EURASIAN JOURNAL OF LAW, FINANCE AND APPLIED SCIENCES
INTERNATIONAL SCIENTIFIC JOURNAL SPECIAL SERIES « ADMINISTRATIVE-LEGAL REFORMS IMPLEMENTED IN THE SYSTEM OF INTERNAL AFFAIRS BODIES: RESULTS AND PROSPECTS »
UIF = 8.3 | SJIF = 5.961

СУЩНОСТЬ АДМИНИСТРАТИВНО-ПРАВОВЫХ РЕФОРМ В ОБЛАСТИ БОРЬБЕ С КИБЕРПРЕСТУПЛЕНИЯМИ И ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ В РЕСПУБЛИКЕ УЗБЕКИСТАН

Халмуратов Айбек Оразбаевич
Преподаватель Кафедры административное право
Академии МВД Республики Узбекистан
https://doi.org/10.5281/zenodo.7544659

Аннотация. В данной статье раскрыты сущность административно-правовых реформ в области борьбе с киберпреступлениями и обеспечение кибербезопасности в Республике Узбекистан. Подробно описывается деятельность органов внутренних дел и также реформы в Академии МВД Республики Узбекистан. Автором разработаны рекомендации и предложения по совершенствованию механизмов по борьбе с киберпреступлениями и обеспечению кибербезопасности в Республике Узбекистан.
Ключевые слова: киберпреступления, кибербезопасность, кибератаки, киберугрозы, механизмы.

Безусловно возникают новые вызовы, угрожающие жизни общества в нынешнюю, стремительно развивающуюся, сложную эпоху XXI века. В результате ускорения обмена информацией такие понятия, как **“киберпреступность”, “кибератака”, “кибербезопасность”** стали популярными и стали актуальными событиями. Поэтому вопрос защиты от угроз в киберпространстве сегодня вызывает серьезную озабоченность мирового сообщества.

Следовательно, ежегодно в мире организуется более **500 миллионов кибератак**. Каждую секунду каждый 12 человек в мире подвергается атаке в киберпространстве, становится его жертвой. В частности, в таких странах, как США, Франция, Великобритания, Бельгия, Германия, Люксембург уровень киберпреступности составляет **60-65 процентов** от общего числа преступлений [1].

По оценкам экспертов, большинство кибератак направлены на получение конфиденциальной информации, ее изменение или хищение, вымогательство денег у пользователей или срыв бизнес-процессов, в результате чего мировая экономика в среднем терпит убытки в размере более **20 миллиардов долларов** США в год [2].

По данным МВД в Узбекистане за последние три года киберпреступления выросли в **8,3 раза**, составив **5%** от общего числа преступлений. Так, случаи кибермошенничества увеличились в 13 раз, хищений — в 20 раз, преступлений, связанных с вымогательством, клеветой и оскорблением — в 4,9 раза [3].

Согласно аналитическим данным, некоторые виды киберпреступлений в нашей республике, в том числе хищения чужих средств на пластиковых картах посредством незаконных банковских и финансовых операций, получение онлайн-микрозаймов на чье-либо имя, организация финансовых пирамид, атаки на компьютеры с помощью вирусных программ, запугивание путем распространения иных личных информации людей. Растет количество таких преступлений, как вымогательство, незаконная торговля наркотиками в Интернете, азартные и рискованные онлайн-игры,

информационные атаки, направленные на религиозный экстремизм, мошенничество в сфере онлайн-покупок.

К сожалению, молодежь составляют большинство людей, совершающих правонарушения и преступления в виртуальном мире. В нашей республике основная часть этого вида преступлений, то есть более **80 процентов**, совершается подростками в возрасте от 16 до 23 лет [4].

