СОВЕРШЕНСТВОВАНИЕ УГОЛОВНО-ПРАВОВОЙ ПОЛИТИКИ В СФЕРЕ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ В РЕСПУБЛИКЕ УЗБЕКИСТАН

Расулев Абдулазиз Каримович
доктор юридических наук, профессор, ученый секретарь Института законодательства и правовой политики при Президенте Республики Узбекистан

Югай Людмила Юрьевна
доктор юридических наук, и.о. доцента кафедры деятельности по профилактике правонарушений Академии МВД Республики Узбекистан

Аннотация. В статье освещается современное состояние и перспективы развития уголовно-правовой политики Республики Узбекистан в сфере противодействия киберпреступности. Автором проводится сравнительно-правовой анализ преступлений в данной сфере Республики Узбекистан, Республики Армения, Российской Федерации, Республики Казахстан и других государств. Определяются тенденции развития уголовно-правового законодательства Республики Узбекистан.

Ключевые слова: интернет, цифровизация, киберпреступление, Уголовный кодекс.

Динамичная цифровизация всех сфер жизни общества и человека, разработка и внедрение инновационных проектов, основанных на использовании передовых информационных технологий, повышают качество жизни человека, создают максимальные удобства при получении каких-либо услуг, но вместе с тем, вышеуказанное обусловливает появление новых видов киберпреступлений, увеличение их количества, а также их повсеместное распространение.

Согласно данным экспертно-аналитической компании ASTRA в 2022 году ущерб от киберпреступности составил около 6 триллионов долларов США. Это больше, чем ВВП Японии, Германии, Индии, Великобритании и Франции. Между тем, предполагаемый ущерб к 2025 году составит 10,5 триллионов долларов США. Для сравнения, этот прогнозируемый показатель превышает ВВП всех стран мира, кроме Китая и США, равен 10 % мирового ВВП [1].

Кибермошенничество, информационные блокады, терроризм, компьютерный шпионаж, неправомерный доступ к личной информации (аккаунты в социальных сетях, электронные почты) и другие преступные посягательства

причиняют значительный имущественный вред, посягают на национальную безопасность государства [2, С. 135-137].

Вместе с тем, ученые отмечают влияние информационной эпохи на проявления современного экстремизма и терроризма, которые на сегодняшний день нашли благодатную почву в киберпространстве [3, С.17-22; 4, С. 293-296; 5, С. 100-104].

По данным «Лаборатории Касперского», в Узбекистане практически ежедневно выявляются в среднем 67 новых инцидентов атак программ-вымогателей. Кроме того, наблюдается рост мошенничества, связанного с фиктивной службой техподдержки банков, в сфере электронной коммерции, краж с пластиковых карт, а также вымогательств, связанных с использованием видео- и фотоматериалов [6].

Государственная политика в сфере противодействия киберпреступности в Республике Узбекистан предусматривает систему правовых, организационных, технических и других мер. При этом, одним из важных направлений противодействия киберпреступности является совершенствование уголовно-правовой политики государства, определяющее новые виды преступлений, гармонизацию законодательства.

Глава XX[1] «Преступления в сфере информационных технологий» Уголовного кодекса Республики Узбекистан на сегодняшний день содержит семь видов преступлений в данной сфере.

Ниже приводим сравнительный анализ киберпреступлений, предусмотренных в уголовном законодательстве ряда стран.

Таблица 1. Содержание соответствующих глав Уголовного кодекса Республики Узбекистан и Республики Армения

УК Республики Узбекистан	УК Республики Армения
Глава XX[1] – преступления в сфере информационных технологий.	глава 24 Преступление против безопасности компьютерной информации
статья 278[1]. Нарушение правил информатизации; статья 278[2]. Незаконный (несанкционированный) доступ к компьютерной информации;	Статья 251. Несанкционированный доступ (проникновение) к системе компьютерной информации Статья 252. Изменение компьютерной информации

статья 278[3]. Изготовление с целью сбыта либо сбыт и распространение специальных средств для получения незаконного (несанкционированного) доступа к компьютерной системе, а также к сетям телекоммуникаций; статья 278[4]. Модификация компьютерной информации; статья 278[5]. Компьютерный саботаж; статья 278[6]. Создание, использование или распространение вредоносных программ; статья 278[7]. Незаконный (несанкционированный) доступ к сети телекоммуникаций.	Статья 253. Компьютерный саботаж Статья 254. Неправомерное завладение компьютерной информацией Статья 255. Изготовление или сбыт специальных средств неправомерного доступа (проникновения) к компьютерной информации Статья 256. Разработка, использование и распространение вредоносных программ Статья 257. Нарушение правил эксплуатации компьютерной системы или сети

