МРНТИ 81.93.29 https://doi.org/10.26577/JAPJ2024-110-b-06

А.М. Сайтбеков[1], Г.М. Сагинбекова[2], Ж.А. Кегембаева[3], Э.А. Алимова[4*]

[1]МВД Республики Казахстан, Казахстан, г. Астана
[2]Специализированный межрайонный экономический суд г. Алматы, Казахстан, г. Алматы;
[3]Казахский университет международных отношений и мировых языков им. Абылай хана, Казахстан, г. Алматы
[4]Алматинская академия МВД Республики Казахстан им. М. Есбулатова, г. Алматы
*e-mail: elvira.alimova.77@mail.ru

СТРАТЕГИЧЕСКИЙ ВЗГЛЯД НА ЦИФРОВОЕ РАЗВИТИЕ КАЗАХСТАНА: АНАЛИЗ РИСКОВ И КИБЕРУГРОЗ

Статья посвящена комплексному изучению процессов цифровизации в Республике Казахстан с акцентом на выявление и оценку связанных с ними правовых рисков и угроз. В рамках исследования применяется метод форсайт-анализа, позволяющий не только оценить текущее состояние цифровой инфраструктуры страны, но и спрогнозировать перспективные направления ее развития в будущем. Основное внимание в статье уделяется анализу правовых аспектов цифровизации, включая законодательные инициативы, направленные на регулирование цифрового пространства, а также проблемы обеспечения кибербезопасности. Авторы выделяют ключевые риски, связанные с ростом киберпреступности, утечкой данных, нарушением прав на интеллектуальную собственность и другими угрозами, которые могут существенно повлиять на успешность процесса цифровой трансформации в Казахстане. Анализ проблем киберпреступности включает фишинг, мошенничество с использованием информационных технологий, а также угрозы для критически важной для государства цифровой инфраструктуры. В работе предложены стратегии и рекомендации по минимизации выявленных рисков и угроз, в том числе совершенствование законодательства, развитие технологий обеспечения кибербезопасности и повышение информационной грамотности населения. Также обсуждаются возможности сотрудничества на международном уровне в целях обмена опытом и лучшими практиками в области цифрового развития и кибербезопасности. Авторы подчеркивают важность разработки комплексных подходов к управлению цифровым развитием, требующего не только технологических инноваций, но и постоянного совершенствования нормативной правовой базы, а также формирования культуры кибербезопасности среди как пользователей цифровых услуг, так и представителей организаций, предоставляющих эти услуги.

Ключевые слова: цифровое развитие, киберпреступность, инфокоммуникационные технологии (ИКТ), форсайт-анализ, кибербезопасность, правовые риски, стратегии минимизации ущерба.

A.M. Saitbekov[1], G.M. Sagynbekova[2], Zh.A. Kegembayeva[2], E.A. Alimova[3]*

[1]Ministry of Internal Affairs of the Republic of Kazakhstan, Astana
[2]Specialized Interdistrict Economic Court of Almaty, Kazakhstan, Almaty
[2]Abylai Khan Kazakh University of International Relations and World Languages, Almaty
[3]Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after M. Esbulatov, Kazakstan, Almaty
*e-mail: elvira.alimova.77@mail.ru

A strategic view on the digital development of Kazakhstan: risk analysis and cyber threats

The article is devoted to a comprehensive study of the digitalization processes in the Republic of Kazakhstan with an emphasis on identifying and assessing the legal risks and threats associated with them. The research uses the method of foresight analysis, which allows not only to assess the current state of the country's digital infrastructure, but also to predict promising directions for its development in the future. The article focuses on the analysis of the legal aspects of digitalization, including legislative initiatives aimed at regulating the digital space, as well as cybersecurity issues. The authors identify

the key risks associated with the growth of cybercrime, data leakage, violation of intellectual property rights and other threats that can significantly affect the success of the digital transformation process in Kazakhstan. The analysis of cybercrime issues includes phishing, fraud using information technology, as well as threats to the state's critically important digital infrastructure. The paper proposes strategies and recommendations to minimize the identified risks and threats, including improving legislation, developing cybersecurity technologies and improving information literacy of the population. They also discuss opportunities for cooperation at the international level in order to share experiences and best practices in the field of digital development and cybersecurity. The authors emphasize the importance of developing integrated approaches to managing digital development, which requires not only technological innovations, but also continuous improvement of the regulatory framework, as well as the formation of a culture of cybersecurity among both users of digital services and representatives of organizations providing these services.

Key words: digital development, cybercrime, information and communication technologies (ICT), foresight analysis, cybersecurity, legal risks, minimization strategies.

