ТЕНДЕНЦИИ УГОЛОВНОЙ ПОЛИТИКИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

А. Р. АЛИМБЕТОВА,

д-р PhD, доц. каф. «Экономика, услуги и право» Алматинского гуманитарно-экономического университета

В современном информационном обществе процессы цифровизации проникают во все сферы жизни, включая сферу правопорядка и уголовного законодательства. В связи с этим возникает неотложная потребность анализа и адаптации уголовной политики к новым вызовам и возможностям, предоставляемым цифровой эпохой. Такие тенденции требуют внимательного изучения и обсуждения в рамках общества и юридического сообщества с целью разработки эффективных мер по обеспечению правопорядка в цифровой среде.

На сегодняшний день мы уже можем отметить успешную интеграцию современных технологий в уголовно-правовую систему.

Органы прокуратуры начали процесс цифровизации надзора еще в 2004 г. Была утверждена среднесрочная программа по укреплению материально-технической базы прокуратуры и внедрению современных информационных систем [1]. Этот шаг создал современную основу для текущих инноваций в различных сферах общественных отношений.

Одной из областей, на которую оказал влияние этот процесс, является уголовный процесс. До 2011 года, сбор достоверной информации о преступности представлял собой сложную задачу, поскольку учет велся вручную, что приводило к трудностям в выявлении тысяч скрытых преступлений. В ответ на это была внедрена Единая программа «Электронная книга учета заявлений и информации» во всех регионах [2]. Она позволила эффективно учитывать более 2 000 000 заявлений о преступлениях, и, что важно, ввести уголовную ответственность за их утаивание. В результате принятых мер удалось сократить число скрытых преступлений в 10 раз.

В 2015 году Генеральная прокуратура продолжила цифровизацию, представив информационную систему «Единый реестр досудебных расследований» [3]. Система полностью автоматизировала регистрацию уголовных дел и содержит полную информацию о ходе расследования и принимаемых процессуальных решениях. В 2016 году система была интегрирована с информационной системой Верховного суда, что стало толчком для автоматизации всех стадий уголовного процесса – от регистрации преступлений до вынесения приговора.

В 2017 году была разработана система электронных уголовных дел, и с января 2018 года, после успешной апробации и внесения поправок в УПК, расследование официально стало возможным в электронном формате. В 2021 году более 80 000 уголовных дел были получены судебные санкции и справки в режиме онлайн [4, с. 6]. Участники процесса и адвокаты получили доступ к оцифрованным материалам через публичный сектор, включая протоколы следственных действий, допросы и экспертизы. Информационные технологии успешно применяются при внедрении трехзвенной модели уголовного процесса. Сегодня следователи готовят процессуальные документы по электронным шаблонам в системе «Единый реестр досудебных расследований», а затем подписывают их цифровой подписью, направляя прокурору. Прокурор проводит онлайн-проверку законности признания лица подозреваемым, прерывания дела и принятия решения. Расширение использования цифрового формата поможет снизить риски злоупотреблений и усилит защиту прав участников процесса.

Одной из главных тенденций в уголовной политике в условиях цифровизации является необходимость адаптации законодательства к новым вызовам и возможностям, которые предоставляют современные технологии. Киберпреступности, нарушения в сфере кибербезопасности и другие цифровые преступления требуют дифференцированного и эффективного подхода со стороны государства.

Важным аспектом уголовной политики в эпоху цифровизации является также баланс между защитой частной жизни граждан и необходимостью обеспечения безопасности общества. Развитие новых технологий, таких как системы видеонаблюдения, распознавание лиц и анализ данных, вызывает вопросы относительно ограничения государственной власти и соблюдения прав граждан.

Следует также отметить, что цифровизация предоставляет новые возможности для улучшения процессов расследования и предотвращения преступлений. Использование аналитики данных, искусственного интеллекта и других технологий может значительно повысить эффективность правоохранительных органов.

Таким образом, уголовная политика в эпоху цифровизации становится важным инструментом поддержания законности и обеспечения безопасности общества, требуя постоянного совершенствования законодательства, применения новых технологий и обеспечения баланса между индивидуальными правами и коллективной безопасностью.

Одним из основных аспектов воздействия цифровизации на уголовную политику является сфера борьбы с киберпреступностью. С развитием

информационных технологий, сетевых коммуникаций и электронной коммерции возникли новые виды преступлений, связанных с компьютерами и интернетом. К ним относятся, например, хакерство, распространение вредоносных программ, кибермошенничество и другие. Для эффективной борьбы с такими преступлениями необходимо разработать и внедрить соответствующие нормативно-правовые акты, а также обеспечить квалифицированных специалистов в сфере кибербезопасности.

Разработка и внедрение соответствующих нормативно-правовых актов в области киберпреступности имеют стратегическое значение для обеспечения эффективной борьбы с современными цифровыми угрозами. Ниже представлены два примера таких актов и их возможных задач:

Закон о кибермошенничестве:

Задачи: Установление ответственности за мошеннические действия, осуществляемые с использованием цифровых технологий. Регулирование электронных финансовых средств и мер по предотвращению кибермошенничества в сфере онлайн-платежей.

1. Установление наказаний: Закон должен предусматривать наказания для лиц, совершающих кибермошеннические действия. Наказания должны быть пропорциональны тяжести совершенного преступления, и могут включать в себя штрафы, тюремное заключение и другие меры.

2. Определение электронных финансовых средств. Закон должен четко определить понятие электронных финансовых средств и включить их в сферу регулирования. Это может включать в себя электронные кошельки, онлайн-платежные системы, криптовалюты и другие цифровые формы финансовых активов.

3. Обеспечение безопасности онлайн-платежей. Закон должен устанавливать стандарты безопасности для онлайн-платежей с целью предотвращения кибермошенничества. Это может включать в себя двухфакторную аутентификацию, защиту от несанкционированного доступа, мониторинг транзакций и другие меры.

Меры по предотвращению кибермошенничества в сфере онлайн-платежей:

1. Обучение и информирование. Закон может предусматривать меры по обучению пользователей онлайн-платежных систем о методах предотвращения мошенничества, такие как проведение образовательных кампаний, предоставление информационных материалов и другие формы обучения.

2. Сотрудничество с платежными системами: Закон должен стимулировать сотрудничество между государственными органами и провайдерами платежных систем для обмена информацией о мошеннических схемах,

а также для разработки и внедрения инновационных методов защиты от кибермошенничества.

В целом, Закон о кибермошенничестве направлен на создание правового каркаса, который не только устанавливает ответственность за преступления, но и регулирует сферу электронных финансовых средств, обеспечивая безопасность онлайн-платежей и предотвращение кибермошенничества

Закон о киберспециалистах:

Задачи: Установление квалификационных требований для специалистов в области кибербезопасности. Регулирование процедур сертификации и обучения в целях повышения квалификации. Содействие формированию высококвалифицированных кадров в сфере кибербезопасности.

Закон о киберспециалистах представляет собой важное регулирующее положение, направленное на установление стандартов и требований к специалистам в области кибербезопасности. Его основные задачи заключаются в следующем:

1. Определение минимальных стандартов. Закон определяет минимальные требования к квалификации киберспециалистов, включая образование, опыт работы и профессиональные навыки. Это может включать в себя высшее образование в сфере кибербезопасности, сертификации от организаций и практический опыт.

2. Квалификация в соответствии с ролями. Закон может определять различные уровни квалификации, соответствующие различным ролям в области кибербезопасности, таким как аналитики, инцидент-менеджеры, специалисты по защите от вредоносных программ и др.

3. Регулирование процедур сертификации и обучения. Закон устанавливает процедуры для сертификации киберспециалистов, включая требования к экзаменам, периодичность пересдачи и актуализацию сертификации в соответствии с изменениями в области кибербезопасности.

4. Обучение и повышение квалификации. Закон стимулирует регулярное обучение и повышение квалификации киберспециалистов. Это может включать в себя участие в профессиональных тренингах, курсах и конференциях, направленных на освежение знаний и усвоение новых технологий.

5. Содействие формированию высококвалифицированных кадров. Закон может предусматривать меры по стимулированию создания и развития образовательных программ в области кибербезопасности на разных уровнях образования – от высших учебных заведений до профессиональных школ.

6. Сотрудничество с индустрией: Закон может способствовать установлению партнерств между образовательными учреждениями и предприятиями в сфере кибербезопасности, обеспечивая, таким образом, более актуальное и практико-ориентированное обучение.

Закон о киберспециалистах стремится обеспечить высокий уровень квалификации и профессионализма в сфере кибербезопасности, а также содействовать формированию кадров, способных эффективно справляться с вызовами в сфере киберугроз.

Эти нормативно-правовые акты направлены на создание системы правовых мер, обеспечивающих защиту от киберугроз, предотвращение киберпреступлений, а также эффективное расследование и привлечение к ответственности лиц, совершивших такие преступления. Вместе они создают целостную и сбалансированную правовую основу для современной кибербезопасности.

В заключение, эра цифровизации оказывает глубокое воздействие на уголовную политику, привнося в нее новые вызовы и возможности. Принятые в последние годы меры, такие как внедрение современных технологий в уголовные процессы, цифровизация систем надзора и обработка данных, являются ключевыми шагами в направлении более эффективного борьбы с преступностью.

Особое внимание следует уделять аспектам кибербезопасности и защите данных граждан в сети интернет. Баланс между приватностью граждан и необходимостью правоохранительных органов вмешиваться в киберпространство представляет собой сложную задачу, требующую разработки гибких и адаптивных правовых механизмов.

Важным направлением развития является углубление сотрудничества между государственными органами, частным сектором и общественностью для создания эффективных стратегий борьбы с киберпреступностью и обеспечения цифровой безопасности.

Подводя итог, цифровизация уголовной политики требует не только технических инноваций, но и внимательного рассмотрения этических, правовых и социальных аспектов. Только в гармонии этих элементов можно достичь более высокого уровня безопасности и справедливости в цифровом мире.

ЛИТЕРАТУРА

1. Постановление Правительства Республики Казахстан № 917 «О Среднесрочном плане социально-экономического развития Республики Казахстан на 2005–2007 годы» [Электронный ресурс]. – Режим доступа: https://adilet.zan.kz/rus/docs/P040000917_. – Дата доступа: 31.08.2004.
2. Совместный приказ Председателя Агентства Республики Казахстан по борьбе с экономической и коррупционной преступностью (финансовая полиция) № 425, Генерального Прокурора Республики Казахстан № 124 и Министра внутренних дел Республики Казахстан № 758 «О переходе на электронный формат ведения единого карточного

учета заявлений, сообщений, жалоб и иной информации о преступлениях, происшествиях, уголовных дел, результатов их расследования и прокурорского надзора» [Электронный ресурс]. – Режим доступа: https://adilet.zan.kz/rus/docs/V1300009056. – Дата доступа: 30.12.2013.

3. Приказ Генерального Прокурора Республики Казахстан от 19 сентября 2014 года № 89. Зарегистрирован в Министерстве юстиции Республики Казахстан № 9744 «Об утверждении Правил приема и регистрации заявления, сообщения или рапорта об уголовных правонарушениях, а также ведения Единого реестра досудебных расследований» [Электронный ресурс]. – Режим доступа: https://adilet.zan.kz/rus/docs/V14W0009744. – Дата доступа: 23.09.2014.
4. Цифровизация уголовного процесса:реалии и перспективы: материалы Междунар. науч.-практ. конф., Караганда 25 июня 2021 г. / Республика Казахстан, Министерство Внутренних Дел, редкол.: Сейтжанов О. Т. [и др.]. – Карагандинская Академия имени Баримбека Бейсенова, 2021. – 6 с.