широкого применения цифровых технологий и в уголовно-процессуальной деятельности. В настоящей статье, полагаем, следует остановиться именно на реализации в жизни цифровых технологий, а именно, взяв узкое ее применение, а именно в рассмотрении уголовных дел частного обвинения судами.

Говоря о цифровых технологиях, применяемых в судах, в первую очередь стоит подразумевать видеоконференц-связь (ВКС), которая нашла свое широкое применение, так как ее применение упрощает работу суда с лицами, которые находятся на расстоянии и по тем или иным причинам не явились в зал судебного заседания. Так, А.В. Казакова в статье упоминает об удобстве использования ВКС, но при этом подчеркивает невозможность ее использования, если лицо находится за пределами нашего государства, Российской Федерации. С вышеизложенным можно согласиться, так как ВКС, используемая в государственных органах, в том числе и в суде, может применяться только в Российской Федерации, так как имеет определенную степень защиты из вне. Сегодня многие страны мира широко применяют цифровые технологии в уголовном судопроизводстве в целом и при рассмотрении дел в суде в частности. Это уже не новая практика применения ВКС. Однако мало случаев подтверждения того, что ВКС применяется при рассмотрении уголовных дел частного обвинения. В первую очередь, из-за того что по данной категории дел участвует в самом разбирательстве и поддерживает обвинение частный обвинитель, а не государственный. Во-вторых, лица, проходящие по таким делам с любой из сторон, в большинстве случаев не находятся, например, в местах лишения свободы и имеют возможность самостоятельно прибыть в суд. Актуальность ВКС, как нам видится, по делам частного обвинения будет тогда, когда лицо, подавшее заявление, находится в местах лишения свободы или в иных местах, где предстоит провести значительное время, примером может также служить больница, где человек проходит лечение.

Стоит обратить внимание на критерии допустимости использования цифровых технологий в уголовном судопроизводстве и выделить их: «законность, соблюдение прав и законных интересов личности, актуальность и открытость их применения». При использовании всех цифровых технологий необходимо помнить и о рисках, связанных с их использованием. ВКС технологично имеет свою степень защиты, но в век прогресса, как показывает практика, все бурно развивается, в том числе и средства противодействия. Поэтому, применяя цифровые технологии, в том числе и при рассмотрении уголовных дел частного обвинения по существу, необходимо обращать внимание на методы защиты применяемых цифровых технологий, которые должны не просто упростить работу суда, но и, главным образом, не навредить, особенно от разглашения сведений, охраняемых законодательством Российской Федерации.

С.В. Зуева и А.С. Титова раскрывают в статье слабые стороны цифровизации уголовного судопроизводства с позиции механизма правового регулирования. Однако на слабые стороны всегда найдутся сильные, которые покажут жизнеспособность и, что немаловажно, применяемость. Л.В. Головко с осторожностью относится к цифровизации уголовного судопроизводства в целом и обращает внимание на то, «что самый мощный научно-технологический прорыв в истории человечества 20–60-х гг. прошлого века не привел к созданию ”космического уголовного процесса“ или ”лунной подследственности“». Полагаем, с точкой зрения вышеуказанного автора можно согласиться, так как цифровизация в первую очередь должна быть безопасной.

Таким образом, используя цифровые технологии при рассмотрении уголовного дела частного обвинения, необходимо обращать внимание на защиту данных. При этом широкое использование данных технологий ускоряло бы рассмотрение уголовных дел, способствовало незатягиванию самого рассмотрения и в конечном итоге приводило бы к более оперативному и всестороннему рассмотрению уголовного дела.

УДК 343.985

А.Н. Тукало, С.В. Король

О НЕОБХОДИМОСТИ СОВЕРШЕНСТВОВАНИЯ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

Использование глобальной компьютерной сети Интернет (далее – Интернет) в повседневной жизни является нормой для каждого человека. Интернет и компьютерные технологии стремительно проникли во все сферы жизнедеятельности человека. Несмотря на неопровержимую полезность Интернета, он таит в себе множество опасностей. В настоящее время мир захлестнула проблема совершения преступлений в сфере информационных технологий. Это не только преступления, связанные с хищением денежных средств или личной информации. Посредством Интернета также совершаются вымогательства, мошенничества, распространение наркотиков и детской порнографии, преступления экстремистской направленности, груминг, кибербуллинг и т. д.

