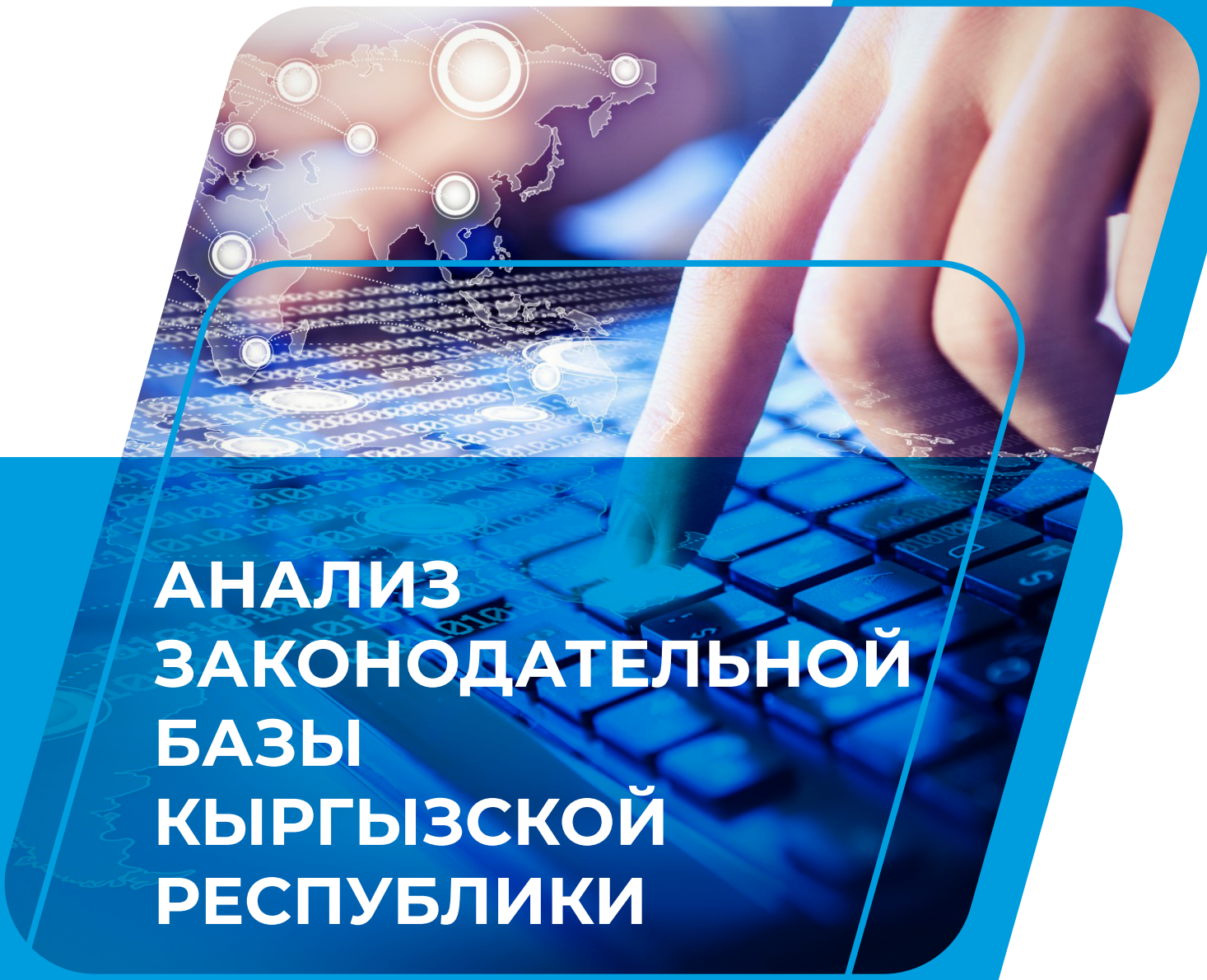
ГРАЖДАНСКАЯ ИНИЦИАТИВА
ИНТЕРНЕТ ПОЛИТИКИ



АНАЛИЗ ЗАКОНОДАТЕЛЬНОЙ БАЗЫ КЫРГЫЗСКОЙ РЕСПУБЛИКИ

В ОБЛАСТИ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

БИШКЕК, СЕНТЯБРЬ 2022

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Быстрые и системные цифровые преобразования, происходящие во всех сферах жизнедеятельности с особой остротой определяют необходимость эффективного обеспечения безопасности в информационной среде. Это касается и Кыргызской Республики, ее экономики, промышленности, социального сектора, правоохранительной деятельности, системы государственных услуг и государственного управления. Повсеместное внедрение в общественные отношения современных информационно-коммуникационных технологий (ИКТ) и растущее использование сети Интернет требует широкого диапазона мер в области сетей связи, их кибербезопасности и противодействия киберпреступности. Процессы цифровой трансформации управления, наряду с цифровыми преобразованиями бизнеса и общества нуждаются в комплексном, актуальном и гибком нормативном правовом обеспечении вопросов безопасности.

Данное исследование направлено на проведение анализа существующей нормативной правовой базы Кыргызской Республики, регулирующей вопросы обеспечения кибербезопасности на предмет его полноты и актуальности. Результаты анализа должны показать пробелы и коллизии и очертить возможные будущие направления и подходы в нормативном правовом регулировании сферы кибербезопасности. В ходе исследования ставилась также задача выработки оптимальных рекомендаций для совершенствования и гармонизации законодательства, на основе лучших международных практик или подходов в области обеспечения кибербезопасности.

