4. Гуценко, К. Ф. Уголовный процесс западных государств : учеб. пособие / К. Ф. Гуценко, Л. В. Головко, Б. А. Филимонов ; под ред. К. Ф. Гуценко. – М. : Зерцало-М, 2001. – 470 с.

5. Зайцева, Л. Л. О совершенствовании права обвиняемого на защиту / Л. Л. Зайцева // Демократизм предварительного расследования : сб. науч. тр. / Мин. высш. шк. МВД СССР ; редкол.: Н. П. Митрохин [и др.]. – Минск, 1990. – С. 73–78.

6. Кожевников, А. В. Допуск адвоката-защитника в процесс / А. В. Кожевников // Актуальные проблемы охраны прав личности в советском уголовном судопроизводстве : межвуз. сб. науч. тр. / Свердл. юрид. ин-т ; редкол.: И. Я. Дюрягин [и др.]. – Свердловск, 1989. – С. 68–72.

7. Лисицин, Р. Д. Участие защитника в обеспечении прав и законных интересов подозреваемого / Р. Д. Лисицин // Защита прав человека и соблюдение законности органами внутренних дел : материалы Междунар. науч.-практ. конф., Москва, 10 дек. 1998 г. / Моск. юрид. ин-т МВД России ; отв. ред.: Л. Ш. Берекашвили, В. П. Игнатов. – М., 1999. – С. 143–150.

8. Лукичев, Н. А. Сторона защиты на предварительном следствии / Н. А. Лукичев // Следователь. – 2003. – № 11. – С. 20–27.

9. Мартинович, И. И. Адвокатура Беларуси: история и современность / И. И. Мартинович. – Минск : Тесей, 2002. – 176 с.

10. Ожегов, С. И. Словарь русского языка : ок. 57 000 слов / С. И. Ожегов ; под ред. Н. Ю. Шведовой. – 16-е изд., испр. – М. : Рус. яз., 1984. – 780 с.

11. Печерский, В. Тактика участия защитника на этапе подготовки к судебному разбирательству / В. Печерский // Юстыцыя Беларусі. – 2004. – № 1. – С. 76–79.

12. Пикалов, И. А. Роль защитника в процессе доказывания, при производстве расследования по уголовному делу / И. А. Пикалов // Закон и право. – 2004. – № 11. – С. 19–21.

13. Питулько, К. В. Право на защиту подозреваемых и обвиняемых, задержанных и заключенных под стражу / К. В. Питулько // Изв. вузов. Правоведение. – 2001. – № 5. – С. 135–147.

14. Шаров, Г. Оказание юридической помощи бесплатно / Г. Шаров // Рос. юстиция. – 2004. – № 6. – С. 44–49.

Дата поступления в редакцию: 19.02.2023

УДК 342.9

***Ю. Н. Заика**, аспирант юридического факультета Белорусского государственного университета*
e-mail: yurizaika@mail.ru

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОЛЬЗОВАТЕЛЕЙ СОЦИАЛЬНЫХ МЕДИА

Акцентируется внимание на необходимости обеспечения информационной безопасности, что обусловлено неоднозначным качеством информации в сети Интернет, детерминируется требованием единого понимания стратегических целей и общих задач и должно опираться на четко выстроенную правовую основу. Анализируется популярность социальных медиа в Республике Беларусь, исследуются угрозы, с которыми могут столкнуться пользователи социальных медиа. Формулируются предложения по совершенствованию законодательства в рамках исследуемого вопроса.

Ключевые слова: социальные медиа, социальные сети, мессенджеры, персональные данные, информационная безопасность.

***Y. N. Zaika**, Postgraduate student of the Faculty of Law of the Belarusian State University*
e-mail: yurizaika@mail.ru

THREATS TO SOCIAL MEDIA USERS' INFORMATION SECURITY

Due to the ambiguous quality of information on the Internet the author focuses attention on the need to ensure information security; the requirement of common understanding of strategic goals and common tasks is determined, that should be based on a clearly built legal framework. Popularity of social media in the Republic of Belarus is analyzed, the threats that social media users may face are investigated. Proposals to improve legislation within the framework of the issue under study are formulated.

