманитарные последствия, – по той простой причине, что стороне, которая подвергается нападению, бывает сложно понять, какова цель нападающего – сбор разведданных или причинение более серьезного ущерба. В результате объект нападения, ожидая самого худшего, может отреагировать жестче, чем необходимо [2].

К кибероперациям во время вооруженных конфликтов применимы нормы международного гуманитарного права:

– запрещаются киберсредства, которые квалифицируются как оружие и по своей природе являются неизбирательными;

– запрещаются непосредственные нападения на гражданских лиц и гражданские объекты, в том числе с использованием кибернетических средств и методов ведения войны;

– запрещаются акты насилия и угрозы насилием, в том числе посредством кибернетических средств и методов ведения войны;

– запрещаются неизбирательные нападения, а именно нападения, которые поражают военные объекты и гражданских лиц или гражданские объекты без всякого различия, в том числе при использовании кибернетических средств и методов ведения войны;

– запрещаются несоразмерные нападения, в том числе при использовании кибернетических средств или методов ведения войны;

– во время военных операций, в том числе при использовании кибернетических средств или методов ведения войны, необходимо постоянно проявлять заботу о том, чтобы щадить гражданское население и гражданские объекты [4].

Киберпространство используется в основном в гражданских целях, за исключением отдельных сетей военного назначения. Однако гражданские и военные сети могут быть связаны друг с другом. Военные сети могут использовать гражданскую киберинфраструктуру: проходящие по морскому дну волоконно-оптические кабели, спутники, маршрутизаторы и узлы. И наоборот, гражданский транспорт, управление морскими перевозками и воздушным движением все больше зависят от спутниковых навигационных систем, которые могут использоваться и военными. Гражданские системы материально-технического снабжения и основные гражданские службы используют те же сети

и системы коммуникации, через которые проходят отдельные сообщения военного характера [4].

Критически важные объекты гражданской инфраструктуры, позволяющие предоставлять населению основные услуги, все больше зависят от цифровых систем. Ограждать такую инфраструктуру и услуги от кибератак или случайного ущерба предельно важно для защиты гражданского населения. Международное гуманитарное право предусматривает защиту конкретных объектов инфраструктуры, таких как медицинские службы и объекты, необходимые для выживания гражданского населения. Объекты, необходимые для выживания населения, нельзя подвергать нападению, уничтожать, вывозить или приводить в негодность.

В настоящее время не существует всеобъемлющей международно-правовой базы в отношении кибербезопасности. Не существует международных органов, уполномоченных расследовать и преследовать в судебном порядке случаи киберагрессии. Конвенция Совета Европы по киберпреступлениям, принятая в 2001 году в Будапеште, является единственным многосторонним, юридически обязательным договором, касающимся преступной деятельности в сфере информационных технологий [4].

Сегодня, в эпоху бурного развития цифровых технологий, которые далеко не всегда используются в интересах человека и общества, особенно важно соблюдать кибербезопасность. Ее значимость многократно увеличивается в условиях вооруженных конфликтов, которых пока не удается избежать. Мир очень хрупок. Политики не всегда могут договориться и прибегают к применению силы. Печальный пример тому – вооруженный конфликт России и Украины, начавшийся 24 февраля текущего года. К сожалению, не удается избежать разрушения гражданских объектов, невинных жертв из гражданского населения. Возможно, здесь имеют место кибератаки, в результате чего уничтожаются не только военные объекты, но и жилые дома, объекты социально-культурного назначения. Этого нельзя допускать!

Список цитированных источников

1. Что такое кибербезопасность? [Электронный ресурс] // Kaspersky. – Режим доступа: https://www.kaspersky.ru/resource-center/definitions/what-is-cyber-security. – Дата доступа: 01.04.2022.

2. Что такое кибербезопасность и почему она важна? [Электронный ресурс] // Multipassword. – Режим доступа: https://multipassword.com/ru/articles/cybersecurity? – Дата доступа: 01.04.2022.

3. Что такое кибербезопасность: основные угрозы [Электронный ресурс] // GeekBrains. – Режим доступа: https://gb.ru/blog/cto-takoe-kiberbezopasnost. – Дата доступа: 01.04.2022.

4. Международное гуманитарное право и кибероперации во время вооруженных конфликтов: изложение позиции МККК [Электронный ресурс] // Reliefweb. – Режим доступа: https://reliefweb.int/sites/reliefweb.int/files/resources/icrc_ihl_and_cyber_operations_during_armed_conflict_ru_0.pdf. – Дата доступа: 01.04.2022.

Диплом 3-й степени

Цу-Кан-Фу Элис Адриановна
ГУО «Средняя школа № 4
г. Дзержинска Минской области»

1000 СЛОВ О КИБЕРБЕЗОПАСНОСТИ В УСЛОВИЯХ ВООРУЖЕННЫХ КОНФЛИКТОВ

Масштабы киберугроз сегодня таковы,
что нейтрализовать их можно, лишь объединив
усилия международного сообщества.
В.В. Путин

Время не стоит на месте. Интернет стал неотъемлемой частью современного мира. Пандемия коронавируса ускорила использование цифровых инструментов в бизнесе и дома. В нашу жизнь приходят новые разработки, интересные гаджеты, устройства, которые раньше было трудно себе представить. Все эти новшества мы называем кибернетика. Слово «кибернетика» впервые произнес Платон, взяв за основу греческое «кибернус» (кормчий). В наше время оно приобрело дополнительный новый смысл – это наука об управлении сложными динамическими системами и процессами любой природы, способной воспринимать, хранить и обрабатывать информацию, используя ее для управления и регулирования.