Очевидно, что вопрос обеспечения кибербезопасности и борьбы с этим видом преступности сегодня становится как никогда актуальным. Вред и опасность преступлений в виртуальном мире превосходят угрозы в реальном мире. В этом смысле в последние годы в нашей стране уделяется внимание вопросу информационной безопасности на уровне государственной политики в рамках административно-правовых механизмов. В процессе глобальных изменений, происходящих в мировом информационном поле, ведется планомерная работа по повышению культуры использования гражданами сети Интернет, созданию эффективных механизмов обеспечения информационной безопасности и противодействия киберпреступлениям, реализации комплексных мероприятий в этой области. Совершенствуя защиту информационных технологий и коммуникаций, внедряются в практику новые подходы к борьбе с киберпреступностью.

В частности, в 2021 году при Управлении оперативно-розыскного сотрудничество МВД был создан Центр кибербезопасности. Любая противоправная деятельность, осуществляемая в настоящее время данным центром в киберпространстве, в том числе хищение интеллектуальной собственности граждан, взлом чужих аккаунтов в социальных сетях, распространение ложной информации, клевета, оскорбление, разжигание межнационального конфликта или межрелигиозной вражды, финансовые пирамиды в сети Интернет, выявляются преступления мобильной связи и иные виды преступлений, а в отношении лиц, их совершивших, принимаются меры административно- и уголовно-правового характера [5].

Вместе с этим, 15 апреля 2022 года впервые в истории независимого Узбекистана принят совершенно новый закон “О кибербезопасности” под номером № ЗРУ-764 [6]. Настоящий Закон служит для регулирования государством кибербезопасности в Республике Узбекистан, определения полномочий, прав и обязанностей соответствующих органов, обеспечения целостности информационных систем и ресурсов, предотвращения незаконного вмешательства в информационные системы и сети наша страна. Кроме того, в целях законодательного укрепления норм кибербезопасности предусмотрено принятие национальной стратегии по кибербезопасности.

Президент Республики Узбекистан Шавкат Миромонович Мирзиёев 26 января 2022 г. на видеоселекторном совещании, посвященном определению Стратегии Развития Узбекистана на 2022-2026 годы и обсуждению вопросов ее реализации в текущем году, создания системы предотвращения атак, связанных с информационными технологиями и обеспечения кибербезопасность, мониторинг внутренних и внешних финансовых потоков, а также подчеркнул внедрение новых механизмов, направленных на предотвращение связанных с этим рисков [7].

Данные неотложные задачи требуют дальнейшего повышения эффективности органов внутренних дел по противодействию кибербезопасности, широкого применения передовых механизмов на местах, подготовки зрелых квалифицированных кадров [8].

В связи с этим в Академии МВД ведется планомерная работа. Курсанты очной формы обучения в настоящее время проходят углубленную подготовку по противодействию киберпреступности в рамках дисциплины “Информационные технологии”.

В целях обеспечения отрасли квалифицированными специалистами были отобраны 75 курсантов 1-го курса обучения, 40 курсантов 2-го курса обучения и 85 курсантов 3-го курса обучения и сформированы специализированные экспериментальные группы. В настоящее время 85 курсантов 3-го курса обучения очной формы обучения проходят практику в Центра кибербезопасности МВД и его территориальных подразделениях.

Кроме того, организуются курсы повышения квалификации, семинары-тренинги и онлайн-тренинги для профессорско-преподавательского состава и слушателей Академии МВД в специализированных вузах зарубежных стран, таких как Турция, Южная Корея, Россия и Беларусь.

Для повышения эффективности обучения проведены дополнительные факультативные занятия по направлениям “Информационные технологии в органах внутренних дел”, “Организация борьбы с киберпреступностью”, “Аппаратно-программные средства борьбы с киберпреступностью”, эффективное использование укрепляются сетевые интернет-возможности курсантов, создание электронных программ и платформ, программные знания и навыки работы с поставками и другими важными отраслями информационно-коммуникационного сектора. Деятельность научного кружка одаренных курсантов в этом направлении налажена при Кафедре информационных технологий. Когда “Группа интернет-мониторинга” в составе членов кружка провела мониторинг сайтов в социальных сетях, была выявлена и разоблачена деятельность ряда интернет-источников, негативно влияющих на нашу национальную духовность.

