ПРЕСТУПЛЕНИЯ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ПРОФИЛАКТИКА И ПРОТИВОДЕЙСТВИЕ

Абдулазиз РАСУЛЕВ,
доктор юридических наук,
Академия
Министерства внутренних дел
Республики Узбекистан

Информационные преступления – это общественно опасные деяния (действия и бездействия), совершаемые как умышленно, так и по неосторожности, причиняющие либо создающие угрозу реального, существенного вреда или материального ущерба общественным отношениям в сфере информационных технологий и безопасности, регламентирующим: 1) безопасное производство, сбор, обработку, хранение, поиск, передачу, распространение, потребление компьютерной информации и информационных ресурсов; 2) безопасное функционирование инфраструктуры информационно-коммуникационных технологий; 3) создание и использование информационных технологий, средств их обеспечения; 4) защиту компьютерной информации и информационных систем, сетей и ресурсов; 5) охрану прав и законных интересов личности, общества и государства в информационной сфере.

Родовой объект преступлений в сфере информационных технологий и безопасности – общественные отношения, обеспечивающие безопасность личности, общества и государства в сфере информационной безопасности и технологий. Данное понятие сформировалось эволюционно и претерпевала различные изменения, в силу чего для правильного его восприятия следует провести ретроспективный анализ отношений в информационной сфере.

Следует выделить три этапа последовательной эволюции информационных отношений и обеспечения их уголовно-правовых мер охраны.

Первый этап – этап первичного осознания опасности компьютерного преступления (1970 – конец 1990 гг.). Характеризуется **зарождением и развитием компьютерной преступности,** а именно первыми фиксируемыми официально фактами использования компьютеров для совершения других (общеуголовных) преступлений, как правило, мошенничеств и краж финансов, и постепенным технологическим развитием компьютерной инфраструктуры, появлением, так называемых **хакеров, кракеров** и прочих лиц, совершающих компьютерные преступления в виде взломов, компьютерных саботажей (пока без активного вовлечения в преступные группировки).

Второй этап – этап развития преступлений в глобальной сети Интернет (конец 1990 – начало 2010 гг.). Характеризуется глобализацией и «интернационализацией» компьютерной преступности, признанием данного вида преступности в качестве глобальной угрозы – **киберпреступности**, дальнейшим усилением вызовов и возникновением угроз против информационной безопасности, стремительным технологическим прорывом, созданием новых информационно-коммуникационных систем и инфраструктуры, так называемого «виртуального пространства», создающего огромные возможности для трансграничного совершения киберпреступлений, активным развитием хакерских сообществ, их прогрессирующим вовлечением в преступную сеть.

Третий этап – современный этап (с 2010 года по настоящее время). Трансформация киберпреступности в преступления в сфере информационных технологий и информационной безопасности, превратившихся в мощный системный инструмент межгосударственного, межнационального и межструктурного противоборства, который характеризуются **усилением информационных атак,** представляющих собой совершенно новый вид информационных вызовов, создающих угрозу не только личности, обществу или государству, но и человеческой цивилизации в целом. В частности, данным авторитетного

Международного Статистического портала (The Statistics Portal) в 2018 году в США ущерб от данных информационных атак составил около 130 миллионов долларов США. Влияние и возможности глобальной сети Интернет часто приводят к **неконтролируемому хаосу,** разжиганию региональных войн и вооруженных конфликтов, смене политических режимов, трансформации международных террористических организаций в государственные институты, выходу из-под контроля международного сообщества, государств и транснациональных корпораций, явному отставанию принятых и принимаемых нормативно-правовых актов в качестве мер своевременного реагирования.

История и тенденции развития уголовно-правовых норм по защите отношений в сфере информационных технологий на территории Республики Узбекистан условно подразделены на три этапа:

Первый этап. Включает период с момента обретения независимости в 1991 г. до принятия Уголовного кодекса (УК) Республики Узбекистан в 1994 г. В этот период были приняты законодательные акты, в общем порядке регулирующие вопросы информатизации и отношения в сфере информационных технологий (например, Закон Республики Узбекистан «О правовой охране программ для электронных вычислительных машин и баз данных»). В 1996 г. Узбекистан вошел во Всемирную сеть Интернет.

Второй этап. Охватывает период с 1994 по 2007 гг. В этот период были приняты УК Республики Узбекистан, который предусматривал ответственность за нарушение правил информатизации, кражу, мошенничество, хищение путем присвоения и растраты с применением средств компьютерной техники, а также общие законы в сфере информационных технологий – «О принципах и гарантиях свободы информации», «О телекоммуникациях», «Об информатизации». Была определена природа информатизации, разработан механизм защиты данного процесса, создана необходимая правовая основа. Также с принятием Гражданского кодекса Республики Узбекистан была определена юридическая природа информации в качестве вещи.

Третий этап. Охватывает период с 2007 г. В этот период информатизации и компьютеризации возникла необходимость совершенствования механизма уголовно-правовой защиты отношений в сфере информационных технологий. С учетом положительного опыта зарубежных стран в УК была введена новая глава XX[I], предусматривающая новые составы преступлений в сфере информационных технологий.

Исходя из вышеизложенного, предлагается принять ряд следующих мер.

На современном этапе **следует предусмотреть и расширить круг преступлений в сфере информационных технологий и безопасности** в аспекте криминализации новых общественно опасных деяний, посягающих на информационную безопасность личности, общества и государства.

Важное значение при противодействии информационным вызовам и угрозам имеет **принятие концептуального нормативно-правового документа в области информационной безопасности.** В этой связи, возникает объективная необходимость разработки проекта **Концепции информационной безопасности Республики Узбекистан** с учетом возникающих вызовов и угроз**.**

Комплекс правовых мер по обеспечению информационной безопасности должен исходить из проводимой государством политики по развитию Республики Узбекистан. Исходя из реализации Стратегии действий по пяти приоритетным направлениям развития Республики Узбекистан в 2017–2021 гг., признается актуальным разработать **проект постановления Кабинета Министров Республики Узбекистан по совершенствованию нормативно-правовой базы в сфере кибербезопасности.**

При криминологической характеристике преступников в сфере информационных технологий и безопасности полагается необходимым исходить из **четырех факторов, оказывающих влияние на формирование правонарушителя в информационно-**

коммуникационном пространстве – черты личности, техническое ноу-хау, социальные особенности, мотивирующие факторы.

Следует выделить **следующие основные аспекты криминологической характеристики преступлений в сфере информационных технологий и безопасности – высокая общественная опасность и транснациональный характер информационных угроз, уязвимость информационно-технологической системы как важнейшего элемента стратегической инфраструктуры, недостаточная эффективность законодательства и несовершенство политических институтов, отсутствие профессионализма и «человеческий» фактор.**

С учетом этого для противодействия преступлениям в сфере информационных технологий и безопасности возникает необходимость принятия комплекса правовых, социальных, политических, организационно-технических мер.

В целях повышения эффективности выявления и расследования инцидентов в области информационной безопасности и киберпреступлений возникает необходимость создания **специальной лаборатории при Центре информационной безопасности** и содействия в обеспечении общественного порядка для проведения испытательных и исследовательских работ, а также тестирования средств защиты в области информационной безопасности. Данная лаборатория будет осуществлять функции своеобразного «полигона» по испытанию новейших средств защиты от компьютерных вирусов, вредоносных программ, взломов и т.д.

Актуально создание **«Клуба инициативных программистов»,** который будет являться местом сбора талантливой и креативной молодежи, обладающей необходимыми знаниями и навыками в сфере информационно-коммуникационных технологий и кибербезопасности, дискуссионной средой и наглядной площадкой для подбора кадров. При этом, данный клуб целесообразно создать при Союзе молодежи Республики Узбекистан, а также при поддержке Мининфокома, Минвуза, Министерства по инновационному развитию с привлечением специалистов, экспертов и аналитиков. Создание такого клуба станет ярким примером открытого диалога с молодежью, своеобразным профилактическим центром по предупреждению и выявлению лиц, имеющих склонность для совершения информационных правонарушений, а также их воспитания в духе патриотизма, уважения к закону и сопричастности к построению развитого государства и информационного общества.

С учетом роста глобализации и информатизации общества, расширения масштабов информационной преступности возникает необходимость принятия единой **Конвенции ООН по борьбе с киберпреступлениями и обеспечению глобальной информационной безопасности.** Данный документ должен быть основополагающим, содержать в себе комплекс четко выработанных на основе ранее принятых международных актов правил, предусматривающих общие принципы борьбы с информационными преступлениями, вопросы гражданской и уголовной ответственности, перечень уголовно наказуемых деяний, конкретные механизмы международного сотрудничества в области противодействия информационным преступлениям и повышения квалификации сотрудников правоохранительных органов, обмена данными и судопроизводства.

В целях анализа состояния и обмена информацией о киберпреступности между странами–участниками ШОС, ЕС и других региональных организаций, оценки принятых на национальном уровне превентивных мер и оперативных мероприятий, а также проведения специальной подготовки сотрудников правоохранительных органов, судебных и прокурорских кадров обосновывается актуальность **создания при Интерполе глобального координационного центра по противодействию киберпреступности.** Создание данного центра позволит системно осуществить сбор, обработку данных, оказание информационной, технической и криминалистической поддержки соответствующим подразделениям правоохранительных органов стран–членов Интерпола, координацию совместных расследований, а также специализированное обучение и подготовку специалистов. Центр может содействовать проведению необходимых исследований и созданию программного

обеспечения, заниматься оценкой и анализом существующих и потенциальных угроз, составлением прогнозов и выпуском заблаговременных предупреждений.

Рекомендуемая
дополнительная литература:

Gouseti, Ioanna. Worry about victimization, crime information processing, and social categorization biases // Legal & Criminological Psychology. – 2018. – Vol.23. – Issue 2. – PP.148-162.

Melgarejo, Miguel; Obregon, Nelson. Information Dynamics in Urban Crime // Entropy. – 2018. – Vol.20. – Issue 11. – P.874.

Danner, Jennifer. The technology of policing: crime mapping, information technology, and the rationality of crime control // Policing: A Journal of Policy & Practice. – 2018. – Vol.12. – Issue 1. – PP.125-128

Шутова А.А. Уголовно-правовое противодействие информационным преступлениям в сфере экономической деятельности. – Москва, 2019.

Шифельман С.А. Особенности применения специальных знаний в области информационных технологий при осмотре места происшествия по компьютерным преступлениям // Приоритетные направления развития науки и образования. Сборник статей V Международной научно-практической конференции. – Пенза, 2019. – С.183-186.

Преступления в сфере информационных технологий и информационной безопасности Профилактика и противодействие

Абдулазиз РАСУЛЕВ,
доктор юридических наук,
Академия
Министерства внутренних дел
Республики Узбекистан

Ключевые слова: новейшая история Узбекистана, правовое государство, компьютерная грамотность, информационные преступления, информационная безопасность, информационные угрозы.

Краткое содержание. Дано определение понятию «информационные преступления», выделены этапы последовательной эволюции информационных отношений и обеспечения их уголовно-правовых мер, уголовно-правовых норм по защите отношений в сфере информационных технологий в новейшей истории Узбекистана, предложен целый ряд изменений и дополнений в действующее национальное законодательство.

Crimes in the field of information technologies and information security. Prevention and counteraction

Abdulaziz RASULEV,
Doctor of Law,
Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan

Keywords: Uzbekistan’s latest history, state ruled by law, computer literacy, information crimes, information safety, information threats.

Summary. The researcher presents a definition to the concept of informational crimes, highlights the stages in the steadfast evolution of information relations and in the provision for their criminal law measures and criminal law norms for the protection of relations in the field of information technologies in the modern history of Uzbekistan, proposes a number of amendments and addenda to the national legislation in force.