ПРОФИЛАКТИКА ПРАВОНАРУШЕНИЙ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

С.У.Шавкатов
Курсант Академии МВД Респулики Узбекстан

Аннотация: *В данной статье автор раскрыл актуальность необходимости внедрения новейшего информационно-коммуникационного обеспечения правоохранительных органов Республики Узбекистан, а в частности, обеспечения направления профилактики правонарушений. Автор также выделил важность совершенствования мер профилактики правонарушений в сфере информационно-коммуникационных технологий, перенятия передового опыта развитых зарубежных стран, ведь данный вопрос нельзя не связывать с безопастностью страны. Учитывая то, что сейчас проблема борьбы с миром киберпреступности выносится на злобу дня, да и вообще если говорить о такой быстротечной цифровизации мира, следует сразу отметить, что данный аспект охватывает и глобальную сеть Интернет, которая в настоящее время является одним из важнейших средств массмедии и плачевно известной "жёлтой прессы". Поэтому стоитещё раз отметить важность освоения сотрудников правоохранительных органов современных технологий и виртуального мира, для осуществлении превенции киберпреступлений и быстрого и полного раскрытия уже совершённых киберпреступлений.*

Ключевые слова: *информационно-коммуникационное обеспечение, правоохранительные органы, профилактика правонарушений, безопасность страны, киберпреступность, сеть Интернет.*

Annotation: *In this article, the author revealed the urgency of the need to introduce the latest information and communication support for law enforcement agencies of the Republic of Uzbekistan, and in particular, to ensure the direction of crime prevention. The author also highlighted the importance of improving crime prevention measures in the field of information and communication technologies, adopting the best practices of developed foreign countries, because this issue cannot but be associated with the security of the country. Considering that now the problem of fighting the world of cybercrime is being brought to the surface and in general, if we talk about such a rapid digitalization of the world, it should be noted at once that this aspect also covers the global Internet,*

which is currently one of the most important means of mass media and the lamentably famous "yellow press". Therefore, it is worth noting once again the importance of law enforcement officers mastering modern technologies and the virtual world in order to prevent cybercrimes and quickly and fully disclose cybercrimes that have already been committed.

Keywords: *information and communication support, law enforcement agencies, crime prevention, national security, cybercrime, the Internet.*

Глобальное развитие мировой цивилизации на современном этапе,
развития всех областей и направлений человеческой деятельности определяется, прежде всего, эффективностью ее информационного обеспечения. От этого во многом зависит экономическая, финансовая и политическая жизнь государств, их процветание и безопасность. Сейчас мы живём в эпоху цифровизации – вовремя, когда информационные
технологии стали неотъемлемой частью нашей жизни. Информационные
технологии существуют сплошь и рядом в нашей повседневной жизни. Сегодня каждый из нас может наблюдать высокий уровень развития информационно-коммуникационных технологий, их обширного внедрения во все сферы нашей жизни. Это ярко отражается и в том, что нашу жизнь невозможно представить без уже для всех нас незаменимой сети Интернет. Так, согласно статистике на период 1 февраля 2022 года, ведущее место по популярности пользования среди узбекистанцев занимает мессенджер Telegram с количеством пользователей в 18 миллионов, на втором месте по популярности в стране оказалась социальная сеть Одноклассники – её посещают 16,7 миллиона жителей Узбекистана, а за ними следуют Facebook, в нём зарегистрировано 4,7 миллиона, 3,7 миллиона в Instagram, 2,6 миллиона посещают социальная сеть В Контакте. Ещё 288 тысяч пользуются LinkedIn, а 51,6 тысячи Twitter [1]. Следует также отметить, что популяризация сети Интернет во многом зависит от внешних факторов. Так, в период пандемии Covid-19, по всему миру виртуальное пространство облегчило людям повседневные заботы. В число которых входят: покупка продуктов, доставка готовой пищи, оплата социальных платежей, обновление гардероба, обучение в онлайн режиме, и даже место встречи с близкими и друзьями перенеслись в виртуальное пространство. Всё это пользовалось и продолжает пользоваться

огромным спросом, ведь для этого не нужно выходить из дома, нужно всего лишь сделать пару нажатий на своём гаджете и необходимый товар прибудет через отведённое время прямо к порогу вашего дома. В этом и отражается большой прирост совершения перевода денежных средств через онлайн платёжные системы. Ввиду этого теперь мы столкнулись с новым явлением преступного мира – киберпреступностью. Да, явление киберпреступности наблюдалось и в конце XX века, но такие масштабы как сейчас, киберпреступность приобрела относительно недавно. По последним данным, объём мирового рынка киберпреступлений составляет 1,5 трлн долл. США. Согласно данным World Bank, эта цифра сопоставима с ВВП Канады или Австралии в 2017 году. А также по некоторым данным, преступники могут зарабатывать в год до полумиллиона долларов США, просто торгуя украденными данными. Этим и обусловлена заинтересованность темы информационных технологий в органах внутренних дел, и в частности, в сфере профилактики правонарушений. Ведь своевременное предупреждение киберпреступлений занимает большую часть при борьбе с этим явлением в целом. Так, уже всем нам известны проявления кибермошенничества выраженные в основном в запросе кода для обратной связи с пользователем в целях снятия денежных средств с банковской карты гражданина через известные платёжные системы. Но, к сожалению, несмотря на большой резонанс данных преступлений, наши граждане всё равно продолжают попадать в ловушку кибермошенников. Ну, а в дальнейшем при получении заявления по данному факту, уполномоченный сотрудник сталкивается с проблемами присущими расследованию данного рода преступлений. Зачастую, те номера откуда приходили звонки или же сообщения попросту отключены или же владелец номера не в курсе, что с его номера кто-то производил звонки и следствие приходит в тупик. Зарождается вопрос: «Можно ли было это всё предотвратить?». По моему мнению, можно. В этом и заключается основная роль и значение своевременной профилактической работы, которая направлена на предупреждение у граждан их виктимного поведения. Да, сейчас проводится общая профилактическая работа касающаяся данной проблемы, но как мы видим, она не даёт нам нужного результата и кибермошенники продолжают обогащаться за счёт
невнимательных и доверчивых граждан. Учитывая это, следует усилить

профилактическую работу в данном русле, ещё более активно обнародывать данные о совершённых киберпреступлениях, а также о том, как можно избежать смены статуса обычного лица, на лицо пострадавшее от кибермошенничества. По оценкам IDC через 5 лет, в 2025 году, объём незащищённых данных, требующих защиты составит почти половину от всего существующего объёма данных, в то время как эта же величина для 2015 года составила лишь четверть. Сам по себе гигантский, постоянно возрастающий объем данных не обязательно облегчает работу органов внутренних дел в части профилактики и борьбы с организованной преступностью. Зачастую избыток сведений оказывается еще более вредным, чем недостаток сотрудников органов внутренних дел, не владеющих соответствующими навыками, которые не только не могут найти в них цифровые доказательства совершенного преступления либо признаки готовящегося, но и связывают с цифровыми доказательствами избыточные надежды. К данной проблеме нужно подходить всесторонне. На сегодняшний день обязательство освоения навыков пользования компьютера и необходимых программ, выше пользовательского уровня для всех сотрудников органов внутренних дел является необходимостью. Ведь чем больше сотрудников будут углублённо разбираться в информационно-коммуникационных технологиях, тем быстрее, своевременнее будет пресечена преступная деятельность, будут найдены и наказаны в соответствующем порядке те самые «злые компьютерные гении», и мы добьёмся снижения криминогенного уровня в нашей стране.

Корпорация RAND [2] выпустила в 2014–2016 гг. целую серию практических исследований под общим названием *«Приоритетность криминальной юстиции»*. Работы выполнялись с привлечением действующих офицеров полиции вместе с университетом Денвера и исследовательским центром Министерства юстиции США.

RAND систематизировала следующие основные приоритеты развития:

– общие системы электронных досье на преступников и преступления, включая единые каталоги и системы классификации;
– системы обучения офицеров полиции web-технологиям по специальным для них программам;
– разработка только тех решений, которые соответствуют общим требованиям;

– улучшение сетевой инфраструктуры с целью поддержки web-технологий, особенно для судов и исправительных учреждений. Понимание и использование новых технологий в контексте преступности имеет двойственный характер. С одной стороны, данные и
технологии используются преступниками для совершения криминальных действий. В этом плане новые технологии входят в число драйверов преступности. С другой стороны, технологии являются инструментом, позволяющим успешно не только бороться с криминалом, но и профилактировать его. Данные и информационно-коммуникационные технологии являются важнейшим фактором создания систем эффективного обмена сведениями
и результативного взаимодействия. Если еще несколько лет назад главные усилия правоохранительных органов были направлены на создание текстовых баз данных об организованной и уличной преступности, то в настоящее время ситуация в корне изменилась. Уже сейчас не менее 70% хранилищ данных о криминале занимают видео- и фотофайлы. С переходом городов Великобритании с населением
свыше 100 тыс. человек и всех транспортных коммуникаций страны на 100%-ный охват видеонаблюдением (не позднее 2018 г.), именно видеофайлы станут основным элементом данных и материалом для профилактики преступности и проведения расследований. В настоящее
время перед системой криминальной юстиции и обеспечения правопорядка в Великобритании стоит задача не только технически ответить на этот вызов, но и оснаститься средствами и инструментами, позволяющими максимально полно использовать видеоинформацию вместе с текстовой и аудиоинформацией. Уже сейчас мы можем видеть, как развитые страны путём активного внедрения информационных
технологий в борьбу с преступностью в целом, достигли больших успехов. К примеру, можно привести единая база данных TES во Франции, которую они разработали уже в 2016 году, и она успешно прошла проверку. С её помощью правоохранительные органы с лёгкостью и высокой скоростью раскрывают преступления. Также следует отметить страстное пристрастие Дубая робототехникой. У них также уже давно имеется крепко укрепившаяся на рынке компания PAL Robotics, которая разработала робокопа. В свою очередь данный

робокоп скорее выполняет функцию гида, чем полицейского, но тем не менее он стал частью дубайской полиции. В этой связи очень ярко просвечивается необходимость перенятия и внедрения передового опыта в сфере обеспечения сотрудников правоохранительных органов информационными технологиями и повышением знаний в пользовании компьютера и сети Интернет. Также юридическая поддержка открытости государственных информационных технологий является необходимой предпосылкой обеспечения интеграции единого информационного пространства Республики Узбекистан с европейским и мировым пространством. Единое информационное пространство представляет собой совокупность баз и банков данных, технологий их ведения и использования, информационнотелекоммуникационных систем и сетей, функционирующих и взаимодействующих на основе единых принципов и по общим правилам, обеспечивающим информационное взаимодействие организаций и граждан, а также удовлетворения их информационных потребностей. Учитывая всё вышеизложенное, считаю рациональным внести ряд предложений, которые по моему мнению в перспективе смогут решить насущные проблемы, связанные с борьбой правоохранительных органов с явлением современного мира – киберпреступностью:

– усилить и увеличить осуществляемую пропаганду в сфере предупреждения становления жертвами от кибермошенничества посредством увеличения рекламных роликах на отечественном телевидении, а также в общественных местах и на общественном транспорте;

– осуществлять профилактическую работу направленную на «информационную грамотность и информационное просвещение» в содействии со специалистами для несовершеннолетних в школах, а также
подростков и молодёжи в колледжах и в ВУЗах;

– посредством мастерклассов, с привлечением специалистов, обучать инспекторов профилактики основам пользования необходимыми компьютерными программами, мониторингу социальных сетей, созданию сайтов, каналов для осуществления онлайн профилактики для граждан на подотчётной территории;

– для завлечения сотрудников профилактики правонарушений освоением компьютерных технологий, осуществлять поощрение активных и инициативных сотрудников, отталкиваясь от их успехов в

создании программ, сайтов и интернетканалов;
– отправлять перспективных сотрудников службы профилактики в развитые страны (такие как ОАЭ (Дубай), Китай, Америка и другие) для перенятия передового эффективного опыта в сфере профилактики правонарушений, направленной на превенцию киберпреступлений посредством работы с гражданами.

ЛИТЕРАТУРА:

1.Nuz.uz
2.RAND (корпорация) аббревиатура от Research and Developmentисследования и разработка) американская некоммерческая организация, которая выполняет функции стратегического исследовательского центра, работающего по заказам правительства США, их Вооружённых сил и связанных с ними организаций.
3. Расулев, Абдулазиз, and Сурайё Рахмонова. «Преступления в сфере информационных технологий и безопасности: детерминанты и предупреждение». Общество и инновации 1.1 (2020): 200–209.
4. Rasulev A.K. «Improvement of criminal-legal and criminological measures of fight against crimes in the sphere of information technologies and
safety: Doctoral (DSc) dissertation abstract on legal sciences». (2018).
5. Расулев А.К. «Повышение качества и результативности юридического образования и науки». Фан ва таълим замонавий босқичда: ислоҳотлар ва
стратегик йўналишлар: 16–23.