УДК 340.132:342.7(575.2)
DOI: 10.36979/1694-500X-2023-23-7-58-63

МЕХАНИЗМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ В КЫРГЫЗСТАНЕ: ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЙ АСПЕКТ

М.У. Алияскарова

Аннотация. Исследуются закономерные правовые явления механизма по обеспечению информационной безопасности личности. Исследование данной сферы правого пласта прав и свобод личности считается и признается многими учеными весьма актуальным, так как феномен личности в нашем обществе находится под угрозой, а именно под угрозой информационной безопасности личности в Кыргызстане. Автором предлагается своя трактовка определения механизма по обеспечению информационной безопасности личности, а также проведен анализ влияния и обеспечения свободы личности на её правовую защищенность в государстве. Выделяется такой пласт, как культура личной информационной безопасности, где есть место исследованию и особенностям данного явления, способствующим обеспечению правовой безопасности личности в информационной сфере: принцип построения информационной безопасности; принцип и основа системы обеспечения информационной безопасности. В свою очередь организационно-правовая проблема реализации личности права на информационную безопасность проявляется прежде всего в принципе неприкосновенности личной информации, а также в правоотношениях того же характера. Разработаны конкретные механизмы по обеспечению информационной безопасности государственных органов.

Ключевые слова: угрозы информационной безопасности; информационное общество; право личности на информационную безопасность; механизм обеспечения права личности на информационную безопасность; информационная культура.

КЫРГЫЗСТАНДА ИНСАНДЫН МААЛЫМАТТЫК КООПСУЗДУГУН КАМСЫЗ КЫЛУУ МЕХАНИЗМИ: ТЕОРИЯЛЫК-МЕТОДОЛОГИЯЛЫК АСПЕКТ

М.У. Алияскарова

Аннотация. Бул макалада азыркы учурда жаңы укуктун өзгөчөлүктөрүн изилдөө арналган-маалымат коопсуздугу боюнча жеке адамдын укугу. Бул укукту изилдөө абдан актуалдуу болуп саналат, анткени азыркы коомдогу инсан көптөгөн маалыматтык коркунучтарга дуушар болот жана маалыматтык коопсуздукту камсыз кылуу чөйрөсүндөгү эң аялуу субъект болуп саналат. Демилгечи тарабынан каралып жаткан укуктун аныктамасы сунушталган, аны камсыз кылуу механизмине кыскача талдоо жүргүзүлгөн. Маалымат коопсуздугу боюнча адамдын укугун камсыз кылуу механизминин жаңы элементи катары жеке маалыматтык коопсуздук маданиятын баса белгилеп, анын өзгөчөлүктөрү каралды. Инсандын маалыматтык коопсуздугун камсыз кылууга өбөлгө түзүүчү уюштуруу шарттары катары төмөнкүлөр каралат: маалыматтык коопсуздук принциптерин сактоо жана алардын негизинде маалыматтык коопсуздукту камсыз кылуу системасын куруу; мамлекеттик органдарда маалыматка санкцияланбаган жетүүдөн коргоону камсыз кылуучу тиешелүү административдик-укуктук режимди иштеп чыгуу жана колдоо; мамлекеттик органдардын маалыматтык коопсуздугун камсыз кылуу боюнча конкреттүү чараларды жана иш-чараларды иштеп чыгуу; мамлекеттик башкаруунун ар кандай деңгээлдеринде инсандын маалыматтык коопсуздугун камсыз кылууга багытталган ченемдик укуктук актыларды иштеп чыгуу жана өркүндөтүү.

Түйүндүү сөздөр: маалыматтык коопсуздукка коркунуч келтирүү; маалыматтык коом; инсандын маалыматтык коопсуздукка болгон укугу; инсандын маалыматтык коопсуздукка болгон укугун камсыз кылуу механизми; маалыматтык маданият.

THE MECHANISM OF ENSURING THE INFORMATION SECURITY OF THE INDIVIDUAL IN KYRGYZSTAN: THEORETICAL METHODOLOGICAL ASPECT

M.U. Aliyaskarova

Abstract. The article is devoted to the study of the features of the new law of modernity – the right of the individual to information security. The study of this right is very relevant, since a person in modern society is exposed to a large number of information threats and is the most vulnerable subject in the field of information security. The author offers his interpretation of the definition of the mechanism for ensuring the information security of the individual, the author also analyzes the impact and ensuring the freedom of the individual on his legal protection of the state. There is such a layer as the culture of personal information security, where there is a place for research and features of this phenomenon. The author considers the following phenomena that can contribute to ensuring the legal security of an individual in the information sphere: the principle of building information security, the principle and basis of the information security system. In turn, the organizational and legal problem of the realization of the individual's right to information security manifests itself primarily in the principle of inviolability of personal information, as well as in legal relations of the same nature. The author also developed specific mechanisms to ensure the information security of state bodies.

