нимности пользователей глобальной компьютерной сети Интернет, существование иных анонимных информационно-телекоммуникационных сетей, таких как сеть Tor и других средств и методов анонимизации пользователей; определенная степень анонимности финансовых операций, проходящих в информационно-телекоммуникационных сетях; наличие программных уязвимостей разного уровня в экономически значимых информационных системах глобальной компьютерной сети Интернет, позволяющих нейтрализовать систему защиты, используя вредоносное программное обеспечение.

Перечисленная совокупность признаков отражает высокую степень общественной опасности данных преступлений и предопределяет потенциальную и реальную возможность нанесения ущерба национальным интересам Республики Беларусь в информационной сфере, т. е. угрозу информационной безопасности.

Таким образом, анализ основных подходов к рассматриваемой проблеме позволяет предложить рассматривать киберпреступность в качестве самостоятельной угрозы информационной безопасности Республики Беларусь. При этом трансформации преступности не только порождают необходимость совершенствования законодательства, но изменения организации и тактики предупреждения, выявления и пресечения киберпреступлений.

УДК 343.2.7

О.О. Лемешевский

О НЕКОТОРЫХ ВОПРОСАХ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В СЕТИ ИНТЕРНЕТ

Развитие информационного общества, переход Республики Беларусь к цифровизации, затрагивающей все сферы общественной жизни, неразрывно связанным с усилением значения достоверности информации и культуры общения в сети. В связи с этим появляется большое количество информационных площадок, социальных сетей, форумов, видео- и фотохостингов, обеспечивающих доступ к актуальной информации.

Каждый гражданин Республики Беларусь, в том числе и сотрудники органов внутренних дел, военнослужащие внутренних войск, имеют возможность получать информацию, общаться, обсуждать повестку дня, оставлять комментарии. Следовательно, наличие авторов контента, имеющих умысел доводить недостоверную (часто заранее заготовленную) информацию до своих подписчиков, имеют возможность влиять на эмоциональное состояние людей, их мнение и взгляды на те или иные вопросы.

На данную проблему указал Президент Республики Беларусь Александр Лукашенко 21 сентября 2022 г., принимая с докладом Государственного секретаря Совета Безопасности Республики Беларусь. Он отметил: «Сейчас идет война, прежде всего в сфере информационной безопасности. И здесь подключены должны быть все – от журналиста до Президента. Война войной. Информационная война – это очень опасно в современном мире. Начиная, опять же, от «газеты-районки» и прочей какой-то частной газеты и заканчивая Интернетом. Везде должны активно работать.».

Привлекает внимание в аспекте проблематики нашего исследования положение Концепции национальной безопасности Республики Беларусь, в частности к угрозам национальной безопасности относится «деструктивное информационное воздействие на личность, общество и государственные институты, наносящее ущерб национальным интересам».

Заслуживает внимания в рассматриваемой сфере также Концепция информационной безопасности Республики Беларусь, которая раскрывает такое понятие, как «информационный суверенитет Республики Беларусь».

Информационный суверенитет Республики Беларусь – неотъемлемое и исключительное верховенство права государства самостоятельно определять правила владения, пользования и распоряжения национальными информационными ресурсами, осуществлять независимую внешнюю и внутреннюю государственную информационную политику, формировать национальную информационную инфраструктуру, обеспечивать информационную безопасность.

Основополагающим национальным интересом Республики Беларусь в информационной сфере с точки зрения гуманитарного аспекта является реализация конституционных прав граждан на получение, хранение и распространение полной, достоверной и своевременной информации, свободу мнений, убеждений и их свободного выражения, а также права на тайну личной жизни.

В этой связи следует сделать вывод: лица, которые публикуют на информационных порталах недостоверную информацию или оскорбляют граждан в сети (в частности, сотрудников органов внутренних дел и военнослужащих внутренних войск), нарушают информационный суверенитет Республики Беларусь, угрожают национальным интересам и должны понести весомую ответственность согласно законодательству.

