Анализ действующего законодательства, регулирующего кибербезопасность и выявление ключевых пробелов с рекомендациями

Разработка национальной политики в области кибербезопасности

Принимая во внимание активное развитие информационно-коммуникационных технологий и растущее использование сети Интернет, с особой остротой встает вопрос необходимости обеспечения безопасности в информационной среде и защиты информационной инфраструктуры, требующей широкого диапазона мер в области сетей связи и их информационной безопасности, борьбы с кибер-преступностью.

Оперативное реагирование и эффективное противодействие киберпреступности требует создания специальных подразделений в правоохранительных органах и развития сети центров реагирования на компьютерные инциденты и организации их взаимодействия с данными подразделениями.

В ходе анализа законодательства были изучены различные международные индексы кибербезопасности, которые являются вспомогательным фундаментом для построения архитектуры. За основу было решено взять эстонские индексы кибербезопасности, которые представляют полное и расширенное описание ступеней для обеспечения кибербезопасности. Эстонская модель состоит из 12 индексов и каждый имеет свою оценку, что в сумме предполагает измерение индекса кибербезопасности, согласно международным принципам.

В соответствии с законом Кыргызской Республики «О Совете обороны Кыргызской Республики», принятым 15 июля 2011 года, **Совет обороны** является конституционным консультативным органом, осуществляющим проведение единой государственной политики в области обеспечения обороны и безопасности. Совет обороны вырабатывает решения по подготовке к защите Кыргызской Республики от современных вызовов и угроз.

В функции Совета обороны КР входят, в том числе и осуществление стратегического планирования в области обороны и обеспечения безопасности; организация работы по подготовке государственных программ в области обороны, обеспечения безопасности и осуществление контроля за их реализацией.

Совет обороны КР отвечает за прогнозирование и анализ угроз безопасности, а также разработку политики по их устранению. Государственный комитет национальной безопасности КР и правоохранительные органы являются постоянными членами Совета Обороны.

При этом Совет Обороны не имеет нормативной базы для реализации политики по кибербезопасности, так как нет четких разграниченных полномочий и стратегии для защиты информационного сообщества. Все полномочия в разделе информационной безопасности описаны размыто и не разграничены.

Законом КР «О стратегических объектах Кыргызской Республики» от 23.05.2003года установлено, что **Правительство Кыргызской Республики** по рекомендации Совета

Обороны определяет перечень стратегических объектов и устанавливает специальные требования к режиму их функционирования и эксплуатации. Но Закон не определяет, в какой форме это происходит.

В соответствии с законом КР «Об органах национальной безопасности Кыргызской Республики» от 11.01.1994года **Государственный комитет национальной безопасности КР**, в пределах своих полномочий:

- организует систему защиты государственных секретов, представляет по запросам компетентных органов власти информацию на отдельных лиц в связи с решением, в установленном порядке, вопроса о допуске к секретным сведениям, участвует в обеспечении информационной безопасности;

- эксплуатирует и обеспечивает защищенность специальных видов связи (правительственной, шифрованной, засекреченной), а также шифровальной и дешифровальной работы;

- участвует в разработке и создании специальной техники в интересах обеспечения национальной безопасности.

Министерство внутренних дел КР, как правоохранительный орган, в части обеспечения кибербезопасности осуществляет функции по выявлению и пресечению киберпреступлений.

Государственный комитет информационных технологий и связи КР уполномочен обеспечивать формирование, хранение, использование и безопасность государственных информационных ресурсов, а также участвовать в разработке технических регламентов в области информационной безопасности государственных информационных ресурсов.

Таким образом, на сегодняшний день в стране не имеется единого уполномоченного государственного органа для обеспечения кибербезопасности в виде созданной и полноценно функционирующей структуры по реагированию на возникающие угрозы и киберинциденты (CERT), не выстроена четким образом и нормативно не закреплена иерархия государственных структур, задействованных в данной сфере (Совет безопасности (обороны), Государственный комитет национальной безопасности, Министерство внутренних дел, Государственный комитет информационных технологий и связи), с чётким распределением задач и функций в информационной сфере.

Термины и определения кибербезопасности, используемые на национальном уровне.

До 2001 года в законодательстве Кыргызской Республики не давалось определения понятию **безопасность** и только с принятием Концепции национальной безопасности Кыргызской Республики появилось нормативное определение безопасности.

Действующая Концепция национальной безопасности Кыргызской Республики была утверждена указом Президента КР 12 июня 2012 года, в которой заложены вопросы обеспечения информационной безопасности.

В Концепции одной из внутренних угроз национальной безопасности страны определена **недостаточная развитость информационно-коммуникационных технологий и слабая защита информационного пространства страны.**

Недостаточное внимание государством уделяется вопросам формирования и реализации единой государственной политики по обеспечению кибербезопасности, координации деятельности органов власти и управления по ее укреплению. Мероприятия, нацеленные на защиту информационной сферы, недостаточно обеспечены финансовыми ресурсами.