Таблица 2. Содержание соответствующих глав Уголовного кодекса Республики Беларусь и Республики Армения

УК Республики Беларусь	УК Российской Федерации
Глава 31. Преступления против компьютерной безопасности	Глава 28. Преступления в сфере компьютерной информации
Статья 349. Несанкционированный доступ к компьютерной информации Статья 350. Уничтожение, блокирование или модификация компьютерной информации Статья 351. Исключена Статья 352. Неправомерное завладение компьютерной информацией Статья 353. Исключена Статья 354. Разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств Статья 355. Нарушение правил эксплуатации компьютерной системы или сети	Статья 272. Неправомерный доступ к компьютерной информации Статья 273. Создание, использование и распространение вредоносных компьютерных программ Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации Статья 274.2. Нарушение правил централизованного управления техническими средствами

	противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования

Таблица 2. Содержание соответствующих глав Уголовного кодекса Кыргызской Республики и Республики Казахстан

УК Кыргызской Республики	УК Республики Казахстан
Глава 40. Преступления против кибер-безопасности	Глава 7. Уголовные правонарушения в сфере информатизации и связи
Статья 319. Несанкционированный доступ к компьютерной информации и электронным документам, в информационную систему или сеть электросвязи Статья 320. Создание вредоносных программных продуктов Статья 321. Кибер-саботаж Статья 322. Массовое распространение электронных сообщений	Статья 205. Неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций Статья 206. Неправомерные уничтожение или модификация информации Статья 207. Нарушение работы информационной системы или сетей телекоммуникаций Статья 208. Неправомерное завладение информацией Статья 209. Принуждение к передаче информации Статья 210. Создание, использование или распространение вредоносных компьютерных программ и программных продуктов Статья 211. Неправомерное распространение электронных информационных ресурсов ограниченного доступа Статья 212. Предоставление услуг для размещения интернет-ресурсов,

	преследующих противоправные цели Статья 213. Неправомерные изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства

По сути, в большинстве своем, содержание данных глав в целом схожее и включает в себя практически аналогичные виды преступлений. Однако, имеются незначительные различия в формулировках и определениях, что при осуществлении международного сотрудничества может создавать отдельные трудности. Киберпреступления носят трансграничный характер и соответственно требуют международного участия. Данный вид преступлений может совершаться в одной стране, а лицо, совершающее преступление, в другой стране. И отсутствие гармонизации в понятиях и определениях может усложнить расследование данной категории преступлений.

Вместе с тем, в уголовном законодательстве Республики Узбекистан была введена ответственность за преступления с квалифицирующими признаками, связанные с использованием компьютерной техники, информационных систем, сетей телекоммуникаций и Интернет:

– доведение до самоубийства (п. «г» ч.2 ст. 103 УК РУз);

– склонение к самоубийству (ч.2 п. «в» ст. 103^1 УК РУз);

– изготовление, ввоз, распространение, рекламирование, демонстрация порнографической продукции (ст. 130 УК РУз);

– изготовление, ввоз, распространение, рекламирование, демонстрация продукции, пропагандирующей культ насилия или жестокости (статья 130^1 УК РУз);

– клевета (ч.2 статья 139 УК РУз);

– оскорбление (ч.2 статья 140 УК РУз);

– нарушение законодательства о персональных данных (статья 141^2 УК РУз);

– посягательство на Президента Республики Узбекистан (ч.3 Статья 158

УК РУз)

– хищение путем присвоения или растраты (ч.4 п. «г» статья 167 УК РУз)

– мошенничество (п «в» ч.2 статья 168. УК РУз)

– кража (п. «б» ч.3 статья 169.);

– незаконная деятельность по привлечению денежных средств и (или) иного имущества (статья 188^{1});

– массовые беспорядки (п. «б» ч.2 ст. 244 УК РУз);

– изготовление, хранение, распространение или демонстрация материалов, содержащих угрозу общественной безопасности и общественному порядку (п. «г» ч.3 ст. 244^{1} УК РУз.);

–. распространение не соответствующих действительности сведений о распространении карантинных и других опасных для человека инфекций (ч.2 статья 244^{5} УК РУз);

–распространение ложной информации (статья 244^{6} УК РУз);

– организация и проведение азартных и других основанных на риске игр (ч.3 статья 278 УК РУз).

