УДК: 343.9(575.2):004.056.5
DOI 10.58649/1694-9099-2026-1-420-423

Евграфова Л.Ю., Колесникова Е.Н., Алиева А.Н., Анапияева Ч.Д., Жылкыбаева А.Б.
КУУнун Каракол шаарындагы гуманитардык - табигый илимдер факультети
Евграфова Л.Ю., Колесникова Е.Н., Алиева А.Н., Анапияева Ч.Д, Жылкыбаева А.Б.
Гуманитарно-естественнонаучный факультет КНУ имени Ж. Баласагына г. Каракол
Evgrafova L.Yu., Kolesnikova E.N., Alieva A.N., Anapiyaeva Ch.D., Zhylkybaeva A.B.
Faculty of humanities and natural sciences, KNU named after Jusup Balasagyn. Karakol

КЫРГЫЗСТАНДА МААЛЫМАТТЫК КООПСУЗДУК ЧӨЙРӨСҮНДӨГҮ МЫЙЗАМДАРДЫН АБАЛЫ ЖАНА ӨНҮГҮҮ КЕЛЕЧЕГИ
СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КЫРГЫЗСТАНЕ
THE STATE AND PROSPECTS OF DEVELOPMENT OF LEGISLATION IN THE FIELD OF INFORMATION SECURITY IN KYRGYZSTAN

Кыскача мүнөздөмө: Бул макалада Кыргыз Республикасындагы маалымат коопсуздугу боюнча мыйзамдардын учурдагы абалы жана өнүгүү келечеги каралат. Анда маалыматты коргоону жөнгө салуучу негизги укуктук актылар, анын ичинде маалыматты коргоо, улуттук коопсуздук, киберкоопсуздук жана жеке маалыматтарды коргоо боюнча мыйзамдар талданат. Анда колдонуудагы мыйзамдардын жаңылануу зарылчылыгы, комплекстүү мамиленин жоктугу, квалификациялуу адистердин жетишсиздиги сыяктуу негизги маселелер баса белгиленген. Макалада ошондой эле ченемдик укуктук актыларды жаңылоо, мамлекеттик органдардын ортосундагы координацияны жогорулатуу, маалыматтык коопсуздук боюнча билим берүү программаларын иштеп чыгууну камтыган укуктук жөнгө салууну өркүндөтүү жолдору сунушталат. Анда киберкоопсуздукка мамлекеттик көзөмөлдүн жана мониторингдин эффективдүү системасын түзүүнүн, ошондой эле мамлекеттик жана жеке сектордун ортосундагы кызматташтыкты стимулдаштыруунун маанилүүлүгү баса белгиленет. Мындан тышкары, санариптик сабаттуулуктун ролу жана мамлекеттик электрондук кызматтарга калктын ишенимин жогорулатуу каралат. Мыйзамдык базаны өнүктүрүү улуттук кибермейкиндиктин туруктуулугун жана өлкөнүн маалыматтык көз карандысыздыгын жогорулатууну камсыз кылган заманбап маалыматтык коопсуздук технологияларын киргизүү менен коштолушу керек.

Аннотация: В статье рассматривается состояние и перспективы развития законодательства в области информационной безопасности в Кыргызской Республике. Анализируются ключевые нормативно-правовые акты, регулирующие защиту информации, включая законы о защите информации, национальной безопасности, кибербезопасности и защите персональных данных. Выделяются основные проблемы существующего законодательства, такие как необходимость его актуализации, отсутствие комплексного подхода и дефицит квалифицированных специалистов. В статье также предлагаются пути улучшения правового регулирования, включая обновление нормативных актов, повышение координации между государственными органами и развитие образовательных программ в сфере информационной безопасности. Подчеркивается важность формирования эффективной системы государственного контроля и мониторинга в области кибербезопасности, а также стимулирования сотрудничества между государственным и частным секторами. Кроме того, рассматривается роль цифровой грамотности населения и повышения уровня доверия граждан к электронным сервисам государства. Развитие правовой базы должно сопровождаться внедрением современных технологий защиты информации, что позволит обеспечить устойчивость национального киберпространства и повысить уровень информационной независимости страны.

Abstract: This article examines the current state and development prospects of information security legislation in the Kyrgyz Republic. It analyzes key legal acts governing information protection, including laws on information protection, national security, cybersecurity, and personal data protection. It highlights key issues with existing legislation, such as the need for updating, the lack of a comprehensive approach, and a shortage of qualified specialists. The article also suggests ways to improve legal regulation, including

updating regulations, increasing coordination between government agencies, and developing educational programs in information security. It emphasizes the importance of establishing an effective system of government oversight and monitoring in cybersecurity, as well as stimulating cooperation between the public and private sectors. Furthermore, the role of digital literacy and increasing public trust in government electronic services is considered. The development of the legal framework should be accompanied by the introduction of modern information security technologies, which will ensure the stability of national cyberspace and increase the country's information independence.

