УДК 342.9 **DOI 10.52928/2070-1632-2024-66-1-56-59**

ЧЛЕНСТВО В КИБЕРДРУЖИНАХ КАК ПЕРСПЕКТИВНАЯ ОРГАНИЗАЦИОННО-ПРАВОВАЯ ФОРМА УЧАСТИЯ ГРАЖДАН РЕСПУБЛИКИ БЕЛАРУСЬ В ОХРАНЕ ОБЩЕСТВЕННОГО ПОРЯДКА

С.С. КОЛЁСКО
(Военная академия Республики Беларусь, Минск)

В информационном пространстве сформировалась новая реальность и новый тип социальных отношений, а, соответственно, и новый тип социальных угроз. Влияние информационного пространства на состояние общественной безопасности очевидно, что и обусловливает необходимость оказания гражданами содействия правоохранительным органам в обеспечении информационной безопасности в сети Интернет так же, как и в общественных местах. В данной статье обосновывается необходимость закрепления кибердружин как одной из перспективных организационно-правовых форм участия граждан в охране общественного порядка.

В статье исследовано влияние информационного пространства на состояние общественной безопасности, общественного порядка, а также рассмотрен международный опыт и меры противодействия влиянию негативной информации на рассматриваемые общественные отношения. Проведенный анализ позволяет рассматривать кибердружины в качестве перспективной организационно-правовой формы участия граждан в охране общественного порядка.

Ключевые слова: *граждане, сеть Интернет, общественный порядок, общественная безопасность, информационная безопасность, кибердружина.*

Введение. На современном этапе именно информационная сфера приобретает ключевое значение в социуме, оказывая всеобъемлющее влияние на человека. Формируемое в глобальном масштабе информационное пространство представляет собой новый этап развития общества с преобладанием знаний и информации, воздействием информационных технологий на все сферы жизнедеятельности, в том числе на общественный порядок и общественную безопасность[1]. В этой связи особую актуальность приобретают вопросы изучения возможности участия граждан в совместном с правоохранительными органами поддержании информационного пространства в состоянии, обеспечивающем минимизацию рисков и угроз в сфере общественной безопасности.

Основная часть. Трансформация социума в информационное общество порождает новые риски, вызовы и угрозы, которые напрямую затрагивают вопросы обеспечения общественной безопасности, негативно воздействуют на общественный порядок. Одной из составляющих современного информационного общества является наличие электронных систем коммуникации и общения, главным среди которых выступает глобальная сеть Интернет. Интернет является одной из самых крупных компьютерных сетей в мире, т.н. универсальной интерактивной средой, позволяющей обществу вступать в коммуникации, транслировать различного рода информацию на большие расстояния при минимальных затратах времени.

В интернете встречается огромное количество различной информации, как полезной, так и негативной. В свою очередь уровень отрицательной информации в сети стремительно растет, что характерно и для Республики Беларусь[2]. Отсутствие должного контроля, регулирования и фильтрации интернета приводит к тому, что именно туда перебираются «новые поколения» злоумышленников и преступников. Как итог – мы имеем одно из важнейших благ цивилизации, в котором, помимо бесчисленного множества плюсов, затаилось огромное количество злоумышленников, использующих и воспроизводящих запрещенную и закрытую информацию, прибегающих к безграничности и анонимности пространства, что позволяет им скрываться от наказания [1, с. 235]. Невозможность контроля сети Интернет сформировало уникальную среду для ведения пропаганды и информационных войн, массовых компаний по дезинформации и распространению фейков.

Главный источник негативной информации в сети Интернет в масштабах нашей страны – это внешние структуры, которые извне производят так называемый деструктивный контент. Такие вещи, как «синие киты», наркоиндустрия, дискредитация традиционных семейных ценностей, пропаганда ЛГБТ-движения и иные материалы неслучайным образом возникают внутри информационного поля государства. Эти явления, как правило, заносятся извне[3]. Так, за последнее время во всемирной сети существенно увеличился уровень содержания и распространения порнографии, экстремистских материалов, информации, пропагандирующей войну, разжигание национальной, расовой, религиозной ненависти и вражды, позитивное отношение к насилию, терроризму, криминальному миру, курению, алкоголю, наркотикам, суицидам, разрушению традиционного семейного уклада и т.д., что закономерно повлияло и на увеличение киберпреступлений в Республике Беларусь.

---

[1] О Концепции информационной безопасности Республики Беларусь [Электронный ресурс]: Постановление Совета Безопасности Респ. Беларусь, 18 марта 2019 г., № 1 // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024.

[2] URL: http://usiazh.by/obsh-zhizn/dobrovolnaja-druzhina/.

[3] URL: https://zavtra.ru/blogs/chto_takoe_kiberdruzhini.

