УДК 349:004.056(575.2)
DOI: 10.36979/1694-500X-2025-25-7-65-73

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В КЫРГЫЗСКОЙ РЕСПУБЛИКЕ: ВОПРОСЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ

А.Т. Алибаев, Г.К. Токтогонова

Аннотация. Информационная безопасность является неотъемлемой частью национальной безопасности и предполагает состояние защищенности человека, общества и государства от внутренних и внешних угроз. В условиях активной трансформации общественных отношений и формирования современного информационного глобального пространства не теряет своей актуальности вопрос правового обеспечения национальной системы информационной безопасности. Проанализированы ведущие отечественные нормативно-правовые акты, заложившие прочную основу для организации и развития системы информационной безопасности. В рамках анализа рассматривается вопрос правового соотношения понятий “информационная безопасность” и “кибербезопасность”, выделяются ключевые современные угрозы, исходящие из информационного пространства и нарушающие целостность всего государства, а также особенности международного сотрудничества и многовекторной международной политики в области стандартизации средств защиты информации.

Ключевые слова: информация; безопасность; информационная безопасность; Концепция информационной безопасности Кыргызской Республики; персональные данные; электронное управление.

КЫРГЫЗ РЕСПУБЛИКАСЫНДАГЫ МААЛЫМАТТЫК КООПСУЗДУК: УКУКТУК ЖӨНГӨ САЛУУ МАСЕЛЕЛЕРИ

А.Т. Алибаев, Г.К. Токтогонова

Аннотация. Маалыматтык коопсуздук улуттук коопсуздуктун ажырагыс бөлүгү болуп саналат жана адамды, коомду жана мамлекетти ички жана тышкы коркунучтардан коргоо абалын болжолдойт. Коомдук мамилелерди активдүү трансформациялоонун жана заманбап маалыматтык глобалдык мейкиндикти калыптандыруунун шарттарында маалыматтык коопсуздуктун улуттук системасын укуктук камсыздоо маселеси актуалдуулугун жоготпойт. Маалыматтык коопсуздук системасын уюштурууга жана өнүктүрүүгө бекем негиз түзгөн ата мекендик алдыңкы ченемдик укуктук актылар талдоого алынган. Талдоонун алкагында “маалыматтык коопсуздук” жана “киберкоопсуздук” түшүнүктөрүнүн ортосундагы укуктук байланыш маселеси каралып, маалымат мейкиндигинен келип чыккан жана бүткүл мамлекеттин бүтүндүгүн бузган негизги заманбап коркунучтар, ошондой эле эл аралык кызматташтыктын өзгөчөлүктөрү жана маалыматтык коопсуздук инструменттерин стандартташтыруу жаатындагы көп векторлуу эл аралык саясаттын өзгөчөлүктөрү белгиленген.

Түйүндүү сөздөр: маалымат; коопсузду; маалыматтык коопсуздук; Кыргыз Республикасынын маалыматтык коопсуздук концепциясы; жеке маалыматтар; электрондук башкаруу.

INFORMATION SECURITY IN THE KYRGYZ REPUBLIC: ISSUES OF LEGAL REGULATIONS

A.T. Alibaev, G.K. Toktogonova

Abstract. Information security is an integral part of national security and implies protection of an individual, society and the state from internal and external threats. In the context of active transformation of public relations

and formation of modern global information space, the issue of legal support for the national information security system does not lose its relevance. This article analyzes the leading domestic regulatory legal acts that have laid a solid foundation for the organization and development of the information security system. The analysis considers the issue of the legal relationship between the concepts of "information security" and "cybersecurity", identifies key modern threats emanating from the information space and violating the integrity of the entire state, as well as the features of international cooperation and multi-vector international policy in the field of standardization of information security tools.

Keywords: information; security; information security; Concept of information security of the Kyrgyz Republic; personal data; electronic governance.