В целом настоящий обзор основан на необходимости наиболее полного изучения правовой системы страны, например в части, затрагивающей вопросы как регулирования критической информационной инфраструктуры; уголовно-правового преследования за преступления в сфере информационно- коммуникационных технологий и компьютерной криминалистики. При работе над ним авторы исходили из изучения содержательного толкования относимости того или иного нормативного установления к тематике кибербезопасности. При анализе был соблюден принцип иерархичности нормативных правовых актов Кыргызской Республики.

ЗАКОНОДАТЕЛЬСТВО КР В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

В ходе настоящего правового анализа были изучены следующие нормативные правовые акты Кыргызской Республики в сфере информатизации, перехода к электронному управлению, регулирования вопросов обеспечения кибербезопасности:

Уровни законодательства	Описание
Стратегические рамки	1. Стратегия кибербезопасности Кыргызской Республики на 2019-2023 годы. 2. Национальная стратегия развития Кыргызской Республики на 2018-2040 годы. 3. Концепция информационной безопасности Кыргызской Республики на 2019-2023 годы. 4. Концепция цифровой трансформации «Цифровой Кыргызстан 2019-2023». 5. Концепция национальной безопасности Кыргызской Республики.
Кодифицированное законодательство	1. Уголовный кодекс КР. 2. Уголовно-процессуальный кодекс КР. 3. Кодекс о нарушениях КР.
Законы КР	1. Закон КР «Об электронном управлении». 2. Закон КР «Об информации персонального характера». 3. Закон КР «О защите государственных секретов Кыргызской Республики».
Подзаконные акты	Нормативные правовые акты подзаконного характера (изданные на уровне Правительства Кыргызской Республики), регламентирующие общественные отношения в цифровой среде.

СТРАТЕГИЧЕСКИЕ РАМКИ

Основополагающим и доктринальным документом в области обеспечения кибербезопасности является Стратегия кибербезопасности Кыргызской Республики на 2019-2023[1] годы, утвержденная постановлением Правительства КР от 24 июля 2019 года №369. Целью документа является формирование отечественной системы и политики кибербезопасности позволяющей защитить жизненно важные интересы государства в киберпространстве и обеспечить устойчивое социально-экономическое развитие, включая цифровую трансформацию экономики.

Это первый стратегический документ, который проясняет суть многих терминов в сфере информатизации, упорядочивает субъекты информационной деятельности, определяет методы обеспечения безопасности информационной сферы и ключевые направления деятельности для формирования единой государственной политики в области обеспечения кибербезопасности. Данную стратегию и план мероприятий пока следует рассматривать как единственное руководство по разработке и принятию комплекса нормативных правовых актов Кыргызской Республики в области кибербезопасности. Стратегия содержит план подробных мероприятий, нацеленных на укрепление координацию, полноценную и эффективную защиту объектов критической информационной инфраструктуры.

Приоритетом документа определены взаимодействие и координация на национальном уровне. Это включает в себя такие меры как создание координационной и консультационной «площадки» при Правительстве КР по вопросам кибербезопасности, определение в качестве органа уполномоченного в области обеспечения кибербезопасности центра по кибер и информационной безопасности при Государственном комитете по национальной безопасности (ГКНБ), и координация деятельности Национального центра по реагированию на компьютерные инциденты.

[1] http://cbd.minjust.gov.kg/act/view/ru-ru/15479

Другим приоритетным направлением является безопасность критической информационной инфраструктуры (КИИ). Стратегия устанавливает меры и задачи по определению секторов и объектов КИИ, а также критериев обеспечения безопасности. Еще одно важное направление – выстраивание системы предупреждения, реагирования и управления компьютерными инцидентами. Эти усилия охватывают требования взаимодействия с координационными центрами и центрами реагирования на инциденты, создание единого репозитария данных уязвимостей, и определение планов действий в случае чрезвычайных ситуаций. Еще одним тематическим приоритетом является формирование системы защиты информации, включая криптографическую защиту.

Кроме этого, Стратегия ставит целью криминализацию составов компьютерных преступлений в Уголовном кодексе КР в соответствии с международными подходами к борьбе с киберпреступностью, а также закрепление в Уголовно-процессуальном кодексе КР понятий, методов и средств компьютерной криминалистики, цифровых доказательств.

Кроме Стратегии кибербезопасности, Кыргызской Республикой приняты несколько связанных стратегических документов национального уровня, в которых также очерчены цели кибербезопасности. В них прослеживаются смешанные подходы, которые с одной стороны четко выделяют кибербезопасность как отдельно взятая стратегическая цель на уровне технической защиты, а с другой стороны, рассматривают кибербезопасность как составную и взаимосвязанную часть более широкой цели информационной безопасности исходящей в целом из вопросов защищенности информационной сферы.

На самом высоком уровне планирования Н**ациональная стратегия развития Кыргызской Республики на 2018–2040 годы**[2] (принятая 31 октября 2018 года) упоминает кибербезопасность достаточно кратко. Пункт 4.5 Стратегии предусматривает необходимость сосредоточения усилий на критически важных направлениях, таких как обеспечение кибербезопасности информационно-коммуникационных технологий, а также информационных систем, создание системы реагирования на киберугрозы и киберинциденты.

[2] https://www.gov.kg/storage/2020/01/-files/program/8/natsional-naya_strategiya_razvitiya_kyrgyzskoy_respubliki_na_2018_2040_gody.pdf

Концепция цифровой трансформации «Цифровой Кыргызстан 2019-2023»[3] (одобрена 14 декабря 2018 года) содержит небольшой раздел, посвященный обеспечению кибербезопасности при использовании технологий. При этом вопросы кибербезопасности ограничиваются общими описанием приоритетов, включая разработку системного подхода к укреплению кибербезопасности, формирование единой политики, и развитие национального технического потенциала с учетом международной практики и расширением партнерских взаимоотношений. Опосредованно, Концепция предусматривает меры, направленные на ускорение цифровизации в государственных структурах, что должно сопровождаться мерами по обеспечению безопасности объектов критической информационной инфраструктуры.

Концепция национальной безопасности Кыргызской Республики[4] (от 20 декабря 2021 года) также рассматривает вопросы кибербезопасности в тесной связке с общими вопросами информационной безопасности. Несмотря на это, среди задач кибербезопасности выделены обеспечение бесперебойной, устойчивой и защищенной эксплуатации сетей связи, повышение уровня защищенности государственных ИКТ систем и объектов КИИ, создание условий для эффективного предупреждения и оперативного выявления/пресечения киберпреступлений.

В схожем ключе **Концепция информационной безопасности Кыргызской Республики на 2019-2023 годы**[5] (от 3 мая 2019 года), выставляет в качестве основных направлений информационной безопасности несколько задач кибербезопасности – однако их перечень полностью дублирует приоритеты, уже указанные в Стратегии кибербезопасности.

[3] https://www.gov.kg/storage/2020/12/files/program/12/kontsept-siya_tsifrovoy_transformatsii_tsifrovoy_kyrgyzstan_2019_2023.doc
[4] hhttp://cbd.minjust.gov.kg/act/view/ru-ru/430815
[5] http://cbd.minjust.gov.kg/act/view/ru-ru/13652

КЛЮЧЕВЫЕ ЗАКОНЫ

Законодательство Кыргызской Республики содержит ряд нормативных правовых актов, прямо или косвенно затрагивающих вопросы кибербезопасности. Однако специальных законов, непосредственно направленных на регламентацию деятельности и процессов обеспечения кибербезопасности, пока не принято. Как такового, отдельного закона по кибербезопасности не имеется и некоторые функции такого закона в настоящее время выполняет Стратегия кибербезопасности. Следует подчеркнуть, что в данной Стратегии предусмотрена разработка и принятие до конца 2023 года отдельного Закона о безопасности критической информационной инфраструктуры, а также связанных подзаконных актов.

Кроме этого, существует небольшая база законодательства, косвенно затрагивающего необходимость правового обеспечения кибербезопасности. Прежде всего, эта база включает в себя законы об электронном управлении и защите персональных данных. К примеру, **в Законе КР «Об электронном управлении»**[6] от 19 июля 2017 года №127 в качестве одной из задач электронного управления определена необходимость обеспечения информационной безопасности. Также отмечено, что защита прав обладателя информации осуществляется в том числе путем внедрения технических мер защиты информации. Кроме того, концептуальные определения кибербезопасности затронуты при описании функций единой идентификационной системы, включая идентификации, аутентификации, авторизации, проверки подлинности ключей, обеспечения достоверности данных.

В Законе КР «Об информации персонального характера»[7] от 14 апреля 2008 года № 58, также прописаны общие требования, касающиеся обеспечения технической безопасности данных, действующие в отношении держателей (обладателей) массива персональных данных и обработчика. В частности законом прописаны разные категории контроля данных – за доступом, за пользованием, за записью и вводом, за средствами передачи и транспортным контролем, за допуском. К примеру, обязанностью держателей и обработчика является обеспечение безопасности любых систем обработки данных, предназначенных для переноса персональных данных независимо от средств передачи данных.

Правовое регулирование кибербезопасности также имеет взаимосвязи с законодательством по защите государственных секретов, коммерческой тайне и криптографии. Однако, многие подзаконные акты не доступны для публичного ознакомления. Регулирующие данные области нормативные акты в большинстве своем также отнесены к документам для служебного пользования, доступ к которым ограничен.

[6] http://cbd.minjust.gov.kg/act/view/ru-ru/111634?cl=ru-ru
[7] http://cbd.minjust.gov.kg/act/view/ru-ru/202269

КОДИФИЦИРОВАННОЕ ЗАКОНОДАТЕЛЬСТВО

Отдельным аспектом законодательства КР по вопросам кибербезопасности являются кодексы, прописывающие ответственность за совершение преступлений в сфере кибербезопасности. Принятый в октябре 2021 года новый Уголовный кодекс КР также, как и предыдущие редакции кодекса содержит ряд специальных норм по киберпреступлениям. Уголовный кодекс уточняет понятие преступлений против кибербезопасности и содержит девять статей, в диспозиции которых компьютерные системы или иные технические средства определяются как объект или элемент объективной стороны преступления. Четыре статьи, непосредственно относящихся к киберпреступности выделены в отдельную главу «Преступления против кибербезопасности» (319-322).

Следующим правовым актом, устанавливающим ответственность в этой сфере, является **Кодекс о правонарушениях Кыргызской Республики** (от 28 октября 2021 года № 128). В главе 26, Кодекс содержит две статьи, касающиеся правонарушений в сфере информационной безопасности, а именно «Неправомерный доступ к компьютерной информации» и «Нарушение требований по защите информации персонального и коммерческого характера». Следет отметить, что специальные нормы Кодекса о нарушениях не отвечают современным и потенциальным угрозам в киберпространстве.

ПОДЗАКОННЫЕ АКТЫ

На уровне подзаконных актов сфера кибербезопасности регулируется несколькими ключевыми постановлениями и требованиями.

В соответствии с постановлением Правительства Кыргызской Республики **«О некоторых вопросах в сфере обеспечения кибербезопасности Кыргызской Республики»** от 21 мая 2020 года №266 Правительство Кыргызской Республики возложило на Координационный центр по обеспечению кибербезопасности, который является структурным подразделением Государственного комитета национальной безопасности Кыргызской Республики, функцию координации деятельности государственных органов, центров реагирования на компьютерные инциденты (ведомственные, отраслевые и иные) по обеспечению кибербезопасности, выявлению, предупреждению и пресечению компьютерных атак, реагированию на компьютерные инциденты.

Требования к защите информации, содержащейся в базах данных государственных информационных систем, (утвержденные постановлением Правительства Кыргызской Республики от 21 ноября 2017 года № 762) определяют меры по защите информации, а также государственных информационных системах и обеспечения безопасности информации, содержащейся в их базах данных. В частности, устанавливаются требования к использованию информационных технологий, к организации кибербезопасности, к информационным системам, к прикладному программному обеспечению, к технологическим платформам, к аппаратно-программным комплексам, к сетям телекоммуникаций, к системам бесперебойного функционирования технических

средств серверного оборудования и к серверному помещению. Таким образом данное постановление практически регламентирует все основные практические аспекты, касающиеся защиты данных и обеспечения кибербезопасности в государственных информационных системах.

На данный документ также ссылается ряд связанных подзаконных актов технического характера, как например **Требования к порядку формирования, актуализации и использования базовых государственных информационных ресурсов (от 6 февраля 2020 года № 66) и Требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем** (от 31 декабря 2019 года № 744).

Требования к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных (утвержденные постановлением Правительства Кыргызской Республики от 21 ноября 2017 года № 760) устанавливают уровни защищенности персональных данных при их обработке в информационных системах, критерии угроз безопасности персональных данных, вошедших в перечень угроз, а также требования к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных. Требования обязательны для всех государственных органов, и держателей массива персональных данных. Данный документ является первым подзаконным актом, использующим принципы управления рисками кибербезопасности, определяя требования к защите в зависимости от уровня угроз и потенциального вреда.

ПРОБЕЛЫ В ПРАВОВОМ ОБЕСПЕЧЕНИИ СФЕРЫ КИБЕРБЕЗОПАСНОСТИ

В целом анализ действующего законодательства в сфере информационной и кибербезопасности, за исключением Стратегии кибербезопасности позволяет делать выводы о том, что оно не определяет правовые рамки, основополагающие принципы и единые подходы в вопросе обеспечения кибербезопасности КР, позволяющие выстроить единую «систему координат» для государственной политики в области обеспечения кибербезопасности.

Например, на уровне стратегий и концепций, текущая Стратегия кибербезопасности в целом выполняет задачу выставления общих рамок политики и законодательного обеспечения. Однако, прослеживаются недостатки, которые выражаются в наличии перекоса с точки зрения выстраивания архитектуры ключевых игроков, входящих в государственную систему обеспечения кибербезопасности, и определения их зон ответственности. Стратегия предусматривает значительную милитаризацию системы кибербезопасности Кыргызстана, не принимая во внимание деятельность гражданских государственных органов и частных структур. В документе не учтены возможные преимущества государственно-частного партнерства в этой области.

Законодательство также представляет собой неполную и устаревшую нормативную базу, поскольку большинство законов были сформированы в принципиально иной технологической и социальной среде, и в силу этого не учитывают современных трендов в сфере кибербезопасности.

На уровне законов, главным пробелом на данный момент, уже обозначенным в Стратегии кибербезопасности является отсутствие закона и защите критической инфраструктуры. Вследствие этого до сих пор законодательно не определены секторы, отрасли и сферы деятельности, в которых функционируют объекты критической информационной инфраструктуры, в том числе государственные системы. Также не утверждены критерии и параметры, определяющие принадлежность объектов к критической информационной инфраструктуре и не установлены обязательные требования по обеспечению безопасности их объектов для операторов критической информационной инфраструктуры.

Если исходить из того, что государственные информационные системы будут составлять существенную часть объектов критической информационной инфраструктуры, а компьютерные атаки в массе своей будут нацелены именно на государственные инфраструктуры – такие вызовы требуют создания надежной системы борьбы с компьютерными атаками на объекты критической информационной инфраструктуры посредством принятия ключевого закона и сопутствующего пакета актов Правительства.

В законодательстве не содержится выверенного и гармоничного свода терминов и определений, связанных с важными компонентами регулирования. Как следствие, законодательство не обеспечивает эффективный контроль обеспечения прав субъектов правовых отношений в сфере кибербезопасности.

В целом в Кыргызской Республике не создан ряд базовых правовых условий, опорных точек, без которых невозможно обеспечить безопасность цифровой трансформации, в частности, и развитие национальной отрасли ИТ и связи в целом. Имеются существенные пробелы в системе нормативных правовых актов и политик обеспечения кибербезопасности, примерами чего являются отсутствие концепций и подходов к реагированию на компьютерные инциденты, обеспечению безопасности критической инфраструктуры и автоматических систем управления технологическими процессами, международному сотрудничеству в области обеспечения кибербезопасности.

В тех нишах и направлениях государственной политики, где система нормативных правовых актов и заданных ими подходов присутствует, наблюдается ее неполнота и отставание от актуальных тенденций развития ИКТ и кибербезопасности (противодействие компьютерной преступности, регулирование в области защиты информации, техническая стандартизация в области ИТ). Также не выстроен подход к повышению уровня компьютерной гигиены и цифровой грамотности, а также в целом к наращиванию потенциала и использованию человеческих ресурсов в рамках государственной политики по обеспечению кибербезопасности.

Еще одна группа пробелов связана с тем, что в действующем уголовном законодательстве отсутствуют составы совершаемых киберпреступлений, а в процессуальном законодательстве – методы поиска, фиксации и оценки цифровых доказательств.

Как отдельный вызов, остаются не реализованными положения Стратегии, касающиеся:
- вопросов криминализации составов компьютерных преступлений в соответствии с международными подходами к борьбе с киберпреступностью;
- методов и средств компьютерной криминалистики, введение в нормативные правовые акты понятия цифрового доказательства, описание и изложение его критериев, характеристик и способов фиксации;

- обеспечения признания юридической силы цифровых доказательств наравне с другими доказательствами;
- гармонизации законодательства КР в части криминализации составов и расследования компьютерных преступлений, трансграничной выдачи с территории КР лиц, подозреваемых в совершении компьютерных преступлений, либо осужденных за их совершение на территории зарубежных государств;
- рассмотрение возможности привлечения частных компаний к сбору цифровых доказательств и проведению судебных экспертиз по цифровым доказательствам для правоохранительных органов Кыргызской Республики.

Поскольку Кыргызская Республика еще не сталкивалась с большим количеством судебных дел о киберпреступлениях, ограниченный потенциал представителей правоохранительных и судебных органов в этой области может потенциально привести к неэффективным расследованиям, преследованиям и приговорам, что позволит киберпреступникам оставаться безнаказанными и продолжать свою преступную деятельность.

Проблема уголовно-правовой оценки киберпреступности вытекает из слабой законодательной основы, сложности сбора доказательств и самого процесса доказывания, недостатка компетентных лиц в области цифровых технологий в органах государственной власти, отсутствия обобщенной судебной системы и иных факторов, влияющих на развитие противодействия киберпреступности[8] . Как следствие, в дополнение к укреплению законодательной базы, важно повышать потенциал системы уголовного правосудия в успешной борьбе и предупреждении киберпреступлений.

Принятые шаги по модернизации законодательной базы юридической ответственности за киберпреступления в целом еще недостаточны, так как не позволяют успешно пресекать киберпреступления, объективно оценить масштабы киберпреступности; и выстроить эффективную правовую базу для противодействия киберпреступности.

Например, в Уголовном кодексе, некоторые квалифицирующие признаки киберпреступлений, предусмотренных соответствующей Главой, уже охватываются признаками других составов преступлений. Некоторые составы преступлений иных категорий, помимо указанной Главы, не содержат квалифицирующих признаков совершения преступлений с использованием Интернет, компьютерных технологий. Следует отметить, что изучение норм Уголовного кодекса показали, что разработчики действующей редакции Уголовного кодекса Кыргызской Республики при формировании данной главы за основу взяли диспозиции статей 304-306 Уголовного кодекса в редакции 2017

[8] Киберпреступность: риски и угрозы: материалы Всероссийского студенческого круглого научно-практического стола с международным участием (Санкт-Петербург, 2021). Под ред. д-ра юрид. наук, доцента Е. Н. Рахмановой. – СанктПетербург :Астерион, 2021. – 22 стр.

года и статей 159-160 Кодекса о проступках, которые на сегодняшний день признаны утратившими силу.

Кроме того, совершение многих других злонамеренных деяний (как например онлайн мошенничество, кража данных, преступные деяния, связанные с персональными данными) остались вне уголовно-правового регулирования. Соответственно такие деяния сегодня не влекут за собой уголовного преследования, хотя большинство стран мира, основываясь на правоприменительной практике и опыте расследования преступлений, определили вышеуказанные виды преступлений в качестве уголовно-наказуемых деяний. Будапештская Конвенция о компьютерных преступлениях от 2001 года, определила исчерпывающий перечень деяний, которые государствам следует квалифицировать в качестве уголовных преступлений.

Специальные термины, используемые в Уголовном кодексе, не соответствуют терминологическому глоссарию, используемому в специальных международных актах и стратегических документах в области кибербезопасности, а также в национальном законодательстве, регулирующем сектор связи и телекоммуникаций. Данные обстоятельства могут негативно отразиться в вопросах международного сотрудничества и в целом не позволит адекватно гармонизировать отечественное законодательство с международным.

Превентивная функция уголовной юстиции предполагает необходимость детализированного подзаконного нормативного регулирования, целью которого является снижение или устранение применения уголовных санкций для участников гражданского оборота. То есть, правительству необходимо установить подробную регламентацию отношений между субъектами использования массивов информации и пользователями, среди которых, наряду с добросовестными пользователями, существуют и лица с преступными целями или наклонностями. Объекты информационной инфраструктуры должны иметь не только надежную уголовно-правовую защиту от преступных посягательств, но и систему предотвращающую и предупреждающую совершение правонаруше-ний и преступлений.

Специальные нормы Кодекса о нарушениях не отвечают современным и потенциальным угрозам в киберпространстве. Требуется кардинальный пересмотр главы 26 Кодекса о правонарушениях, в том числе через призму необходимости создания условий для уголовно-правовой защиты от нарушения существующих требований законодательства в области защиты информации персонального характера. Существует конкуренция правовых норм Уголовного кодекса и Кодекса о нарушениях в части преюдиции. Используемые термины не соответствуют терминологии действующего уголовно-правового законодательства, международных актов и требований.

Несмотря на значительное возрастание количества правонарушений, связанных с использованием цифровых технологий или совершаемых в сфере информационных технологий, Уголовно-процессуальное и гражданско-процессуальное законодательство Кыргызской Республики до сих не содержат норм, касающихся идентификации, сбора, исследования и закрепления цифровых доказательств. Отсутствуют и конкретные положения, устанавливающие четкие процедуры, защитные меры и принципы и порядок проведения расследований с использованием цифровых доказательств.

Поскольку одним из ключевых моментов при расследовании киберпреступлений и проведении цифровой экспертизы является сохранение целостности электронных доказательств и обеспечение их подлинности и допустимости использования в качестве доказательств в соответствующем уголовном или гражданском судопроизводстве, принципиальное значение имеют такие вопросы, как порядок хранения и передачи доказательств и создание криминалистических копий. Исходя из этого следует уделять первоочередное внимание совершенствованию специальных методов расследования, предназначенных не только для сбора электронных доказательств[9] .

В условиях цифровой трансформации многих секторов общественных отношений остается открытым вопрос разрешения гражданских споров. Гражданско-процессуальное законодательство не имеет основы для собирания электронных (цифровых) доказательств.

Также обилие нормативных правовых актов в области связи, цифровизации и телекоммуникаций ведет к неоднозначному толкованию многих терминов и определений, а разрозненность субъектов информационного рынка, ответственных за обеспечение информационной безопасности, мешает проведению четкой политики в этой сфере.

[9] Доклад о работе совещания Группы экспертов для проведения всестороннего исследования проблемы киберпреступности. Вена, 2020, стр. 20/27

ПРИМЕНИМАЯ МЕЖДУНАРОДНАЯ ПРАКТИКА

Кыргызстан значительно отстает от мировых тенденций в области кибербезопасности. Сегодня парадигма обеспечения кибербезопасности начала меняться и все больше государств и компаний приходят к пониманию, что построение защиты, которую нельзя сломать практически невозможно. Кроме защиты информации все больше говорится об обеспечении киберустойчивости, суть которой заключается в обеспечении бесперебойного и устойчивого функционирования информационной инфраструктуры в условиях существования постоянных рисков кибербезопасности. Тем самым основные усилия необходимо направить на проектирование систем с учетом требований обеспечения их киберустойчивости, которая подразумевает способность быстрого восстановления после киберинцидентов.

Более того, современные тенденции кибербезопасности уже выходят за пределы традиционных подходов защиты информации, в том числе киберустойчивости. Широко используется термин **«цифровая устойчивость»,** которая предполагает системный подход, ориентированный на предотвращение и адаптивность, включающий в себя вопросы управления рисками и состоящий из: предотвращения, сокращения рисков, готовности, реагирования и восстановления. Это более комплексный подход, требующий активного участия всех заинтересованных сторон, включая правительство, бизнес и гражданское общество.

Цифровая устойчивость сегодня - это набор возможностей, методов и благоприятных условий, которые обеспечивают непрерывность деятельности правительства, бизнеса и общества перед лицом изменений в окружающей среде, включая техногенные катастрофы и другие кризисы. Многие страны пришли к тому, что необходимо переосмыслить кибербезопасность как цифровую устойчивость - набор стратегий, практик и возможностей, которые помогают нам предвидеть, готовить, предотвращать и реагировать на неизбежные кризисы и катастрофы, которые будут зависеть от нашего все более зависимого от цифровых технологий общества и оказывать на него влияние.

В ходе настоящего правового анализа были изучены следующие нормативные правовые акты Кыргызской Республики в сфере информатизации, перехода к электронному управлению, регулирования вопросов обеспечения кибербезопасности:

Что такое цифровая устойчивость?

На прикладном уровне цифровая устойчивость состоит из четырех ключевых основ/компонентов: непрерывность, кибербезопасность, данные и конфиденциальность, а также цифровое гражданство.

1) Кибербезопасность: состоит из стандартов, практики и людских ресурсов, необходимых для поддержания функционирования цифровых систем и обеспечения безопасной цифровой экосистемы. Она включает в себя систему управления рисками, которая позволяет лицам, принимающим решения, рассчитывать величину риска, связанного с цифровыми системами, и регулярно поддерживать возможности, достаточные для прогнозирования и реагирования на инциденты и чрезвычайные ситуации на постоянной основе.

2) Непрерывность - включает планирование и возможности для управления кризисными ситуациями и восстановления, которые практикуются для обеспечения того, чтобы учреждения и организации могли продолжать функционировать в неблагоприятных условиях. Непрерывность зависит от наличия соответствующих правил и стандартов, которые обеспечивают непрерывность бизнеса и операций, обеспечивая при этом быструю адаптацию в рамках предсказуемого и общепринятого набора правил и передовой практики.

3) Защита данных и конфиденциальность включают в себя надежную экосистему данных, состоящую из законов, учреждений и возможностей, которые определяют и регулируют сбор, хранение и удаление данных. Функционально это включает в себя определение прав собственности и то, как данные, включая личную информацию, собираются и используются правительствами, предприятиями и другими третьими сторонами. Конфиденциальность и защита данных важны для предотвращения ущерба, обеспечения целостности государственных и деловых операций и защиты отдельных лиц от потенциальных злоупотреблений или эксплуатации, а также для обеспечения экономической деятельности.

4) Цифровое гражданство означает готовность граждан пользоваться преимуществами цифровых систем и инфраструктуры. Цифровое гражданство включает в себя базовую компьютерную грамотность, базовые методы цифровой гигиены и навыки, обеспечивающие безопасность и безопасность работы в Интернете, а также осведомленность о правах и обязанностях использования цифровых систем и данных.

Другой тенденцией мировой практики в области обеспечения кибербезопасности является использование подходов по обеспечению **безопасности цепочки поставок** (supply chain security), суть которой заключается в обеспечении безопасности всей цепочки поставок (товаров, услуг, работ и т.д.). Международная практика регулирования данного направления исходит из того, что из-за взаимосвязанности цепочек поставок слабая безопасность одного звена может поставить под угрозу функциональность всей цепочки поставок.

Еще одним значимым компонентом законодательного обеспечения кибербезопасности на международном уровне является укрепление механизмов **государственно-частного партнерства.** В последние годы многие страны пришли к пониманию необходимости сотрудничества между государственным и частным секторами, а также между международными и региональными сообществами в целях обеспечения принятия эффективных стратегий управления рисками и обеспечения отказоустойчивости в сфере ИКТ, а также обязательство развивать необходимый национальный потенциал для повышения доверия и безопасности в сфере ИКТ, устранения недостатков и реагирования на значительные риски в области кибербезопасности[10].

В дополнение можно отметить, что чаще всего страны сосредотачивают свои усилия на создании правовых основ для повышения готовности к рискам, связанных с развитием **трансграничной компьютерной преступности, активизацией террористической и экстремистской деятельности, осуществляемой при помощи цифровых коммуникаций, и рисков возрастающих масштабах государственного и корпоративного кибершпионажа.**

В целом страны и сектора лидирующие в процессах совершенствования законодательства в области кибербезопасности признают не только неотвратимость цифровых трансформаций, но и необратимость, неизбежность рисков и угроз безопасности, которые несет с собой развитие ИКТ и цифровой экономики.

[10] Managing National Cyber Risks, Melissa Hathaway

РЕКОМЕНДАЦИИ

В связи вышеприведенным анализом, видится необходимым принять следующие меры совершенствования законодательной базы КР:

1. Законодательно определить правовые и организационные основы, цели, направления и принципы, а также подходы государственной политики в сфере обеспечения кибербезопасности Кыргызской Республики. Это возможно сделать через внедрение в Цифровой кодекс отдельной главы, касающейся вопросов кибербезопасности. При этом целесообразно здесь же обязательно раскрыть базовые понятия в области кибербезопасности.

2. Начать пересмотр законодательства в области противодействия киберпреступности и использования электронных доказательств, ориентируясь на положительные примеры и успешный мировой опыт проведения реформ. Разработать единую методологию в области идентификации, сбора, получения и хранения свидетельств, представленных в цифровой форме как для уголовного судопроизводства, так и для гражданского. При разработке такого документа в том числе целесообразно за основу взять международный стандарт ИСО/МЭК 27037:2012[11]

Данный стандарт был принят Международной организацией по стандартизации (ISO – International Organization for Standardization) в 2012 году и является руководством по конкретным процессам при обращении с потенциальными доказательствами, представленными в цифровой форме (далее – цифровые доказательства); этими процессами являются: идентификация, сбор, получение и сохранение потенциальных цифровых доказательств. Эти процессы необходимы при проведении расследования и предназначены для поддержки целостности цифровых доказательств, т.е. являются приемлемой методикой получения цифровых доказательств, которая будет способствовать их допустимости для правовых и дисциплинарных действий, а также для других необходимых случаев. Настоящий стандарт также предоставляет общее руководство по сбору цифровых доказательств, которые могут быть полезны на этапе анализа таких доказательств.

[11] «Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме" (ISO/IEC 27037:2012 «Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence».

Настоящий стандарт предназначен для предоставления руководства лицам, отвечающим за идентификацию, сбор, получение и сохранение потенциальных свидетельств, представленных в цифровой форме. К таким лицам относятся специалисты «оперативного реагирования» по цифровым доказательствам, специалисты по реагированию на инциденты и руководители лабораторий судебной экспертизы. Настоящий стандарт обеспечивает уверенность в том, что ответственные лица осуществляют менеджмент потенциальных цифровых доказательств, рациональными общепризнанными способами, чтобы систематически и беспристрастно содействовать расследованию, использующему цифровые устройства и цифровых доказательств, сохраняя при этом их целостность и подлинность[12].

Другим основанием для использования данного стандарта является то, что некоторые страны ЕАЭС уже внедрили их в свои стандарты и широко используют в практической деятельности, что позволит использовать совместимые технические стандарты для цифровой криминалистической экспертизы и трансграничного поиска электронных доказательств. Кроме этого, другим базовым международным документом является Будапештская Конвенция о компьютерных преступлениях 2001 года[13], которая также может стать основой для формирования национальной уголовно-процессуальной базы по борьбе с киберпреступлениями и позволит гармонизировать национальное законодательство с международным. Учитывая трансграничный характер киберпреступлений такой подход в формировании отечественного законодательства очень важен с точки зрения необходимости создания условий для эффективного сотрудничества с другими странами мира.