Анализ действующего законодательства Республики Беларусь и правоприменительной практики показывает наличие соответствующих

статей в Уголовном кодексе Республики Беларусь (УК), регламентирующих общественные отношения, касающиеся информационной безопасности, защиты персональных данных, чести и достоинства граждан и вопроса о «фейках» в сети. Приведем их ниже.

Так, в соответствии со ст. 369 «Оскорбление представителя власти» УК предусмотрена уголовная ответственность за оскорбление представителя власти или его близких в связи с выполнением им служебных обязанностей, совершенное в публичном выступлении, либо в печатном или публично демонстрирующемся произведении, либо в средствах массовой информации, либо в информации, размещенной в глобальной компьютерной сети Интернет.

Статьей 391 УК предусмотрено, что оскорбление судьи или народного заседателя в связи с осуществлением ими правосудия наказывается штрафом, или исправительными работами на срок до двух лет, или арестом, или ограничением свободы на срок до трех лет.

В соответствии со ст. 19.11 Кодекса Республики Беларусь об административных правонарушениях предусмотрена административная ответственность за распространение информационной продукции, содержащей призывы к экстремистской деятельности или пропагандирующей такую деятельность, а равно изготовление, хранение либо перевозка с целью распространения такой информационной продукции.

Таким образом, необходимо подчеркнуть, что главным инструментом воздействия на Республику Беларусь является информационно-психологическое воздействие. В этих условиях отсутствие контроля за информационными ресурсами, телеграм-каналами может привести к ложному восприятию информации отдельными гражданами и совершению преступлений. Следовательно, работу по изучению способов ведения информационной войны и совершения киберпреступлений необходимо продолжать. Актуальным остается вопрос о создании военизированных подразделений для противодействия информационным атакам.

УДК 342.732

П.В. Лутович

АКТУАЛЬНЫЕ АСПЕКТЫ РАЗВИТИЯ МЕХАНИЗМОВ ЗАЩИТЫ ГРАЖДАН ПРИ РЕАЛИЗАЦИИ ИМИ ПРАВ И СВОБОД В ИНФОРМАЦИОННОЙ СФЕРЕ

Уровень демократического развития общества определяется не только формальным признанием приоритета прав и свобод человека и

гражданина и их закреплением в национальном законодательстве, но и наличием реальной возможности реализации всего комплекса прав и свобод, гарантированных международными договорами в области прав человека.

Потребности современного общества обусловливают создание эффективно действующего государственно-правового механизма охраны и защиты прав и свобод человека, позволяющий индивиду воспользоваться существующими правовыми и организационными процедурами с целью фактической реализации своих прав и свобод.

Сегодня существующие проблемы защиты прав человека выходят далеко за пределы отдельного государства. Сформировались и получили всеобщее признание международные нормы и принципы в области прав человека, являющиеся стандартом, к достижению которого должны стремиться все государства. Среди основополагающих прав человека ключевую роль в формировании (воспитании) всесторонне развитой личности играет свобода информации, под которой следует понимать группы прав и свобод, включая «свободу выражения убеждений, свободное функционирование средств массовой информации, право общества на получение от государственных служб информации, имеющей общественное значение, свободу распространения информации любым законным способом».

Доступность информации в современных общественных отношениях рассматривается как фактор экономического развития. Особенно это актуально для развивающихся стран, где существуют ограничения по распространению данных в отдельных сферах деятельности. Отсутствие или ограничение предоставления информации создает дополнительные препятствия для функционирования конкурентоспособной экономики, создания эффективного государства и институтов его управления.

Развитие информационных технологий не только облегчают жизнь рядовым гражданам, но и способствуют созданию и производству высокотехнологичных, конкурентоспособных продуктов, пользующихся высоким спросом на международных рынках. Сегодня можно сделать вывод о значительном повышении времени, проводимого различными категориями лиц, в сети Интернет, что объясняется следующим. Современные технологии обеспечивают не только качественное ведение бизнеса, выполнение трудовых обязанностей, но и позволяют эффективно выстраивать коммуникацию.

Вместе с тем в качестве побочного негативного эффекта инновационные процессы способствуют появлению новых угроз противоправного характера, на которые необходимо своевременно реагировать соответствующим правоохранительным органам.