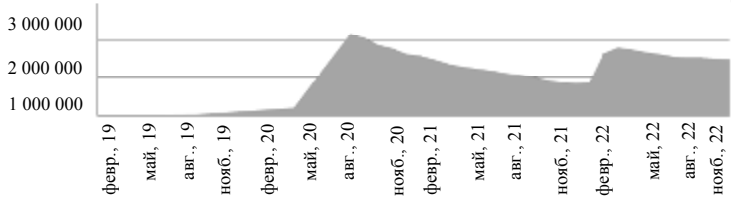
Деструктивное информационное воздействие включало осуществление информационного влияния на политические и социально-экономические процессы, деятельность государственных органов, а также на физических и юридических лиц в целях ослабления обороноспособности государства, нарушения общественной безопасности, принятия и заключения заведомо невыгодных решений и международных договоров, ухудшения отношений с другими государствами, создания социально-политической напряженности, формирования угрозы возникновения чрезвычайных ситуаций, разрушения традиционных духовных и нравственных ценностей, создания препятствий для нормальной деятельности государственных органов, причинения иного ущерба национальной безопасности.

Анализ статистики посещений деструктивных сайтов показывает, что количество белорусов, пользующихся мессенджером, стало расти с сентября 2017 г. В 2019 г. наблюдался устойчивый рост (в два раза относительно предыдущих лет), который сменился взрывным ростом в марте 2020 г. (рис. 1).

Наш анализ показывает, что Telegram лидировал в наиболее молодой группе пользователей в возрасте 15–24 года: по состоянию на 2019 г., 50 % опрошенных этой возрастной категории пользовались этим мессенджером. Уже в 2019 г. рост популярности Telegram был связан с увеличением числа телеграм-каналов, в первую очередь фиксирующих внимание на общественно-политической повестке, а в 2020 г. они стали еще и средством массовой организации и самоорганизации, в дальнейшем произошел спад внимания пользователей к данной повестке дня (рис. 2, примеры 1 и 2).

На основании данных нашего исследования можно выделить ряд следующих тенденций развития «новых медиа». Рост цифровой грамотности населения, развитие мобильных коммуникаций способствуют распространению смарт-устройств и приложений, способных увеличить интерактивность информационных потоков.

Пример 1. Изменение числа подписчиков одного из деструктивных телеграм-каналов



Пример 2. Изменение числа подписчиков одного из деструктивных телеграм-каналов

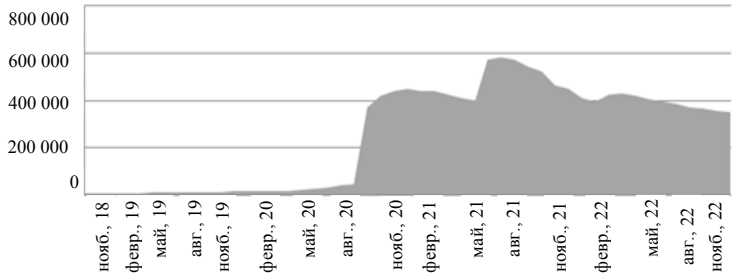


Рис. 2

«Новые медиа» создают технологические условия для развития персонализированного контента для целевой аудитории, они уже способны учитывать форматы подачи информации, вероятно появление новых форм взаимодействия с аудиторией на основе метаданных. Изменяются способы подачи информации «новыми медиа», получают развитие форматы «клипового мышления», при которых человек воспринимает информацию фрагментарно, асинхронно, на коротких интервалах с привлечением ярких образов. С учетом специфики распространения информации в среде «новых медиа», их возможностей по манипулированию, дезорганизации, дезинформации, пропаганде, сложности правового регулирования сохранится их роль как инструмента деструктивного информационного воздействия в условиях гибридных конфликтов.

УДК 004:34

Е.Н. Мисун, А.А. Ластовский

РОЛЬ ПРОФИЛАКТИКИ В ПРОТИВОДЕЙСТВИИ КИБЕРПРЕСТУПНОСТИ

Информационное общество, формируемое сегодня активными способами, представляет собой новый этап развития цивилизации. Повсеместное внедрение и использование компьютерных информационных технологий создает возможности для более эффективного развития экономики, политики и общества в целом. Вместе с тем трансформация социума в информационное общество порождает новые риски, вызовы

и угрозы, которые напрямую затрагивают вопросы обеспечения национальной безопасности, в том числе защищенность информационного пространства. Глобальное проникновение цифровых технологий во все сферы жизни ставит вопрос о необходимости актуализации существующих механизмов правоохранительной деятельности в сфере противодействия преступности в информационном пространстве.