Основными направлениями обеспечения кибербезопасности выступают:

- *правовое обеспечение* (применение правовых норм обеспечения кибербезопасности);
- *организационное обеспечение* (регламентация деятельности, исключающая нанесение ущерба, наличие соответствующих служб);
- *инженерно-техническое обеспечение* (использование технических средств, препятствующих нанесению ущерба, физические, аппаратные, программные и криптографические средства защиты).

На предмет выявления терминов и определений, связанных с кибербезопасностью была проанализирована нормативная правовая база, регулирующая обеспечение информационной безопасности, а именно:

- Конституция Кыргызской Республики;
- закон КР «О защите государственных секретов Кыргызской Республики»;
- закон КР «Об информатизации»;
- закон КР «О гарантиях и свободе доступа к информации»;
- закон КР «О Национальном архивном фонде»;
- закон КР «Об электрической и почтовой связи»;
- закон КР «Об электронной цифровой подписи»;
- закон КР «О средствах массовой информации»;
- закон КР «О правовой охране программ для ЭВМ и баз данных»;
- закон КР «Об основах технического регулирования в Кыргызской Республике»;
- закон КР «О доступе к информации, находящейся в ведении государственных органов и органов местного самоуправления КР» и другие;
- Гражданский, Уголовный и др. кодексы;
- прочие подзаконные акты, регламентирующие общественные отношения в информационной сфере.

Следует отметить, что ни один вышеперечисленных нормативно-правовой акт не содержит понятия «кибербезопасность».

В целом анализ действующего законодательства в сфере информационной безопасности позволяет делать выводы о том, что оно:

1. представляет собой устаревшую базу, не содержит терминов и определений информационной безопасности, кибербезопасности, киберпространства, кибергигиены, нет понятий критической инфраструктуры и т.п.;

2. в определенной степени остается противоречивым, отражает ведомственные интересы и не подкреплено реальными ресурсами;
3. не обеспечивает эффективный контроль обеспечения прав субъектов правовых отношений.

На основе анализа нормативной правовой базы уже сейчас можно сделать вывод о целесообразности создания специализированного документа, отражающего суть и значение развития кибербезопасности в Кыргызской Республике, такого как Концепция/Стратегия по кибербезопасности. Данный документ позволит определить конкретные понятия и термины по кибербезопасности, выстроить четкую структуру органов, задействованных в ее обеспечении, расставить акценты по международному взаимодействию и тому подобные вопросы. Принятие подобного документа будет означать значимый шаг в признании проблемы уязвимого киберпространства, а также методов и способов защиты последней.

Учитывая отсутствие Концепции/Стратегии по кибербезопасности, соответственно и нет плана по ее реализации.

По результатам разработки и принятия Концепции/Стратегии по кибербезопасности необходимо разработать план мероприятий, направленный на реализацию стратегических целей по защите информационных ресурсов, критической инфраструктуры от киберугроз.

В Плане мероприятий по реализации Концепции/стратегии должны быть определены организации, ответственные за осуществление мер, четко обозначенных для каждого государственного органа, принимающего участие в реализации Плана. Также документом должны быть определены четкие сроки выполнения мероприятий. Все это должно быть подкреплено прописанными финансовыми ресурсами с четким распределением на каждое конкретное мероприятие Плана.

Анализ киберугроз на национальном уровне.

Согласно закона Кыргызской Республики «О Совете обороны Кыргызской Республики», Совет обороны вырабатывает решения по подготовке к защите Кыргызской Республики от современных вызовов и угроз.

В соответствии с Положением «О секретариате Совета обороны КР», утвержденном Указом Президента КР от 09.12.2011г. № 24, в задачи Секретариата Совета обороны входит: накопление, анализ и обработка информации о функционировании системы обеспечения обороноспособности и национальной безопасности Кыргызской Республики, а также подготовка аналитических докладов о состоянии безопасности в различных сферах жизнедеятельности общества и государства.

Секретарь Совета обороны отвечает за разработку аналитических отчетов об угрозах национальной безопасности в целом. Цель данной отчетности состоит в информировании и повышения правового сознания общественности и построение устойчивого информационного общества в стране.

Для реализации данных правовых норм государством должен быть создан орган - центр по реагированию на компьютерные инциденты (CERT), который будет нести ответственность за управление инцидентами в сфере безопасности в кыргызских компьютерных сетях.

Задачами данного центра, в первую очередь, необходимо определить помощь кыргызским пользователям интернета в осуществлении превентивных мер для сокращения возможного ущерба от инцидентов в сфере кибербезопасности и оказание помощи при реагировании на возникающие киберугрозы.