В частности, общее количество зарегистрированных преступлений в Республике Беларусь в 2010 г. – 140920, из них киберпреступлений – 2514 (1,8% от общего числа преступлений). В 2015 г. общее количество зарегистрированных преступлений – 96982, из них киберпреступлений – 2440 (2,5% от общего числа преступлений), а в 2023 г. количество преступлений – 85456, из которых киберпреступления – 18459, что составило уже 21,5% от общего объема преступлений[4]. Главная причина роста – резкое увеличение преступлений, связанных с хищением путем использования компьютерной техники, и преступлений против информационной безопасности. Получается, что каждое четвертое преступление, которое было совершено в нашей стране в 2020 г., каждое пятое в 2021, 2023 гг. и каждое шестое в 2022 г. было связано с информационными технологиями[5].

Таким образом, при наблюдающейся общей тенденции к снижению преступности в Республике Беларусь, количество киберпреступлений кратно растет. Приведенные выше данные в очередной раз доказывают необходимость развития в Республике Беларусь эффективных, соответствующих времени, правовых норм, касающихся регулирования отношений в сети Интернет, а также поиска форм и способов противодействия деструктивному контенту.

Частичным выходом из сложившейся ситуации послужила активизация государства по приведению законодательства Республики Беларусь в состояние, обеспечивающее безопасность в информационном пространстве.

Так, в целях создания условий для развития национального сегмента глобальной компьютерной сети Интернет был принят Указ Президента Республики Беларусь от 1 февраля 2010 г. № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет»[6]. В 2019 г. была принята Концепция информационной безопасности Республики Беларусь, которая представляет собой систему официальных взглядов на сущность и содержание обеспечения национальной безопасности в информационной сфере, определяет стратегические задачи и приоритеты в области обеспечения информационной безопасности. А сравнительно недавно в целях повышения уровня защиты национальной информационной инфраструктуры от внешних и внутренних угроз был принят Указ Президента Республики Беларусь от 14 февраля 2023 г. № 40 «О кибербезопасности»[7].

Таким образом, анализ нормативных правовых актов, регулирующих защиту интересов личности, общества и государства в информационной сфере, позволяет сделать вывод, что законодательство Республики Беларусь в целом обеспечило создание правовых механизмов, обеспечивающих устойчивость к негативному воздействию деструктивной информации в сети Интернет. Вместе с тем, основной акцент в указанных нормативных правовых актах сконцентрирован на защите национальной информационной инфраструктуры, в то время как практически без внимания остается защита интересов личности, что, с учетом стремительного роста информации в мире, только усугубляет положение. В настоящее время специальных служб, в компетенции которых находится Интернет-безопасность нашего государства, явно недостаточно. Об этом свидетельствует выше приведенные статистические данные. Выходом в сложившейся ситуации видится привлечение социально активной части общественности, которая, с одной стороны, будет посредством имеющихся знаний не «засорять» сеть Интернет, а с другой, – оказывать содействие правоохранительным органам в борьбе с интернет-ресурсами, содержащими негативную и противоправную информацию.

Стоит отметить, что с подобными проблемами сталкивается большинство стран в мире, в связи с чем интересен их опыт борьбы и противодействия деструктивному контенту.

Генеральная ассамблея ООН 27 декабря 2019 г. приняла резолюцию «Противодействие использованию информационно-коммуникационных технологий в преступных целях», призванную бороться с деструктивным контентом. Согласно документу, учрежден специальный межправительственный комитет экспертов, представляющий все страны и предназначенный для улучшения координации действий и сотрудничества между государствами в борьбе с использованием высоких технологий[8].

Больших успехов в сфере борьбы с негативной и противоправной информацией в глобальном информационном пространстве достигли США. В стране функционирует большое количество общественных организаций по борьбе с деструктивной и экстремистской информацией в интернет-пространстве, которые работают на правительство США. В общественных местах, где имеется свободный доступ в глобальную сеть, включая библиотеки и школы, применяются фильтры, которые ограничивают доступ к интернет-ресурсам, содержащим антиобщественную информацию, в том числе материалы экстремистского и террористического толка [2, с. 79]. С 2007 г. в Германии функционирует специальная группа, в обязанности которой входит выявление случаев радикальной пропаганды, а также анализ работы отдельных интернет-ресурсов, представляющих потенциальную опасность [3, с. 189]. В Великобритании довольно успешно ведется работа интернет-сайта, на страницах которого представлен обзор стратегии деятельности полиции по деструктивному контенту. На сайте регулярно размещается конкретная информация о том, как отдельные граждане, являющиеся членами местного сообщества, могут оказать

[4] URL: https://zavtra.ru/blogs/chto_takoe_kiberdruzhini.
[5] Там же.
[6] О мерах по совершенствованию использования национального сегмента сети Интернет: Указ Президента Респ. Беларусь, 1 февр. 2010 г., № 60: в ред. Указа Президента Респ. Беларусь от 18 сент. 2019 г. № 350 // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024.
[7] О кибербезопасности [Электронный ресурс]: Указ Президента Респ. Беларусь, 14 февр. 2023 г., № 40 // КонсультантПлюс. Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024.
[8] URL: https://www.mid.ru/ru/foreign_policy/news/1770170/.