Keywords: social media, social networks, messengers, personal data, information security.

Информационная сфера для любого государства и гражданина сегодня имеет определяющее значение. Обилие информационных источников и легкость доступа к ним предоставляют возможность любому человеку развиваться всесторонне еще больше. Для сбора информации об интересующем объекте достаточно ввести, используя сеть Интернет, поисковый запрос, чтобы получить не только текстовую информацию, но и видеоинструкции. Ресурсы сети Интернет позволяют обмениваться информацией практически без привязки к местности и технической оснащенности. В связи с этим возрастает значение коммуникационных технологий, расширяется область их использования населением, увеличивается роль информации в жизни общества. Вместе с тем качество информации в сети Интернет не всегда однозначно. Так, нередко можно встретить непроверенные, а иногда и целенаправленно искаженные сведения (фейки). Информационная агрессия на глобальном и национальном уровнях перестает быть редкостью, становясь центральным звеном гибридных войн. В связи с этим невозможно игнорировать принципиально новые риски, связанные с информатизацией: распространение недостоверной информации, осуществляемое с целью манипулирования массовым сознанием, наращивание и повышение деструктивного воздействия на общество. Вследствие этого сегодня необходима эффективная деятельность государства по обеспечению информационной безопасности, которая должна опираться на единое понимание стратегических целей, общих задач и разумно выстроенную правовую основу. Успешное осуществление этой деятельности невозможно без понимания всеми жителями Республики Беларусь потенциала и сопутствующих рисков, которые несет в себе современная информационная среда.

В настоящее время сеть Интернет не только выступает пространством для общения, но и является одним из основных источников получения новостей. Средствам массовой информации (СМИ) принадлежит сейчас основная роль в формировании ценностных ориентаций личности и общества, сохранении исторической памяти. Подавляющее большинство современных СМИ имеют собственные интернет-ресурсы. Многие государства, в том числе Республика Беларусь, относят к сфере действия законодательства о СМИ интернет-ресурсы, распространяющие массовую информацию.

Так, по данным компаний We Are Social и Hootsuite, отраженным в отчете о состоянии цифровой сферы Global Digital, в настоящее время во всем мире интернетом пользуются 4,95 млрд человек, что составляет 62,5 % населения Земли. Это количество из года в год увеличивается, и можно с уверенностью говорить, что эта тенденция к росту только продолжится, так как сегодня 67,1 % мирового населения, или 5,31 млрд человек, используют мобильные телефоны, а современные мобильные телефоны позволяют пользователям активно использовать ресурсы сети Интернет [9].

Социальные медиа, к которым могут быть отнесены все интернет-площадки, способные на основе онлайн-технологий предоставлять пользователям возможность устанавливать коммуникацию друг с другом и производить пользовательский контент, являются одними из наиболее популярных интернет-ресурсов. В мире насчитывается 4,62 млрд их пользователей (58,4 % мирового населения), их количество только за 2021 г. возросло на 424 млн человек. В среднем 9 из 10 пользователей сети Интернет используют социальные медиа хотя бы раз в месяц. Невозможно отрицать, что социальные медиа выступают сейчас в качестве основной платформы для распространения массовой информации [11].

На начало 2022 г. 85,1 % жителей Республики Беларусь являлись пользователями сети Интернет, что составляет более 7 млн человек. Из них 4,35 млн являются пользователями социальных медиа, или 46,1 % населения. Только за 2021 г. их количество возросло на 450 тыс. человек. Столь массовое использование социальных медиа приводит к тому, что они становятся полноценными коммуникационными центрами [9].

Растущая популярность социальных медиа требует их законодательного определения и регулирования. Определение интернет-ресурса, представленное в Законе Республики Беларусь от 17 июля 2008 г. № 427-З «О средствах массовой информации» (далее – Закон о СМИ), охватывает данное понятие, поскольку включает в себя форумы, блоги и части информационных ресурсов, однако, по нашему мнению, необходимо это определение конкретизировать и включить в него социальные сети и мессенджеры.