При всех плюсах научно-технического прогресса, само собой, имеются и минусы. Обратная сторона стремительного развития науки и техники – это возрастание проблем, с которыми столкнулось человечество. Взлом важных данных, перебои в работе сети, компьютерные вирусы и другие кибернетические угрозы влияют на нашу жизнь от незначительных угроз до серьезных инцидентов.

Решение глобальных проблем – задача чрезвычайной важности и сложности, и пока не найдены пути их преодоления. По своему характеру глобальные проблемы различны. К их числу относят: проблемы мира и разоружения, предотвращения новой мировой войны; экологическая; демографическая; энергетическая; сырьевая; продовольственная; использование Мирового океана; мирное освоение космоса; преодоление отсталости развивающихся стран.

Всемирный экономический форум (WEF) показал, что на текущий момент кибербезопасность занимает 5 место в списке глобальных проблем человечества. Кибербезопасность борется с тремя видами угроз:

– киберпреступление – действия, организованные одним или несколькими злоумышленниками с целью атаковать систему, чтобы нарушить ее работу или извлечь финансовую выгоду;

– кибератака – действия, нацеленные на сбор информации, в основном политического характера;

– кибертерроризм – действия, направленные на дестабилизацию электронных систем с целью вызвать страх и панику.

Киберугроза – это самый быстрорастущий вид экономической преступности. По данным Международного Союза Электросвязи ООН, 53,6 % населения планеты используют сеть Интернет. Ускорение глобализационных процессов сделало информационные и цифровые технологии неотъемлемой частью человеческой жизни, что повлияло на мировую экономику. Масштаб распространения киберугроз и утечки информации растет с каждым годом.

«Благими намерениями вымощена дорога, ведущая в АД»…

Стремясь к всеобщему миру и благополучию, человечество изобретает все более изощренные способы уничтожения самого же себя. Вооруженные конфликты возникают именно на почве пути к миру, независимости и призрачному счастью. Военный стратег Клаузевиц говорил, что «война есть не что иное, как продолжение политики иными средствами». Поиски путей предотвращения мировых конфликтов начались с окончанием Второй мировой войны и победы над нацизмом. Тогда же, вместо Лиги Наций, была создана ООН – Организация Объединенных Наций, глобальная цель которой – развитие международного сотрудничества и в случае конфликтов между странами – оказание помощи противостоящим сторонам в урегулировании спорных вопросов мирным путем.

Возрастание возможности применения в вооруженном конфликте кибертехнологий сделало необходимостью принятие норм Международного Гуманитарного права.

Кибератака может ассоциироваться со способом военных действий. Объектами атак зачастую служат правительственные структуры, дипломатические ведомства, посольства, исследовательские институты, ядерные базы, военные ведомства и компании. В Будапештской Конвенции Совета Европы, принятой 23 ноября 2001 г. «О киберпреступности» особое внимание уделено вариациям киберпреступлений и процессуальным нормам относительно уголовного процесса, а также решаются вопросы относительно компетенции государств в отношении киберугроз. Однако, Международное правовое регулирование до конца еще не сформулировано, а существуют лишь правовые наработки и направления.

В вооруженном конфликте, не исключена «чисто» кибернетическая война, без применения обычного оружия и без ведения боевых действий. В таком случае, чтобы приравнять кибератаку к обычной атаке, нужно сравнить ущерб, причиненный кибероружием и ущерб от обычного оружия, для применения норм Международного Гуманитарного права относительно гражданских объектов (нападение на которые запрещены ст. 52 Дополнительного Протокола № 1 Женевской конференции 1949 года).

С приходом кибертехнологий увеличилась возможность их применения во время вооруженных конфликтов, безнаказанно приводить в действие свои планы, запутав следы в мировой Интернет-паутине, находясь на другом конце Земли. Ведь эта группа, организованная в интернете и знающая друг друга виртуально, может успешно действовать сконцентрировано, получая приказы от виртуального руководства. В данном случае, по решению Международного Суда

ООН, требуется еще доказать причастность человека или группы, к их действиям по указанию или под руководством и контролем этого государства.

«Это сродни биологическому оружию, и еще даже мощнее. Не надо ни танки, ни пулеметы, ни ракеты высокоточные. Достаточно совершить массированные кибератаки на экономические объекты любой страны. И этого будет достаточно, чтобы перевернуть страну» (А. Г. Лукашенко).

Кибероружие страшнее атомной бомбы. Для производства бомбы нужно наукоемкое оборудование, в домашних условиях его не сделать. Боевой софт производит небольшая группа людей, которых невозможно проконтролировать.