А.М. Сайтбеков[1], Г.М. Сагинбекова[2],
Ж.А. Кегембаева[2], Э.А. Алимова[3*]

[1]Қазақстан Республикасының ІІМ, Қазақстан, Астана қ.
[2]Алматы қ. Мамандандырылған ауданаралық экономикалық соты, Қазақстан, Алматы қ.
[2]Абылай хан ат. Қазақ халықаралық қатынастар
және әлем тілдері университеті, Қазақстан, Алматы қ.
[3]Қазақстан Республикасы ІІМ М. Есболатов ат. Алматы академиясы, Қазақстан, Алматы қ.
*e-mail: elvira.alimova.77@mail.ru

Қазақстанның цифрлық дамуына стратегиялық көзқарас: тәуекелдер мен киберқауіптерді талдау

Мақала құқықтық тәуекелдер мен қатерлерді анықтауға және бағалауға баса назар аудара отырып, Қазақстан Республикасындағы цифрландыру процестерін кешенді зерделеуге арналған. Зерттеу аясында елдің цифрлық инфрақұрылымының ағымдағы жай-күйін бағалап қана қоймай, болашақта оның дамуының перспективалық бағыттарын болжауға мүмкіндік беретін форсайт-талдау әдісі қолданылады. Мақалада цифрлық кеңістікті реттеуге бағытталған заңнамалық бастамаларды, сондай-ақ киберқауіпсіздік мәселелерін қоса алғанда, цифрландырудың құқықтық аспектілерін талдауға ерекше назар аударылады. Авторлар киберқылмыстың өсуіне, деректердің таралуына, зияткерлік меншік құқықтарының бұзылуына және Қазақстандағы цифрлық трансформация процесінің табыстылығына елеулі әсер етуі мүмкін басқа да қауіптерге байланысты негізгі тәуекелдерді бөліп көрсетеді. Киберқылмыс мәселелерін талдау фишингті, ақпараттық технологияларды қолданудағы алаяқтықты, сондай-ақ мемлекет үшін маңызды цифрлық инфрақұрылымға төнетін қауіптерді қамтиды. Жұмыста анықталған тәуекелдер мен қатерлерді азайту, оның ішінде заңнаманы жетілдіру, киберқауіпсіздікті қамтамасыз ету технологияларын дамыту және халықтың ақпараттық сауаттылығын арттыру бойынша стратегиялар мен ұсынымдар ұсынылды. Сондай-ақ цифрлық даму және киберқауіпсіздік саласында тәжірибе және үздік тәжірибелермен алмасу мақсатында халықаралық деңгейдегі ынтымақтастық мүмкіндіктері талқыланады. Авторлар тек технологиялық инновацияларды ғана емес, сонымен қатар нормативтік құқықтық базаны үнемі жетілдіруді, сондай-ақ цифрлық қызметтерді пайдаланушылар мен осы қызметтерді ұсынатын ұйымдардың өкілдері арасында киберқауіпсіздік мәдениетін қалыптастыруды талап ететін цифрлық дамуды басқарудың кешенді тәсілдерін әзірлеудің маңыздылығын атап көрсетеді.

Түйін сөздер: цифрлық даму, киберқылмыс, ақпараттық коммуникациялық технологиялар (АКТ), форсайт-талдау, киберқауіпсіздік, құқықтық тәуекелдер, зардап азайту стратегиялары.

Введение

В эпоху глобализации и быстрого прогресса в области информационно-коммуникационных технологий, цифровизация становится важнейшим фактором, определяющим экономическое развитие и социальный прогресс страны. Республика Казахстан активно движется по пути цифровой трансформации, однако это сопровождается появлением новых рисков и правовых угроз.

На сегодняшний день Казахстаном достигнуты определенные успехи в сфере цифрового развития. По данным ООН, Казахстан занимает 56-е место среди 191 страны по индексу человеческого развития (0,811 из 1) (The 2021/2022

HDR: 299). Базовая цифровая грамотность в стране превышает 87,3%, а индекс информационной инфраструктуры оценивается в 0,75200 из 1 (Концепция цифровой трансформации, 2023). В рейтинге Speedtest Global Index Казахстан находится на 66-м месте по скорости мобильного интернета и на 96-м месте по скорости стационарного широкополосного интернета (Speedtest Global Index, 2023). Можно отметить также, что сформирован рынок специализированных услуг, увеличено количество образовательных грантов в области кибербезопасности, усилен контроль за информационными системами «электронного правительства», повышено осведомление населения о киберугрозах и разработаны первые национальные антивирусные решения (Концепция кибербезопасности «Киберщит Казахстана», 2017).