Негизги сөздөр: маалыматтык коопсуздук; кибер коопсуздук; жеке маалыматтар; маалымат коргоо; улуттук коопсуздук; кибер коркунучтар; укуктук жөнгө салуу.

Ключевые слова: информационная безопасность; кибербезопасность; персональные данные; защита информации; национальная безопасность; киберугрозы; правовое регулирование.

Keywords: information security; cybersecurity; personal data; information protection; national security; cyber threats; legal regulation.

Информационная безопасность является одной из ключевых составляющих национальной безопасности современного общества. В условиях стремительного развития цифровых технологий и глобализации интернет-пространства, безопасность информационных систем приобретает критическую важность для обеспечения стабильности государства, защиты интересов граждан и предотвращения угроз в сфере киберпреступности. В этой связи, обеспечение информационной безопасности в Кыргызстане становится не только важной, но и актуальной задачей для всех участников информационного пространства: государства, бизнеса и граждан.

Целью настоящей работы является анализ текущего состояния законодательства в области информационной безопасности Кыргызстана, выявление проблем и перспектив его развития.

Правовая основа информационной безопасности в Кыргызстане формировалась с начала 2000-х годов в ответ на возникающие угрозы в области информационных технологий. В этом контексте следует выделить несколько ключевых нормативных актов, которые составляют основу правового регулирования в области информационной безопасности.

Закон Кыргызской Республики “Об информации персонального характера", принятый в 2008 г. был первым шагом в создании правовой базы для защиты данных в Кыргызстане. Он направлен на правовое регулирование работы с персональными данными на основе общепринятых международных принципов и норм в соответствии с Конституцией и законами Кыргызской Республики в целях обеспечения защиты прав и свобод человека и гражданина, связанных со сбором, обработкой и использованием персональных данных [1]. Этот закон стал основой для регулирования вопросов, связанных с конфиденциальностью данных, защитой от несанкционированного доступа и другими аспектами безопасности.

Закон КР «О национальной безопасности» регулирует вопросы, связанные с охраной национальных интересов, в том числе информационной безопасности [3]. В разделе, посвященном информационной безопасности, устанавливаются требования к защите критической информационной инфраструктуры и безопасности государственных информационных ресурсов. Этот закон также предусматривает необходимость формирования и внедрения национальных программ по защите информации, что отражает важность информационной безопасности как компонента национальной безопасности.

Закон «О кибербезопасности» был принят в ответ на растущие угрозы, связанные с развитием интернета и цифровых технологий [2]. Он регулирует вопросы защиты информационных систем, сетевой инфраструктуры, защиты данных от кибератак и других киберугроз. Закон включает в себя нормы, касающиеся не только государственных органов, но и частных организаций, определяя их обязательства по обеспечению безопасности своих информационных систем. Особое внимание в законе уделяется вопросам взаимодействия с международными организациями по вопросам кибербезопасности.

Важным шагом в правовом регулировании защиты информации стало принятие закона «О защите персональных данных», который регулирует обработку персональной информации граждан. Закон предусматривает, что персональные данные должны быть собраны, обработаны и

защищены с учетом прав граждан на конфиденциальность. Этот закон также устанавливает обязанности организаций по защите данных, которые могут быть подвергнуты утечке или неправомерному доступу.

Помимо вышеупомянутых законов, в Кыргызстане существуют и другие нормативные акты, регулирующие отдельные аспекты информационной безопасности, такие как:

- Кодекс о правонарушениях Кыргызской Республики (в части киберпреступлений);
- Закон «О связи» (который регулирует вопросы безопасности телекоммуникационных систем);
- Закон «О защите авторских прав и смежных прав» (регулирующий вопросы защиты интеллектуальной собственности в цифровом формате).

Несмотря на наличие определенной правовой базы, в Кыргызстане существует ряд проблем, связанных с эффективностью применения законодательства в области информационной безопасности.

Недостаточная актуализация законодательства

Быстрое развитие технологий и изменение характера угроз требует оперативного обновления нормативных актов. Например, вопросы, связанные с киберпреступностью, использованием технологий искусственного интеллекта, криптовалют, пока что не нашли должного отражения в законодательстве Кыргызстана. Отсутствие четкой регламентации таких новых угроз создает пробелы в правовом регулировании.

Проблемы в координации между государственными органами

В Кыргызстане существует несколько государственных органов, которые отвечают за информационную безопасность, однако между ними не всегда имеется должная координация. Это может приводить к дублированию функций, недостаточной координации усилий и, как следствие, снижению эффективности государственной политики в сфере кибербезопасности.