Опережающие темпы освоения Интернета в Республике Беларусь являются одним из стимулирующих факторов рассматриваемого вида преступлений. Беларусь вышла на среднеевропейские показатели по

плотности широкополосного доступа в Интернет, а если говорить о скорости передачи данных – на передовые в мире позиции.

На протяжении последних лет наблюдается волнообразный рост количества регистрируемых киберпреступлений. Изучение и анализ международного опыта показывает, что подобная тенденция к росту свойственна большинству стран мира. В связи с постоянным бурным развитием общественных отношений в сфере информационных технологий, тенденции к росту преступлений в данной сфере будут сохраняться.

Государством уделяется повышенное внимание обеспечению защищенности информационного пространства, информационной структуры, информационных систем и ресурсов. Постановлением Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 утверждена Концепция информационной безопасности Республики Беларусь (далее – Концепция). В рамках реализации Концепции противодействие киберпреступности возложено на Министерство внутренних дел (МВД) Республики Беларусь. На основании Концепции разработан «Комплексный план мероприятий, направленных на принятие эффективных мер по противодействию киберпреступлениям, профилактике их совершения, повышению цифровой грамотности населения на 2021–2022 годы» (далее – Комплексный план), в рамках которого в целях повышения эффективности борьбы с вышеуказанной проблемой одним из направлений деятельности обозначена «необходимость объединения усилий государственных органов, общественных объединений, гражданских инициатив, направленных на повышение уровня компьютерной грамотности и цифровой безопасности граждан».

Стоит отметить, что уровень киберграмотности населения не в полной мере соответствует скорости внедрения тех или иных информационных процессов в повседневную жизнь. Существует также формализм в отношении граждан к собственной информационной безопасности, который часто является последствием непонимания реальности угрозы рассматриваемого вида преступлений.

Согласно исследованию, проведенному GlobalWeblndex совместно с Snap Inc. в 2019 г. (соответственно, показатели, полученные в ходе исследования, с каждым годом, в связи с процессом информатизации общества, увеличиваются), у 97 % представителей так называемого поколения Z (молодые люди, родившиеся между 1997 и 2015 гг.) есть мобильный телефон. В данную категорию входят учащиеся школ, которые, в силу своего возраста, не всегда могут распознать обман, мошеннические действия или же иные истинные цели злоумышленника, находящегося по ту сторону Интернета.

С целью повышения компьютерной грамотности населения, считаем целесообразным ввести изучение форм и методов информационной безопасности в учреждениях дошкольного и среднего образования. Данное направление нашло свое частичное отражение в вышеприведенном Комплексном плане в разд. «Профилактические мероприятия» (п. 35, 36, 39, 40, 41, 42, 45, 51).

Анализ указанных пунктов позволяет сделать выводы о том, что профилактические мероприятия в учреждениях образования проводятся на классных (кураторских) часах, в том числе с представителями правоохранительных органов; профилактические мероприятия включают в себя проведение конкурсов, размещение листовок на стендах, распространение информации на интернет-ресурсах, освещение вопросов ответственности за правонарушения, распространение листовок среди учащихся по данной тематике; организация методических сборов на тему «Деятельность специалистов социально-психологической службы по обучению учащихся навыкам информационной безопасности».

Несмотря на целенаправленную профилактическую работу со стороны учреждений образования и подразделений криминальной милиции, рассматриваемый вид преступлений составляет существенное количество от общего числа совершаемых преступлений. Это связано с тем, что способы совершения таких преступлений постоянно совершенствуются.

На наш взгляд, профилактика киберпреступлений была бы более эффективной, если бы поток профилактической информации был приведен в единую систему и подавался поступательно и постоянно. Любая познавательная деятельность должна сопровождаться изучением основ в той или иной отрасли. В силу возраста учащиеся должны получать информацию, начиная с основ информационной безопасности и структуры киберпреступности и заканчивая мерами по ее предупреждению и профилактике. Исходя из изложенного, считаем целесообразным ввести в учебную программу учреждений образования учебную дисциплину «Кибергигиена».

Полагаем, что повышение эффективности профилактики киберпреступлений возможно посредством поступательного обучения основам информационной безопасности с раннего возраста специалистами учреждения образования во взаимодействии с сотрудниками подразделений криминальной милиции. К подготовке учебной программы необходимо привлечь все заинтересованные органы (в том числе профильные отделы Министерства образования, учреждения образования МВД Республики Беларусь, подразделения криминальной милиции и т. д.).