Деятельность CERT должна быть направлена на сбор, хранение и обработку статистических данных, связанных с распространением вредоносных программ и сетевых атак, совершаемых на территории государства. В их компетенцию также должна входить обработка компьютерных инцидентов с целью их выявления и дальнейшей нейтрализации.

Предоставление образования в области кибербезопасности

Анализ обучающих программ показал следующее.

На уровне общеобразовательных школ:

5-9 классы: в основном детям даются знания по предмету «Основы информатики и вычислительной техники», куда входит история возникновения ЭВМ, общая теоретическая часть по работе с системой «Windows PC», «QBasic», а также базовые основы работы на компьютере. Вопросы кибергигиены и кибербезопасности не даются.

10-11 классы: даются основы навыков работы с пакетом Microsoft Office, с некоторыми компонентами пакета Adobe. Также даются базовые понятия о вирусах, методах заражения компьютера и основах базы Антивирусов NOD32. Незначительное количество часов даётся на навыки работы с сетью Internet.

На уровне средне-специального образования: в профессиональных технических лицеях на базе неполного среднего образования осуществляется обучение по специальности «Специалист по безопасности IT», где изучаются способы защиты конфиденциальной информации, а выпускники затем могут работать в подразделениях обеспечения информационной безопасности, а также в любых структурах, связанных с использованием технических средств обработки, хранения и передачи конфиденциальной информации.

На уровне высшего образования: в Кыргызской Республике функционируют 50 высших учебных заведений. Предмет «Информатика» или «ОИВТ» является базовым предметом первого курса для всех специальностей.

Для юридических специальностей преподается «Информационное право», где освещаются вопросы информационной безопасности, защиты и категорий секретной информации и меры ответственности.

Для технических специальностей в программе освещаются вопросы информационной безопасности в специализациях «Информационные технологии и программирование». Специализация «Информационная безопасность» имеется на факультете Информационных технологий в Кыргызской Государственном Техническом Университете. Данная специализация принадлежит кафедре «Программного Обеспечения компьютерных систем».

Кыргызской Государственный Университет Строительства, Транспорта и Архитектуры осуществляет набор на кафедру «Обеспечение информационной безопасности» на базе Института новых информационных технологий (ИНИТ), куда входят:

- факультет информационных технологий;
- Кыргызско-Германский факультет прикладной информатики;
- Индийско-Кыргызский центр информационных технологий;
- Кыргызско-Китайский образовательный центр;
- Учебно-исследовательский центр лингвистики и новых информационных технологий (филиал кафедр МКиАСП и КЛ);
- Кыргызско-Российский центр образования и культуры.

Также данный факультет предоставляет магистерские программы по специализации «Информационная безопасность»:
1.Комплексные системы информационной безопасности;
2.Аудит информационной безопасности автоматизированных систем;
3.Информационная безопасность телекоммуникационных систем;

Кафедра имеет тесную связь с Западно-Саксонским университетом Цвикау (Германия), а также ведущими вузами Российской Федерации по направлению информационных технологий и безопасности, такими как Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Национальный исследовательский ядерный университет «МИФИ», Томский государственный университет систем управления и радиоэлектроники и т.д.

Таким образом, образовательные программы охватывают в основном область информационной безопасности, нет специализации именно по кибербезопасности.

Обеспечение базовых показателей кибербезопасности

Согласно действующего законодательства Кыргызской Республики, внедрение методов, координацию и контроль за кибербезопасностью уполномочены осуществлять Государственный комитет национальной безопасности КР и специализированный отдел Министерства внутренних дел КР.

Каждый из указанных органов имеет свой собственный блок полномочий, сосредоточенных на кибербезопасности. При этом следует отметить, что указывающие на это законодательные акты не доступны для общественности и имеют статус «для служебного пользования».

Государству необходимо создание отдельного органа либо отдела, специализирующего именно на разработке базовых подходов к борьбе с киберпреступностью, а также выработке общих базовых рекомендаций по обеспечению кибербезопасности, которые могли бы использоваться, а также были бы открыты и доступны для всех.

В 2008 году был принят закон КР «Об информации персонального характера» (далее – закон об ИПХ), направленный на правовое регулирование работы с персональными данными на основе общепринятых международных принципов и норм в соответствии с Конституцией и

законами КР в целях обеспечения защиты прав и свобод человека и гражданина, связанных со сбором, обработкой и использованием персональных данных.

Законом установлены основные принципы работы с персональными данными, которые не носят исчерпывающий характер и могут дополняться в соответствии с законодательством КР.

Следует отметить, что закон играет ключевую роль при предоставлении государственных и муниципальных в электронном формате, требующих персонификации/аутентификации и обработки персональных данных. Кроме того, он важен с точки зрения соблюдения прав граждан при осуществлении процедур межведомственного взаимодействия госорганов при предоставлении электронных услуг.