Keywords: threats to information security; information society; the right of the individual to information security; the mechanism of ensuring the right of the individual to information security; information culture.

В современную цифровую эпоху безопасность личной информации стала серьезной проблемой как для государства, так и для граждан. С ростом использования технологий и интернета риск компрометации личной информации становится все более распространенным. Механизм обеспечения безопасности личной информации включает в себя различные меры и практики, направленные на защиту личной информации от несанкционированного доступа, использования, раскрытия или уничтожения. В этой статье будет рассмотрен механизм обеспечения безопасности личной информации и различные меры, которые отдельные лица и организации могут предпринять для защиты своей личной информации.

Механизм обеспечения безопасности личной информации включает в себя несколько шагов, которые можно разделить на три основные фазы: предотвращение, обнаружение и реагирование. Меры предотвращения направлены на снижение риска компрометации личной информации, меры обнаружения направлены на выявление любого несанкционированного доступа или использования личной информации, а меры реагирования направлены на смягчение последствий любой утечки личной информации.

Превентивными мерами для обеспечения эффективности механизма информацио-нной безопасности личности будет первый шаг – предотвращение. Превентивные меры направлены на снижение риска компрометации личной информации [1].

Механизм обеспечения безопасности личной информации включает в себя различные меры и практики, направленные на защиту личной информации от несанкционированного доступа, использования, раскрытия или уничтожения. Частные лица и организации должны предпринимать упреждающие шаги для предотвращения компрометации личной информации, обнаружения любого несанкционированного доступа или использования личной информации и реагирования на любую утечку личной информации. Следуя этим мерам и практикам, отдельные лица и организации могут гарантировать, что их личная информация защищена от киберугроз.

Безопасность личной информации является критической проблемой во всем мире, в том числе и в Кыргызстане. Все более широкое использование цифровых технологий и интернета принесло значительные выгоды, но это также создало более высокий риск компрометации личной информации. Механизм обеспечения безопасности личной информации включает в себя различные меры и практики, направленные на защиту личной информации от несанкционированного доступа, использования, раскрытия или уничтожения.

В теории права и государства механизм обеспечения прав и свобод личности рассматривают как комплексную процедуру (процесс) воплощения правовых предписаний в сфере

прав человека в реальную действительность. Ю.В. Анохин предлагает «рассматривать механизм обеспечения прав и свобод личности и в статике, и в динамике. При этом, статическая сторона включает в себя механизм государства, механизм действия права, включающий в себя механизм правового регулирования общественных отношений, реализации, охраны и защиты прав и свобод граждан, гарантии обеспечения действия исследуемого механизма, механизм юридической ответственности. Правовая культура, правовое сознание, законность и состояние правопорядка в стране выступают в качестве системообразующих компонентов организма. Динамическая сторона, в свою очередь, показывает деятельность системообразующих элементов, направленную на реализацию основных целей и задач этого механизма. Данный подход позволяет рассмотреть механизм обеспечения прав и свобод личности с точки зрения его внутренней организации в виде статической стороны, а также в процессе функционирования его составных частей – динамической стороны, что дает возможность оценить его эффективность при обеспечении прав и свобод личности» [2].

Закон Кыргызской Республики о защите персональных данных был принят в 2019 году для регулирования сбора, обработки, хранения и защиты персональных данных. Закон обеспечивает правовую основу для обеспечения безопасности личной информации в Кыргызстане. Ниже приведены некоторые из мер, которые отдельные лица и организации могут предпринять для обеспечения безопасности личной информации в Кыргызстане.

Оценка воздействия на защиту данных. Частным лицам и организациям следует провести оценку воздействия на защиту данных для выявления и снижения рисков, связанных со сбором, обработкой и хранением персональных данных.

План реагирования на инциденты. Частные лица и организации должны разработать план реагирования на инциденты, чтобы гарантировать, что они смогут быстро и эффективно реагировать на любое нарушение персональных данных.

Обеспечение безопасности личной информации в Кыргызстане требует внедрения различных мер и практик для защиты личной информации от несанкционированного доступа, использования, раскрытия или уничтожения. Частные лица и организации должны разработать и внедрить политику защиты данных, использовать шифрование, регулярно обновлять свое программное обеспечение, использовать надежные пароли, проводить регулярное обучение, внедрять двухфакторную аутентификацию, проводить оценку воздействия защиты данных и разрабатывать планы реагирования на инциденты. Следуя этим мерам и практикам, отдельные лица и организации могут гарантировать, что их личная информация защищена от киберугроз в Кыргызстане.

Несмотря на то, что механизм обеспечения безопасности личной информации в Кыргызстане за последние годы добился значительного прогресса, все еще существуют проблемы, которые необходимо решить [3].

Несмотря на усилия по повышению осведомленности о защите персональных данных, многим частным лицам и организациям в Кыргызстане по-прежнему не хватает знаний и понимания важности защиты персональных данных и мер, которые необходимо принять для ее обеспечения. Многим организациям в Кыргызстане, особенно малым и средним предприятиям, не хватает необходимых ресурсов и инфраструктуры для внедрения адекватных мер защиты персональных данных, таких как шифрование, безопасное хранение и регулярные обновления программного обеспечения.

Хотя Закон Кыргызской Республики о защите персональных данных создал правовую основу для защиты персональных данных, существуют опасения по поводу его внедрения и правоприменения. Некоторые организации могут не соблюдать требования закона, и могут быть приняты недостаточные правоприменительные меры.

Угрозы кибербезопасности, такие как фишинговые атаки, вредоносные программы и программы-вымогатели, продолжают представлять значительный риск для личной информационной безопасности в Кыргызстане. Растущее использование цифровых технологий и интернета

создало новые уязвимости, которые необходимо устранить.

Отсутствие координации и сотрудничества. Существует необходимость в большей координации и сотрудничестве между различными заинтересованными сторонами [4], включая правительственные учреждения, частный сектор и организации гражданского общества, для эффективного решения проблем безопасности личной информации.

Лица, чья личная информация была скомпрометирована, могут столкнуться с трудностями при доступе к средствам правовой защиты и обращении за возмещением ущерба. Несмотря на то, что механизм обеспечения безопасности личной информации в Кыргызстане добился прогресса, все еще существуют проблемы, которые необходимо решить. Эти проблемы включают недостаточную осведомленность и образование, недостаточные ресурсы и инфраструктуру, неадекватное внедрение и правоприменение закона, угрозы кибербезопасности, отсутствие координации и сотрудничества, а также ограниченный доступ к средствам правовой защиты. Решение этих проблем потребует совместных усилий всех заинтересованных сторон для обеспечения надлежащей защиты личной информации в Кыргызстане.

Механизм обеспечения безопасности личной информации в Кыргызстане за последние годы продемонстрировал значительный прогресс. Реализация Закона Кыргызской Республики о защите персональных данных в 2019 году создала правовую базу для защиты персональных данных в стране. Этот закон установил права физических лиц на их персональные данные и регулирует сбор, обработку, хранение и защиту персональных данных.

Законом также учреждено Агентство по защите персональных данных (PDPA), ответственное за надзор за исполнением закона и обеспечение защиты персональных данных в Кыргызстане. PDPA имеет полномочия расследовать нарушения персональных данных, назначать штрафы и санкции, а также предоставлять рекомендации по вопросам защиты данных [5].

Внедрение Закона о защите персональных данных повысило осведомленность о защите персональных данных среди частных лиц и организаций в Кыргызстане. Многие организации предприняли шаги для соблюдения закона и обеспечения того, чтобы их практика обработки персональных данных соответствовала требованиям закона. Кроме того, правительство Кыргызстана приняло меры по повышению безопасности личной информации в стране. Правительство учредило Государственный комитет информационных технологий и коммуникаций, который отвечает за разработку и реализацию политики и стратегий по повышению информационной безопасности в стране. Правительство также учредило Национальную CERT (Computer Emergency Response Team) для реагирования на киберинциденты и координации с другими CERT в регионе [6].

Однако, несмотря на достигнутый прогресс, угрозы кибербезопасности, такие как фишинговые атаки, вредоносные программы и программы-вымогатели, продолжают представлять значительный риск для личной информационной безопасности в стране. Необходимо продолжать инвестировать в инфраструктуру кибербезопасности и образование для повышения осведомленности и наращивания потенциала в области личной информационной безопасности.

Перспективы механизма обеспечения личной информационной безопасности в Кыргызстане многообещающие. Внедрение Закона о защите персональных данных и учреждение PDPA создали правовую базу и регулирующий орган для их защиты. Усилия правительства по повышению информационной безопасности и растущая осведомленность отдельных лиц и организаций о защите персональных данных являются позитивными признаками для будущего личной информационной безопасности в Кыргызстане.

Следует отметить, что механизм обеспечения безопасности личной информации в Кыргызстане за последние годы добился значительного прогресса, но все еще существуют проблемы, требующие решения. Необходимы постоянные инвестиции в инфраструктуру кибербезопасности, образование и повышение осведомленности.

Кыргызстан является членом Совета Европы, который разработал Конвенцию о защите

физических лиц в отношении автоматической обработки персональных данных. Ратифицировав эту конвенцию, Кыргызстан взял на себя обязательство защищать персональные данные в соответствии с международными стандартами. Кроме того, международное сотрудничество может помочь в решении трансграничных проблем безопасности личной информации, таких как киберпреступность и утечка данных.

Оценка воздействия на защиту данных. Закон Кыргызской Республики о защите персональных данных требует от организаций проведения оценки воздействия на защиту данных (DPIA) при обработке персональных данных, которые представляют высокий риск для прав и свобод физических лиц. DPIA – это инструмент, который помогает организациям выявлять и снижать потенциальные риски, связанные с деятельностью по обработке персональных данных.

Локализация данных. Локализация данных относится к требованию о том, что персональные данные физических лиц в определенной стране должны храниться и обрабатываться в этой стране. Эта мера направлена на усиление защиты персональных данных и предотвращение трансграничной передачи данных, которая может подвергать персональные данные рискам.

Конфиденциальность по замыслу и по умолчанию. Закон Кыргызской Республики о защите персональных данных требует от организаций соблюдения принципов конфиденциальности по замыслу и по умолчанию при разработке и внедрении мероприятий по обработке персональных данных. Конфиденциальность по замыслу и по умолчанию – это принципы, направленные на то, чтобы включить соображения конфиденциальности в дизайн систем и процессов, а не добавлять их запоздало.

Риск-ориентированный подход. Организации в Кыргызстане обязаны применять риск-ориентированный подход при внедрении мер по защите персональных данных. Этот подход предполагает оценку рисков, связанных с деятельностью по обработке персональных данных, и осуществление соответствующих мер по снижению этих рисков. Риск-ориентированный подход позволяет организациям сосредоточить свои ресурсы и усилия на областях, которые представляют наибольший риск для защиты персональных данных.

Также следует отметить, что механизм обеспечения безопасности личной информации в Кыргызстане развивается и сталкивается с различными вызовами. Однако внедрение Закона о защите персональных данных, создание PDPA и усилия правительства по повышению информационной безопасности являются позитивными шагами на пути к обеспечению безопасности личной информации.

Очевидно, что обеспечение информационной безопасности – это многофункциональный и непрерывный процесс, заключающийся в деятельности государственных органов по созданию организационных условий, при которых нанесение вреда зависящим от информации элементам системы становится невозможным или крайне затруднительным. В связи с этим в качестве организационных условий, способствующих обеспечению информационной безопасности личности, могут рассматриваться:

1) актуальность и значимость проблем информационной безопасности в современных условиях развития информационных технологий. Анализ показал, что Кыргызстан также сталкивается с вызовами и угрозами, связанными с нарушением информационной безопасности личности;
2) теоретические основы обеспечения информационной безопасности: обширный обзор существующих теорий и концепций в области информационной безопасности. Основываясь на этом анализе, была разработана собственная методологическая модель, учитывающая специфику кыргызской ситуации;
3) механизмы обеспечения информационной безопасности личности. Было выделено несколько ключевых механизмов, которые следует рассматривать как основу для разработки эффективных стратегий по обеспечению информационной безопасности личности;
4) рекомендации и практические аспекты: разработка и внедрение более эффективных механизмов защиты информации, повышение

осведомленности граждан о рисках и методах защиты, а также совершенствование законодательства в области информационной безопасности.

Таким образом, данная статья предоставляет комплексный взгляд на проблему информационной безопасности личности в Кыргызстане, а также предлагает практические рекомендации для повышения уровня защиты личной информации граждан. Результаты и выводы данного исследования могут служить основой для дальнейших исследований и разработок в области обеспечения информационной безопасности.

Поступила: 15.02.23; рецензирована: 02.03.23;
принята: 06.03.23.

Литература

1. 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).
2. *Анохин Ю.В.* Механизм государственно-правового обеспечения прав и свобод личности (на материалах Российской Федерации): дис. … д-ра юрид. наук / Ю.В. Анохин. Саратов, 2007.
3. *Тамодлин А.А.* Государственно-правовой механизм обеспечения информационной безопасности личности: дис. … канд. юрид. наук / А.А. Тамодлин. М., 2006.
4. *Беляева Г.С.* К вопросу о структуре механизма защиты прав и свобод граждан / Г.С. Беляева, Ж.Д. Антонова // Юридические исследования. 2017. № 6. URL: http://e-notabene.ru/lr/article_19070.html (дата обращения: 17.02.2023).
5. *Cumbley R.* Is “Big Data” Creepy? / R. Cumbley, P. Church // Computer Law and Security Review. 2013. № 29.
6. *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)..