Автор считает целесообразным реализовать следующие предложения в целях дальнейшего совершенствования принимаемых административно-правовых мер по обеспечению кибербезопасности в нашей стране:

– привлечение квалифицированных специалистов правоохранительных органов зарубежных стран в сфере противодействия киберпреступлениям для обмена опытом [9];

– наделить Центр кибербезопасности МВД и входящих в его состав структур правом контролировать информацию о банках, платежных операторах (“HUMO” и “UzCard”), виртуальных и банковских пластиковых картах, историю совершенных операций через них, а также прекращать (блокировать) финансовые операции в случае совершения преступного деяния;

– введение порядка обязательного ввода идентификационной и аутентификационной информации мобильных телефонов и их пользователей при использовании мобильных и компьютерных приложений банков, платежных организаций и операторов;

– внедрение технических возможностей идентификации IP-адресов в виртуальной частной сети (VPN) в мобильных приложениях для банков и денежных переводов и

ограничение использования приложения через них (из 31 банка и 6 частных мобильных платежных приложений, работающих в нашей стране, только PayMe организовал подобное во второй половине 2021 г. В результате частичного технического запрета на использование (VPN) IP-адресов уровень преступлений, совершаемых через это приложение, резко снизился);

– введение порядка установления сотрудничества с Центром кибербезопасности МВД при разработке проекта требований безопасности цифровой платформы приложений мобильного банкинга и онлайн-счетов.

– в целях повышения эффективности борьбы с преступлениями в сфере информационно-коммуникационных технологий организовать специальный курс по выявлению и расследованию данного вида преступлений в Академии МВД и подготовить квалифицированных специалистов;

– изучение передового опыта зарубежных стран по подготовке кадров в области кибербезопасности и широкое внедрение в национальную практику (например, в Соединенных Штатах Америки, помимо отдельных центров и научно-исследовательских институтов по борьбе с киберугрозами, кадров на уровне бакалавра и магистра в этой области также эффективно созданы. 9 из 15 самых престижных высших учебных заведений в области кибербезопасности работают именно в США [10]).

Автор полагает, что мнения, предложения и рекомендации, высказанные в рамках сегодняшней конференции, послужат практическому решению проблем в данной сфере, разработке современных механизмов кибербезопасности, координации взаимодействия государственных органов, предприятий и организаций в этой сфере. Пользуясь случаем, хочу пожелать вам успехов в работе конференции.

References:

1. https://www.tadviser.ru/index.php
2. https://www.bcg.com/press/14september2021-navigating_rising_cyber_risks_in_transportation_and_logistics
3. https://iiv.uz/ru/news/kiberjinoyatchilikka-qarshi-kiberxavfsizlik
4. https://kun.uz/ru/news/2022/06/17/kolichestvo-kiberprestupleniy-v-uzbekistane-za-posledniye-tri-goda-vyroslo-v-neskolko-raz
5. https://yuz.uz/ru/news/mvd-kolichestvo-kiberprestupleniy-za-poslednie-tri-goda-uvelichilos-v-neskolko-raz
6. https://lex.uz/ru/docs/5960609
7. https://yuz.uz/ru/news/shavkat-mirziyoev-hamma-islohotlarni-hamma-harakatlarni-jamiyat-bilan-birga-qilamiz
8. Qushboqov S., Yetmishboyev M. Jazoni ijro etish muassasalari ishtirokida tuziladigan fuqarolik-huquqiy shartnomalarning mohiyati va ahamiyati //Eurasian Journal of Law, Finance and Applied Sciences. – 2022. – Т. 2. – №. 9. – С. 76-80.
9. Yuldashev D. Characteristics and Legal Regulation of Labor Migration Relations in Uzbekistan in the Conditions of Pandemic // International Journal of Development and Public Policy. – 2022. – Т. 2. – №. 5. – С. 97-99.

10. Смекалова М.В. Эволюция доктринальных подходов США к обеспечению кибербезопасности и защите критической инфраструктуры // Вестник Московского университета. Международные отношения и мировая политика. – 2019. – Т. 25. – №. 1. – С. 47-68.