Социальные сети – это интернет-площадки, где можно размещать сведения о себе и обмениваться с другими пользователями информацией, фотографиями, сообщениями, различными файлами. Они позволяют общаться на расстоянии, искать утерянные контакты и новые знакомства, изучать иностранные языки, эффективно организовывать учебный процесс. Однако в социальных сетях всегда есть риск натолкнуться на вредную информацию, стать жертвой мошенников или приобрести интернет-зависимость. Существует множество негативных факторов влияния социальных сетей на человека. К ним можно отнести распространение информации, призывающей к потреблению наркотиков, суициду, вступлению в псевдорелигиозные секты или экстремистские организации, распространение порнографии, пропаганду насилия и жестокости. Наиболее популярными социальными сетями у белорусов являются «ВКонтакте» (3,8 млн пользователей), Instagram (3,7 млн) и TikTok (3,08 млн) [10].

Мессенджер – это программа, мобильное приложение или веб-сервис для мгновенного обмена сообщениями. Понятие «мессенджер» уже давно не связывают только с обменом текстовыми сообщениями. Современные мессенджеры реализуют голосовую и видеосвязь, обмен файлами, веб-конференции. Если рассматривать мессенджеры как средство обмена информацией со знакомыми между собой людьми, то здесь видится их неоспоримая польза. В то же время мессенджеры дают возможность вступать в различные группы с незнакомыми между собой пользователями. Такие группы могут становиться платформой для распространения непроверенной информации, влияющей на общественное мнение, а также информации деструктивного характера, направленной на разжигание вражды. Некоторые группы способны носить экстремистский характер. Существование подобных групп может причинить существенный вред правам их пользователей, в связи с чем видится необходимым принятие мер государственного регулирования указанного вопроса.

Законодательство Республики Беларусь не дает определения социальных медиа, в связи с этим предлагаем представить его в следующем виде: «социальные медиа – социальные сети, мессенджеры, форумы, блоги, сайты знакомств, видеохостинги и иные информационные ресурсы, позволяющие пользователям устанавливать коммуникацию друг с другом и производить пользовательский контент». Наиболее уместным видится закрепление данного определения в Законе о СМИ, так как значительная часть отношений, происходящих в социальных медиа и требующих правового регулирования, связана с распространением с их помощью массовой информации.

В данном контексте важно определить, могут ли социальные медиа быть отнесены к СМИ. По нашему мнению, СМИ они не являются, так как по сути не предназначены для периодического распространения массовой информации. Массовая информация часто распространяется в них в виде единичного сообщения. В то же время полагаем, что социальные медиа относятся к интернет-ресурсам, посредством которых распространяется массовая информация, и, следовательно, действие Закона о СМИ распространяется и на них согласно ч. 2 ст. 3.

Введение понятия «социальные медиа» и конкретизация понятия «интернет-ресурс» позволит более эффективно осуществлять правовое регулирование общественных отношений, связанных с распространением массовой информации в наиболее популярной сфере коммуникации в сети Интернет.

Проанализировав спектр угроз, с которыми могут столкнуться пользователи социальных медиа, логично выделить три основные группы негативных проявлений: угрозы в отношении персональных данных пользователя, угрозы в отношении имущества и угрозы, связанные с распространением непроверенной информации деструктивного характера.

Сегодня персональные данные – это источник богатства сам по себе. Предпочтения человека, его любимые места, близкие люди или любые другие подробности о нем являются ценной информацией. Раньше такие данные были бы мгновенно использованы для совершения кражи личности. Но сегодня злоумышленникам не менее выгодно их продать специальным организациям и сервисам, использующим такую информацию, чтобы настраивать целевую рекламу, запускать кампании социальной инженерии или влиять на пользователей с помощью других манипулятивных приемов. Многие персональные данные размещаются пользователями самостоятельно и добровольно на собственных страницах в социальных сетях. Другие данные, в том

числе данные о знакомствах, злоумышленники могут получить из переписки с пользователем или его информационных сообщений.