Однако, анализ ключевых аспектов цифрового развития Республики Казахстан выявляет, что быстрое внедрение информационных технологий, хотя и улучшает качество жизни населения и эффективность государственного управления, одновременно создает новые угрозы информационной безопасности страны. Возрастает актуальность вопросов защиты информационного пространства и конфиденциальности данных граждан от кибератак, фишинга и других видов киберпреступлений. Это подчеркивает необходимость всестороннего изучения проблематики, оценки ее масштабов и разработки действенных способов борьбы с киберугрозами. Современный опыт демонстрирует, что киберпреступления в Казахстане имеют как внутренний, так и международный характер, что затрудняет их предупреждение и раскрытие. Увеличение количества инцидентов, связанных с высокими технологиями, свидетельствует о существующей проблеме, требующей немедленного вмешательства.

В этом контексте особенно важен научный подход к проблеме, который позволяет объективно оценить национальные меры по предотвращению кибератак и снижению уровня киберпреступности в сравнении с международными практиками. Основная цель данного исследования заключается в анализе современного состояния и направлений цифрового развития Республики Казахстан, а также связанных с этим киберпреступлений, выявлении ключевых угроз информационной безопасности и предложении мер для создания эффективной системы противодействия киберугрозам.

Материалы и методы

Исследование основывается на анализе уровня цифровизации в Казахстане и инцидентах в сфере кибербезопасности, подчеркивая актуальность темы для устойчивого развития страны в цифровую эпоху. Рассматривались показатели цифровой трансформации, оцениваемые как государственными органами, так и квазигосударственным сектором, через программы и концепции, такие как: Программа по развитию информационных и коммуникационных технологий в Республике Казахстан на 2010-2014 годы (2010); «Информационный Казахстан – 2020» (2013); «Цифровой Казахстан» (2017); Концепция кибербезопасности («Киберщит Казахстана») (2017); Концепция цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023-2029 годы (2023) и др.

При работе с негосударственными отчетными данными были проанализированы показатели Казахстана в таких мировых рейтингах, как Глобальный индекс конкурентоспособности (Global Competitiveness Index (GCI)), Рейтинг цифровой конкурентоспособности (IMD World Digital Competitiveness Ranking); Индекс скорости мобильного интернета (Speedtest Global Index) и др.

Исследование проводилось с применением различных научных подходов, включая анализ и синтез, исторический, логический методы. Использование исторического метода позволило изучить динамику развития цифрового пространства в Казахстане на протяжении различных периодов, выявляя ключевые этапы и показатели цифровизации. Логический подход обеспечил структурирование информации и выявление взаимосвязей между различными факторами. Методы анализа и синтеза были применены для обработки обширных данных и формирования целостного представления о состоянии кибербезопасности. Форсайт-анализ, как метод прогнозирования и стратегического планирования, использовался для идентифи-

кации потенциальных тенденций и сценариев цифрового развития Казахстана. Этот метод позволил оценить возможные будущие изменения в области цифровизации и кибербезопасности, а также определить стратегические направления для адаптации к предстоящим вызовам.

На основе этих методов были выявлены основные проблемы и перспективы в области кибербезопасности и цифровизации Казахстана, что позволило сформулировать рекомендации для улучшения текущей ситуации.

Обсуждение и результаты

Исследование развития ИКТ в Казахстане, процесс которого отражен в ряде государственных программ и проектов, многие из которых уже полностью или частично реализованы, показывает, что цифровая трансформация заняла достаточно большой промежуток времени, являясь частью более широкой стратегии общегосударственной модернизации. Процесс, который охватывает множество сфер от экономики до образования и государственного управления, подчеркивает значимость и масштабы изменений. За последние годы были реализованы следующие ключевые инициативы: «Информационный Казахстан 2020», «Цифровой Казахстан» и др. Анализ этих программных документов показал, что они направлены не столько на цифровую трансформацию как самоцель, сколько на повышение качества жизни граждан путем развития цифровой экономики, создания инновационной экосистемы, обеспечения цифровой грамотности и внедрения электронного правительства (Государственная программа «Цифровой Казахстан» 2017). Вместе с тем, несомненно, эти программы стали основой для дальнейшего развития инфраструктуры ИКТ: строительства и модернизации широкополосного доступа в интернет, развития электронного правительства, повышения цифровой грамотности населения, стимулирования инноваций, стартапов в кибериндустрии и создания технопарков. Но главным результатом реализации этих проектов стало получение кумулятивного эффекта для развития сфер государственного управления, образования, здравоохранения, экономики и культуры. Как подчеркивают специалисты, объем информации в мире каждые пять лет удваивается, и чем больше информации производится, тем выше ее потребительские свойства. Чем быстрее осваиваются новые знания в реальном секторе экономики, тем выше оказывается жизненный уровень населения, экономический и политический вес страны (Майдырова 2022: 48).