Киберугрозы, вирусоносители, все новые разработки потенциально могут использоваться в военных целях. На международном уровне государствам нужны определенные договоренности по контролю киберпространства.

Мы живем в симуляторе реального времени.

Ограничить развитие киберпространства невозможно, в современном мире реальность и виртуальность превратились в единую реальность.

Кибервойна и информационная война, применяемые в вооруженных конфликтах, хотя и является цифровыми, но имеют отличия:

– информационная – воздействует на массовое или индивидуальное сознание и психику;

– кибервойна – использует программный код, в целях причинения ущерба, перехвата управления, внесения неполадок, разрушения физических объектов, где используются компьютеры и телекоммуникационные сети.

Сегодня хакер может взломать любое устройство, связанное с компьютерными системами, вплоть да управления человеком, через электронный имплантант (всеобщая чипизация, биометрические технологии и данные только сыграют на руку злоумышленникам), прибегая к подлогу и искажению информации, может все, что угодно создать, а также все разрушить. Уже не ракеты, подлодки и танки играют важную роль, а простой хакер-одиночка, ради личного интереса, способен влезть в арсенал бактериологического оружия и уничтожить весь мир. Кевин Митник в 16 лет, взломал сеть Пентагона и противовоздушную оборону штата Колорадо, а после пятилетнего заключения стер из госреестра данные о своей судимости.

Кибербезопасность – это своего рода совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, данных. Профессионалы в области кибербезопасности ищут и анализируют новые угрозы, а затем разрабатывают способы борьбы с ними.

«Сегодня, когда открывается дверь в новый мир, где наряду с человеческим уже почти на равных проявляет себя искусственный интеллект, надо помнить, что мы не должны потерять главное – самого человека и все человеческое в этом человеке» (А. Г. Лукашенко)

Время – ключ к успеху. Сегодня, как и на ближайшее завтра, нет 100 % гарантии безопасности, еще не найдена «волшебная таблетка», способная решить все проблемы кибербезопасности. Переход от кибербезопасности к киберустойчивости – это важный шаг на пути к более надежному и устойчивому будущему.

Победители конкурса эссе среди обучающихся учреждений высшего образования *«Международное гуманитарное право и киберугрозы: новые вызовы современности»*

Диплом 1-й степени

Боярович Виктория Игоревна
Международный университет «МИТСО»,
студентка 3-го курса

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЗАЩИТЫ ГРАЖДАНСКОГО НАСЕЛЕНИЯ И ГРАЖДАНСКИХ ОБЪЕКТОВ В ПЕРИОД КИБЕРОПЕРАЦИЙ С ПОЗИЦИЙ МЕЖДУНАРОДНОГО ГУМАНИТАРНОГО ПРАВА

В современном мире в период научно-технического прогресса высокие технологии начали привносить новации в наши жизни и, в частности, в международное гуманитарное право (далее – МГП). В вооруженных конфликтах начали использоваться новые средства и методы ведения военных действий, наблюдается вторжение цифровых технологий на поле боя в виде кибероперациий, также произошли радикальные изменения в природе боевых действий в целом – человек перестает играть явную роль и вооруженные конфликты ведутся в новом пространстве – киберпространстве. На данный момент в повестке дня находится важный вопрос в отношении дальнейшей применимости и эффективной реализации общепризнанных принципов и норм МГП в области защиты гражданского населения и гражданских объектов в условиях кибернетических операций в период вооруженных конфликтов.

В первую очередь для исследования необходимо провести анализ положений Таллинского руководства 2.0 по международному праву, применимого к определению кибернетических войн (далее – Таллинское руководство 2.0), чтобы в дальнейшем ссылаться на дефиниции, имеющие разработанные определения, а именно: киберпространство – это среда, созданная на базе физических (кинетических) и нефизических (некинетических) компонентов для хранения, изменения, обмена данными с использованием компьютерных сетей [1]; кибероперация – это использование компьютерных возможностей (кибервозможностей) для достижения целей в киберпространстве или через него [1]. Согласно правилу 92, кибератака – это кибероперация, будь то наступательная или оборонительная, с использованием компьютерных технологий, которая способна привести к ранениям и гибели людей или нанести ущерб и разрушить объекты инфраструктуры [1]; кибероружие – это оружие, которое может быть а) направлено на конкретный военный объект или б) ограничено по критериям соразмерности, гуманности

и необходимости, как того требует право вооруженных конфликтов, следовательно, они могут нанести удары по военным и гражданским объектам [1].

В мире участились случаи кибератак против гражданского населения посредством дестабилизации работы инфраструктуры жизнеобеспечения. Например, в октябре 2021 года было осуществлено кибернападение на компьютерные системы медицинского центра «Гилель Яфе» в Израиле, которое подвергло опасности жизни людей в связи с вынужденной отсрочкой множества медицинских процедур. Подобные события становятся нередким явлением в мировой практике. В 2003 году в Ираке был зафиксирован взлом военной компьютерной системы, и в последующем незадолго до вторжения иракские военные получили письма на электронную почту министерства обороны Ирака с предупреждением, что против них готовится вооруженное нападение; в письме было упомянуто, что иракской стороне необходимо приготовить военную технику для обороны.

Многим известен вирус *Stuxnet*, запрограммированный на уничтожение компьютерной системы SCADA (Supervisory Control and Data Acquisition – диспетчерское управление и сбор данных) на объектах критической информационной инфраструктуры в Иране. Данный вирус-червь был классифицирован как кибероружие. Он в 2010 году вывел из строя центрифуги, которые использовались на ядерных объектах Ирана. Был нанесен ущерб оборонной системе страны и разработкам ядерной программы в целом. Современные тенденции демонстрируют, что гражданское население и инфраструктура крайне уязвимы, кибероперации в период вооруженных конфликтов также наносят значительный ущерб и ведение военных операций при помощи кибероружия – это вопрос настоящего, а не будущего.

В рамках рассматриваемой проблематики, представляется возможным в соответствии с нормами Женевских конвенций 1949 года [2] и дополнительных протоколов к ним вынести тезис, что гражданское население, а также отдельные гражданские лица не должны являться объектом кибератак. Статья 51 (2) Дополнительного протокола I (далее – ДП I) [3] и ст. 13 (2) Дополнительного протокола II (далее – ДП II) [4] применимы и подтверждают, что необходимо руководствоваться принципом различия между некомбатантами и комбатантами и гражданское население пользуется общей защитой, если оно не принимает участия в вооруженных конфликтах. Киберпространство не должно быть исключением в контексте данных норм, потому что гражданские субъекты находятся в такой же опасности, что и в вооруженных конфликтах, происходящих в наземных, воздушных, морских пространствах, знакомых нам. Вышеупомянутые случаи подтверждают на практике, что гражданское население уязвимо, когда, например, производится кибератака на больницу и медицинский персонал не может оказать помощь пациентам, потому что медицинская база данных была уничтожена. Невозможно исключить тот факт, что кибератака, направленная на военный объект, может привести к сопутствующему ущербу в виде гибели гражданского населения и ликвидации гражданской инфраструктуры, однако в соответствии с нормами МГП, это

недопустимо. Таким образом, мы видим, что в кибер-пространстве возможно и необходимо соблюдение основополагающих принципов МГП: принцип проведения различий между комбатантами и некомбатантами, принцип пропорциональности и принятия мер предосторожности при воору-женном нападении, а также запрет на причинение излишних страданий субъектам.

Следующий тезис – гражданские объекты не должны являться объектом кибератак, а киберинфраструктура может стать таковой целью в случае, если она квалифицируется как военный объект. В первую очередь необходимо дать определение понятию «киберинфраструктура». В соответствии с правилами Таллинского руководства 2.0, киберинфраструктура включает в себя системы, информационные и коммуникационные электронные сервисы и информацию, содержащуюся в этих системах и сервисах [1]. Исторически было закреплено в Санкт-Петербургской декларации 1868 года [5, с. 11], что единственной законной целью для противоборствующих сторон в период вооруженного конфликта являются военные объекты. Эта норма была регламентирована в статье 52 (1) ДП I [3] и данное правило применяется в условиях между-народных и немеждународных военных операций. Неизбирательные нападения также запрещены, поскольку они не направлены на конкретный объект и могут привести к сопутствующим жертвам. Соблюдение вышеперечисленных норм в киберпространстве является приоритетной задачей, так как главной целью в условиях вооруженного конфликта является защита гражданских объектов и гражданского населения. В киберпространстве особенно актуально соблю-дение общепринятых правил ведения боевых действий, начиная от принципов пропорциональности, соразмерности и мер предосторожности, до конкретных правил, таких как запрет на нападение на гражданскую инфраструктуру, необходимую для выживания населения, обязательство уважать и защищать медицинский персонал и многое другое.

С юридической точки зрения не должно быть сомнений в том, применимы ли существующие принципы и нормы МГП к новым видам оружия, средствам и методам ведения вооруженных конфликтов, в том числе основанных на информационных и телекоммуникационных технологиях и использующихся в киберпространстве. Когда государства в 1949 году принимали Женевские конвенции и в последующем дополнительные протоколы к ним, в первую очередь создавались нормы для урегулирования будущих конфликтов и договаривающиеся стороны предусмотрели разработку и использование новых средств и методов ведения военных операций, предполагая, что к ним будут применяться международно-правовые акты МГП. Например, ст. 36 ДП I является доказательственным примером, поскольку закрепляет, что «при изу-чении, разработке, приобретении или принятии на вооружение новых видов оружия, средств или методов ведения войны Высокая Договаривающаяся Сторона должна определить, подпадает ли их применение, при некоторых или при всех обстоятельствах, под запрещения, содержащиеся в настоящем Протоколе или в каких-либо других нормах международного права, применя-емых к Высокой Договаривающейся Стороне» [3].

Исходя из вышеизложенного представляется возможным сделать вывод, что мировому сообществу необходимо прийти к консенсусу и создать новые международно-правовые акты, которые будут включать новые правовые дефиниции, положения о применимости существующих норм международного гуманитарного права в киберпространстве и будут содержать запрет на то, что гражданское население и гражданская инфраструктура не должны являться объектами кибероперациий. Петер Маурер – президент Международного Комитета Красного Креста – в 2021 году подчеркнул, что обеспокоен гуманитарными последствиями в условиях кибератак и призывает к объединению усилий среди правительств стран мира, дабы своевременно среагировать на современный вызов, представляющий опасность всему человечеству. Однако в настоящее время, несмотря на отсутствие определенных универсальных и императивных норм в рассматриваемой области, необходимо придерживаться положений Женевских конвенций 1949 года и дополнительных протоколов к ним и ссылаться на оговорку Мартенса, которая гласит, что «в случаях, не предусмотренных принятыми постановлениями, население и воюющие остаются под охраною и действием начал международного права, поскольку они вытекают из установившихся между образованными народами обычаев, из законов человечности и требований общественного сознания».

Список цитированных источников

1. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / M. N. Schmitt [at al.] ; M. N. Schmitt [ed.]. – Cambridge : Cambridge University Press, 2017. – P. 563–576.

2. Женевские конвенции от 12 августа 1949 г. // Междунар. журнал Красного Креста. – 2000. – № 465. – С. 65–71.

3. Первый Дополнительный протокол к Женевским конвенциям от 12 августа 1949 года, касающийся защиты жертв международных вооруженных конфликтов // Междунар. журнал Красного Креста. – 2006. – № 861. – С. 23–44.

4. Второй Дополнительный протокол к Женевским конвенциям от 12 августа 1949 года, касающийся защиты жертв немеждународных вооруженных конфликтов // Междунар. журнал Красного Креста. – 2006. – № 861. – С. 105–144.

5. Санкт-Петербургская декларация: истоки, история принятия и современные задачи. Основной доклад : материалы Междунар. конф. по вопросам между-народного гуманитарного права, посвящ. 140-й годовщине принятия Санкт-Петербургской декларации 1868 г., 24 ноября 2008 г. : в 2 ч. / под ред. М. И. Кротова, Ф. Беллона. – М. : Региональная делегация МККК в Российской Федерации, Беларуси, Молдове и Украине, 2009. – Ч. 2. – 136 с.

Диплом 2-й степени

Коледа Антон Сергеевич
Международный университет «МИТСО»,
студент 4-го курса

ПРОБЛЕМЫ РЕГЛАМЕНТАЦИИ ВОЕННЫХ ДЕЙСТВИЙ В КИБЕРПРОСТРАНСТВЕ В КОНТЕКСТЕ СОВРЕМЕННОГО МЕЖДУНАРОДНОГО ГУМАНИТАРНОГО ПРАВА

Значительный прогресс в кодификации и имплементации норм международного гуманитарного права, достигнутый с момента его появления, впрочем, не исключил того, что на данный момент в указанной сфере существует достаточно большое количество проблем. Указанные проблемы – это, прежде всего, проблемы правового и гуманитарного характера, связанные с развитием информационно-коммуникационных технологий и появлением киберпространства.

Вопрос регламентации военных действий в киберпространстве является одним из самых серьезных и противоречивых в современном международном гуманитарном праве. Развитие информационных технологий оказывает серьезное влияние на ход современных вооруженных конфликтов. С одной стороны, компьютеризация средств ведения войны позволяет создать высокоточные типы вооружения, что потенциально снижает риски жертв среди гражданского населения. С другой стороны, распространение информационных технологий и средств связи трансформирует не только вооружение, но и критически важные объекты гражданской инфраструктуры, что позволяет сделать их потенциальной целью кибератак.

В современную эпоху, характеризующуюся ускорением процессов глобализации и информатизации, вопрос разработки единых международных норм, регулирующих процессы ведения военных действий в киберпространстве, переходит из разряда теоретических в разряд необходимых. Как отмечено выше из-за интенсивного использования компьютерных систем, гражданская инфраструктура становится крайне уязвимой для кибератак.

Например, нарушение работы учреждений здравоохранения, нефтеперерабатывающих заводов, банковских систем, систем управления автомобильным, воздушным и железнодорожным транспортом, плотин, может привести к серьезным катастрофам гуманитарного и экологического характера. Повреждение электронных сервисов по оповещению населения также повышает риски для гражданского населения, особенно во время вооруженных конфликтов. В таком случае гражданское население может быть недостаточно информировано, либо дезинформировано о времени работы гуманитарных коридоров, местонахождении пунктов эвакуации и приема пострадавших, а также об угрозе артиллерийских обстрелов и расположении бомбоубежищ.

Однако наиболее серьезный ущерб от кибератак может быть нанесен в результате повреждения атомных электростанций. Это может привести

к выбросу радиации в атмосферу, что повлечет за собой заражение почвы и питьевой воды, а также уничтожение гражданских объектов в результате взрыва. Угрозы подобного рода не являются теоретическими и имеют под собой вполне реальную основу. Известным примером является атака на электронные системы иранского завода по обогащению урана в Натанзе при помощи компьютерного вируса *Stuxnet*. В результате, около тысячи центрифуг были частично выведены из строя, а некоторые и разрушены [1].

Учитывая всю серьезность угрозы, исходящей от кибератак в контексте вооруженных конфликтов, на данный момент не существует какого-либо кодифицированного правового документа, регламентирующего все аспекты ведения военных действий в киберпространстве. Порядок привлечения к ответственности за кибератаки регулируется преимущественно на уровне национального законодательства. Такие нормы, как правило, применяются вне контекста вооруженных конфликтов и международного гуманитарного права. В настоящее время проводится разработка первых норм и регламентов, целью которых является наднациональная регламентация средств и методов ведения войны в киберпространстве.

В сентябре 2009 года эксперты из Центра киберзащиты НАТО, располагающегося в Таллине, разработали руководство (далее – Таллинское руководство), позволяющее регламентировать проведение кибероперaций стран-участниц НАТО. Оно содержит 95 правил проведения кибероперaций, основывающихся на существующих нормах международного гуманитарного права [2]. Таллинское руководство затрагивает как общие вопросы, связанные с проведением операций в киберпространстве, так и специфические, касающиеся суверенитета, нейтралитета и ответственности государств. Следует отметить, что, несмотря на свою прогрессивность, применение данного документа сильно ограничено. Таллинское руководство не является юридическим документом, носит рекомендательный характер и выражает лишь мнение отдельных экспертов. В 2017 году была разработана вторая версия Таллинского руководства, во многом дополнившая первоначальный документ.

Попытки регламентации военных действий в киберпространстве предпринимаются и на уровне международных организаций. В частности, Резолюция ООН A/RES/73/27 от 5 декабря 2018 г. призывает государства-участников соблюдать свои обязательства в информационной сфере и пресекать «совершения действий в сфере ИКТ, признанных вредоносными или способных создать угрозу международному миру и безопасности» [3].

В 2019 году, в соответствии с Резолюцией ООН A/RES/73/266, была создана группа правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности. ООН призывает государства-члены принимать во внимание ежегодные доклады данной группы экспертов и руководствоваться ее рекомендациями в процессе использования информационно-коммуникационных технологий [4].

Несмотря на фактическое отсутствие четкого регулирования военных действий в киберпространстве на международном уровне, специалисты Международного Комитета Красного Креста считают, что международное гуманитарное

право «применяется и, следовательно, ограничивает кибероперации во время вооруженного конфликта так же, как оно регулирует применение любого другого оружия, средств и методов ведения войны в вооруженном конфликте нового или старого типа» [5]. С данным мнением нельзя не согласиться, поскольку в тех случаях, когда средства и методы ведения войны прямо не ограничиваются действующими международными конвенциями, их использование по-прежнему регулируется общими запретами и правилами ведения военных действий. В частности, обычные нормы международного гуманитарного права запрещают нападения на гражданские объекты и гражданских лиц, несоразмерные нападения и применение неизбирательного оружия [6].

В тоже время отличительной чертой многих инструментов для проведения кибероперацій, например, компьютерных вирусов, является функция самокопирования, что подвергает потенциальному риску любое устройство, имеющее доступ в Интернет. Вредоносное программное обеспечение такого типа носит неизбирательный характер и, следовательно, их применение является незаконным в контексте международного гуманитарного права [7]. Вместе с тем инструменты, использующиеся для проведения кибероперацій, не обязательно приводят к нанесению вреда гражданской инфраструктуре. Специалисты Международного Комитета Красного Креста определили, что существует класс киберинструментов, которые были разработаны и используются с целью нанесения вреда только конкретным военным объектам, однако кибероперации подобного рода требуют тщательного планирования и подготовки личного состава [7].

Следует отметить, что на данном этапе привлечение к ответственности за несанкционированное использование кибероружия является крайне сложным процессом. В силу анонимности, предоставляемой киберпространством, многие пользователи могут скрывать или подделывать свою настоящую идентичность. Это создает трудности во время вооруженных конфликтов, поскольку невозможность идентификации атакующего не позволяет определить, применимы ли нормы международного гуманитарного права в каждом конкретном случае. Стороны конфликта могут воспользоваться данным фактором, отрицая свою причастность к операции, что во многом создает угрозу неисполнения действующих международных норм.

Исходя из вышеизложенного полагаем, что международно-правовое регулирование военных действий в киберпространстве на текущий момент является недостаточным. Возможным решением данной проблемы может стать принятие международной конвенции о кибероружии. В силу изменчивой природы информационного пространства и быстрого прогресса в сфере информационно-коммуникационных технологий, такая конвенция должна носить рамочный характер и содержать четкие определения таких понятий, как кибероружие, кибервойна и кибероперации, для превентивного регулирования всех новых типов вооружения.

Список цитированных источников

1. Cyber Warfare and International Humanitarian Law : A Study [Electronic resource] // ResearchGate. – Mode of access: https://www.researchgate.net/publication/335365277_Cyber_Warfare_and_International_Humanitarian_Law_A_Study. – Date of access: 03.05.2022.
2. Tallinn manual on the international law applicable to cyber warfare [Electronic resource] // Cambridge University Press. – Mode of access: https://dixon.hh.se/urbi/SCADA/TallinnManual.pdf. – Date of access: 03.05.2022.
3. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности [Электронный ресурс] : Резолюция Генер. Ассамблеи ООН от 5 дек. 2018 г. A/RES/73/27 // ODS – Sedok. – Режим доступа: https: // documents-dds-ny.un.org/doc/UNDOC/GEN/N18/418/07/PDF/N1841807.pdf?OpenElement. – Дата доступа: 03.05.2022.
4. Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности [Электронный ресурс] : Резолюция Генер. Ассамблеи ООН от 22 дек. 2018 г. A/RES/73/266 // ODS – Sedok. – Режим доступа: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/418/07/PDF/N1841807.pdf?OpenElement – Дата доступа: 03.05.2022.
5. International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, 2019 [Electronic resource] // ICRC. – Mode of access: https://rcrcconference.org/app/uploads/2019/10/33IC-IHL-Challenges-report_EN.pdf. – Date of access: 03.05.2022.
6. Rule 71. Weapons That Are by Nature Indiscriminate [Electronic resource] // ICRC. – Mode of access: https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule71. – Date of access: 03.05.2022.
7. International humanitarian law and cyber operations during armed conflicts [Electronic resource] // ICRC. – Mode of access: https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts. – Date of access: 03.05.2022.

Диплом 3-й степени

Греков Алексей Сергеевич
Белорусский государственный
экономический университет,
студент 2-го курса

УГРОЗА ЭКОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВ ПРИ ВЕДЕНИИ ВОЕННЫХ ДЕЙСТВИЙ С ИСПОЛЬЗОВАНИЕМ АВТОНОМНЫХ СИСТЕМ

Обеспечение безопасности – одна из ключевых функций государства. Концепция национальной безопасности Республика Беларусь, утвержденная Указом Президента Республики Беларусь № 575 от 9 ноября 2010 г. (далее – Концепция), определяет основные направления обеспечения безопасности и закрепляет такое понятие, как экологическая безопасность. Согласно статье 4 Концепции, под экологической безопасностью понимается «состояние защищенности окружающей среды, жизни и здоровья граждан от угроз,

возникающих в результате антропогенных воздействий, а также факторов, процессов и явлений природного и техногенного характера» [1].

Благоприятная окружающая среда – один из главнейших факторов для существования человека. Любые изменения состояния окружающей среды, причиной которых иногда становятся вооруженные конфликты, могут негативно воздействовать как на население одной страны, так и на человечество в целом. Учитывая исторический аспект, следует отметить, что результатом военных действий может являться нанесение значительного экологического ущерба. Так, в августе 1945 года произошли две атомные бомбардировки Хиросимы и Нагасаки, по итогу которых большая часть территории Японии подверглась радиоактивному загрязнению.

Содержание понятия «война» в современном мире сильно изменилось. В настоящее время военные действия носят преимущественно гибридный характер, в том числе используются информационные технологии и достижения научно-технического прогресса. До сих пор не согласовано определение кибервойны, которая, на наш взгляд, включает в себя использование технических средств или повреждение компьютеров, сетей и систем онлайн-контроля в условиях вооруженного конфликта. Поскольку кибервойны еще не велись, по крайней мере открыто, возникает вопрос о том, существуют ли нормы международного права, которые регулируют общественные отношения в данной сфере. В 2013 и 2017 годах группа экспертов по международному гуманитарному праву собиралась для создания Таллинского руководства (далее – Руководство), которое на сегодняшний день представляет собой наилучшую попытку адаптировать традиционное право ведения войны к киберпространству.

Концепция Руководства заключается в том, чтобы традиционные нормы и принципы международного гуманитарного права можно было применить по аналогии и к кибервойне. Например, Таллинское руководство определяет кибератаку как кибероперацию и акцентирует внимание на том, что разумно ожидать от кибератаки нанесение телесных повреждений или причинение смерти, либо повреждение или разрушение объектов инфраструктуры. Это определение аналогично общему определению термина «нападение» в международном гуманитарном праве. Однако в Руководстве также учитывается тот факт, что люди могут пострадать в результате прямого нападения на компьютерную систему, которое приведет к отказу какого-либо механизма, необходимого для их жизнедеятельности. Например, кибератака на систему очистки воды, в результате чего зараженная вода подается гражданскому населению, что принесет не только материальный, но и экологический ущерб.

Точно так же определение правила (принципа) соразмерности в Таллинском руководстве очень похоже на его общее определение в международном гуманитарном праве. В комментарии к Руководству подчеркивается, что характер атаки как «кибератаки» не меняет того факта, что Правило применимо только тогда, когда гражданские лица ранены или убиты или гражданские объекты уничтожены.

В современных реалиях появилась возможность внедрения боевых технологий, включающих автономные системы вооружений, к примеру, дронов, управляемых издалека, хотя и контролируемых операторами. Кроме того,

разрабатываются все более сложные автоматизированные системы. Более совершенные системы могут работать полностью автономно, и оператор может остановить операцию только в случае необходимости.

