

Разиков Азамат Мухитдинович

*Ўзбекистон Республикаси Бош прокуратураси Ахборот коммуникация
технологияларини жорий этиш ва ахборот хавфсизлигини таъминлаш
бошқармаси бошлиғининг ўринбосари*

РАҚАМЛИ ТЕХНОЛОГИЯЛАР СОҲАСИДАГИ ЖИНОЯТЛАРНИ ТЕРГОВ ҚИЛИШ УСТИДАН ПРОКУРОР НАЗОРАТИ

Разиков Азамат Мухитдинович

*Заместитель начальника Управления внедрения информационно-
коммуникационных технологий и обеспечения информационной
безопасности Генеральной прокуратуры Республики Узбекистан*

ПРОКУРОРСКИЙ НАДЗОР ЗА РАССЛЕДОВАНИЕМ ПРЕСТУПЛЕНИЙ В СФЕРЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Razikov Azamat

*Deputy Head of the Department for Implementation of Information and
Communication Technologies and Information Security of the Prosecutor General's
Office of the Republic of Uzbekistan*

PROSECUTORIAL SUPERVISION OVER THE INVESTIGATION OF CRIMES IN THE FIELD OF DIGITAL TECHNOLOGIES

В связи с интенсивным развитием информационных технологий и телекоммуникаций в мире увеличилось количество преступлений в сфере информационных технологий. Согласно докладу о глобальных рисках Всемирного экономического форума 2019 года, изменения данных и кибератаки оцениваются четвертым и пятым глобальными рисками, с которыми сталкивается каждая организация.

Также в нашей республике наблюдается тенденция к росту преступности в сфере информационных технологий, так к 2018 году число совершенных преступлений в сфере информационных технологий сравнительно к 2017 году выросло в 4,5 раза, а к 2019 году по сравнению с 2016 годом выросло на 17,2 раза, а к сравнению 2017 года на 4,3 раза. В 2020 году на фоне пандемии по всему Узбекистану число совершенных преступлений в данной сфере продолжало расти.

В свою очередь это говорит о том, что требуется проведение инвентаризации законодательных актов о прокурорском надзоре за расследованием преступлений в сфере информационных технологий, совершенствование правовых механизмов прокурорского надзора над

проведением дознания таких деяний, имплементация в национальное законодательство положительных аспектов законодательств зарубежных стран.

Здесь важно устранить действующие пробелы в законодательстве о прокурорском надзоре за расследованием преступлений в сфере информационных технологий, а также внедрить новые понятия и институты.

В 70-е годы было совершено одно из первых киберпреступлений в США, где обычный консультант компании SPNBS по безопасности информационных технологий сумел расшифровать специальный код, который управлял системой банка в Лос-Анжелесе, и с помощью программы дал команду на трансфер 10 миллионов долларов США. Как утверждают другие аналитики и ученые, первое киберпреступление было совершено 1969 году итальянцем из США Альфонсо Конфессорро, который сумел незаконно получить доступ к ЭВМ и совершить налоговое преступление в сумме 620 тысяч долларов США [1].

Факт совершения киберпреступлений привлек внимание правоохранительных органов и правоведов США. Тем временем началось интенсивное исследование этого нового феномена.

Сначала правоохранительные органы начали квалифицировать подобные преступления по статьям кражи, мошенничества, кража государственных секретов, злоупотреблением доверием.

Потом такой устаревший метод не дал свои результаты, так как преступления, совершенные с помощью информационных технологий, не попадали в состав вышеуказанных преступлений. Например, транзакция денег, путём обмана компьютера не квалифицируется как кража и не квалифицируется как мошенничество.

Проблемы

Также на сегодняшний день несогласованность национального законодательства в сфере борьбы с киберпреступностью, информационной безопасности и наличие пробелов негативно сказываются на должном реагировании на современные глобальные вызовы и борьбе с этим видом преступности, в частности:

1) законодательство в сфере информационных технологий и безопасности фрагментарно и непоследовательно.

В частности, нормативно-правовая база включает 29 законов, 51 указов и постановлений Президента, 96 постановлений правительства.

2) Нормы Уголовного кодекса не соответствует современным угрозам кибербезопасности:

в частности, глава XX¹ не полностью охватывает преступления в сфере информационных технологий. Уголовное преследование за преступления в сфере информационных технологий и безопасности установлено с 16 лет. Это позволит молодым хакерам избежать уголовной ответственности.

Следует отметить, что возраст привлечения к уголовной ответственности (14 лет в Германии, 12 лет в Канаде, 10 лет в Австралии и 14 лет в Южной Корее) в зарубежных странах ниже 16 лет.

3) Нехватка кадров со специальной подготовкой, знаниями и навыками в области права и информационных технологий для борьбы с киберпреступностью.

Для справки: В Санкт-Петербургском университете МВД РФ готовятся юристы по специальности «Информационная безопасность в сфере правоохранительной деятельности».

Рассмотрим действующие организационно-правовые основы прокурорского надзора за расследованием преступлений в сфере информационных технологий в Республике Узбекистан.

Согласно Закону Республики Узбекистан «О прокуратуре» от 29 августа 2001 года № 257-II, органы прокуратуры осуществляют свою деятельность по следующим основным направлениям:

- надзор за исполнением законов министерствами, государственными комитетами, ведомствами, органами самоуправления граждан, общественными объединениями, предприятиями, учреждениями, организациями, хокимами и другими должностными лицами;

- надзор за исполнением законов, направленных на обеспечение прав и свобод гражданина;

- надзор за соблюдением законов в Вооруженных Силах, воинских формированиях министерств, государственных комитетов и ведомств Республики Узбекистан;

- надзор за исполнением законов органами, осуществляющими оперативно-розыскную деятельность, доследственную проверку, дознание, предварительное следствие, и координация их деятельности по борьбе с преступностью;

- производство предварительного расследования преступлений;

- поддержание государственного обвинения при рассмотрении в судах уголовных дел, участие в рассмотрении в судах гражданских дел, дел об административных правонарушениях и экономических споров, опротестование несоответствующих закону судебных актов;

- надзор за исполнением законов, направленных на укрепление налоговой дисциплины, борьбу с налоговыми, валютными преступлениями и правонарушениями, а также возмещение экономического ущерба, нанесенного государству;

- надзор за соблюдением законов в местах содержания задержанных, заключенных под стражу, при исполнении уголовных наказаний и иных мер уголовно-правового воздействия;

- участие в законотворческой деятельности и работе по повышению правовой культуры в обществе [2].

Один из основных направлений деятельности органов прокуратуры является надзор за исполнением законов органами дознания и предварительного следствия, а также органами, осуществляющими доследственную проверку.

Данное направление подробно раскрывается в Уголовно-процессуальном кодексе Республики Узбекистан. Согласно статье 345 Уголовно-процессуального кодекса Республики Узбекистан «предварительное следствие по делам о преступлениях в сфере информационных технологий производится следователями органов внутренних дел», а надзор за этими преступлениями принадлежит Генеральной прокуратуры Республики Узбекистан.

Следующим важным нормативно-правовым актом является Закон Республики Узбекистан «Об оперативно-розыскной деятельности» от 05.12.2012г. № ЗРУ-344, который заложил основу прокурорского надзора за расследованием преступлений (в сфере информационных технологий). Так, одним из «оснований для проведения оперативно-розыскных мероприятий указано письменное поручение органов дознания, следствия, указание и поручение прокурора, согласованием с прокурором».

Ещё одним нормативно-правовым актом стал приказ Генерального прокурора Республики Узбекистан «Об эффективном обеспечении защиты прав и свобод граждан, верховенства закона в ходе борьбы с преступностью, дознания предварительного следствия и оперативно-розыскной деятельности», который определил основными задачами прокурора – это «надзор и координация деятельности органов, осуществляющих доследственную проверку, дознание, предварительное следствие и оперативно-розыскную деятельность, обеспечение верховенства закона, укрепление законности, защиту прав и свобод граждан, охраняемых законом интересов общества и государства, конституционного строя Республики Узбекистан путем производство доследственных проверок и предварительного следствия, предупреждение и профилактику правонарушений».

«Прокурор в целях борьбы с преступностью координирует деятельность органов, осуществляющих оперативно-розыскную деятельность доследственные проверки, дознание и предварительное следствие».

Согласно вышеуказанному приказу Генерального прокурора «прокурор вправе требовать от руководителей и других должностных лиц органов, осуществляющих оперативно-розыскную деятельность, выделения специалистов в сфере информационных технологий для выяснения возникших вопросов в ходе оперативно-розыскной деятельности. Должностные лица органов, осуществляющих оперативно-розыскную деятельность, обязаны приступить к выполнению такого требования незамедлительно. Например, такая ситуация может возникнуть, когда проводится осмотр место происшествия преступлений в сфере информационных технологий».

Таким образом, **прокурорский надзор за законностью оперативно-розыскной деятельности в сфере информационных технологий** считается составной частью надзора за следствием и дознанием.

Предложения

Первое. Изучение прокуратуры зарубежных стран показывает, что в прокуратуре Южной Кореи существует отдельное управление по борьбе с киберпреступлениями, которое имеет право расследовать и надзирать за расследованиями преступлений в сфере информационных технологий.

В прокуратурах Германии, ОАЭ, Франции, Швейцарии существуют отдельные подразделения, занимающиеся вопросами киберпреступлений.

В структуре Генеральной прокуратуры Республики Узбекистан подобного управления нет. Исходя из этого, на базе управления по внедрению информационно-коммуникационных технологий и обеспечению информационной безопасности Генеральной прокуратуры Республики Узбекистан необходимо открыть новое управление по надзору за исполнением законодательства в сфере информационных технологий и обеспечению информационной безопасности.

Основными задачами управления определить:

- осуществление системного анализа состояния законности и практики прокурорского надзора за расследованием преступлений в сфере информационных технологий, а также выявление системных нарушений и принятие мер по устранению причин и условий, им способствующих;

- осуществление непосредственного надзора за своевременной регистрацией и разрешением заявлений и сообщений о киберпреступлениях, соблюдением требований законов при проведении оперативно-розыскных мероприятий;

- осуществление надзора за расследованием преступлений в сфере информационных технологий органами дознания и предварительного следствия;

- изучение уголовных дел, материалов доследственных проверок, розыскных, оперативно-поисковых, профилактических дел, принятие мер по отмене незаконных постановлений и обеспечению законности принимаемых решений.

Второе. Предлагается дополнить Уголовный кодекс Республики Узбекистан термином «кибератака» и статьей 278⁸ «Кибератака на объект критической информационной инфраструктуры», предусмотрев уголовную ответственность за следующие действия:

Кибератака на объект критической информационной инфраструктуры – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации.

Третье. Принять соответствующий нормативно-правовой акт, предусматривающий обязательное повышение квалификации сотрудников в сфере ИКТ и ИБ в высших учебных заведениях Министерства внутренних дел, Генеральной прокуратуры, Службы государственной безопасности республики.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ:

1. Медведев С.С. Мошенничество в сфере высоких технологий: дис... канд. юрид. наук. Краснодар, 2008. – С. 31.
2. Закон Республики Узбекистан «О прокуратуре» от 29 августа 2001 года № 257-II ст. 3 <https://lex.uz/acts/33203>. Дата обращения: 10.05.2019 г.
3. Расулев, Абдулазиз Каримович. «Криминологическая характеристика преступлений в сфере информационных (компьютерных) преступлений». Вопросы современной юриспруденции 2 (53) (2016).
4. Расулев, Абдулазиз, and Сурайё Рахмонова. «Преступления в сфере информационных технологий и безопасности: детерминанты и предупреждение». Общество и инновации 1.1 (2020): 200–209.
5. Расулев А.К. «Повышение качества и результативности юридического образования и науки». Фан ва таълим замонавий босқичда: ислохотлар ва стратегик йўналишлар: 16–23.