Можно констатировать, что результаты этих программ показали положительный эффект на развитие отраслей экономики. Это подтверждается цифровыми показателями новых разработанных государственных планов и программ: «С 2018 по 2021 годы достигнут общий экономический эффект в размере 1629,196 миллиарда тенге и привлечено 114,8 миллиарда тенге в инновационную экосистему. На данный момент более 99% населения имеют доступ к интернету, более 90% государственных услуг доступны онлайн, и доля крупных и средних предприятий, использующих элементы Индустрии 4.0, составляет 5%. Инфокоммуникационная инфраструктура расширяется, и начато внедрение технологии мобильной связи нового поколения 5G» (Концепция цифровой трансформации, 2023).

На сегодня в стране ведется активная разработка по оптимизации бизнес-процессов, цифровизации государственного управления, нацеленного на создание унифицированной модели «электронного правительства». Особое внимание уделяется сокращению уровня бюрократии в отношениях между государственными организациями. Для повышения эффективности управленческих процессов проводится детальный анализ и постоянный мониторинг с целью выявления и исключения ненужных операций и дублирования функций. Такое изучение состояния ИКТ и систем, задействованных в «электронном правительстве», показало, что существует более 400 различных информационных систем, работающих на разнообразных технологиях, в силу чего возникают сложности при их интеграции из-за неоднородности и несовместимости. Эта проблема является одной из часто встречающихся проблем в мире при внедрении технологий «электронного правительства». Исследователи выделяют среди основных неудач, связанных с работой над такими проектами, отсутствие согласованности при применении ИКТ

между различными государственными органами и структурами, что приводит к нелогичному и иррациональному характеру принимаемых решений (Gorelova 2019).

В Казахстане решением данной проблематики стало принятие стандарта унифицированной структуры «электронного правительства», позволившего установить четкие связи между различными компонентами системы и учесть потребности разнообразных государственных организаций. Государство взяло на себя инициативу и обязательства по построению стандартизированной архитектуры цифровых платформ, единых баз данных, без которых было бы невозможно дальнейшее развитие киберуслуг и киберэкономики. Был разработан и принят ряд нормативных правовых актов, установивших правила интеграции шлюза «электронного правительства», платежного шлюза «электронного правительства», правил учета сведений об объектах информатизации «электронного правительства», объектов информационно-коммуникационной инфраструктуры «электронного правительства» и т.п. (ИПС «Адилет», 2023).

В Казахстане цифровая трансформация не ограничивается сервисами и платформами «электронного правительства». Быстрыми темпами идет внедрение высоких технологий не только в сферу государственного управления, интеллектуальные сферы экономики, но и в сферу материального производства. В частности, для материальных производств цифровая платформа может представлять собой оцифрованную систему базовых технологических процессов и дополнительных сервисных модулей, которые позволяют компаниям – поставщикам комплектующих элементов изделия воспользоваться этими модулями и в виртуальном режиме и доработать свои продукты до нужного поставщику качества (Притворова 2020: 2735).

Цифровизация активно проникает во все сферы, даже изначально казавшиеся далекими от применения высоких ИКТ. Ключевую роль в этих процессах играет государство, которое, через формулирование политики, выделение бюджетов и поддержку инноваций, способствует активному внедрению и распространению ИКТ. Государственная поддержка инициатив в сфере высоких технологий, таких как создание технопарков, инкубаторов стартапов и центров разработки, стимулирует развитие частного сектора и привлечение иностранных инвестиций.

В таких условиях повсеместной цифровизации роль права состоит в обеспечении должного уровня правового регулирования объективно происходящих процессов в обществе с целью сохранения общественного порядка и общественной безопасности. При регулировании новых для социума процессов и явлений неизбежно возникают определенные правовые риски, заключающиеся в некачественном нормативном обеспечении, не только не соответствующем реалиям, но и препятствующем дальнейшему прогрессивному развитию. Само понятие риска встречается и широко распространено в самых различных сферах человеческой деятельности, отражая возможность выбора поведения в зависимости от предполагаемых последствий действия или бездействия.

В теории права риск рассматривается в аспекте легального признания и допущения, установления средств предупреждения и минимизации негативных последствий, определения мер ответственности и компенсаторных средств (Тихомиров 2014: 12).

Правовые риски обладают целым рядом внутренне свойственных им черт, на которых учёные акцентируют особое внимание:

- неопределённость (существует лишь вероятность, а не предопределенность наступления тех или иных событий и ситуаций, которые изменчивы и не известны заранее);

- возможность убытков (возможен неожиданно негативный исход событий);

- оцениваемость (при ситуациях риска субъект имеет способности к анализу и возможности к предположению о неблагоприятном ходе событий);

- временная привязка (риск представляет собой вероятность возникновения ущерба в будущем);

- значимость (в случае отрицательного исхода может быть причинен существенный вред) (Павлов В., 2019: 276).