Недостаток профессиональных кадров

Одной из серьезных проблем в области информационной безопасности является дефицит специалистов, способных разрабатывать и внедрять системы защиты данных, а также квалифицированных правозащитников, которые могут эффективно применять законы, регулирующие киберпреступления. Это связано с низким уровнем образования в сфере информационных технологий и безопасности в стране.

Проблемы обеспечения гражданских прав и свобод

Вопросы, касающиеся защиты частной жизни и личных данных граждан, не всегда получают должное внимание в законодательной практике. Законодательство о защите персональных данных, например, требует улучшения в части правоприменения и создания эффективных механизмов защиты прав граждан в случае утечки или неправомерного использования личной информации.

Неопределенность правового статуса в отношении защиты информации в частных компаниях и среди граждан. В частности, до сих пор остается нерешенным вопрос о правовых последствиях утечек личных данных, а также о механизмах защиты интеллектуальной собственности в цифровом формате.

Недостаточный уровень цифровой грамотности населения и специалистов. Важно не только создавать законодательные нормы, но и обеспечивать их грамотное применение. На сегодняшний день в Кыргызстане наблюдается дефицит специалистов в области информационной безопасности, а также низкий уровень осведомленности населения о рисках, связанных с использованием информационных технологий.

Перспективы развития законодательства

Для того чтобы улучшить текущую ситуацию и подготовиться к новым вызовам в области информационной безопасности, необходимо провести следующие шаги.

1. Актуализация законодательства. В первую очередь следует обновить существующие законы с учетом новых угроз, таких как кибертерроризм, утечки данных, преступления в сфере Интернета вещей и защиты интеллектуальной собственности в цифровом пространстве. Необходима актуализация существующих норм с учетом международных стандартов, таких как Общий регламент защиты данных (GDPR) Европейского Союза.
2. Создание единой стратегии информационной безопасности. Важно выработать и внедрить долгосрочную стратегию по обеспечению информационной безопасности, которая будет направлена на защиту всех участников информационного

процесса: государственных органов, частных компаний и граждан. Она должна учитывать как технические, так и правовые аспекты.

3. Повышение квалификации специалистов. Одним из ключевых элементов успешной реализации законодательных инициатив является подготовка кадров в сфере информационной безопасности. В этом контексте важным шагом станет развитие образовательных программ и тренингов для специалистов, а также повышение уровня цифровой грамотности среди населения.

4. Международное сотрудничество. Кыргызстан должен активно участвовать в международных соглашениях и форумах по вопросам кибербезопасности, чтобы выработать эффективные механизмы защиты от транснациональных киберугроз. Это позволит внедрить лучшие мировые практики и усовершенствовать национальную правовую базу [5].

Развитие законодательства в области информационной безопасности является приоритетной задачей для Кыргызстана. Модернизация законодательства, усиление международного сотрудничества и повышение уровня киберграмотности населения – ключевые факторы обеспечения национальной безопасности в цифровую эпоху. Необходимо учитывать лучшие международные практики, адаптируя их к национальным условиям. Активное участие государственных органов, представителей бизнеса и гражданского общества необходимо для успешной реализации рекомендованных мер [4].

Правовая основа информационной безопасности в Кыргызстане продолжает развиваться, но требует дальнейшего совершенствования. Актуализация законодательства, улучшение координации государственных органов и повышение квалификации специалистов – это те шаги, которые помогут создать эффективную правовую систему защиты информации в стране. В условиях глобальных угроз и стремительного развития технологий, эффективное регулирование информационной безопасности становится важной задачей для обеспечения стабильности и безопасности общества.

Список использованной литературы

1. Кыргызская Республика. Законы. Об информации персонального характера : Закон Кыргызской Республики от 14 апр. 2008 г. № 58 (в ред. Закона КР от 29 нояб. 2021 г. № 142). – Бишкек, 2008.

2. Кыргызская Республика. Законы. О кибербезопасности : Закон Кыргызской Республики от 17 июля 2024 г. № 121. – Бишкек, 2024.

3. Кыргызская Республика. Законы. О национальной безопасности : Закон Кыргызской Республики от 26 февр. 2003 г. № 44 (в ред. Закона КР от 1 дек. 2017 г. № 197). – Бишкек, 2003.

4. Конвенция о киберпреступности : [заключена в г. Будапеште 23 нояб. 2001 г.]. – Будапешт, 2001.

5. Шарипов, М. К. Правовые аспекты защиты персональных данных в Кыргызстане / М. К. Шарипов // Право и общество. – Бишкек, 2019. – С. 136

Рецензент: к.ю.н. Кылчыкбаев Т.