Одним из способов завладения конфиденциальной информацией является перенаправление с помощью гиперссылок на сайты, для входа на которые требуется наличие аккаунта в социальной сети. Пользователю предлагается повторно выполнить вход в его учетную запись на сайте, внешне похожем по оформлению на сайт соответствующей социальной сети, что пользователь может сделать машинально и по невнимательности. В таком случае данные для входа в учетную запись могут оказаться в руках злоумышленника. Для этого часто используются заманчивые и невероятные «кликбейтные» заголовки информационных статей. Такие заголовки также могут быть подобраны адресно с учетом персональных данных пользователя и его интересов. Многие социальные сети предоставляют возможность пользователю скрыть свои личные данные и предоставить возможность доступа к ним только пользователям из круга его «друзей» – подтвержденного пользователем списка. Чтобы обойти такой способ защиты, злоумышленники могут непосредственно использовать запрос на добавление в список друзей, также могут выполнить подобный запрос от имени человека, уже находящегося в таком списке, якобы с его новой страницы. Злоумышленник рассчитывает, что пользователь примет такой запрос по невнимательности или ссылаясь на сбой системы, при этом веря, что это действительно его знакомый [3].

Угрозы в отношении имущества пользователя напрямую связаны с угрозами в отношении персональных данных. Эти угрозы проявляются посредством финансового мошенничества, связанного с завладением данными о банковской платежной карточке. Форм такого мошенничества достаточно много, и они постоянно совершенствуются. Так, помимо привычных уже сообщений о получении неожиданного выигрыша или подарка, для получения которого необходимо внести некоторые комиссионные, пользователю может быть предложено пройти платный тест, опрос или конкурс, по итогу которого нужно лишь оставить данные банковской платежной карточки, чтобы получить вознаграждение. Помимо сведений о банковской платежной карточке таким способом злоумышленники могут получить информацию о круге знакомств и интересах пользователя. При этом, используя взломанную учетную запись, злоумышленники могут попросить денег в долг у пользователя из списка контактов жертвы взлома и завладеть денежными средствами. Реквизитами банковской платежной карточки также можно завладеть, используя предупреждения о чрезвычайных ситуациях от имени какой-либо организации, в том числе банковской, содержащие якобы срочную и важную информацию об учетной записи пользователя и требующие сообщить данные карточки, пароли или секретные проверочные слова [8].

Наибольшую угрозу, по нашему мнению, представляет распространение деструктивной информации, направленной на дестабилизацию общества и содержащей призывы к участию в массовых беспорядках и незаконных акциях. Для этих целей, как правило, используются специальные группы в мессенджерах, которые предоставляют часто непроверенную информацию в выгодном их администраторам ключе и координируют действия пользователей, откликнувшихся на содержащиеся в сообщениях призывы. В качестве примера таких групп могут быть приведены так называемые дворовые чаты, которых по состоянию на март 2021 г. в Республике Беларусь было создано более тысячи. Деструктивная агитация этих групп была направлена на усиление протестных настроений, использовались призывы к действиям, причиняющим вред национальной безопасности и направленным на дестабилизацию ситуации в обществе [4].

Организаторы наиболее радикальных групп, носящих явно выраженный экстремистский характер, привлекаются к административной или уголовной ответственности. Отправка ссылок на признанные запрещенными группы, а также пересылаемые оттуда материалы и сообщения также могут считаться распространением экстремистской информации [2].

Республика Беларусь идет по пути усиления ответственности за распространение заведомо ложных сведений о политическом, экономическом, социальном положении государства, правовом положении граждан, деятельности органов государственной власти и управления, дискредитирующих государство, если такие действия совершены в любом публичном выступлении, включая СМИ и социальные медиа. Об этом свидетельствует внесение изменений в Уголовный кодекс Республики Беларусь законом от 26 мая 2021 г. № 112-З, согласно которому кодекс до-

полнен ст. 369^1 «Дискредитация Республики Беларусь», устанавливающей ответственность за указанные действия, направленные на причинение существенного вреда государственным или общественным интересам.