В специальной литературе сегодня можно наблюдать актуализацию темы правовых рисков, исследуемых через призму самых различных явлений правовой действительности. При

этом риски описываются в таких аспектах, как: возможность появления опасности; возможность понести потери; возможность причинения убытков и т.п. (Масловская 2013: 17).

В общем, правовые риски воспринимаются как потенциально неблагоприятные итоги запланированных или уже выполненных действий в сфере правотворчества. Имеются риски как недостаточного, так и чрезмерного правового регулирования.

В эпоху цифровизации исследование правовых рисков критично необходимо для понимания потенциальных последствий и уровня угроз, связанных с внедрением цифровых технологий, а также для своевременного создания стратегий и механизмов для их нейтрализации.

Оценка цифровых технологий должна основываться на правовой модели, учитывающей правовую природу отношений и способной сбалансировать частные и публичные интересы в цифровом обращении (Sidorenko 2020: 32). Только с учетом баланса личных, общественных и государственных интересов возможна эффективная корреляция происходящих многообразных процессов цифровизации.

Кроме того, быстрое цифровое развитие Казахстана актуализирует проблему противодействия киберпреступности, методы которой совершенствуются с каждым днем, с использованием самых инновационных технологий и способов.

Анализируя уголовно-правовой аспект преступлений, совершаемых в киберпространстве, следует отметить, что понятие уголовного правонарушения в сфере информатизации и связи и уголовного правонарушения, совершенного с помощью инфокоммуникационных технологий, не являются идентичными (Dumchikov 2022: 292). Предусмотренные в главе 7 Уголовного кодекса Республики Казахстан уголовные правонарушения в сфере информатизации, компьютерной информации являются лишь частью более широкого круга уголовных правонарушений, совершаемых с помощью ИКТ (Уголовный кодекс РК, 2014).

С увеличением числа подключенных устройств и объемов цифровых данных, киберпреступники находят всё новые способы для осуществления своих противоправных действий. Вот несколько ключевых аспектов, которые часто рассматриваются при анализе киберпреступности (Aslan 2023: 1-42):

- методы и техники киберпреступников: сюда входит использование вредоносного программного обеспечения (включая вирусные программы), фишинговых атак, атак на веб-приложения, DDoS-атак (распределённые отказы в обслуживании) и инсайдерских угроз (Al-Khater 2020);

- цели киберпреступников, которые могут включать в себя кражу данных (личных или корпоративных), финансовое мошенничество, шпионаж (коммерческий или государственный), вандализм, распространение запрещенного контента и дестабилизацию критически важных систем и др.;

- уязвимость общества и инфраструктуры: повсеместная зависимость от цифровых технологий, растущая с появлением все новых и новых цифровых платформ и расширения цифровых услуг, делает частных лиц, организации и государственные органы уязвимыми перед лицом киберпреступников (Conteh 2016);

- нормативное правовое регулирование: во многих странах законодательство в области кибербезопасности развивается, чтобы идти в ногу с новыми методами киберпреступности, но даже при этом возникает определенная временная разница между появлением новых угроз и внедрением соответствующих законодательных мер;

- международное сотрудничество: киберпреступность относится к трансграничному виду преступности, она не знает границ, охватывая самые различные государства, в силу чего требует усиленной международной кооперации для эффективного противодействия;

- инновации в кибербезопасности: разработка новых технологических решений для обеспечения защиты данных и информационных систем – это постоянная «гонка вооружений» между киберпреступниками и специалистами по безопасности (Hypponen 2012);

- профилактика и обучение: повышение осведомлённости и обучение пользователей и специалистов в области кибербезопасности играют ключевую роль в профилактике киберпреступлений.

В Казахстане активно реализуются меры по противодействию киберпреступности. К сожалению, пока не приходится говорить о полном поражении преступников. Так, только за первые

два месяца 2024 года было зафиксировано 3645 случаев интернет-мошенничества, причинивших гражданам убытки на сумму свыше 4 миллиардов тенге. Наиболее частым методом мошенничества является интернет-торговля, когда объявления размещаются на популярных торговых платформах, а также в социальных сетях и мессенджерах. Мошенники обычно предлагают товары или услуги по заниженным ценам и требуют предоплату или полную оплату (https://forbes.kz/news). Помимо кибермошенничества не менее значимой угрозой по Казахстану является подмена номеров. Современные технологии (особенно связанные с VoIP) позволяют абонентам передавать ложный идентификатор и представлять ложные имена и номера, которые используются в недобросовестных целях (Skopik 2020). Обзор материалов практической деятельности правоохранительных органов свидетельствует о постоянном совершенствовании преступных методов и технологий в арсенале киберпреступников. Такое появление все новых преступных технологий предопределяет необходимость в подготовке кадров, обладающих необходимыми профессиональными навыками для эффективного противодействия киберпреступности. С учетом этого МВД Республики Казахстан делает акцент на подготовку IT-специалистов. Сегодня в Алматинской академии МВД Республики Казахстан имени М. Есбулатова реализуется целый ряд образовательных программ высшего, послевузовского и дополнительного образования, нацеленных на формирование необходимых компетенций в области информационной безопасности, противодействия киберпреступности (Almaty police academy, 2024). Особое внимание уделяется практикоориентированному подходу, это предполагает не только освоение теоретических положений, но и активное внедрение симуляционных тренингов, использование киберполигона, кейсов с реальными ситуациями, что позволяет обучающимся накапливать необходимый практический опыт уже в процессе обучения.

Заключение, выводы

Исследование подтвердило, что без активного вовлечения государства, бизнеса и гражданского общества в процесс создания надёжной системы защиты информационного пространства, достижение устойчивого цифрового развития будет затруднительным. Только скоординированные действия всех заинтересованных сторон позволят снизить риски и последствия киберпреступлений, обеспечив при этом дальнейшее прогрессивное развитие цифровой инфраструктуры в Казахстане. Необходимо признать определяющую роль государства в процессах цифровой трансформации в Казахстане, выступающего не только как регулятор и координатор различных инициатив, но и как ключевой инвестор в инфраструктуру и образование. Политическая воля и стратегическое планирование на высшем уровне обеспечивают необходимый импульс для интеграции высоких технологий во все сферы жизни общества, что приводит к созданию устойчивой основы для долгосрочного экономического роста и повышения благосостояния.

Цифровое развитие Казахстана неизбежно сопряжено с появлением новых правовых рисков и угроз, основным из которых можно признать киберпреступность.

Успешное противодействие возникающим правовым киберрискам и киберпреступности требует ряда скоординированных шагов. Базовыми из них являются обновление образовательных программ по подготовке квалифицированных ИТ-специалистов и повышению уровня цифровой грамотности среди населения, а также проведение тематических научных исследований, без которых невозможно адекватное понимание текущего состояния и проблематики цифровизации и кибербезопасности в Казахстане.

Акцент должен был сделать на предпринимаемых на национальном уровне мерах для предотвращения кибератак и сокращения уровня киберпреступности. Такие меры должны охватывать работу по совершенствованию законодательной базы, улучшению методов обнаружения и реагирования на киберугрозы, а также формированию культуры кибербезопасности среди граждан. Комплексный подход к решению вопросов кибербезопасности должен включать в себя как технологические инновации, так и социально-образовательные меры.

Литература

The 2021/2022 Human Development Report: By the United Nations Development Programme. New York, 2022. – 308 p. https://hdr.undp.org/system/files/documents/global-report-document/hdr2021-22pdf_1.pdf..

Постановление Правительства Республики Казахстан от 28 марта 2023 года № 269 «Об утверждении Концепции цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023 – 2029 годы» // https://adilet.zan.kz/rus/docs/P2300000269.

Speedtest Global Index, 2023 // https://www.speedtest.net/global-index.

Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407 "Об утверждении Концепции кибербезопасности ("Киберщит Казахстана")" // https://adilet.zan.kz/rus/docs/P1700000407.

Постановление Правительства Республики Казахстан от 12 декабря 2017 года № 827 Об утверждении Государственной программы "Цифровой Казахстан" (утратило силу) // https://adilet.zan.kz/rus/docs/P1700000827.

Майдырова А.Б. Информационное общество: вопросы становления в Республике Казахстан // Обеспечение качества образования. – 2022. – № 1 (26). – С. 41-49.

Gorelova J. E-government in Russia: Practices and Developments // Journal of society and the state. – 2019. – No. 2(5) (in Eng.) https://sgpjournal.mgimo.ru/2019/2019-5/russian-egovernment.

Притворова Т.П., Абзалбек Е.Ж., Кизимбаева А. IT-услуги в Казахстане: динамика и возможности цифровизации промышленности // Экономика, предпринимательство и право. – 2020. – Том 10. – № 11. – С. 2727-2744.

Тихомиров Ю. Прогнозы и риски в правовой сфере // Журнал российского права. – 2014. – №3 (207). – С. 5-16.

Павлов В.И., Савенок А.Л. Риск в праве как теоретико-правовой и антрополого-правовой феномен (на примере уголовно-правового понятия риска) // Юридическая техника. – 2019. – № 13. – С. 275-282.

Масловская Т.С. Риски в конституционном праве: теоретико–правовой взгляд // Право. – 2013. – № 6. – С.17-22.

Sidorenko E., Arx P. Transformation of law in the context of digitalization: Defining the correct priorities // Digital Law Journal. – 2020. – No. 1. – Pp. 24-38 (in Eng.). https://doi.org/10.38044/DLJ-2020-1-1-24-38.

Dumchikov M., Fomenko A., Yunin, O. et al. The essence and classification of cybercrime in the field of computer information // Amazonia Investiga. – 2022. – No.11(51). – Pp. 291-299.

Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V // https://adilet.zan.kz/rus/docs/K1400000226.

Aslan Ö., Serkant S., Ozkan-Okay M. et al. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions (in Eng.) // Electronics/ – 2023. – No. 12(6). – Pp. 1-42. https://doi.org/10.3390/electronics12061333.

Al-Khater W., Al-Ma'adeed S., Ali Ahmed A. et al. Comprehensive Review of Cybercrime: Detection Techniques // IEEE Access, 2020. doi 10.1109/ACCESS.2020.3011259.

Conteh N., Schmick P. Cyber security: risks, vulnerabilities and countermeasures to prevent social engineering attacks // International Journal of Advanced Computer Research, 2016. – No. 6(23). – Pp. 31-38. doi:10.19101/IJACR.2016.623006.

Hypponen M. The cyber arms race // Info & Claims CCS '13: Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. November, 2013.Pp. 941–942. https://doi.org/10.1145/2508859.2516756.

В Казахстане с начала года зарегистрировали более 3 тысяч фактов интернет-мошенничества. 2024 // https://forbes.kz/news.

Skopik F., Pahi T. Under false flag: using technical artifacts for cyber attack attribution // Cybersecurity. – 2020. – No. 3. https://doi.org/10.1186/s42400-020-00048-4.

Almaty police Academy: website // https://alpolac.edu.kz.

References

Al-Khater W., Al-Ma'adeed S., Ali Ahmed A. et al. Comprehensive Review of Cybercrime: Detection Techniques // IEEE Access, 2020. doi 10.1109/ACCESS.2020.3011259.

Almaty police Academy: website // https://alpolac.edu.kz.

Aslan Ö., Serkant S., Ozkan-Okay M. et al. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions (in Eng.) // Electronics/ – 2023. – No. 12(6). – Pp. 1-42. https://doi.org/10.3390/electronics12061333.

Conteh N., Schmick P. Cyber security: risks, vulnerabilities and countermeasures to prevent social engineering attacks // International Journal of Advanced Computer Research, 2016. – No. 6(23). – Pp. 31-38. doi:10.19101/IJACR.2016.623006.

Dumchikov M., Fomenko A., Yunin, O. et al. The essence and classification of cybercrime in the field of computer information // Amazonia Investiga. – 2022. – No.11(51). – Rr. 291-299.

Hypponen M. The cyber arms race // Info & Claims CCS '13: Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security. November, 2013.Pp. 941–942. https://doi.org/10.1145/2508859.2516756.

Gorelova J. E-government in Russia: Practices and Developments // Journal of society and the state. – 2019. – No. 2(5) (in Eng.) https://sgpjournal.mgimo.ru/2019/2019-5/russian-egovernment.

Maslovskaya T.S. Riski v konstitutsionnom prave: teoretiko–pravovoy vzglyad [Risks in constitutional law: theoretical and legal view] // Pravo. – 2013. – № 6. – S.17-22.

Maydyrova A.B. Informatsionnoye obshchestvo: voprosy stanovleniya v Respublike Kazakhstan // Obespecheniye kachestva obrazovaniya [Information society: issues of formation in the Republic of Kazakhstan // Ensuring the quality of education]. – 2022. – № 1 (26). – S. 41-49.

Pavlov V.I., Savenok A.L. Risk v prave kak teoretiko-pravovoy i antropologo-pravovoy fenomen (na primere ugolovno-pravovogo ponyatiya riska) [Risk in law as a theoretical-legal and anthropological-legal phenomenon (using the example of the criminal legal concept of risk)]// Yuridicheskaya tekhnika. – 2019. – № 13. – S. 275-282.

Pritvorova T.P., Abzalbek Ye.ZH., Kizimbayeva A. IT-uslugi v Kazakhstane: dinamika i vozmozhnosti tsifrovizatsii promyshlennosti // Ekonomika, predprinimatel'stvo i parvo [IT services in Kazakhstan: dynamics and opportunities for digitalization of industry // Economics, entrepreneurship and law]. – 2020. – Tom 10. – № 11. – S. 2727-2744.

Postanovleniye Pravitel'stva Respubliki Kazakhstan ot 30 iyunya 2017 goda № 407 "Ob utverzhdenii Kontseptsii kiberbezopasnosti ("Kibershchit Kazakhstana")" [Decree of the Government of the Republic of Kazakhstan dated June 30, 2017 No. 407 "On approval of the Cyber Security Concept ("Cyber Shield of Kazakhstan")"]// https://adilet.zan.kz/rus/docs/P1700000407.

Postanovleniye Pravitel'stva Respubliki Kazakhstan ot 28 marta 2023 goda № 269 "Ob utverzhdenii Kontseptsii tsifrovoy transformatsii, razvitiya otrasli informatsionno-kommunikatsionnykh tekhnologiy i kiberbezopasnosti na 2023 – 2029 gody" // https://adilet.zan.kz/rus/docs/P2300000269.

Postanovleniye Pravitel'stva Respubliki Kazakhstan ot 12 dekabrya 2017 goda № 827 Ob utverzhdenii Gosudarstvennoy programmy "Tsifrovoy Kazakhstan" (utratilo silu) [Decree of the Government of the Republic of Kazakhstan dated December 12, 2017 No. 827 On approval of the State Program "Digital Kazakhstan" (lost force] // https://adilet.zan.kz/rus/docs/P1700000827.

Speedtest Global Index, 2023 // https://www.speedtest.net/global-index.

Sidorenko E., Arx P. Transformation of law in the context of digitalization: Defining the correct priorities // Digital Law Journal. – 2020. – No. 1. – Rr. 24-38 (in Eng.). https://doi.org/10.38044/DLJ-2020-1-1-24-38.

Skopik F., Pahi T. Under false flag: using technical artifacts for cyber attack attribution // Cybersecurity. – 2020. – No. 3. [Since the beginning of the year, more than 3 thousand cases of Internet fraud have been registered in Kazakhstan. 2024] https://doi.org/10.1186/s42400-020-00048-4.

The 2021/2022 Human Development Report: By the United Nations Development Programme. New York, 2022. – 308 p. https://hdr.undp.org/system/files/documents/global-report-document/hdr2021-22pdf_1.pdf.

Tikhomirov YU. Prognozy i riski v pravovoy sfere // Zhurnal rossiyskogo prava [Forecasts and risks in the legal sphere // Journal of Russian Law]. – 2014. – №3 (207). – S. 5-16.

Ugolovnyy kodeks Respubliki Kazakhstan ot 3 iyulya 2014 goda № 226-V [Criminal Code of the Republic of Kazakhstan dated July 3, 2014 No. 226-V] // https://adilet.zan.kz/rus/docs/K1400000226.

V Kazakhstane s nachala goda zaregistrirovali boleye 3 tysyach faktov internet-moshennichestva. 2024 // https://forbes.kz/news.

Сведения об авторах:

Сайтбеков Айдар Муталикович - заместитель министра внутренних дел Республики Казахстан, доктор политических наук, кандидат юридических наук, профессор, генерал-майор полиции (Казахстан, г. Астана, e-mail: kense@mvd.gov.kz)

Сагынбекова Гульнар Мейрхановна – доктор юридических наук, судья специализированного межрайонного экономического суда г. Алматы (Казахстан, Алматы, e-mail: gulnar.s007@mail.ru)

Кегембаева Жанар Аманжановна - профессор кафедры международного права Казахского университета международных отношений и мировых языков имени Абылай хана, доктор юридических наук, профессор (Казахстан, Алматы, e-mail: Kegembaeva@mail.ru)

Алимова Эльвира Абдикапбаровна - ученый секретарь Ученого совета Алматинской академии МВД Республики Казахстан имени М. Есбулатова, доктор PhD, ассоциированный профессор (доцент), полковник полиции (Казахстан, Алматы, e-mail: e-mail: elvira.alimova.77@mail.ru)

Information about authors:

Saitbekov Aidar Mutalikovich - Deputy Minister of Internal Affairs of the Republic of Kazakhstan, Doctor of Political Sciences, Candidate of Law, Professor, Major General of the police (Kazakhstan, Astana c., e-mail: kense@mvd.gov.kz)

Gulnar Sagynbekova – Doctor of Law, judge of the specialized Interdistrict Economic Court of Almaty (Kazakhstan, Almaty c., e-mail: gulnar.s007@mail.ru)

Kegembayeva Zhanar Amanzhanovna – Professor of the Department of International Law of the Kazakh University of International Relations and World Languages named after Abylai Khan; Doctor of Law, Professor; (Kazakhstan, Almaty c., e-mail: Kegembaeva@mail.ru)

Alimova Elvira Abdikapbarovna –Academic Secretary of the Academic Council of the Almaty Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after M. Esbulatov; PhD, Associate Professor, Police Colonel (Kazakhstan, Almaty, e-mail: elvira.alimova.77@mail.ru)

Зарегестрирована: 20 апреля 2024 г.
Принята: 20 июня 2024 г.