Мировой тренд по “виртуализации” общественной жизни определяет качественную трансформацию общества посредством его динамичного встраивания в новое пространство информационно-цифровых технологий. Вместе с тем поступательный процесс цифровизации общественных отношений содержит глобальную угрозу несанкционированного использования информационных данных, что в результате приводит к подрыву целостности национальной безопасности государства. Кроме того, криминализация информационного пространства способствует потере деловой репутации отдельных организаций, значительным финансовым потерям и снижению их рыночной стоимости. В этой связи, развитие современного информационного общества требует разработки эффективной государственной политики в области обеспечения сохранности информации, а также нейтрализации угроз повсеместного использования информационных и телекоммуникационных технологий [1, с. 195]. Немаловажным аспектом обеспечения информационной безопасности на всех ключевых уровнях является прочная, систематизированная правовая основа, способствующая единообразному пониманию природы и роли информационной безопасности как непосредственного элемента национальной безопасности государства.

Современное состояние правового обеспечения информационной безопасности Кыргызской Республики (далее – КР) определяется отдельными нормативно-правовыми актами, содержащими требования по формированию единой политики управления информацией. Так, к основополагающим нормативным актам в сфере информационной безопасности относятся следующие:

1. Конституция Кыргызской Республики.
2. Законы КР: “О праве на доступ к информации”, “О кибербезопасности”, “Об информации персонального характера”, “Об электронном управлении”, “О защите государственных секретов”, “О средствах массовой информации” и др.
3. Концепция информационной безопасности КР.
4. Стратегия кибербезопасности КР на 2019–2023 годы.

Одним из приоритетных направлений в области обеспечения информационной безопасности КР является конституционно-правовое регулирование основных прав человека в информационной среде. В частности, конституционное право на получение объективной и достоверной информации закреплено в нескольких статьях Конституции КР. Так, в ст. 33 определено, что каждый имеет право свободно искать, получать, хранить, использовать и распространять информацию в любой форме (письменно или иным способом), получать информацию о деятельности государственных органов, органов местного самоуправления, их должностных лиц, а также государственных и муниципальных юридических лиц и иных организаций [2]. Право на доступ к информации содержится также в ст. 10 (“средствам массовой информации гарантируется право на получение информации от государственных органов, органов местного самоуправления”), в ст. 29 (“не допускается сбор, хранение, использование и распространение конфиденциальной информации, информации о частной жизни человека без его согласия, кроме случаев, установленных законом”), в ст. 37 (“граждане имеют право получать информацию о фактически расходуемых средствах из республиканского бюджета”) [2]. Важным условием эффективной реализации

конституционного права на доступ к информации является гарантированность его охраны и защиты. К примеру, в п. 5 ст. 29 отмечено, что государство гарантирует судебную защиту от неправомерного сбора, хранения, распространения конфиденциальной информации и информации о частной жизни человека, а также право на возмещение материального и морального вреда, полученного в результате таких неправомерных действий.

Таким образом, приведенные выше нормы составляют конституционно-правовую основу государственного регулирования в сфере информационных прав, а также свидетельствуют о преемственности КР к глобальному движению цифровизации общественной жизни.

В целях обеспечения реализации и защиты конституционного права на доступ к информации был принят ряд специальных законов, прямо или косвенно затрагивающих сферу информационной безопасности государства. Так, в Законе КР "О праве на доступ к информации" предусмотрены основополагающие гарантии данного права, к числу которых относятся:

1. Обязанность обладателей информации предоставлять и обнародовать информацию.
2. Определение обладателями информации специальных структурных подразделений или должностных лиц, организующих в установленном порядке доступ к информации, которой они владеют.
3. Максимальное упрощение процедуры подачи запроса и получения информации.
4. Доступ к открытым заседаниям коллегиальных органов субъектов государственного сектора.
5. Осуществление парламентского, общественного и государственного контроля за соблюдением права на доступ к информации.
6. Ответственность за нарушение законодательства о доступе к информации.
7. Иные меры, направленные на эффективную реализацию права на доступ к информации [3].

Кроме того, данный Закон устанавливает правила работы как с общедоступной информацией, так и с информацией, доступ к которой ограничен. В частности, в ст. 7 указано, что общедоступная информация не предполагает ограничения доступа к ней и может быть использована лицами по их усмотрению. При этом важным условием пользования такой информацией является соблюдение исключительных прав на объекты интеллектуальной собственности, а также ограничений, вводимых на различные формы ее обработки (к примеру, распространение, предоставление и др.).

В некоторых случаях право на доступ к информации может быть ограничено. Так, в ст. 8 Закона отмечается, что ограничение устанавливается в отношении:

1. Информации, содержащей государственные секреты;
2. Информации персонального характера;
3. Информации, содержащей сведения об оперативно-розыскной, внешней разведывательной и контрразведывательной деятельности, о производстве по уголовному делу в случаях, установленных законом в сфере оперативно-розыскной деятельности, уголовно-процессуальной деятельности;
4. Информации, содержащей охраняемую законом тайну (коммерческую, банковскую, нотариальную, врачебную, адвокатскую и др.);
5. Информации, содержащей индивидуальные данные, применяемые в официальной статистике [3].

Ограничение на доступ к информации устанавливается только на основании закона в целях защиты национальной безопасности, общественного порядка, охраны здоровья и нравственности населения, защиты прав и свобод других лиц. По справедливому замечанию некоторых экспертов, важным условием использования ограничительных мер, принимаемых в отношении информации, является соблюдение принципа соразмерности, т. е. их объем должен быть соразмерным ценности, на защиту которой направлено это ограничение [4, с. 18]. Это было учтено в п. 1 ст. 8 рассматриваемого Закона.

По своему содержанию информация ограниченного доступа предполагает специфичные правила ее обработки и дальнейшего использования. К примеру, в п. 6 ст. 8 Закона установлено, что при работе с информацией

ограниченного доступа для ознакомления предоставляется только та ее часть, которая не подлежит ограничению. В случае использования конфиденциальной информации обладатель может распространять ее только при условии наличия согласия лиц, которые ограничили доступ к этой информации (п. 7 ст. 8).

Наряду с вышеприведенными положениями Закон также определяет правовой статус субъектов в сфере доступа к информации, процедуру предоставления информации на основе запроса, особенности обнародования информации о деятельности субъектов государственного сектора и предоставления доступа к такой информации, организационные гарантии реализации права на доступ к информации и порядок обжалования отказа в предоставлении информации.

Возрастающие угрозы несанкционированного использования информации, в том числе "утечки" персональных данных, создают благоприятную почву для подрыва целостности информационной инфраструктуры государства и требуют принятия соответствующих системообразующих нормативно-правовых актов. Так, в области обеспечения защиты персональных данных в КР действует ряд законов и подзаконных актов, таких как: Закон КР "Об информации персонального характера" [5], Требования к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных [6], Положение "Об осуществлении контроля за использованием персональных данных, полученных органами государственной власти и органами местного самоуправления от других государственных держателей (обладателей) персональных данных" [7] и др.

Закон КР "Об информации персонального характера" (далее – Закон) определяет основные направления государственной политики в области работы с персональными данными, а также ключевые условия по их охране и защите от несанкционированного сбора, обработки и использования. Несомненным преимуществом Закона является разработанное определение персональных данных, согласно которому под персональными данными следует понимать "зафиксированную информацию на материальном носителе о конкретном человеке, отождествленную с конкретным человеком или которая может быть отождествлена с конкретным человеком, позволяющая идентифицировать этого человека прямо или косвенно, посредством ссылки на один или несколько факторов, специфичных для его биологической, экономической, культурной, гражданской или социальной идентичности" [5]. По справедливому замечанию некоторых исследователей, предложенное законодателями определение персональных данных представляется весьма обширным, поскольку включает практически любую информацию о человеке, которую можно использовать для его идентификации [8, с. 208]. Так, в Законе указано, что к персональным данным относятся следующие сведения: "биографические и опознавательные данные, личные характеристики, сведения о семейном положении, финансовом положении, состоянии здоровья и др." [5].

Положения ст. 5 Закона устанавливают правовые основы работы с персональными данными. В частности, любые операции в отношении персональных данных возможны только при условии: 1) получения письменного согласия их субъекта; 2) если они требуются для реализации органами государственной власти и органами местного самоуправления своих полномочий; 3) если они требуются для достижения законных интересов держателя персональных данных; 4) если они требуются для защиты законных интересов субъекта персональных данных; 5) если их обработка реализуется исключительно в творческих целях с обязательным соблюдением права на неприкосновенность частной жизни и свободы слова.

Кроме того, Законом определены права и обязанности не только субъектов персональных данных, но и их держателей и обработчиков. Важно заметить, что последние берут на себя обязательства по обеспечению охраны и защиты персональных данных от несанкционированных действий. В ст. 21 Закона предложен достаточно широкий перечень организационных и технических мер, необходимых для использования

в процессе работы с персональными данными. К числу таких мер, к примеру, относятся:

- исключение доступа посторонних лиц к оборудованию, используемому для обработки персональных данных;
- воспрепятствование самовольному чтению, копированию, изменению или выносу носителей данных;
- воспрепятствование самовольной записи персональных данных и изменению или уничтожению записанных персональных данных и обеспечение возможности установления задним числом, когда, кем и какие персональные данные были изменены;
- обеспечение безопасности систем обработки данных, предназначенных для переноса персональных данных независимо от средств передачи данных;
- обеспечение контроля за допуском;
- обеспечение возможности установления задним числом, когда, кем и какие персональные данные вводились в систему обработки данных;
- недопущение несанкционированного чтения, копирования, изменения и уничтожения персональных данных при передаче и транспортировке персональных данных;
- обеспечение конфиденциальности информации, полученной при обработке персональных данных и др. [5].

Безусловно, приведенные меры по защите персональных данных не являются исчерпывающими и требуют более детальной законодательной "проработки". В этой связи разработаны и утверждены ***Требования к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных*** (далее – Требования), содержащие уровни защищенности персональных данных в информационных системах, критерии современных угроз их безопасности, а также конкретные требования к обеспечению их безопасности и защиты. Так, согласно п. 4 Требований, выделяется четыре уровня защищенности персональных данных: синий, зеленый, желтый и красный. При этом "интенсивность" этих уровней проявляется в зависимости от наличия или отсутствия угроз безопасности персональных данных. Не вдаваясь в детальное изучение методики определения угроз безопасности персональных данных, следует отметить, что для каждого представленного уровня защищенности предусматриваются конкретные обязательные меры по возможной нейтрализации угроз и обеспечению требуемого уровня защищенности персональных данных. В частности, в п. 9 Требований отмечается, что синий уровень защищенности как менее подверженный негативному воздействию внешних и внутренних угроз требует, к примеру, разработки целостной политики в отношении обработки персональных данных, осуществления внутреннего контроля для выявления соответствия политики обработки персональных данных действующему законодательству, ведения учета лиц, имеющих непосредственный доступ к персональным данным и др. В свою очередь, наиболее "восприимчивым" к угрозам является красный уровень, и, соответственно, он требует более эффективных мер защиты персональных данных, к примеру, установление системы контроля помещений, ведение электронного журнала с обязательной фиксацией всех операций с персональными данными, проведение регулярного аудита информационных систем и др.