Зарубежный опыт насчитывает свыше 25 лет в решении проблемы защиты информации персонального характера, в международной практике подобные отношения урегулированы Директивой Европейского Парламента и Совета Европы 95/46/ЕС от 24 октября 1995 г. «О защите личности в отношении обработки персональных данных и свободном обращении этих данных».

Он определяет **случаи**, при которых держатель (обладатель) массива персональных данных может осуществлять работу с персональными данными. При этом держатель и обработчик персональных данных обязаны обеспечить гарантии в отношении мер технической безопасности и организационных мер, регулирующих обработку персональных данных. Законом также закрепляется общий перечень таких мер.

При передаче персональных данных **по глобальной информационной сети (Интернет и т.п.)** держатель (обладатель) массива персональных данных, передающий такие данные, обязан обеспечить передачу необходимыми средствами защиты, соблюдая при этом конфиденциальность информации.

Законом также определены условия обработки **специальной категории персональных данных**. Так сбор, накопление, хранение и использование персональных данных, раскрывающих расовое или этническое происхождение, национальную принадлежность, политические взгляды, религиозные или философские убеждения, а также касающихся состояния здоровья и сексуальных наклонностей, исключительно в целях выявления этих факторов, не допускаются.

В настоящее время есть необходимость в принятии подзаконного акта, который определил бы уровни безопасности персональных данных, требуемые при их обработке в конкретном массиве персональных данных, исходя из конкретных условий работы с персональными данными и уровнем технического развития, а также разработанной моделью угроз безопасности персональных данных.

Необходимо отметить, что закон КР об ИПХ устанавливает, что Правительство КР определяет **уполномоченный государственный орган** Кыргызской Республики, на который возложены функции по контролю и надзору за работой с персональными данными.

Отсутствие до настоящего времени уполномоченного государственного органа (далее – УГО) создает угрозу охраняемой Конституцией КР тайне частной жизни граждан страны в

случае злонамеренного или случайного завладения третьими лицами персональными данными.

Однако до настоящего времени данный уполномоченный орган так и не определен. Кроме того, в 2010 году гражданскими активистами в судебном порядке было оспорено бездействие Правительства КР, которое не определило уполномоченный орган, согласно требованиям закона об ИПХ. Решением Межрайонного суда г.Бишкек иск был удовлетворен, суд обязал Правительство КР в течение 6 месяцев определить УГО. До настоящего времени судебное решение так и не исполнено.

Законодательством КР установлены правила классификации информации, согласно которым информация разделена на государственные секреты, военную, служебную, коммерческую тайны, информацию для служебного пользования, не для печати, тайну следствия, врачебную, личную и другие виды тайны. Каждой категории информации даны определения и установлены принципы её защиты.

Правовые основы функционирования системы защиты государственных секретов во всех видах деятельности государственных органов, предприятий, объединений, организаций, независимо от форм собственности, воинских формирований и граждан Кыргызской Республики на всей территории республики и в ее учреждениях за границей регулируются законом КР «О защите государственных секретов КР».

Отнесение информации к государственным секретам осуществляется в соответствии с Положением о порядке определения и установления степени секретности сведений, содержащихся в работах, документах и изделиях, на основании Перечня главнейших сведений, составляющих государственные секреты, и Перечня сведений, подлежащих засекречиванию, утвержденных постановлением Правительства КР от 07.07.1995г. Следует отметить, что указанные Положение и Перечни являются документами для служебного пользования, **доступ к которым ограничен**.

Правовые основы защиты коммерческой тайны на территории Кыргызской Республики установлены законом КР «О коммерческой тайне», согласно которого порядок защиты коммерческой тайны определяется субъектом предпринимательства или назначенным им руководителем, который доводит его до работников, имеющих доступ к сведениям, составляющим коммерческую тайну. Субъектами коммерческой тайны разрабатываются инструкции, положения по обеспечению сохранности коммерческой тайны.

Для обеспечения защиты коммерческой тайны на хозяйствующих субъектах могут создаваться специальные режимные подразделения, функции и полномочия которых отражаются в соответствующих инструкциях, положениях, приказах.

Из-за отсутствия анализов риска по кибербезопасности и единой политики в её обеспечении возникает необходимость в государственной стандартизации информационной безопасности, в том числе в области межведомственного взаимодействия.

Для поддержания интероперабельности, 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 быть доступны бесплатно или за номинальную плату;
- 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.

При этом, законом КР «Об основах технического регулирования в КР» от 22 мая 2004 года № 67 устанавливаются правовые основы в области: разработки, принятия, применения и исполнения на добровольной основе требований к продукции или процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, хранения, перевозки, реализации, эксплуатации, утилизации, выполнению работ, оказанию услуг, а также оценки соответствия.

Закон КР «Об информатизации и электронном управлении» от 08 октября 1999 года №107 подразделяет информационных ресурсы на уровни доступа к ним. Государственные информационные ресурсы Кыргызской Республики являются открытыми и общедоступными, за исключением документированной информации, отнесенной законом к категории ограниченного доступа. Документированную информацию и государственные информационные ресурсы с ограниченным доступом составляет информация, отнесенная к государственной тайне, и конфиденциальная. Отнесение информации к государственной тайне или к конфиденциальной информации осуществляется в соответствии с законодательством Кыргызской Республики.

Действующие ЕДИНЫЕ ТРЕБОВАНИЯ по созданию и поддержке веб-сайтов государственных органов и органов местного самоуправления Кыргызской Республики, утвержденные постановлением Правительства Кыргызской Республики от 14 декабря 2007 года № 594, состоят из обязательных требований, которые необходимо обеспечить, и рекомендуемых требований, которые целесообразно выполнять с учетом возможностей и развития технологий. В них включена и Политика безопасности: должна быть разработана концепция обеспечения защиты решения от несанкционированного доступа. Она должна базироваться на сочетании надежных базовых программных продуктов с возможностью подключения необходимого дополнительного специализированного программного обеспечения и аппаратных средств соответствующего установленным нормам и требованиям в этой области. Данный подзаконный акт устарел и требует его доработки.

Таким образом, существует необходимость в разработке решений для государственного сектора по проведению регулярного аудита безопасности ИКТ-продуктов.

Необходимость проведения аудита безопасности обуславливается тем, что рынок ИКТ решений находится в постоянном развитии, в том числе и в вопросах безопасности. Регулярный аудит позволит выявлять недочеты в вопросах защиты киберпространства, а также определить причины и методы их устранения.

В Кыргызской Республике деятельность в области криптографии (шифровании) регулируется незначительным количеством нормативно-правовых актов.

Существует «Национальный контрольный список Кыргызской Республики контролируемой продукции», утвержденный постановлением Правительства КР от 02.04.2014г. № 197, в который включены в том числе ЭВМ, сопутствующее оборудование и программное обеспечение, выполняющие функции **криптографии, криптоанализа**, сертифицируемой многоуровневой защиты информации или сертифицируемые функции изоляции пользователей либо ограничивающие электромагнитную совместимость (ЭМС).

Законом КР "Об органах национальной безопасности Кыргызской Республики" на **Государственный комитет национальной безопасности КР (ГКНБ КР)** возложены обязанности:

- осуществлять государственный контроль за исполнением требований при обеспечении криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, систем шифрованной, засекреченной и иных видов специальной связи;

- осуществлять контроль за соблюдением режима секретности при обращении с шифрованной информацией в шифровальных подразделениях государственных органов и организаций на территории Кыргызской Республики и в ее учреждениях, находящихся за ее пределами, а также контроль за обеспечением защиты особо важных объектов (помещений) и находящихся в них технических средств от утечки информации по техническим каналам;

- осуществлять контроль и выдачу разрешений на ввоз в Кыргызскую Республику и вывоз за ее пределы, транзит, а также на разработку, производство, реализацию, приобретение на территории Кыргызской Республики в порядке, установленном Правительством Кыргызской Республики шифровальных средств и нормативно-технической документации к ним.

Законом КР «О лицензионной разрешительной системе в КР» закреплено, что для осуществления ввоза на территорию Кыргызской Республики и вывоза из Кыргызской Республики шифровальных средств (включая шифровальную технику, части для шифровальной техники и пакеты программ для шифрования), нормативно-технической документации к шифровальным средствам (включая конструкторскую и эксплуатационную) требуется получение **разрешения**.

Шифровальные (криптографические) средства внесены в перечень товаров, ввоз/вывоз которых на/с территории Кыргызской Республики **ограничен**.

Так как контроль и выдачу разрешений на ввоз и вывоз шифровальных средств осуществляет ГКНБ КР, имеющиеся подзаконные акты, регламентирующие требования к шифровальным средствам и порядку их ввоза/вывоза, существуют под грифом «для служебного пользования».

Функции по технической защите информации, как и криптографической защите, отнесены к полномочиям органов национальной безопасности. Регулируемые данную область нормативные акты также отнесены к документам для служебного пользования, доступ к которым ограничен.

Ввоз в Кыргызскую Республику и вывоз за ее пределы, а также разработка, производство, сертификация, реализация, приобретение и использование специальных технических средств, предназначенных для негласного получения информации, осуществляются в порядке, устанавливаемом Правительством Кыргызской Республики. Перечень видов специальных технических средств, предназначенных для негласного получения информации в процессе осуществления оперативно-розыскной деятельности, устанавливается Правительством Кыргызской Республики.

Оперативно-розыскные мероприятия, связанные с использованием сети связи, в интересах решения задач органами, наделенными правом осуществления оперативно-розыскных мероприятий, технически осуществляются органами национальной безопасности в порядке, определяемом Правительством КР.

Таким образом, вся правовая база, связанная с оборотом и применением технических средств для шифрования и использования в оперативно-розыскной деятельности, относится к категории ограниченного доступа и не позволяет сделать детальный анализ на предмет выработки рекомендаций по её улучшению.

Обеспечение безопасной среды для электронных услуг

Положением “О Государственной регистрационной службе при Правительстве Кыргызской Республики”, утвержденное постановлением Правительства Кыргызской Республики от 20 февраля 2012 года №128, в задачи ГРС включены:

- обеспечение развития и формирования единой государственной регистрационно-учетной системы с использованием современных информационных технологий на основе единства информационно-регистрационных ресурсов и внедрение системы электронного документооборота;

- создание единого пространства электронной цифровой подписи для унифицированного оказания юридически значимых государственных услуг в электронном виде и обеспечения межведомственного информационного взаимодействия;

- обеспечение безопасности и защиты государственных информационно-регистрационных ресурсов, информационных систем и сетей, находящихся в компетенции ГРС.

Положением «О Государственном комитете информационных технологий и связи КР» (ГКИТиС), утвержденным постановлением Правительства Кыргызской Республики от 15 июля 2016 года № 402, определены функции ГКИТиС, такие как:

- формирует и реализует механизмы для создания единого национального центра обработки данных, портала государственных услуг в сфере информационно-коммуникационных технологий;

- создает условия для развития и администрирования интегрированных правительственных веб-ресурсов, единой системы электронного документооборота, единых государственных систем по учету кадров, единой системы финансового управления в соответствии с законодательством Кыргызской Республики;

- обеспечивает формирование, хранение, использование и безопасность государственных информационных ресурсов;

- разрабатывает стандарты и технические регламенты в области разработки и внедрения программно-технических комплексов, информационных систем и сетей, в том числе электронной цифровой подписи;

- разрабатывает и внедряет проекты по созданию технической архитектуры электронного правительства, внедрению электронных государственных и муниципальных услуг и других электронных приложений;

Таким образом, необходима более эффективная работа по введению системы межведомственного электронного взаимодействия (СМЭВ) в действие, подключение всех ведомств к данной сети, а также установление принципов защиты данной системы. Необходим четкий перечень государственных услуг, запускаемых в электронном формате, а также разработка и утверждение на государственном уровне стандартов и административных регламентов к электронным услугам. При этом особое внимание следует уделить обеспечению безопасности и защиты используемой информации при межведомственном взаимодействии от неправомерных действий.

Предоставление электронных трастовых услуг

Согласно Положению «О Государственной регистрационной службе при Правительстве Кыргызской Республики», и Положению “О Едином государственном реестре населения Кыргызской Республики”, утвержденном Постановлением Правительства Кыргызской Республики от 21 октября 2013 года № 573, ГРС осуществляет присвоение каждому гражданину Кыргызской Республики, иностранным гражданам и лицам без гражданства персонального идентификационного номера (ПИН).

ПИН присваивается ГРС каждому субъекту регистрации при первоначальном внесении данных о нем в реестр населения и остается неизменным на протяжении всего периода существования этих данных. ПИН в обязательном порядке должен указываться в паспорте (ID-карта, общегражданский, дипломатический и служебный паспорта), свидетельстве о рождении, государственном удостоверении социальной защиты, водительском удостоверении и во всех других документах, удостоверяющих личность гражданина Кыргызской Республики. ПИН должен быть использован для учета и идентификации разных категорий граждан на уровне информационных систем государственных органов и органов местного самоуправления.

На сегодняшний день действующий закон КР "Об электронном документе и электронной цифровой подписи" является технически не нейтральным и имеет много недочётов. Так, он предусматривает единственную технологию и вид электронной подписи – ЭЦП, а также напрямую связывает понятие электронного документа с наличием в нем ЭЦП. Столь жесткие рамки делают фактически невозможным развертывание общедоступной системы удостоверяющих центров, запрещают использование электронных документов, не подписанных ЭЦП. Тем самым, данный закон является системным препятствием на пути развития электронного управления в КР, и требует полной его переработки.

В настоящее время разработан новый законопроект «Об электронной подписи», который ставит перед собой задачу урегулирования следующих видов отношений в области использования электронных подписей:

1) использование различных видов электронных подписей;

2) выдача и использование сертификатов ключа подписи, проверка электронных подписей;

3) оказание услуг удостоверяющих центров, а также аккредитация удостоверяющих центров.

Вносимые изменения в действующий закон направлены на совершенствование правого регулирования этой сферы, гармонизацию кыргызского законодательства с законодательством стран-участниц Евразийского экономического Союза, что является важным в связи с подписанными Кыргызстаном обязательствами по вступлению в указанное интеграционное объединение. Эти изменения важны с точки зрения предстоящего в рамках ЕАЭС электронного взаимодействия, как государственных органов, так и юридических и физических лиц.

Выводы: Имеющаяся на сегодняшний день правовая база электронной подписи является устаревшей и не содержит современных необходимых терминов и определений, а также не регулирует в достаточной мере вопросы защиты электронной подписи и персональных данных её владельцев.

Защита критической информационной инфраструктуры

На данный момент законодательство Кыргызской Республики не содержит термина «критическая инфраструктура». Следовательно, данный раздел не имеет никакой нормативной базы для построения правового регулирования и осуществления киберзащиты.

Закон КР «Об информатизации и электронном управлении» не специфицирует и не выделяет критическую информационную инфраструктуру, а лишь содержит расплывчатую информацию об информатизации инфраструктуры:

информационная инфраструктура (инфраструктура информатизации) - совокупность информационных центров, баз и банков данных, систем связи и передачи данных, других структур, которые обеспечивают функционирование информационной сети государства.

Закон КР «О стратегических объектах Кыргызской Республики» от 23.05.2008года № 94 к стратегическим объектам также относит и национальную электрическую сеть, распределительные электрические сети, магистральные линии связи.

Данный закон определяет, что перечень стратегических объектов и требования к их функционированию и эксплуатации утверждается Правительством КР.

Так, постановлением Правительства КР от 17 февраля 2014 года № 99 утвержден перечень стратегических объектов, куда к категории «важные объекты» отнесены операторы мобильной сотовой связи с абонентской базой свыше 1 млн. человек.

А к требованиям, утвержденным постановлением Правительства КР от 12 февраля 2015 года № 56, отнесена организация системы безопасности объекта. При этом следует отметить, что перечисленные в документе меры по обеспечению безопасности содержат только требования физической защиты объекта, в них отсутствуют меры информационной и кибербезопасности. С учетом этого, требуется доработка данного закона.

Законом КР «Об органах национальной безопасности КР», от 11 января 1994 года, в обязанности органов национальной безопасности включены:

- организация системы защиты государственных секретов, представление по запросам компетентных органов власти информацию на отдельных лиц в связи с решением, в установленном порядке, вопроса о допуске к секретным сведениям, участие в обеспечении информационной безопасности;
- участие в разработке мероприятий и осуществление мер по обеспечению безопасности объектов оборонной промышленности, транспорта, связи, финансово-кредитной системы и других стратегических объектов, перечень которых определяет Правительство Кыргызской Республики;
- эксплуатация и обеспечение защищенности специальных видов связи (правительственной, шифрованной, засекреченной), а также шифровальной и дешифровальной работы, участие в разработке и создании специальной техники в интересах обеспечения национальной безопасности.

Выводы: К критической инфраструктуре необходимо относить информацию и киберпространство, как одно целое, в котором данные создаются, передаются и хранятся. Итоговый комплект областей должен включать телекоммуникации, энергетику, банки, финансы, транспорт, снабжение водой и службы спасения. Защита должна быть выстроена не только в отношении «традиционной» опасности, к которой относятся военные конфликты, стихийные бедствия и аварии, но и к новой опасности в форме терроризма, прежде всего, кибертерроризма. Это отражается в постоянно растущей зависимости общества от информации и технологий, которые с ней работают. Таким образом, необходимо конкретизировать объекты критической инфраструктуры и вопросы доступа к ней.

Требуется не только разработка и правовое закрепление критической инфраструктуры, но создание государственного органа или отдела, специализирующегося на её защите, возложив на него ответственность за разработку надлежащих мер безопасности, а также координацию и контролирование мероприятий по их осуществлению.

Управление кризисом и инцидентами

Правительством КР не создан орган, специализирующийся на обнаружении и реагировании на киберинциденты на национальном уровне и принятии ответных мер.

На сегодняшний день существует частный центр (CERT), который взаимодействует с органами национальной безопасности по реагированию на компьютерные инциденты.

В Министерстве внутренних дел КР создан отдел оперативно-технического обеспечения и противодействия киберугрозам Десятого главного управления МВД КР. Но понять и

проанализировать рамки полномочий данного управления невозможно ввиду отсутствия в открытом доступе правовых актов.

На фоне увеличивающихся угроз в киберпространстве, государство должно рассмотреть возможность создания государственного центра оперативного реагирования на киберугрозы, на который следует возложить ответственность:

- за отслеживание инцидентов кибербезопасности,
- за распространение соответствующей информации об инцидентах кибербезопасности,
- за предупреждение организаций и широкой общественности о значимых инцидентах кибербезопасности,
- за предоставление своевременной помощи,
- за подготовку отчетов об инцидентах, на основании которых могли бы быть разработаны меры по предупреждению киберугроз.