В противодействии распространению заведомо ложных сведений нам видится необходимым проведение работы, направленной на повышение интернет-грамотности граждан, формирование у них скептического отношения к любой предоставляемой информации. В этой связи уместным видится введение правовой нормы, обязывающей лицо, размещающее ту или иную информацию, в обязательном порядке указывать источник этой информации. Информация, не имеющая подтвержденного источника, вызовет у пользователя обоснованное подозрение в ее достоверности. Принятие ложной информации за реальную может подтолкнуть к действиям, опасным не только для самого человека, но и для общества в целом.

В настоящее время Закон о СМИ не относит физическое лицо, не являющееся владельцем интернет-ресурса или сетевого издания и распространяющее массовую информацию, к субъектам правоотношений в сфере массовой информации. Следует понимать, что пользователь социальных медиа часто не является владельцем социальной сети, мессенджера или блога, но в то же время может осуществлять там распространение информации, создавая специальные группы или публикуя пользовательский контент. Таким образом, значительная часть общественных отношений оказывается вне сферы регулирования Закона о СМИ.

В связи с этим предлагаем дополнить ст. 1 Закона о СМИ следующим определением: «пользователь социального медиа – лицо, осуществляющее сбор, получение, передачу и распространение массовой информации с использованием социального медиа» и дополнить п. 21 указанной статьи словами «пользователь социального медиа».

По нашему мнению, содержание действий владельца интернет-сайта, размещающего на интернет-ресурсе (принадлежащем ему) массовую информацию, и пользователя социальной сети или мессенджера, размещающего на своей странице или в своей группе (владельцем которой он не является) массовой информации, является идентичной.

Введение указанных изменений позволит обеспечить реализацию пользователями социальных медиа принципа достоверности информации, а также порядка распространения сообщений и (или) материалов, ранее распространенных другим СМИ или интернет-ресурсом с указанием ссылки на источник информации, предусмотренных ст. 4 и ст. 17 Закона о СМИ.

Предлагаем также дополнить Закон о СМИ ст. 30^2 «Права и обязанности пользователя социального медиа» следующего содержания:

«1. Пользователь социального медиа имеет право:

1) собирать, получать, передавать и распространять информацию любым способом в соответствии с законодательством;

2) излагать в социальных медиа личные суждения и оценки с указанием собственного имени или псевдонима;

3) совершать иные действия в соответствии с законодательством.

2. Пользователь социального медиа обязан:

1) соблюдать основные принципы деятельности средств массовой информации;

2) анализировать содержание информации, размещаемой другими пользователями в созданной им группе в социальной сети или мессенджере, в принадлежащем ему блоге или на принадлежащей ему странице, где пользователь наделен правами модерирования сообщений;

3) не допускать распространения информации, распространение которой запрещено законодательством, а также материалов, содержащих нецензурные слова и выражения;

4) не допускать распространение информации, которая может причинить вред государственным или общественным интересам;

5) распространять информационные сообщения, ранее распространенные другим средством массовой информации или интернет-ресурсом, с указанием ссылки на источник информации;

6) не допускать использования созданной им группы в социальной сети или мессенджере, принадлежащего ему блога или принадлежащей ему страницы для осуществления запрещенной в соответствии с законодательными актами деятельности;

7) осуществлять удаление информации, содержание которой противоречит требованиям законодательства, размещенной другими пользователями в созданной им группе в социальной

сети или мессенджере, в принадлежащем ему блоге или на принадлежащей ему странице, где пользователь наделен правами модерирования сообщений».

Рассматривая техническую защищенность пользователей социальных медиа, необходимо отметить, что она во многом возложена на их владельцев и администраторов, что в значительной степени затрудняет обеспечение защиты граждан любым государством. Известны случаи утечки персональных данных пользователей, например Facebook. Так, в апреле 2021 г. на одном из хакерских форумов были размещены даты рождения и номера мобильных телефонов 533 млн пользователей из 106 стран мира [3].

Вопросы ответственности лиц, виновных в подобном широкомасштабном распространении данных, относятся к области гражданской и трудовой ответственности сотрудников компании. Каких-либо механизмов привлечения к иной ответственности законодательством не предусмотрено. Отказаться от использования Facebook по понятным причинам, связанным с ее массовостью, невозможно. Число пользователей Facebook на начало 2022 г. составило около 3 млрд человек. Другие социальные медиа не застрахованы от подобных ситуаций [9].

Анализируя техническую безопасность наиболее распространенных в Республике Беларусь социальных медиа, мы выделили ряд положительных сторон каждой из них.

Определенным плюсом социальной сети «ВКонтакте» является тот факт, что она не так сильно популярна за пределами СНГ, как Facebook. Кроме того, значительная часть ее кода написана кириллицей, что сужает круг людей, способных взломать или использовать такой код. Социальная сеть поддерживает двухфакторную аутентификацию (метод идентификации пользователя при помощи запроса данных двух типов, первый из которых – это логин и пароль, а второй – специальный код, приходящий по SMS или электронной почте, реже – это специальный USB-ключ или биометрические данные пользователя) и антивирусные программы. «ВКонтакте» поддерживает использование VPN (программа, изменяющая IP-адрес страны пользователя на IP-адрес той страны, где расположен сервер, в связи с чем все сайты начинают считать его пользователем, который физически находится в выбранной стране, и защищающая от перехвата пересылаемые пользователем данные) [7].

В числе плюсов социальной сети Instagram следует отметить защиту всех проходящих через серверы сообщений шифрованием, в связи с чем к ним невозможно получить доступ даже напрямую со стороны разработчиков Facebook – владельца Instagram. Кроме того, при использовании VPN стираются все возможные геотэги (указание о местонахождении пользователя). Сеть также поддерживает двухфакторную аутентификацию.

Приложение TikTok позволяет пользователю создавать и загружать короткие видеоролики любой тематики. Поддерживает регистрацию с помощью номера телефона, адреса электронной почты или учетной записи Facebook либо Instagram. При этом двухфакторная аутентификация не предусмотрена, что делает его менее безопасным, чем вышеуказанные социальные сети.

Существенным минусом всех представленных социальных сетей является сбор ими информации о пользователе, его данных, поисковых запросах, просмотренной информации. Цели подобного сбора в первую очередь коммерческие (адресная реклама), однако невозможно предугадать, как распорядятся такой информацией злоумышленники в случае, если получат к ней доступ [5].

Существенным плюсом мессенджера WhatsApp является отсутствие единого централизованного сервера. Коммуникация между пользователями происходит путем P2P-соединения (каждый узел сети как является клиентом, так и выполняет функции сервера в отличие от многоранговой сети, где осуществляется соединение с сервером и все данные хранятся на нем). Информация хранится на самих устройствах. К тому же, чтобы добавить кого-то в WhatsApp, необходимо знать телефонный номер этого человека, что создает трудности для злоумышленников. Мессенджер предоставляет полную анонимность, поддерживает VPN и антивирусные программы.

Telegram предоставляет условия безопасности даже более высокие, чем WhatsApp. Имеет превосходное P2P-шифрование и анонимность для всех желающих. Как и WhatsApp, требует номер телефона, чтобы подтвердить учетную запись, но как только подключение совершено, он больше не требуется, что создает еще большие условия для анонимности.

Большую часть мер, которые использует Viber для защиты данных, можно назвать стандартными. Так, в мессенджере применяется шифрование канала связи. Для пользователей предусмотрены дополнительные меры защиты, например верификация контактов. Эта функция позволяет синхронизировать ключи с собеседником. При подозрении в том, что чьим-то контактом завладели третьи лица, можно запросить сравнение ключа, т. е. проверить верификацию. Если ключи не совпадут, такого пользователя можно будет заблокировать. Существуют и другие способы повысить безопасность в мессенджере. Во-первых, это секретные чаты. В них работает end-to-end шифрование, которое позволяет скрыть содержимое переписки от третьих лиц. Во-вторых, в Viber есть скрытые чаты. Их содержимое не так защищено, как в секретных чатах, однако их будет сложнее найти всякому, кто получит доступ к устройству.

В пользовательском соглашении Viber отмечается, что персональную информацию пользователя могут раскрыть не только по запросу суда и органов надзора, но и для тех третьих лиц, которые могут помогать осуществлять деятельность сервиса. При этом всех вышеперечисленных третьих лиц никак не ограничивают в использовании этих данных. Другой подозрительный момент связан с секретными чатами. Их суть заключается в том, что данные из такой переписки не хранятся на сервере провайдера, а доступны исключительно на устройствах собеседников. Однако сервис предлагает получить к ним доступ и с третьего устройства. Это значит, что информация все же может покидать пределы секретного чата, а при желании ее могут использовать провайдер или даже другие лица [6].

В сравнении с социальными сетями мессенджеры имеют более высокий уровень безопасности, однако ввиду их принадлежности иностранным компаниям осуществить защиту пользователя на уровне отдельного государства очень тяжело. Установить и привлечь к ответственности лицо, нарушившее права гражданина Республики Беларусь и находящееся в другом государстве, крайне сложно. В этой связи наиболее перспективным видится международное сотрудничество в вопросах обеспечения безопасности пользователей социальных медиа.

С точки зрения защиты граждан Республики Беларусь со стороны государства видятся повышение их грамотности в вопросах интернет-безопасности, в том числе информирование об использовании VPN, и осведомленность о возможных угрозах, формирование скептического отношения к размещаемой в сети информации, недоверчивость к СМИ, публикующим сведения без указания их источника.

Мощным средством защиты белорусских пользователей социальных медиа видится использование белорусского языка как средства общения. Он может послужить своего рода естественным кодом, понятным белорусам, но сложным к прочтению иностранным пользователям и организациям. Это позволит обеспечить основательную защиту белорусских пользователей от злоумышленников, находящихся за пределами Республики Беларусь и не владеющих белорусским языком. Действия государства в указанном направлении обоснованно перспективные [1].

Внешнее вмешательство во внутреннюю политику Беларуси заставляет внимательно посмотреть на законодательный опыт других стран и с учетом имеющейся специфики внедрить его в правовое поле Республики Беларусь. В Германии в июне 2017 г. был принят Закон о защите прав пользователей в социальных сетях, направленный на цензуру онлайн-экстремизма. Он обязывает социальные сети, у которых больше 2 млн пользователей в ФРГ, в течение 24 ч с момента получения жалобы удалять посты, содержащие призывы к ненависти и ложную информацию. В апреле 2021 г. Европейский парламент принял закон, требующий от интернет-компаний «удалять или отключать доступ к контенту, помеченному как террористический» в течение 1 ч после уведомления национальных властей [8].

Подводя итог, следует сделать вывод: социальные медиа являются неотъемлемой частью современных общественных отношений. В связи с этим остро стоит вопрос правовой регламентации действий их пользователей. Ввиду того что круг пользователей не ограничивается пределами одной страны, крайне актуальным является международное сотрудничество в данной сфере. Помимо этого Республике Беларусь необходимо принимать собственные меры, направленные на защиту граждан. Основные риски пользователей социальных медиа связаны с несанкционированным использованием их персональных данных и воздействием на них информации деструктивного характера. Деятельность государства должна быть направлена в первую очередь на повышение интернет-грамотности пользователей и разъяснение необходимости са-

мостоятельно обеспечивать собственную безопасность в сети Интернет. Одним из действенных способов обеспечения безопасности может стать использование белорусского языка для хранения персональных данных и общения. В контексте защиты от деструктивной информации действенным видится введение в законодательство такой категории, как «пользователь социального медиа» – лицо, наделенное правом собирать, получать, передавать и распространять массовую информацию в социальных медиа и обязанностью обеспечить соответствие размещаемой информации требованиям законодательства.