В качестве отдельной проблемы можно выделить неоднозначное толкование терминологии в сфере киберпреступности. В уголовном законодательстве Республике Узбекистан отдельные понятия и термины по преступлениям в сфере информационных технологий раскрыты непосредственно в диспозиции соответствующей статьи. В Российской Федерации принято Постановление Пленума Верховного суда №37 от 15 декабря 2022 г., где раскрыты отдельные понятия, такие как компьютерные устройства, компьютерная программа, уничтожение, копирование компьютерной информации и т.д. В данном Постановлении даются разъяснения и определения по применению норм законодательства, что направлено для правильной квалификации преступлений в сфере информационных технологий.

Кроме того, имеются международные стандарты определения данных понятий. И не всегда все эти понятия соответствуют имеющемуся законодательству, что вызывает сложности у правоприменителя.

При формулировании уголовно-правовой нормы, определяющей преступления в данной сфере, целесообразно участие не только соответствующих юристов, но и специалистов в сфере информационной технологий и безопасности. Важное значение имеет унификация в определении понятий в

национальных кодексах.

К примеру, имеются различные мнения по определению законодателями разных стран данной категории преступлений. В Уголовном кодексе Республике Казахстан данная глава определена как «Уголовные правонарушения в сфере информатизации и связи», Кыргызской Республике в кодексе 2017 г. — «Преступления против информационной безопасности», в последнем 2021 г. — «Преступления против кибер-безопасности», в России – «Преступления в сфере компьютерной информации», в Республике Беларусь – «Преступления против компьютерной безопасности», в Республике Таджикистан – «Преступления против информационной безопасности», в Республике Узбекистан «Преступления в сфере информационных технологий» и т.д.

Даже понятие «киберпреступность» не имеет однозначного толкования. Ван Гуанлун определяет его любое преступление, совершаемое с помощью компьютерной системы или сети, в ее рамках или против нее [7, С.661-677].

По мнению Е.В. Христининой, киберпреступления – это умышленные преступления, выражающиеся в виде незаконных действий (бездействий), совершенные с использованием кибертехнологий в виртуальной среде (киберпростанство) с применением телекоммуникационных способов и средств, в том числе сети Интернет, которые выступают преступными орудиями или предметами противоправных посягательств [8, С. 150-154].

Вместе с тем, группа экспертов Организации экономического сотрудничества и развития определила киберпреступление, как любое незаконное, неэтичное или неразрешенное поведение, затрагивающее автоматизированную обработку и (или) передачу данных [9].

При этом, должны отметить, что сравнительный анализ уголовно-правового законодательства зарубежных стран показывает, что на сегодняшний день не все виды преступлений, охватываемые данной сферой, урегулированы рамками национального законодательства Республики Узбекистан.

К примеру, статья 274.1 УК РФ предусматривает уголовную ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации с помощью создания, распространения или использования компьютерных программ..

В Республике Казахстан предусмотрена уголовная ответственность по статье 209 УК за принуждение к передаче информации, статье 212 УК за

предоставление услуг для размещения интернет-ресурсов с запрещенным контентом, статье 213 УК за неправомерное изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства и т.д.

Уголовное законодательство Кыргызской Республик предусматривает ответственность за массовое распространение электронных сообщений по статье 322 УК.

Изучение мнения специалистов, зарубежного законодательства и правоприменительной практики влечет за собой необходимость внесения соответствующих изменений и дополнений в уголовно-правовое законодательство Республики Узбекистан:

– включение нового раздела «Преступления в сфере информационных технологий и безопасности, средств телекоммуникаций и связи», который будет включать в себя отдельные главы:

Глава 1. «Преступления против информационной безопасности»;

Глава 2. «Преступления против безопасности стратегической информационной инфраструктуры»;

Глава 3. «Преступления в сфере телекоммуникаций и связи»;

– предусмотреть уголовную ответственность за кибератаку на объект критической информационной инфраструктуры в соответствии с Законом Республики Узбекистан № ЗРУ-764 «О кибербезопасности» от 15 апреля 2022 г. Причем имеются два варианта включения данного деяния в Уголовный кодекс. В РФ предусмотрена отдельная статья 274.1. неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации. В Республике Казахстан, Кыргызской Республике воздействие на критическую информационную структуру идет в качестве квалифицирующего признака по соответствующим статьям;

– определить уголовную и административную ответственность за нарушение правил электронной коммерции;

– анализ зарубежного опыта (Российской Федерации, Республики Казахстан, Республики Молдова, Республики Беларусь, Азербайджанской Республики, Республики Грузия, Кыргызской Республики) и правоприменительной практики свидетельствует о необходимости объединения ст.