В целом отечественное законодательство о персональных данных представляется как единая согласованная система нормативно-правовых актов, обеспечивающих правовые гарантии защиты от неправомерных действий в отношении персональных данных и снижения риска деформации информационной безопасности государства. Учитывая достаточно динамичный характер ведущих нормативно-правовых документов в анализируемой сфере, стоит предположить о возможности исключения тех или иных законодательных пробелов и последующего повышения их практической эффективности.

В целях формирования наиболее ёмкого представления о сущности информационной безопасности в современных условиях целесообразно, по мнению авторов статьи, опираться на положения ***Концепции информационной безопасности Кыргызской Республики***

на 2019–2023 годы [9]. Этот документ имеет стратегическое значение, поскольку содержит целостный подход государства к формированию надежного и эффективного информационного пространства, отвечающего современным вызовам и угрозам. Преимуществом Концепции является разработка понятийного аппарата с учетом таких элементов, как "цифровая экономика", "электронное управление", "электронное правительство" и др. Так, под информационной безопасностью Концепция предлагает понимать "состояние защищенности личности, общества и государства от информационных угроз" [9]. Несмотря на достаточно широкий подход законодателя к выявлению сущности информационной безопасности, отраженный в данном определении, следует отметить позитивное влияние четко обозначенного определения в процессе анализа его роли и места в системе государственной политики.

Среди несомненных позитивных моментов, отраженных в Концепции, выявление и обозначение ключевых проблем, возникающих в отечественном информационном пространстве. В частности, к таким проблемам Концепция относит: использование информационных каналов и ресурсов экстремистскими и террористическими организациями; распространение киберпреступности; информационное манипулирование общественным сознанием, противоречащее национальным интересам КР; значительное снижение конкурентоспособности отечественного информационного контента и др. Основной "посыл" Концепции заключается в разработке и реализации мер, обеспечивающих не только нейтрализацию указанных угроз, но и эффективную защиту прав личности, общества и государства в информационной среде. В п. 34 Концепции подчеркивается, что она направлена на "создание эффективной национальной системы обеспечения информационной безопасности КР, представляющей собой совокупность правовых, организационных и экономических методов по реализации государственной политики в данной сфере" [9]. Это положение позволяет сделать вывод о том, что государственная политика в рассматриваемой сфере носит системный и комплексный характер.

Повсеместное использование информационных технологий неизбежно ведет к росту деструктивного воздействия на информацию, обращаемую в кибернетическом пространстве (киберпространстве). В этой связи, система информационной безопасности должна "отвечать" новым угрозам и вызовам, формируя дополнительные меры защиты.

Актуальным на сегодняшний день остается вопрос соотношения понятий "информационная безопасность" и "кибербезопасность". Так, большинством исследователей отмечается, что несмотря на некоторую схожесть данных понятий, имеются принципиальные значения в их содержании [10, с. 90]. В частности, кибербезопасность сосредоточена на защите информации, исходящей исключительно в цифровой форме, в то время как информационная безопасность направлена на защиту любой информации вне зависимости от источника ее происхождения. Кроме того, международное сообщество признает кибербезопасность в качестве самостоятельного элемента информационной безопасности, нуждающегося в постоянном анализе и мониторинге на предмет выявления и минимизации киберрисков [11].

Принимая во внимание исключительную важность обеспечения эффективной защиты цифровых информационных ресурсов, в КР принято несколько стратегических документов, обеспечивающих единую правовую основу для организации и развития отечественной системы кибербезопасности. Так, Закон КР *"О кибербезопасности Кыргызской Республики"* определяет кибербезопасность как "сохранение свойств целостности, которая может включать аутентичность и отказоустойчивость, доступности и конфиденциальности информации в объектах информационной инфраструктуры, обеспечиваемое за счет использования совокупности средств, стратегий, принципов обеспечения безопасности, гарантий безопасности, подходов к управлению рисками и страхования, профессиональной подготовки, практического опыта и технологий" (ст. 2) [12]. Как видно, в данном определении законодателем предпринята попытка показать системный характер государственной политики в области обеспечения

кибербезопасности посредством включения таких стратегически важных элементов, как принципы обеспечения безопасности, управление рисками, требования к профессиональной подготовке и практическому опыту субъектов системы и др. Здесь также говорится об информации, находящейся в объектах информационной инфраструктуры, под которой законодателем понимается "совокупность информационных систем, информационно-телекоммуникационных систем, сетей электросвязи, сетей электросвязи общего пользования КР, баз данных, центров обработки данных и автоматизированных систем управления, используемых для формирования, создания, преобразования, передачи, использования и хранения информации, а также управления технологическими процессами". Анализируя эти определения, можно сделать вывод о том, что кибербезопасность направлена на защиту той информации, которая обращается в цифровой информационной среде и имеет цифровую форму.

Эффективность обеспечения кибербезопасности достигается комплексным использованием организационно-технических мер, направленных на защиту цифровых данных. Так, в ст. 5 Закона отмечается, что КР использует системный подход в сфере обеспечения кибербезопасности, т. е. привлекает современные силы и средства для своевременного предупреждения, выявления, реагирования и минимизации последствий от киберинцедентов и кибератак. Под средствами обеспечения кибербезопасности понимается программное обеспечение, технические и другие средства. В свою очередь, силы обеспечения кибербезопасности включают в себя государственные органы и различные организации, отвечающие за эффективную борьбу с киберугрозами.

Принимая во внимание возможность проведения кибератак на объекты критической инфраструктуры, отечественным законодателем предусмотрена практика ведения единого реестра киберугроз, позволяющая своевременно информировать заинтересованных лиц о существующих угрозах в киберпространстве. Согласно ст. 13 Закона, создание и ведение такого реестра возлагается на уполномоченный государственный орган в сфере обеспечения кибербезопасности – Государственный комитет национальной безопасности КР (далее – ГКНБ). Единый реестр киберугроз представляет собой сводный перечень сведений не только о существующих киберугрозах, но и вредоносном программном обеспечении, ключевых угрозах информационной безопасности и уязвимостях информационной инфраструктуры.

Ведение единой базы киберугроз является не единственным действенным механизмом в борьбе с кибератаками и киберинцедентами. Так, ст. 15 Закона предлагается проведение аудита кибербезопасности – комплексной документированной проверки количественных и качественных показателей текущего состояния кибербезопасности объектов критической инфраструктуры. Аудит кибербезопасности проводится на систематической основе и может быть трех видов – внутренним, государственным и независимым. Каждый вид аудита отличается не только содержанием контрольных мероприятий, но и субъектным составом. К примеру, государственный аудит проводится ГКНБ в отношении объектов критической инфраструктуры. В свою очередь, независимый аудит осуществляется аккредитованными юридическими лицами и проводится в отношении объектов критической инфраструктуры.

Таким образом, Закон в сфере обеспечения кибербезопасности предполагает создание необходимых условий для формирования единого киберпространства, отвечающего современным вызовам и угрозам, а также комплексной защиты цифровых ресурсов от кибератак и киберинцидентов.

Комплексный и системный характер государственной политики в области обеспечения кибербезопасности отражается также в *Стратегии кибербезопасности КР*, принятой на 2019–2023 годы. Этот фундаментальный документ формирует доктринальную основу реализации многовекторной деятельности субъектов, участвующих в системе национальной кибербезопасности, а также единую политику в области защиты данных от возможных кибератак, тестирования и сертификации средств защиты информации. Не вдаваясь в детальное изучение

содержания Стратегии, следует отметить важную ее особенность. Так, заложенная в ее основе идея о создании единой системы обеспечения кибербезопасности предполагает не только модернизацию существующих национальных механизмов, но и активное использование международного опыта в сфере технической стандартизации в области безопасности киберпространства. В частности, в п. 5.8 Стратегии отмечается, что для повышения отечественного потенциала в сфере кибербезопасности информационных технологий целесообразно обратить внимание на необходимость гармонизации национальных стандартов с аналогичными международными стандартами, включая "профильные стандарты ISO/МЭК, IEEE, стандарты стран ЕАЭС, а также документы Рабочей группы по проектированию Интернет (IETF)" [13].

Подытоживая анализ ведущих нормативно-правовых актов в сфере обеспечения информационной безопасности, необходимо отметить следующее. В условиях активного перехода к цифровым общественным отношениям возрастает актуальность правового обеспечения безопасности информационных ресурсов и создаются предпосылки для институционализации таких элементов, как искусственный интеллект, блокчейн, цифровые активы, большие данные и др. Действующее национальное законодательство в области информационной безопасности отличается своей новизной, что подтверждается сформированностью понятийного аппарата и включением таких определений, как критическая информационная инфраструктура, кибер-инцидент, аудит кибербезопасности и др. Кроме того, правовое регулирование национальной системы информационной безопасности предполагает создание прочной нормативной основы для реализации комплексной, единой и системной государственной политики в борьбе с современными информационными угрозами. В процессе организации системы информационной безопасности отечественный законодатель исходит, прежде всего, из понимания важности обеспечения защиты прав и интересов человека, общества и государства в цифровой среде, а также необходимости координации усилий для эффективной борьбы с цифровыми преступлениями. Важным аспектом комплексной работы с информационными ресурсами признается также многовекторное международное сотрудничество, в том числе в сфере стандартизации средств защиты информации, гармонизации национальных стандартов с аналогичными международными стандартами и т. д.

Поступила: 19.03.2025;
рецензирована: 02.04.2025; принята: 04.04.2025.

Литература

1. *Пелевина Е.С.* Особенности системы информационной безопасности как элемента международной безопасности в современном мире // Теории и проблемы политических исследований. 2017. № 6.
2. Конституция Кыргызской Республики. Принята референдумом (всенародным голосованием) 11 апреля 2021 года. Ст. 33.
3. Закон Кыргызской Республики "О праве на доступ к информации" от 29 декабря 2023 года № 217. Ст. 5.
4. *Голованов Д.* Комментарии к проекту Концепции информационной безопасности Кыргызской Республики на 2019–2023 годы. М., 2019.
5. Закон Кыргызской Республики "Об информации персонального характера" от 14 апреля 2008 года № 58 (в редакции Закона КР от 12 июля 2022 года № 61).
6. Требования к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных (в редакции Постановления Кабинета Министров от 27 сентября 2022 года № 536).
7. Положение "Об осуществлении контроля за использованием персональных данных, полученных органами государственной власти и органами местного самоуправления от других государственных держателей (обладателей) персональных данных". Принято постановлением Кабинета Министров Кыргызской Республики от 22 марта 2023 года № 158.
8. *Машекуашева М.Х.* Правовое регулирование персональных данных в России / М.Х. Машекуашева, Л.В. Геляхова // Проблемы

экономики и юридической практики. 2020. Т. 16. № 5.
9. Концепция информационной безопасности Кыргызской Республики на 2019–2023 годы. Принята Постановлением Правительства Кыргызской Республики от 3 мая 2029 года № 209.
10. *Козлова Н.Ш.* Кибербезопасность и информационная безопасность: сходства и отличия / Н.Ш. Козлова, В.А. Довгаль // Вестник Адыгейского государственного университета. 2021. Вып. 3 (286).
11. *Голубчиков Д.М.* Квантовая криптография: принципы, протоколы, системы / Д.М. Голубчиков, К.Е. Румянцев. М., 2008.
12. Закон Кыргызской Республики “О кибербезопасности Кыргызской Республики” от 17 июля 2024 года № 121.
13. Стратегия кибербезопасности Кыргызской Республики на 2019–2023 годы. Утверждена Постановлением Правительства Кыргызской Республики от 24 июля 2019 года № 369.