Список использованных источников

1. Горошко, Е. И. Социальные медиа (особенности языкового сознания) / Е. И. Горошко // Лингвистика гипертекста и компьютерно-опосредованной коммуникации : сб. материалов науч.-практ. конф., Самара, 30 авг. 2019 г. / Самар. гос. соц.-пед. ун-т ; отв. ред. С. А. Стройков. – Самара, 2019. – С. 24–33.

2. Готовы умножать багаж опыта, профессионализма и компетенций [Электронный ресурс] // Министерство внутренних дел Республики Беларусь : официал. сайт. – Режим доступа: https://www.mvd.gov.by/ru/news/8001/. – Дата доступа: 26.07.2022.

3. Замаратская, А. С. Социальные медиа и социальные сети / А. С. Замаратская // Социальная реальность виртуального пространства : материалы III Междунар. науч. конф., Иркутск, 20 сент. 2021 г. / Иркут. гос. ун-т ; отв. ред. О. А. Полюшевич. – Иркутск, 2021. – С. 30–34.

4. Как перековать информационные мечи на орала. Мессенджеры массового поражения [Электронный ресурс] // СБ. Беларусь сегодня. – Режим доступа: https://mir.pravo.by/edu/pravonarusheniya-nesovershennoletnikh-i-posledstviya-ikh-sovershenіya/messendzhery-massovogo-porazheniya/. – Дата доступа: 25.06.2022.

5. Осипюк, Е. Г. Социальные медиа как социальный феномен / Е. Г. Осипюк // Навстречу будущему. Прогнозирование в социологических исследованиях : материалы VII Междунар. социол. конф., Новосибирск, 15–16 марта 2017 г. / Новосиб. гос. техн. ун-т ; отв. ред. А. В. Кулешова. – Новосибирск, 2017. – С. 748–750.

6. Политика конфиденциальности Viber [Электронный ресурс]. – Режим доступа: https://www.viber.com/ru/terms/viber-privacy-policy/. – Дата доступа: 20.04.2022.

7. Ротман, Д. Г. Социальные медиа в информационном поле Республики Беларусь / Д. Г. Ротман, А. В. Посталовский, И. Д. Расолько // Социология. – 2014. – № 4. – С. 90–99.

8. Сургуладзе, В. Ш. Социальные медиа – инструменты социально-политической дестабилизации общества: уроки, тенденции, перспективы / В. Ш. Сургуладзе // Гуманитар. науки. Вестн. финансового ун-та. – 2020. – № 1. – С. 6–13.

9. Digital 2022: Another year of bumper growth [Electronic resource]. – Mode of access: https://wearesocial.com/. – Date of access: 20.04.2022.

10. Internet Society: Build, Promote and Defend the Internet [Electronic resource]. – Mode of access: https://www.internetsociety.org/. – Date of access: 25.03.2022.

11. The ICT Development Index [Electronic resource]. – Mode of access: https://www.itu.int/. – Date of access: 25.03.2022.

Дата поступления в редакцию: 25.07.2022

УДК 343.1

***В. В. Мелешко**, кандидат юридических наук, доцент, профессор кафедры уголовного процесса Академии Министерства внутренних дел Республики Беларусь*
e-mail: mvmvd@yandex.ru

ЗАПРЕТ ОПРЕДЕЛЕННЫХ ДЕЙСТВИЙ В УГОЛОВНОМ ПРОЦЕССЕ РЕСПУБЛИКИ БЕЛАРУСЬ И РОССИЙСКОЙ ФЕДЕРАЦИИ

Рассматривается достаточно новая мера пресечения в уголовном процессе Республики Беларусь – запрет определенных действий. Проводится сравнительно-правовой анализ белорусского и российского уголовно-процессуального законодательства относительно содержания запретов и ограничений, оснований и порядка их применения, изменения и отмены данной меры пресечения.

Ключевые слова: меры пресечения, запрет определенных действий, домашний арест, виды и содержание запретов, контроль за их исполнением.