278[4] «Модификация компьютерной информации» и ст. 278[5]. «Компьютерный саботаж». За последние 5 лет в республике не было зарегистрировано ни одного преступления по ст. 278-5 «Компьютерный саботаж»;

– судебная практика свидетельствует о необходимости ответственности за клонирование IMEI-кодов сотовых телефонов.

На сегодняшний день вопрос противодействия киберпреступности приобретает особую актуальность во всем мире. Постоянное развитие информационных технологий и компьютерных сетей влечет за собой появление её новых форм и особенностей. При этом, киберпреступность выходит за рамки географических и национальных границ, а также без особого труда проникает в самые защищенные отрасли национальной экономики, включая кредитно-финансовую сферу, оборонно-промышленный комплекс. Трансграничный характер киберпреступности обусловливает необходимость тесного международного сотрудничества, унификации понятий и терминов. Вместе с тем, уголовно-правовая политика государства должна своевременно реагировать на современные вызовы и угрозы в киберпространстве, однако на сегодняшний день имеется ряд вопросов требующих разрешения.

Список литературы

1. Расулев А.К. Перспективы правовой политики в области противодействия киберпреступности в Узбекистане/ URL: https://illp.uz/%D0%BF%D0%B5%D1%80%D1%81%D0%BF%D0%B5%D0%BA%D1%82%D0%B8%D0%B2%D1%8B-%D0%BF%D1%80%D0%B0%D0%B2%D0%BE%D0%B2%D0%BE%D0%B9-%D0%BF%D0%BE%D0%BB%D0%B8%D1%82%D0%B8%D0%BA%D0%B8-%D0%B2-%D0%BE%D0%B1%D0%BB%D0%B0/. (дата обращения: 20.05.2023.)
2. Бородкина Т.Н., Павлюк А.В. Киберпреступления: понятие, содержание и меры противодействия // Социально-политические науки. 2018. № 1. С.135-137.
3. Буткевич С.А. Экстремизм и терроризм в киберпространстве: выявление, нейтрализация и предупреждение // Вестник Краснодарского университета МВД России. 2018. № 1 (39). С. 17-22.
4. Веренич И.Г. Противодействие терроризму в информационном пространстве // Государственное и муниципальное управление. Ученые записки. 2023. № 1. С. 293-296.

5. Лапунова Ю.А., Голяндин Н.П. Распространение идеологии экстремизма и терроризма в киберпространстве: проблемы и пути их решения // Труды Академии управления МВД России. 2017. № 3 (43). С. 100-104.
6. Боровикова А. Борьба с киберугрозами: время новых решений. URL: https://yuz.uz/ru/news/borba-s-kiberugrozami-vremya-novx-resheniy (дата обращения 12.05.2023).
7. Ван Гуанлун. Уголовно-правовое регулирование противодействия киберпреступности в Китае: состояние, тенденции и недостатки // Вестник СПбГУ. Право. 2022. Т. 13. Вып. 3. С.661-677.
8. Христинина Е.В. К вопросу об уголовно-правовом противодействии киберпреступности // Вестник Сибирского юридического института МВД России. 2021. №3 (45). С. 150-154.
9. OECD, Computer – Relates Crime: Analysis of Legal Policy. Paris, 1986.

IMPROVING THE CRIMINAL LAW POLICY IN COMBATING CYBERCRIME IN THE REPUBLIC OF UZBEKISTAN

Abdulaziz Rasulev
Scientific Secretary of the Institute of Legislation and Legal Policyunder the President of the Republic of Uzbekistan, Doctor of Law, Professor

Lyudmila Yugay
Acting Associate Professor of the Department of Crime Prevention Activities of the Academy of the MIA of the Republic of Uzbekistan, Doctor of Law

Annotation. The current state and prospects for the development of the criminal law policy of the Republic of Uzbekistan in combating cybercrime are covered in the article. The author conducts a comparative legal analysis of crimes in this sphere in the Republic of Uzbekistan, the Republic of Armenia, the Russian Federation, the Republic of Kazakhstan, and other states. The development trends of the criminal law of the Republic of Uzbekistan are defined.

Key words: Internet, digitalization, cybercrime, Criminal Code.

Հոդվածը գրախոսվել է՝ 01. 08.2023թ.:
Ներկայացվել է տպագրության՝ 01.08.2023թ.: