15. The Nilson Report. [Online]. – URL: https://nilsonreport.com/mention/1313/1link/

16. X. Hou, K. Wang, C. Zhong, and Z. Wei, “ST-Trader: A Spatial-Temporal Deep Neural Network for Modeling Stock Market Movement,” IEEE/CAA Journal of Automatica Sinica, vol. 8, no. 5, pp. 1015–1024, 2021.

17. Dou Y., Liu Z., Sun L., Deng Y., Peng H., Yu P. S. Enhancing graph neural network-based fraud detectors against camouflaged fraudsters // Proceedings of the 29th ACM International Conference on Information & Knowledge Management, 2020. – Pp. 315–324.

18. Yue Tian, Guanjun Liu, Jiacun Wang, Mengchu Zhou Transaction Fraud Detection via an Adaptive Graph Neural Network // JOURNAL OF LATEX CLASS FILES, VOL. 14, NO. 8, AUGUST 2021. Pp. 1–10

Т. Э. Кылчыкбаев,
кандидат юридических наук, доцент,
Кыргызский национальный университет
имени Ж. Баласагына

ПОНЯТИЕ КИБЕРБЕЗОПАСНОСТИ В КЫРГЫЗСКОЙ РЕСПУБЛИКЕ

Аннотация. В современном цифровом мире понятие кибер-угрозы все больше проникает в нашу жизнь. Кибербезопасность становится важной проблемой для всех, от отдельных лиц до мировых компаний, корпораций и стран. В данной статье на основе анализа законодательных инициатив и практических мер органов исполнительной власти в сфере информационной безопасности Кыргызской Республики рассматриваются возможности государства по противодействию современным кибер-угрозам и формированию культуры личной информационной безопасности.

Ключевые слова: информационные технологии, кибербезопасность, цифровая информация, защита личных данных, законодательное регулирование

THE CONCEPT OF CYBERSECURITY IN THE KYRGYZ REPUBLIC

Abstract. In today's digital world, the concept of a cyber threat is increasingly penetrating our lives. Cybersecurity is becoming an important issue for everyone, from individuals to global companies, corporations and countries. This article, based on an analysis of legislative initiatives and practical measures of executive authorities in the field of information security of the Kyrgyz Republic, examines the state’s capabilities to counter modern cyber threats and create a culture of personal information security.

Key words: information technology, cybersecurity, digital information, personal data protection, legislative regulation

Введение. Цифровая революция, которая началась в конце XX века, продолжает стремительно развиваться, оказывая глубокое влияние на все сферы жизни современного общества. По данным Международного союза электросвязи

(ITU), к концу 2019 года более половины населения земного шара, а именно 53,6% или 4,1 миллиарда человек, имели доступ к интернету. Примечательно, что основная часть пользователей интернет-сети проживает в развивающихся странах, где число пользователей интернет-сети составляет 3,02 миллиарда человек. Однако, несмотря на очевидные преимущества, которые приносит цифровая революция, она порождает и целый комплекс угроз и вызовов, затрагивающих безопасность как отдельных граждан, так и целых государств [1].

Основная часть. Среди наиболее актуальных проблем можно выделить:

1. *Киберпреступность*: распространение вирусов, хакерских атак, кража личных данных, фишинговые схемы и другие виды киберпреступности становятся все более изощренными и опасными.

2. *Дезинформация и пропаганда*: распространение ложной информации в сети Интернет, а также использование социальных сетей для манипулирования общественным мнением представляет серьезную угрозу для демократических ценностей и стабильности общества.

3. *Проблемы конфиденциальности:* цифровые технологии позволяют собирать и хранить огромное количество личных данных, что ставит под вопрос конфиденциальность частной жизни и создает предпосылки для злоупотреблений.

4. *Неравенство доступа*: неравномерное распространение цифровых технологий и отсутствие доступа к качественному интернету в некоторых регионах страны усугубляет существующее социальное неравенство и препятствует развитию.

5. *Риски для национальной безопасности*: киберугрозы могут нанести серьезный ущерб инфраструктуре государства, экономике и обороноспособности, создавая предпосылки для дестабилизации и конфликтов. В связи с этим возрастает важность комплексной и скоординированной политики государства, направленной на минимизацию рисков и обеспечение безопасной цифровой среды для своих граждан. В этом контексте ключевую роль играет разработка и реализация национальных киберстратегий, которые должны включать в себя:

Законодательное регулирование: установление правовых норм, регулирующих деятельность в киберпространстве, борьбу с киберпреступностью, защиту личных данных и информационной безопасности.

Развитие кибербезопасности: создание сильных систем кибербезопасности, повышение уровня осведомленности населения о киберугрозах, развитие информационной инфраструктуры, создание специализированных подразделений по кибербезопасности в правоохранительных органах.

Международное сотрудничество: координация действий с другими странами в борьбе с киберпреступностью, обмен информацией и технологиями, создание международных механизмов реагирования на киберугрозы.

Развитие цифровой культуры: пропаганда цифровых компетенций, формирование у населения критического мышления и способности различать достоверную информацию от фейковых новостей.

Кыргызстан, как многие другие страны, сталкивается с вызовами цифровой революции, и в последние годы вопрос обеспечения кибербезопасности страны активно обсуждается в политических кругах и на академических пло-

щадках. Президент Кыргызстана Садыр Жапаров на церемонии открытия здания координационного центра по обеспечению кибербезопасности Государственного комитета национальной безопасности заявил: «Можно сказать, что это новое направление в общей системе обеспечения национальной безопасности страны в настоящее время находится на стадии становления. Учитывая, что в последнее время наблюдаются хакерские атаки на государственные и другие информационные системы, есть необходимость как можно скорее поднять и развить это направление до качественного уровня» [2]. Данное заявление свидетельствует о том, что сфера ИКТ в Кыргызстане стала приоритетным направлением развития страны, и показывает, насколько серьезно правительство относится к цифровизации и сопутствующим ей проблемам.

Однако Кыргызстан имеет относительно низкие показатели в Глобальном индексе кибербезопасности, который разработан Международным союзом электросвязи ООН [3]. Индекс ориентирован на выявление рисков в развитии цифровой среды, формулирование рекомендаций по укреплению киберзащиты государств и формирование глобальной цифровой культуры. Кыргызстан находится на низких позициях в индексе, что подчеркивает необходимость усиления мер по обеспечению кибербезопасности, поэтому было принято «правовые основы единой системы кибербезопасности, целью которой является защита личности, общества и государства путем обеспечения цифровой устойчивости информационной инфраструктуры КР» [4]. Несмотря на эти шаги, страна нуждается в дальнейшей разработке и реализации национальной киберстратегии, которая должна учитывать уникальные особенности Кыргызстана и опираться на лучшие практики других стран. В рамках этой стратегии необходимо осуществить ряд важных шагов:

– Укрепление законодательной базы: принятие новых законов и изменение существующих для обеспечения эффективной борьбы с киберпреступностью, защиты личных данных и информационной безопасности.

– Развитие системы кибербезопасности: создание централизованных систем мониторинга киберугроз, внедрение современных технологий киберзащиты, подготовка специалистов в области кибербезопасности.

– Повышение осведомленности населения: проведение программ по киберграмотности, просвещение граждан о киберугрозах, обучение безопасным практикам в интернете.

– Развитие международного сотрудничества: участие в международных программах по кибербезопасности, обмен опытом с другими странами, создание межведомственных структур для координации действий по кибербезопасности.

– Поддержка развития цифровой экономики: создание благоприятных условий для развития цифровых технологий и инноваций, стимулирование цифрового предпринимательства.

Заключение. Реализация этих шагов поможет Кыргызстану сделать шаг вперед в обеспечении цифровой безопасности и создании благоприятных условий для развития цифровой экономики. Важно понимать, что кибербезопасность – это не только техническая задача, но и вопрос общественной ответственности. Каждый пользователь интернета должен быть осведомлен о киберугрозах

и принимать меры для защиты своей личной информации. Цифровая революция создает огромные возможности для развития Киргизстана, но вместе с тем она несет в себе и определенные риски. Правильное понимание этих рисков разработка эффективных стратегий для их минимизации являются ключевыми факторами для успешной цифровизации страны.

Список литературы

1. 2,9 млрд. человек все еще лишены подключения. [Электронный ресурс]. – URL: https://www.itu.int/ru/mediacentre/Pages/PR-2021-11-29-FactsFigures.aspx

2. Президент Киргизии дал поручение усилить кибербезопасность государства // ТАСС [Электронный ресурс]. – URL: https://tass.ru/mezhdunarodnaya-panorama/17739891

3. Основные показатели измерения уровня развития цифровой инфраструктуры Кыргызской Республики [Электронный ресурс]. – URL: https://internetpolicy.kg/wp-content/uploads/2022/11/%D0%9F%D0%BE%D0%BA%D0%B0%D0%B7%D0%B0%D1%82%D0%B5%D0%BB%D0%B8-%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%BE%D0%B8%CC%86-2.pdf

4. Закон Кыргызской Республики «О кибербезопасности Кыргызской Республики» принятым Жогорку Кенешем КР от 12-июня 2024 г. // Сайт Министерства юстиции Кыргызской Республики [Электронный ресурс]. – URL: https://cbd.minjust.gov.kg/4-5260/edition/1939/ru

Н. И. Легостаева,
кандидат социологических наук,
Санкт-Петербургский государственный университет
О. В. Медяник,
кандидат психологических наук, доцент,
Санкт-Петербургский государственный университет

ДУАЛЬНЫЙ СИМБИОЗ ЦИФРОВЫХ ФИНАНСОВЫХ ТЕХНОЛОГИЙ И КИБЕРМОШЕННИЧЕСТВА

Аннотация. Быстрая цифровая трансформация экономического сектора способствует развитию новых бизнес-моделей и улучшению прозрачности финансовых операций. При этом она открывает двери для кибермошенников, что подчеркивает необходимость комплексного подхода к изучению цифровых финансовых технологий и киберрисков. Взаимодействие традиционных финансовых услуг с инновационными финансовыми технологиями одновременно создает новые возможности и риски, поэтому компании должны соблюдать осторожность в использовании инновационных решений, чтобы избежать уязвимости перед киберугрозами. В статье акцентируются внимание на важности разработки единого правового подхода к определению понятия «кибермошенничество». Это