3. Обеспечить реализацию национальных стратегических рамок кибербезопасности, через разработку и принятие Закона о безопасности критической информационной инфраструктуры (КИИ) и ряда актов Правительства, обеспечивающих его реализацию. При принятии закона предпочтительно руководствоваться анализом сравнительных преимуществ объектного и субъектного и подходов к регулированию безопасности КИИ в зависимости от непосредственного предмета регулирования. При этом необходимо иметь в виду, что без установления четких критериев категорирования, оставляя определение категории объекта на усмотрение государственного органа или самого лица – владельца объекта КИИ, будет

[12] http://docs.cntd.ru/document/1200112857
[13] Будапештская конвенция стала открытой для подписания более 20 лет назад, с 23 ноября 2001 года. На сегодняшний день Конвенцию ратифицировали 66 стран, две подписали ее и 10 получили приглашения присоединиться. Более 140 стран работают с Советом Европы над укреплением своего законодательства и потенциала по борьбе с киберпреступностью. Данная конвенция содержит ряд полномочий и процедур, таких как обыск компьютерных данных, сетей и перехват, определяет принципы международного сотрудничества при расследовании киберпреступлений, обмена технической информацией.

затруднительно обеспечить единообразие в сфере защищенности объектов КИИ от потенциальных угроз. Один из подходов предполагает также выделение категории значимых объектов КИИ. Отношение к определенной категории значимости означает большую вероятность негативных последствий в определенной сфере и повышенные требования к титульным владельцам таких объектов. Конкретный список сфер, зависящий от значений тех или иных отраслей с экономической и социальной точек зрения для государства, подлежит определению в соответствии с последующим категорированием объектов критической информационной инфраструктуры.

4. Обеспечить дополнительную криминализацию деяний, связанных с киберпреступностью. При реализации данного подхода целесообразно учитывать правоприменительную практику других стран и использовать положения международных актов в области кибербезопасности. В целях гармонизации национального законодательства с международными подходами возможно принять во внимание положения Будапештской конвенции о киберпреступности от 2001 года. Данная конвенция является самым первым международным договором о преступлениях, совершенных через Интернет и другие компьютерные сети, и касается, в частности, нарушений авторских прав, компьютерных мошенничеств, детской порнографии и нарушений безопасности сети.

Также следует обратить внимание на создание уголовно-правовой основы для привлечения к ответственности лиц, совершивших деяния, связанные с противозаконным доступом, перехватом данных с использованием технических средств, воздействия на информацию и функционирование системы, противозаконное использование устройств, мошенничество с использованием информационно-коммуникационных технологий и т.п.

5. Необходимо обеспечить реализацию требований Закона Кыргызской Республики «Об информации персонального характера», который подразумевает наличие ответственности за нарушение требований законодательства о персональных данных, в том числе ответственность за: обработку персональных данных без законного основания; необоснованный отказ в представлении субъекту персональных данных информации, касающейся обработки его персональных данных; невыполнение законных требований уполномоченного государственного органа по персональным данным; и необоснованный отказ уполномоченному государственному органу по персональным данным или Омбудсмену (Акыйкатчы) Кыргызской Республики.

6. Обратить внимание на вопросы унификации терминов и понятий не только с Будапештской конвенцией, но и с глоссарием МСЭ, международными стандартами, Стратегией кибербезопасности и законодательством Кыргызской Республики в области связи и телекоммуникаций, в том числе в целях обеспечения принципа правовой определенности.

7. Разработать и принять акты, касающиеся процессуальных полномочий при проведении досудебного производства по киберпреступлениям и преступлений, с использованием электронных доказательств.

8. Следует учесть рекомендации изложенные в Докладе Группы экспертов Генеральной Ассамблеи ООН, который был подготовлен по итогам всестороннего исследования проблемы киберпреступности в 2020 году, касающиеся вопросов законодательного закрепления положений по международному сотрудничеству в области обеспечения кибербезопасности.

9. Учитывая слабый потенциал правоохранительных и судебных органов в области расследования и рассмотрения дел, связанных с цифровыми доказательствами необходимо на систематической основе проводить мероприятия по повышению их квалификации. При этом весьма важно постоянно осведомлять о международной практике и международных тенденциях в области кибербезопасности.

10. Рассмотреть возможность присоединения к региональным и международным инициативам, координации движений и программам развития потенциала в сфере борьбы с кибепреступлениями в целях укрепления международного сотрудничества в данной области.

11. Из-за отсутствия анализов риска по кибербезопасности возникает необходимость в государственной стандартизации информационной безопасности, в том числе в области межведомственного взаимодействия. Для поддержания интероперабельности информационных систем, стандарты должны быть открытыми и соответствовать следующим критериям: принятие и дальнейшее развитие стандарта должно осуществляться на основе процедуры открытого принятия решений, доступной для всех заинтересованных сторон; документы, описывающие стандарт должны находиться в свободном доступе; в патентные требования на использование стандарта не должна входить выплата роялти; стандарт должен быть технологически нейтральным; стандарт должен поддерживать локализацию, в тех случаях, когда это необходимо.

12. Рассмотреть возможность упрощения или разделения на отдельные положения Требований к защите информации, содержащейся в базах данных государственных информационных систем. При этом, внести коррективы с точки зрения существующих стандартов и актуальных тенденций развития ИКТ и кибербезопасности. В данном контексте возможно применить отдельные положения и принципы американского национального института стандартов и технологий (NIST), в том числе Минимальные требования безопасности для Федеральных информационных систем и информации. Этот стандарт определяет спецификацию минимальных требований безопасности для государственных информационных систем (организационных, эксплуатационных и технических мер).

ГРАЖДАНСКАЯ ИНИЦИАТИВА
ИНТЕРНЕТ ПОЛИТИКИ

ул. Рыскулова 79-Б
3 Этаж Офис №13

+996 312 54 04 40

info@gipi.kg

@internet_policy

+996 770 700 300

internetpolicy.kg