помощь полиции в ликвидации угроз терроризма, экстремизма, другой опасной информации [4, с. 38]. В Израиле целенаправленную работу по профилактике Интернета осуществляют некоторые неправительственные организации. Среди них Международный институт по противодействию терроризму (International Institute for Counter-Terrorism) – израильская общественная организация, которая работает с информацией, касающейся терроризма и экстремизма[9].

Однако, в большей степени интересен опыт Российской Федерации. Так, помимо всех государственных структур, занятых в области контроля Интернета, в 2011 г. в России появилось молодежное общественное движение «Кибердружина», созданное Лигой безопасного интернета (общественной организацией, созданной с целью цензурирования Интернета). По состоянию на 2022 г. в рядах общественного движения «Кибердружина» числится более 20 тыс. добровольцев со всей России, которые работают с деструктивным контентом в сети Интернет, а также помогают правоохранительным органам выявлять и привлекать к ответственности преступников из виртуальной среды. На данный момент отделения «Кибердружины» действуют в 38 регионах Российской Федерации[10]. По своей сути «Кибердружины» в России – это новое направление организации взаимодействия гражданского общества и уполномоченных органов власти в сфере выявления, профилактики и противодействия распространению противоправной информации.

По примеру «Кибердружин» Российской Федерации в 2020 г. на базе Витебского филиала УО «Белорусская государственная академия связи» возникла первая кибердружина в Республике Беларусь, которая действует на основании положения, утвержденного администрацией Железнодорожного района г. Витебска[11]. Также налицо одиночные случаи возникновения кибердружин в других регионах нашей страны. Однако из-за отсутствия законодательной базы, регламентирующей деятельность таких объединений, организации их взаимодействия с органами власти, а также отсутствие механизма стимулирования кибердружинников к осуществляемой деятельности, работа последних неоднородна, малоэффективна, а, соответственно, широкого распространения в нашей стране не получила[12]. Вместе с тем, на основании имеющегося опыта Витебской кибердружины, а также достижений в области противодействия деструктивному контенту кибердружинами Российской Федерации, представляется полезным закрепление данной инициативы как одной из организационно-правовых форм участия граждан в охране общественного порядка в Республике Беларусь.

В нашем понимании кибердружина должна представлять собой именно основанное на членстве объединение граждан Республики Беларусь, которое предназначено для оказания содействия правоохранительным органам в поддержании безопасной информационной среды в сети Интернет. Иными словами, кибердружина должна представлять собой общественную, то есть, неправительственную организацию, которая ни в коем случае не должна подменять полномочия правоохранительных органов в вопросах поддержания информационной безопасной. И здесь изначально главным дискуссионным аспектом выступает перечень негативной и противоправной информации, которая будет являться объектом поиска членами кибердружин.

По нашему мнению, информация политического и государственного характера изначально должна быть вне поля деятельности членов кибердружин. В свою очередь, информация, касающаяся охраны жизни, здоровья, свобод личности должна стать главным объектом для работы кибердружин. То есть сделать основной акцент не на каких-либо политических высказываниях граждан, не пытаться использовать потенциал кибердружин для борьбы с «инакомыслием» в сети, а сосредоточиться на поиске пропаганды самоубийств, суицидов, наркоиндустрии, порнографии, проституции и т.д., того, что прямо влияет на жизнь и здоровье граждан.

Таким образом, под негативной и противоправной информацией, предлагаемой для поиска кибердружинниками, мы видим информацию:

– содержащую признаки призывов к самоубийствам и суицидам, пропаганды наркотиков, порнографии, проституции, курения, алкоголя и азартных игр;

– содержащую пропаганду насилия, терроризма, криминального мира;

– пропагандирующую разжигание национальной, расовой, религиозной, этнической ненависти и вражды;

– способную причинить вред имущественного характера;

– иную информацию, способную причинить вред здоровью и развитию личности.

Таким образом, кибердружины, собирая, систематизируя и передавая указанную негативную и противоправную информацию в правоохранительные органы, должны стать своеобразным фильтром, помогающим отсекать всё вредоносное, опасное и дестабилизирующее, и в то же время не ограничивать свободы выражения мнений граждан согласно ст. 33 Конституции Республики Беларусь.

