УДК 340.132:342.7(575.2)
DOI: 10.36979/1694-500X-2023-23-7-64-68

ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ПРОБЛЕМЫ РЕАЛИЗАЦИИ ПРАВА НА ЛИЧНУЮ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ В КЫРГЫЗСТАНЕ

М.У. Алияскарова

Аннотация. Рассматривается актуальная проблема реализации права на личную информационную безопасность в Кыргызстане. В статье проанализированы основные нормативные акты, регулирующие данную сферу, выявлены проблемы и недостатки в их реализации. Особое внимание уделено механизмам контроля и ответственности за нарушение норм о защите личной информации. Исследованы препятствия, с которыми сталкиваются граждане при попытке осуществить свои права на личную информационную безопасность. Предложены рекомендации по усовершенствованию организационных и правовых механизмов в данной области, включая разработку более детальных нормативных актов и улучшение информированности населения. Организационно-правовая проблема реализации личности права на информационную безопасность проявляется прежде всего в принципе неприкосновенности личной информации, а также в правоотношениях того же характера. Гарантия права личности на неприкосновенность частной жизни является исходящим элементом определенных механизмов по обеспечению информационной безопасности личности. Общий подход к решению проблемы подчеркивает важность взаимодействия государства, бизнес-сектора и общественности для обеспечения эффективной личной информационной безопасности в современном информационном обществе.

Ключевые слова: информационное право; информационная безопасность личности; информационная безопасность; защита информации; кибербезопасность; критическая информационная инфраструктура; право на информацию; информационные правоотношения; конфиденциальность; персональные данные; цифровая экономика.

КЫРГЫЗСТАНДА ЖЕКЕ МААЛЫМАТТЫК КООПСУЗДУККА БОЛГОН УКУКТУ ИШКЕ АШЫРУУНУН УЮШТУРУУЧУЛУК-УКУКТУК КӨЙГӨЙЛӨРҮ

М.У. Алияскарова

Аннотация. Бул макалада жеке маалымат коопсуздугуна болгон укукту ишке ашыруунун актуалдуу суроолор каралат. Кыргызстанда «маалыматтык коопсуздук» түшүнүгү, эреже катары, «инсандын, коомдун жана мамлекеттин турмуштук маанилүү кызыкчылыктарынын корголуу абалы» аркылуу ачылат. Көптөгөн башка мамлекеттерде, «маалыматтык коопсуздук» аныктамасы маалыматтын жана маалымат тутумдарынын купуялуулугун, бүтүндүгүн жана жеткиликтүүлүгүн укуктук принциптерге байланыштуу. Бул принциптерди ишке ашыруу укуктук мамилелердин ар кандай катышуучуларынын кызыкчылыктарынын балансын камсыз кылууга мүмкүндүк берет, ошону менен адам укуктарынын кепилдиги болот. Заманбап технологиялардын таасири жеке укуктар чөйрөсүндө баарынан жогору турат, алардын арасында жеке жашоого болгон укук өзгөчө орунду ээлейт. Бир жагынан, жеке жашоого болгон укуктун кепилдиги катары бул укукту коргоого түздөн-түз багытталган чаралар колдонулат. Изилдөө тарабынан инсандык маалыматтык коопсуздук чөйрөсүнө киргизилген мамилелердин чөйрөсү талданат. Инсандын маалыматтык коопсуздук институтун гармониялуу өнүктүрүү үчүн техникалык, социалдык багыттагы чараларды жана стимулдарды күчөтүү зарыл деген тыянак чыгарылды.

Түйүндүү сөздөр: маалымат укугу; жеке маалымат коопсуздугу; маалымат коопсуздугу; коргоо; киберкоопсуздук; критикалык маалымат инфраструктурасы; маалымат укугу; маалыматтык укук мамилелери; купуялуулук; жеке маалыматтар; санариптик экономика.

ORGANIZATIONAL AND LEGAL PROBLEMS OF REALIZATION THE PERSONAL INFORMATION SECURITY RIGHT IN KYRGYZSTAN

M.U. Aliyaskarova

Abstract. The article is devoted to the actual problem of the realization of the right to personal information security. In Kyrgyzstan, the concept of "information security" is usually revealed through "the state of protection of vital interests of the individual, society and the state." In almost every state, the phenomenon of information security is a guarantor of confidentiality, general legal identification and respect for individual rights, which in turn allows us to take into account the comprehensive interests of all subjects of certain legal relations, thus acting as a guarantor of natural law and inalienable human rights. The organizational and legal problem of the realization of the individual's right to information security is manifested primarily in the principle of inviolability of personal information, as well as in legal relations of the same nature. Firstly, the guarantee of the individual's right to privacy is an outgoing element of certain mechanisms to ensure the information security of the individual. Making a conclusion about the objects of research that are included by researchers in the field of personal information security, we can say that for the harmonious development of the institute of personal information security in Kyrgyzstan, it is necessary to strengthen non-technical, socially oriented measures and incentives.