С точки зрения международного гуманитарного права в целом и принципа соразмерности в частности, можно выделить преимущества автономных систем оружия, которые оснащены искусственным интеллектом. Текущие разработки в области вычислительной техники могут быстро и точно собирать информацию в большом объеме, что превосходят человеческие возможности. Автономные системы могут быть запрограммированы на учет большого количества переменных и применять более строгие процедуры. На наш взгляд, автономное оружие может реализовать принцип соразмерности с большей точностью, чем комбатанты. Кроме того, достижение соглашения относительно алгоритма применения указанного принципа, способствовало бы единообразному его применению, позволило бы избежать двусмысленности и неопределенности. Таким образом, использование таких автоматизированных систем обладает определенными преимуществами.

Несмотря на рассмотренные выше преимущества, можно выделить несколько аргументов против использования автономных систем.

Первый – искусственный интеллект не должен принимать решения в отношении комбатантов. Более того, принцип соразмерности, требует сложных правовых оценок относительно ценности военных преимуществ, способов и средств ведения военных действий, принятия решений в непредвиденных ситуациях.

Второй аргумент состоит в том, что автономное оружие может подвергаться кибератакам. Если военные действия будут вестись с участием роботов, требует разрешения вопрос защиты их от взлома. Также представляется, что есть два основания, которые представляют собой серьезную проблему для способности автономных систем вооружений применять принцип соразмерности: обучение автономной системы и ее ответственность.

Идея о том, что автономная система вооружения может быть «запрограммирована» на включение норм международного гуманитарного права, противоречива. Современное машинное обучение основано на идее о том, что используя и анализируя большой массив данных, компьютеры могут устанавливать закономерности лучше, чем люди. В настоящее время человек может вмешиваться в работу систем, обучать и направлять их. Однако достаточно скоро мы можем столкнуться с реальностью, в которой машины будут учиться работать у машин, при очень небольшом участии человека.

Соблюдение международного гуманитарного права основано на концепции о том, что ответственность за нарушения его норм возлагается на конкретное государство (международно-правовая ответственность), а также физическое лицо (индивидуальная уголовная ответственность). Данную концепцию достаточно просто понять на примере комбатанта, управляющего ракетной установкой. В этом случае солдат получает приказы от командира, который является частью цепочки командования государства.

Закономерно возникает вопрос о том, как эту ситуацию экстраполировать на автономную систему вооружений, в которой единственное лицо, участ-

вовавшее на этапе создания, было программистом? Подлежит ли программист уголовной ответственности за действия, которые могут быть совершены искусственным интеллектом через много лет после прекращения его участия? Будет ли нести международно-правовую ответственность государство, купившее систему, за отсутствие проверки системы вооружений на соответствие нормам международного гуманитарного права?

Необходимо отметить, что человек, как комбатант, не способен нанести значительного материального и экологического ущерба, в отличие от автономных систем вооружения. Особое внимание надо уделить тому, что подобного рода системы могут быть использованы воюющими сторонами против стратегически важных объектов посредством кибератаки. К таким объектам можно отнести атомные электростанции. При совершении кибератаки на атомную электростанцию возможным последствием может стать причинение значительного экологического ущерба в результате радиоактивного загрязнения.

Как уже отмечалось ранее, автономные системы вооружения могут влиять на экологическую безопасность государств. Так, например, 14 сентября 2019 г. произошла атака дронов на нефтяные объекты Саудовской Аравии, в результате которой пострадала установка подготовки нефти. Данное событие принесло не только материальный ущерб, но и экологический вследствие пожара и разлива нефти на большую часть территории. Атака дронами, как автономными или полуавтономными системами, ставит большое количество вопросов перед международным сообществом. Кто является субъектом запуска дронов? Какие нормы применимы к такой ситуации? Как квалифицировать данное деяние?

Любое военное столкновение зачастую носит, прежде всего, либо завоевательный, либо оборонительный характер. В процессе вооруженного конфликта стороны могут не просчитывать возможные варианты причинения вреда окружающей среде, ставя перед собой задачи сугубо военного характера. В тоже время экологическая безопасность остается одним из факторов, влияющих на другие виды безопасности государства, такие как экономическая безопасность и демографическая безопасность.

Таким образом, окружающая среда, а также ее охрана остается одной из основных задач не только государства, но и мирового сообщества в целом. Развитие технологий активизирует сотрудничество государств по правовому регулированию использования автономных систем в условиях вооруженного конфликта. Вопросы кибербезопасности, поскольку они могут воздействовать на состояние окружающей среды, должны быть урегулированы как на международном, так на национальном уровнях, с учетом развития научно-технического прогресса.

Список цитированных источников

1. Концепция национальной безопасности Республики Беларусь [Электронный ресурс] : Указ Президента Респ. Беларусь, 9 нояб. 2010 г., № 575 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

Научное издание

КИБЕРУГРОЗЫ КАК НОВЫЙ ВЫЗОВ ДЛЯ МЕЖДУНАРОДНОГО ГУМАНИТАРНОГО ПРАВА

СБОРНИК МАТЕРИАЛОВ
СТУДЕНЧЕСКОЙ НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ

(г. Минск, 27 мая 2022 г.)

Редактор *Н. И. Рудович*
Компьютерная верстка *Т. С. Тимошенко*
Дизайн обложки *Е. А. Полторжицкая*