Информация, поиск которой должны осуществлять кибердружинники, накладывает отпечаток на возрастной ценз для членов кибердружины. Так, по нашему мнению, в кибердружину могут вступать граждане Республики Беларусь, достигшие 18-летнего возраста, способные по своим деловым и моральным качествам, уровню

[9] URL: https://crss.uz/2018/12/25/iskusstvo-borby-s-terrorizmom-v-izraile/.
[10] URL: http://ligainternet.ru/liga/activity-cyber.php.
[11] URL: https://vitebsk.gov.by/ru/gorod-ru/view/kakimi-uspexami-mogut-poxvastatsja-vitebskie-kiberdruzhinniki-21545/.
[12] Кибердружина [Электронный ресурс] / Средняя школа № 11 г. Гомеля. – URL: https://gomelschool11.by/vospitatelnaja-i-ideologicheskaja-rabota/detskie-i-molodezhnye-obedinenija/kiberdruchina/.

ИКТ-компетентности противодействовать распространению в сети Интернет негативной и противоправной информации. Стоит отметить наличие у потенциальных членов кибердружин достаточного уровня ИКТ-компетентности, т.е. необходимо владение способностями использовать информационные и коммуникационные технологии для доступа к информации, её поиска, организации, обработки, оценки и передачи в условиях развитого информационного общества[13]. Компетенции и возраст, которыми должны обладать кибердружинники, позволяют утверждать, что это будут, как правило, учащиеся и студенты ссузов и вузов страны, а также граждане специализированных и профильных учреждений и организаций, задействованных в IT-индустрии. К, примеру, состав кибердружин в Российской Федерации показывает тождественные взгляды по принципу их комплектования.

Заключение. Таким образом, в настоящее время Интернет открыл широкие возможности для манипулирования общественным сознанием, причем уже не только в виртуальном пространстве, но и в реальности, что заставляет государство и общество искать дополнительные инструменты нивелирования указанных результатов отрицательного воздействия. Для борьбы с распространением негативной информации в сети Интернет ежегодно отрабатываются многочисленные алгоритмы работы, один из которых по примеру международного опыта видится в привлечении социально активной части общественности, которая, с одной стороны, будет посредством имеющихся знаний не «засорять» Интернет, а с другой, – оказывать содействие правоохранительным органам в борьбе с интернет-ресурсами, содержащими негативную и противоправную информацию. На основании изложенного представляется полезным рассмотрение кибердружин как одной из перспективных организационно-правовых форм участия граждан в охране общественного порядка в Республике Беларусь.

ЛИТЕРАТУРА

1. Савоськин К.Г. К вопросу о создании «кибердружин» // Юридические науки, правовое государство и современное законодательство: VII Междунар. науч.-практ. конф., Пенза, 05 июня 2019 г.: тез. докл. / Орлов. гос. ун-т им. И.С. Тургенева. – Пенза, 2019. – С. 235–236.
2. Круглова А.Ю. Зарубежный опыт противодействия деструктивным сетевым исламистским и тюркско-исламистским структурам в сети Интернет // Обзор.НЦПТИ. – 2020. – № 2(21). – С. 77–83.
3. Бураева Л.А. Кибертерроризм как новая и наиболее опасная форма терроризма // Проблемы экономики и юридической практики. – 2017. – № 2. – С. 188–190.
4. Завьялов С. Зарубежный опыт в области борьбы с пропагандой терроризма в интернете // Зарубежное военное обозрение. – 2014. – № 4. – С. 34–39.

Поступила 19.03.2024

MEMBERSHIP IN CYBER FRIENDS AS A PROMISING ORGANIZATIONAL AND LEGAL FORM OF PARTICIPATION OF CITIZENS OF THE REPUBLIC OF BELARUS IN SECURITY PUBLIC ORDER

S. KOLIOSKO
(Military Academy of the Republic of Belarus, Minsk)

A new reality and a new type of social relations have formed in the information space, and, accordingly, a new type of social threats. The influence of the information space on the state of public security is obvious, which determines the need for citizens to assist law enforcement agencies in ensuring information security on the Internet, as well as in public places. This article substantiates the need to consolidate cyberdrugs as one of the promising organizational and legal forms of citizen participation in the protection of public order.

The article examines the influence of the information space on the state of public safety and public order, as well as international experience and measures to counteract the influence of negative information on the considered public relations. The analysis allows us to consider cyberdrugs as a promising organizational and legal form of citizen participation in the protection of public order.

Keywords: *citizens, Internet, public order, public safety, information security, cyber friends.*

[13] Информационно-коммуникационно-технологическая компетенция (ИКТ-компетенция) [Электронный ресурс] / Молодой ученый. – URL: https://moluch.ru/archive/63/9900/.