Кроме этого, целесообразно ввести отдельные занятия в старших группах детских дошкольных учреждений, где в игровой форме доводить детям основы кибербезопасности (в том числе приглашать кур-

сантов учреждений образования МВД Республики Беларусь, сотрудников подразделений криминальной милиции для проведения различных мероприятий по обучению навыкам информационной безопасности).

В целях выработки наиболее оптимальных путей повышения эффективности борьбы с киберпреступностью в Республике Беларусь посредством более тесного взаимодействия граждан и организаций с правоохранительными органами считаем необходимым продолжить изучение рассматриваемой проблематики в рамках комплексного исследования, в котором будут изучены ее правовые, социальные, психологические и иные аспекты.

УДК 343.9

Д.Д. Урстенова

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СЕТИ ИНТЕРНЕТ

В наше время наступила информационная эра, т. е. переход от традиционной индустрии промышленности к оцифрованной, компьютеризованной индустрии, направленный на моментальный обмен информации, что послужило началом цифровой революции во всех сферах жизни человечества. В своем послании Глава государства Президент Республики Казахстан Касым-Жомарт Токаев пояснил, что «Цифровизация – это не следование модной тенденции, а ключевой инструмент достижения национальной конкурентоспособности. Прежде всего предстоит устранить цифровое неравенство, обеспечить максимальный доступ к интернету и качественной связи для всех граждан. Сегодня это такая же базовая потребность, как дороги и электричество» [1]. В период всеобщей цифровизации правительства и экономических процессов преступность трансформируется под современные реалии.

Мошенничество в сети Интернет на данный момент имеет масштабный характер, о чем свидетельствуют статистические данные регистрации уголовных правонарушений. Преступники используют все более изощренные способы и методы совершения мошенничества в сети Интернет, что даже самые бдительные граждане попадаются на ловушку преступника.

В настоящее время в интернет-ресурсах Казахстана имеется огромное количество онлайн-сервисов объявлений (olx.kz, krisha.kz, kolesa.kz и т. д.), которые содержат различные виды услуг, купли-продажи и т. д.

Каждый пользователь сети Интернет может выставить любое объявление без указания достоверных личных данных и описание товара или услуги. Проверить достоверность данных пользователей не предоставляется возможным, так как затрагивает права человека, указанные в Законе Республики Казахстан от 21 мая 2013 г. № 94-V «О персональных данных и их защите».

Во всем цивилизованном мире права человека стоят на первом месте и защищаются международными соглашениями, такими как Международный пакт о гражданских и политических правах (International Covenant on Civil and Political Rights – ICCPR) и Всеобщая декларация прав человека (Universal Declaration of Human Rights – UNDP). Анонимность – это невозможность идентифицировать субъект. Также это не допускает возможности несанкционированного использования персональной информации, которой могут воспользоваться в корыстных целях.

Однако у данного утверждения имеется обратная сторона, так как то, что нельзя контролировать, может быть опасным. Вопрос о защите персональных данных пользователей сети Интернет с правовой точки зрения был не до конца изучен. Республика Казахстан при форсированном развитии цифровизации и почти полном переходе документооборота в цифровой формат параллельно проводит законотворческую работу по изменению законодательства с целью наиболее качественной защиты персональных данных граждан.

Так, по мнению К.В. Кецко, для субъектов электронной коммерции анонимность в сети Интернет, с одной стороны, является преимуществом, с другой – вызывает опасения участников, несет определенные риски, в частности, доступность внешнего проникновения, спам-атаки, создание сайтов-дубликатов [2].

Другие авторы относят анонимность в сети Интернет к проблемам правового регулирования цифровых технологий, связанным с реализацией прав и свобод граждан. Они утверждают, что анонимность пользователя – это его конституционная гарантия, обеспечивающая охрану тайн его личной жизни. При этом авторы не исключают ограничение анонимности, когда она используется во вред охраняемым законом общественным отношениям [3].

Сегодня на просторах глобальной компьютерной сети Интернет имеются различные фишинговые сайты, с помощью которых интернет-мошенники осуществляют преступные деяния в сети Интернет.

Фактической профилактикой интернет-мошенничества занимаются как правоохранительные органы, так и государственные структуры, кроме того и IT-гиганты, такие как Google, Yandex и др. Кроме того, профилактикой занимаются и субъекты предпринимательской дея-