Keywords: information law; information security of the person; information security; information protection; cybersecurity; critical information infrastructure; the right to information; legal relations; confitdentiality; personal data; data economy.

Право на личную информационную безопасность является основополагающим правом человека, которое обеспечивает неприкосновенность частной жизни, конфиденциальность и защиту данных. В современную цифровую эпоху, когда различные организации регулярно обмениваются, хранят и обрабатывают личную информацию, важность этого права стала более важной, чем когда-либо. Однако обеспечение защиты личной информации не всегда является простым делом, и при его реализации может возникнуть ряд организационных и юридических проблем. В этой статье исследуются некоторые организационные и правовые проблемы, которые могут препятствовать реализации права на личную информационную безопасность.

Одной из основных организационных проблем в реализации права на личную информационную безопасность является недостаточная осведомленность и понимание важности защиты данных. Многие организации, особенно малые и средние предприятия, могут не иметь четкого представления о своих обязательствах в соответствии с законами о защите данных или о рисках, связанных с неправильным обращением с персональными данными. Следовательно, они могут не принять адекватных мер по защите личной информации, что приведет к утечкам данных, краже личных данных и другим киберпреступлениям [1].

Другой организационной проблемой является нехватка ресурсов, таких как квалифицированный персонал и адекватные технологии для внедрения эффективных мер по защите данных. Безопасность данных требует постоянного мониторинга, анализа угроз и обновления мер безопасности. Организациям, которым не хватает необходимых ресурсов, может быть сложно идти в ногу с постоянно меняющимся ландшафтом угроз и надлежащим образом защищать личную информацию.

Кроме того, многие организации собирают персональные данные от физических лиц без их осознанного согласия. Это является нарушением права на неприкосновенность частной жизни, поскольку отдельные лица имеют право контролировать сбор, использование и раскрытие своей личной информации [2]. Отсутствие согласия также может привести к сбору ненужной или не относящейся к делу личной информации, что может подвергнуть людей риску кражи личных данных и других киберпреступлений.

В Кыргызской Республике одной из таких проблем является недостаточная осведомленность и понимание защиты данных. Многие организации, особенно малые и средние предприятия, могут не иметь четкого представления о своих обязательствах в соответствии с законами о защите данных или о рисках, связанных с неправильным обращением с персональными данными. Следовательно, они могут не принять адекватных мер по защите личной информации, что приведет к утечкам данных, краже личных данных и другим киберпреступлениям.

Также можно выделить присущую Кыргызстану проблему – нехватка ресурсов, таких как квалифицированный персонал и адекватные технологии для внедрения эффективных мер

по защите данных. Безопасность данных требует постоянного мониторинга, анализа угроз и обновления мер безопасности. Организациям, которым не хватает необходимых ресурсов, может быть сложно идти в ногу с постоянно меняющимся ландшафтом угроз и надлежащим образом защищать личную информацию [3].

Одной из существенных юридических проблем в реализации права на личную информационную безопасность является отсутствие всеобъемлющих законов о защите данных. Хотя во многих странах действуют законы о защите данных, они сильно различаются с точки зрения сферы охвата, применимости и правоприменения. Некоторые законы могут применяться только к определенным типам персональных данных, в то время как другие – только к определенным секторам или отраслям промышленности. Отсутствие гармонизации законов о защите данных может создать правовые лазейки, приводящие к непоследовательной защите личной информации.

Еще одной юридической проблемой является отсутствие эффективных механизмов правоприменения. Даже в странах с всеобъемлющими законами о защите данных правоприменение может быть слабым или вообще отсутствовать. Это может быть связано с такими факторами, как ограниченные ресурсы, неадекватная правовая база или коррупция [4]. Без эффективного правоприменения организации могут быть менее мотивированы к внедрению адекватных мер по защите данных, что приводит к увеличению рисков утечки данных и киберпреступлений.

В Кыргызской Республике одной из существенных юридических проблем в реализации права на личную информационную безопасность является отсутствие всеобъемлющих законов о защите данных. Хотя в стране действует закон о защите данных, он применяется только к обработке персональных данных государственными органами и не обеспечивает всестороннюю защиту личной информации. Это может создать юридические лазейки, приводящие к непоследовательной защите личной информации.

Отсутствие эффективных механизмов правоприменения, слабое или вообще отсутствие может быть связано с такими факторами, как ограниченные ресурсы, неадекватная правовая база или коррупция. Без эффективного правоприменения организации могут быть менее мотивированы к внедрению адекватных мер по защите данных, что приводит к увеличению рисков утечки данных и киберпреступлений.

Кроме того, отсутствие трансграничных правил и соглашений о защите данных может создать значительные юридические проблемы. Поскольку глобальная экономика становится все более взаимосвязанной, персональные данные часто передаются через границы, и важно обеспечить, чтобы такая передача не нарушала право на неприкосновенность частной жизни. Однако отсутствие трансграничных соглашений о защите данных может создать правовую неопределенность, приводящую к несоответствиям в защите личной информации.

Область безопасности личной информации постоянно развивается, регулярно появляются новые технологии, угрозы и нормативные акты. Несмотря на проблемы, в этой области есть несколько многообещающих перспектив, которые могут усилить защиту личной информации и улучшить реализацию права на неприкосновенность частной жизни.

Одной из наиболее многообещающих перспектив является растущее внедрение передовых технологий в области защиты данных. Искусственный интеллект, машинное обучение и блокчейн – это лишь несколько примеров технологий, которые могут быть использованы для усиления безопасности данных. Например, алгоритмы машинного обучения могут использоваться для выявления и блокирования подозрительных действий, в то время как блокчейн может обеспечить безопасный и децентрализованный способ хранения личных данных и обмена ими. По мере того как эти технологии становятся все более доступными, все больше организаций могут использовать их для повышения безопасности своих данных [5].

Еще одной многообещающей перспективой является растущее осознание важности защиты данных. Люди все больше осознают свое право на неприкосновенность частной жизни и потенциальные риски, связанные с неправильным обращением с персональными данными. Это осознание привело к увеличению спроса на улучшенную защиту данных, что может побудить организации внедрять более строгие меры безопасности данных.

Более того, правительства признают важность защиты данных и принимают всеобъемлющие законы о защите данных. Общее положение о защите данных (GDPR) в Европейском Союзе и Калифорнийский закон о защите прав потребителей (CCPA) в Соединенных Штатах – это лишь несколько примеров таких законов. Эти законы обеспечивают четкие рамки для защиты личной информации и могут служить образцом для подражания в других странах.

Другой многообещающей перспективой является расширение сотрудничества между организациями и правительствами в решении проблем личной информационной безопасности. Многие организации в настоящее время тесно сотрудничают с регулирующими органами и правоохранительными органами для обмена информацией, выявления угроз и внедрения эффективных мер безопасности данных. Это сотрудничество может помочь устранить правовые лазейки, снизить риски киберпреступлений и улучшить общую защиту личной информации [6].

Основными механизмами защиты права на неприкосновенность частной жизни, которые находят выражение в соответствующих правовых принципах, являются согласие субъекта персональных данных на обработку персональных данных и его уведомление о такой обработке. «Если доступ или возможности сбора и обработки предоставляются на основании закона, то обязательным является уведомление об обработке персональных данных их обладателя. Уведомление также обязательно при иных случаях, определенных субъектом персональных данных или установленных законодательством, например, при нарушении конфиденциальности или целостности персональных данных. Указанные механизмы предоставляют субъекту персональных данных правовые возможности контроля за их использованием и, соответственно, гарантии неприкосновенности его частной жизни» [7].

Хотя существует ряд организационных и правовых проблем в реализации права на личную информационную безопасность, есть также и многообещающие перспективы: внедрение передовых технологий; повышение осведомленности о защите данных; всеобъемлющие законы о защите данных и сотрудничество между организациями и правительствами – вот лишь несколько примеров таких перспектив. Поскольку эти перспективы продолжают развиваться, важно сохранять бдительность и быть в курсе последних событий в области защиты данных, чтобы усилить защиту личной информации и улучшить реализацию права на неприкосновенность частной жизни.

Право на личную информационную безопасность является основополагающим правом человека, которое требует защиты персональных данных от несанкционированного доступа, использования и раскрытия. В Кыргызской Республике реализации этого права может препятствовать ряд организационных и правовых проблем [8]. Недостаточная осведомленность и понимание защиты данных, нехватка ресурсов и несанкционированный сбор личной информации могут создавать уязвимости, которыми могут воспользоваться киберпреступники. Юридические проблемы, такие как отсутствие всеобъемлющих законов о защите данных и слабые механизмы правоприменения могут привести к непоследовательной защите личной информации. Для решения этих проблем организации и правительство Кыргызской Республики должны работать сообща, чтобы обеспечить эффективное внедрение и правоприменение законов о защите данных и внедрение передовой практики в области безопасности данных [9]. Правительство также должно предпринять шаги по обновлению действующих законов о защите данных и внедрению трансграничных правил и соглашений о защите данных для усиления защиты личной информации и улучшения реализации права на неприкосновенность частной жизни.

Будет справедливым вывод о том, что в текущих нормативных правовых актах не содержится достаточной регламентации института информационной безопасности личности. «Более того, некоторые российские исследователи толкуют такой стратегический документ как Доктрину в качестве инструмента для незамедлительного и постоянного противодействия деструктивной деятельности иностранных элементов в информационной сфере, что также не позволяет в полной мере определить место личности в системе мер обеспечения информационной безопасности» [10].

Институт информационной безопасности личности в своем развитии в обязательной мере должен затрагивать такой понятийный аппарат, как «баланс интересов», еще лучше если данное понятие будет возведено в статус обязательного

принципа информационной безопасности личности, что будет находить свое отражение в разработке новых механизмов утверждения свобод личности в информационной сфере. Организационно-правовая проблема реализации личности права на информационную безопасность проявляется прежде всего в принципе неприкосновенности личной информации, а также в правоотношениях того же характера.

В данной научной статье были рассмотрены и проанализированы организационно-правовые проблемы, связанные с реализацией права на личную информационную безопасность в Кыргызстане. Исследование подчеркнуло важность защиты личных данных в современном цифровом обществе, особенно в контексте быстрого развития информационных технологий и распространения интернета. В статье были выявлены основные правовые нормы и нормативные акты, регулирующие сферу личной информационной безопасности в Кыргызстане. Был проведен анализ эффективности действующего законодательства и выявлены пробелы и недостатки в его реализации. Особое внимание уделено механизмам контроля за соблюдением норм о защите личных данных, а также ответственности за их нарушение.

В ходе исследования были выявлены препятствия, с которыми сталкиваются граждане при попытке осуществить свое право на личную информационную безопасность. Среди них – недостаточная информированность граждан о своих правах и способах их защиты, а также сложности в вопросах технической реализации защиты данных. Предложены пути усовершенствования организационных и правовых механизмов обеспечения личной информационной безопасности в Кыргызстане, что включает разработку более подробных и четких нормативных актов, повышение уровня информированности населения, укрепление механизмов контроля за соблюдением законодательства и повышение ответственности за его нарушение. В целом статья акцентирует внимание на актуальности проблемы личной информационной безопасности в современном обществе и призывает к комплексным мерам по её решению с участием государства, бизнес-сектора и общественности.

Поступила: 06.02.23; рецензирована: 20.02.23;
принята: 24.02.23.

Литература

1. *Терещенко Л.К.* Информационная безопасность органов исполнительной власти на современном этапе / Л.К. Терещенко, О.И. Тиунов // Журнал российского права. 2015. № 8. URL: http://cbd.minjust.gov.kg/act/view/ru-ru (дата обращения: 15.02.2023).
2. *Марков А.С.* Руководящие указания по кибербезопасности в контексте ISO 27032 / А.С. Марков, В.Л. Цирлов // Вопросы кибербезопасности. 2014. № 1. URL: https://ru.scribd.com/doc/456568043 (дата обращения: 15.02.2023).
3. Концепция информационной безопасности Кыргызской Республики на 2019–2023 годы. URL: http://cbd.minjust.gov.kg/act/view/ru-ru/13652 (дата обращения: 20.01.2023).
4. Конвенция об обеспечении международной информационной безопасности (концепция). URL: http://www.mid.ru/en/foreign_policy (дата обращения: 21.01.2023).
5. Ministry of Public Security of the People's Republic of China published the Draft Regulations on the Classifi ed Protection of Cybersecurity. URL: https://www.huntonprivacyblog.com/2018/07/17/china-publishes-draft-regulations-classified-protection-cybersecurity/ (дата обращения: 19.02.2023).
6. Cybersecurity Act. Электронный доступ на сайте Министерства связи и информации Сингапура. URL: https://www.csa.gov.sg/legislation/cybersecurity-act (дата обращения: 20.01.2023).
7. *Cumbley R.* Is "Big Data" Creepy? / R. Cumbley, P. Church // Computer Law and Security Review. 2013. № 29.
8. *Орозбаева А.Ж.* Обзор законодательства КР о информационной безопасности / А.Ж. Орозбаева. URL: https://internetpolicy.kg/wp-content/uploads/2018/01 (дата обращения: 15.02.2023).
9. *Касымбеков Б.К.* Проблемы правового регулирования государственно-социальных отношений в Кыргызской Республике / Б.К. Касымбеков // Вестник «Alikhan Bokeikhan University». 2022. Т. 4. № 55. URL: https://vestnik.semuniver.kz/index.php/main/article/view/485 (дата обращения: 19.02.2023).
10. *Ищенко А.Н.* Новая доктрина информационной безопасности Российской Федерации как основа противодействия угрозам безопасности России в информационной сфере / А.Н. Ищенко, А.Н. Прокопенко, А.А. Страхов // Проблемы правоохранительной деятельности. 2017. № 2.