Республика Беларусь, как и все мировое сообщество, ориентирована на развитие и популяризацию безналичных расчетов, сопровождающихся увеличением количества устройств, ростом числа пользователей электронных платежных систем и сети Интернет. Повсеместное и нарастающее использование различных форм дистанционного обслуживания рассматривается одной из основных причин значительного количества регистрируемых киберпреступлений, а ключевым моментом их совершения – недостаточная информационная грамотность населения.

В этой связи актуальным направлением в противодействии киберпреступности рассматривается полноценное и всеобъемлющее использование профилактического инструментария. Этот тезис также был озвучен заместителем Министра внутренних дел – начальником криминальной милиции генерал-майором милиции Г.А. Казакевичем. Так, в мае 2022 г. на заседании Брестского облисполкома он заявил, что, несмотря на положительную динамику снижения количества хищений посредством модификации компьютерной информации, поводов для самоуспокоения нет, поскольку структура преступности меняется. Больше стало преступлений, связанных с применением методов социальной инженерии, направленных на отдельные категории граждан, как правило, социально не защищенные (пенсионеры и одиноко проживающие люди, которые не владеют компьютерной грамотностью). Руководитель отметил, что профилактика подобного вида правонарушений – задача не только милиции, но и местной власти, образования, здравоохранения, социальных служб.

Данное мнение полностью коррелирует с основополагающим нормативным правовым актом в сфере обеспечения информационной безопасности. Так, в соответствии со ст. 76 Концепции информационной безопасности Республики Беларусь одним из приоритетных направлений деятельности уполномоченных государственных органов является профилактика киберпреступности, основанная на популяризации среди населения, прежде всего молодежи, нетерпимости к асоциальному поведению в информационном пространстве, проведении разъяснительной работы в СМИ и сети Интернет в целях формирования безопасной национальной информационной экосистемы.

В качестве примера такой работы можно отметить комплекс профилактических мероприятий, проводимых Министерством внутренних

дел (МВД) Республики Беларусь на протяжении двух последних лет, – декаду кибербезопасности (далее – Декада). Инициаторами проведения данной акции выступило руководство главного управления по противодействию киберпреступности и управления информации и общественных связей МВД Республики Беларусь. Основание для этого – возрастающие информационные риски для населения и экспоненциальный рост киберпреступности.

Проведению каждой Декады предшествовал продолжительный организационный этап. К проведению Декады подготовили документы, разъяснили цели и задачи территориальным подразделениям, достигали договоренности о привлечении к проведению мероприятий заинтересованные государственные органы и др. Основными мероприятиями в ходе проведения Декад являлись выступления в трудовых коллективах и учреждениях образования, а также выступления в средствах массовой информации.

Особого внимания заслуживает практический опыт проведения Декады «Киберкидз» с 23 мая по 1 июня 2022 г. Ее главной целью стало обучение основам безопасного поведения в цифровой среде во время летних каникул учащихся, их родителей, педагогического состава учреждений образования. Проведена широкомасштабная работа по доведению профилактической информации до населения посредством средств массовой информации (выступления на телеканалах «Беларусь-1», «ОНТ», «СТВ», на интернет-портале «Спутник», на радиостанциях «Сталіца», «Мир», «Альфа Радио»). Всего было проведено свыше 9 тыс. выступлений в средствах массовой информации, большая часть из которых пришлась на интернет-выступления (7,8 тыс.). Территориальными органами внутренних дел в соответствии с компетенцией активно был задействован весь допустимый ресурс ведомств и организаций для распространения в подростковой среде информации о мерах по соблюдению цифровой гигиены. Информационно-профилактическая работа активно осуществлялась сотрудниками органов внутренних дел в трудовых коллективах (5,6 тыс. выступлений) и учреждениях образования (4 тыс.).

Пристальное внимание было уделено распространению наглядной агитации, размещаемой в местах массового присутствия граждан в самых посещаемых объектах транспортной инфраструктуры и социального назначения. Информационные материалы в массовом порядке звучали из радиоприемников, транслировались на мониторах в торговых объектах и автозаправках, в общественном транспорте и объектах транспортной инфраструктуры.

Активно проводились встречи с обучающимися и профессорско-преподавательским составом учреждений высшего образования, при-

чем как в формате реального присутствия, так и в режиме онлайн-конференций. Главная их цель – в преддверии летних каникул довести до обучающихся основные виды киберугроз и меры по защите от них.

В целом проведение указанного комплекса профилактических мероприятий позволило достичь поставленных целей, всесторонне и качественно довести необходимую информацию до населения (в особенности до молодежи). С высокой степенью эффективности были задействованы заинтересованные государственные органы и организации, предприятия, социальная, транспортная и спортивная инфраструктура, мобильные операторы сотовой связи.

Как свидетельствует статистика, проведение данных широкомасштабных профилактических мероприятий весьма существенным образом сказываются на формировании положительной динамики в противодействии киберпреступности. Массированным информированием граждан всеми доступными способами о самых актуальных способах хищений денежных средств правоохранительные органы достигают главной цели: обеспечение превентивной самозащиты населения от преступных киберпосягательств. Вместе с тем важнейшее значение в противодействии киберпреступности имеет консолидация и партнерские отношения между правоохранительными органами, организациями государственного и частного секторов, образовательными и научными учреждениями.

Таким образом, профилактическая работа, направленная на правовое просвещение населения, и впредь должна носить системный характер с привлечением всех заинтересованных структур органов государственного управления.

УДК 343.9.01

И.С. Митряев

ВЛИЯНИЕ КИБЕРПРОСТРАНСТВЕННОЙ АНОНИМНОСТИ НА МОТИВАЦИЮ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ IT-ТЕХНОЛОГИЙ

Совершенствование информационных систем упрощает доступ к информации, предлагает ее разновидности. В то время как безопасность личных данных подвергается высокому риску, анонимность, невидимость и сокрытие следов преступления становятся большой проблемой в сфере интернет-отношений между людьми.

Киберпреступность во многом отличается от традиционных преступлений, в том числе универсальностью и сложностью, в частности

анонимностью, сокрытием и незаметностью. Анонимность киберпространства делает отслеживание личности серьезной проблемой, которая создает препятствия для обнаружения и расследования.

Анонимизация киберпространства делает отождествление личности глобальной проблемой, которая создает препятствия для расследования данного рода преступлений и поимки преступников.

Киберанонимность оказывает влияние на преступную мотивацию и явление виктимизации, которое представляет из себя процесс или конечный результат превращения в жертву преступного посягательства лица или группы лиц, поэтому решать эту задачу необходимо на разных уровнях, включая технологии и правоохранительные органы.

Анонимное общение – отличительная особенность интернет-пространства. При использовании интернета анонимность может сохраняться от начала до конца. Но при этом данный тип общения может нести достаточно серьезную угрозу конфиденциальности личных данных пользователей, организаций. Интернет повсюду. Но достаточно часто его используют в торговых центрах, ресторанах, барах, аэропортах и т. п. Из-за особенности распространения интернета злоумышленники часто пользуются этим, взламывая средства связи обычных пользователей, которые подключены к одной общественной сети.

Существуют специальные программы и сервисы, которые позволяют полностью сохранить свою анонимность в сети Интернет. Этот механизм затрудняет установление личности пользователя. Ведь посредником может являться программа. Но вполне реально отследить данный путь посредством следования процессам прямо противоположным передачам.

Анонимное подключение представляет собой фундаментальное субъективное право, необходимое каждому посетителю интернета. В определенных случаях это отдельные компьютерные сети, созданные для достижения анонимности в сети Интернет. Особенность таких сетей в том, что они сочетают в себе определенную степень защищенности пользователя, легкость использования и наличие «прозрачности» для конечного пользователя.

Наиболее известным примером программ для обеспечения анонимности является браузер Tor и VPN, что позволяет добиться полной анонимности в сети Интернет. Следует отметить, что использование данных программ законодательно не регламентируется, то пользоваться такими программами может любой желающий.

Статистика о количестве киберпреступлений в России за 2021 г. говорит о 518 тыс. киберпреступлений, что на 1,4 % больше, чем годом ранее, но сразу в 1,8 раза превосходит показатель 2019 г. В частности,