Борьба с киберпреступлениями

Уголовный кодекс Кыргызской Республики на сегодняшний день содержит главу «Преступления в сфере компьютерной информации», состоящую всего из одной статьи «Создание, использование и распространение вредоносных программ для ЭВМ». Она включает в себя такие противоправные деяния, как создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами.

Из данной главы были исключены следующие статьи: статья 289. Неправомерный доступ к компьютерной информации и статья 291. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Следует отметить, что законом КР от 24.01.2017года № 10 была принята новая редакция Уголовного кодекса Кыргызской Республики, которая вступает в силу с 1 января 2019 года. В новой редакции УК КР глава, посвященная преступлениям в сфере информационной безопасности, дополнена новыми видами преступлений, такими как неправомерный доступ к компьютерной информации и компьютерный саботаж.

Неправомерный доступ к компьютерной информации представляет собой доступ к чужой охраняемой компьютерной информации, сопряженный с ее уничтожением, блокированием, модификацией или копированием и причинивший умышленно или по неосторожности значительный вред.

Компьютерный саботаж представляет собой умышленные изменение, уничтожение, блокирование, приведение в непригодное состояние компьютерной информации или программы без права на это либо вмешательство в работу компьютерных систем с намерением помешать функционированию компьютерной или телекоммуникационной системы, а также вывод из строя компьютерного оборудования либо разрушение компьютерной системы или сети.

Новой редакцией УК КР применение к юридическому лицу мер уголовно-правового воздействия в случае совершения преступлений против информационной безопасности, не распространяется. Таким образом, уголовная ответственность юридических лиц законодательно не закреплена. По данной категории преступлений к ответственности привлекаются только физические лица.

Выводы: принятые изменения недостаточны для борьбы с киберпреступлениями, учитывая ощутимое интенсивное развитие и распространение информационных технологий и глобализацию компьютерных сетей.

На основе международной практики и опыте зарубежных стран необходимо дополнить уголовное законодательство нормами, устанавливающими ответственность за совершение преступлений против конфиденциальности, целостности и доступности компьютерных данных и систем, деяний, связанных с подлогом компьютерных данных и других противоправных действий, способных причинить тяжкие и необратимые последствия, связанные не только с имущественным ущербом, но и с физическим вредом. К таким преступлениям можно отнести: незаконный доступ к компьютерной системе или ее части; умышленный перехват не предназначенных для общественности передач компьютерных данных на компьютерную систему; незаконное вмешательство в данные путём умышленного повреждения, стирания, порчи, изменения или подавления компьютерных данных; подлог компьютерных данных, компьютерное мошенничество и т.п.

Сбор и использование доказательств в электронной форме.

Действующее уголовно-процессуальное законодательство не предусматривает понятия доказательств в электронной форме. На сегодняшний день существуют большие препятствия с доказыванием в суде по делам о преступлениях против информационной безопасности. Проблемы существуют как в период предварительного следствия, так и в судебном процессе.

Новая редакция Уголовно-процессуального кодекса КР, который вступит в силу с 1 января 2019года, относит к вещественным доказательствам электронные носители информации, а также предусматривает отдельный порядок их хранения. Электронные носители информации:

а) хранятся в опечатанном виде в условиях, исключающих возможность ознакомления посторонних лиц с содержащейся на них информацией и обеспечивающих их сохранность и сохранность указанной информации;

б) возвращаются их законному владельцу после осмотра и производства других необходимых следственных действий, если это возможно без ущерба для доказывания.

После производства следственных действий в случае невозможности возврата изъятых в ходе производства следственных действий электронных носителей информации их законному владельцу содержащаяся на этих носителях информация копируется по ходатайству законного владельца изъятых электронных носителей информации или обладателя содержащейся на них информации. Копирование указанной информации на другие электронные носители информации, предоставленные законным владельцем

изъятых электронных носителей информации или обладателем содержащейся на них информации, осуществляется с участием законного владельца изъятых электронных носителей информации или обладателя содержащейся на них информации и (или) их представителей и специалиста в органе дознания, следствия или в суде. При копировании информации должны обеспечиваться условия, исключающие возможность ее утраты или изменения. Не допускается копирование информации, если это может воспрепятствовать расследованию преступления и (или) проступка. Электронные носители информации, содержащие скопированную информацию, передаются законному владельцу изъятых электронных носителей информации или обладателю содержащейся на них информации. Об осуществлении копирования информации и о передаче электронных носителей информации, содержащих скопированную информацию, законному владельцу изъятых электронных носителей информации или обладателю содержащейся на них информации составляется протокол в соответствии с требованиями УПК КР.

Также статья 91 УПК КР устанавливает, что электронный документ признается доказательством, равным по своей значимости письменным доказательствам и имеет одинаковую юридическую силу с документом, воспроизведенным на бумажном носителе, в соответствии с законом Кыргызской Республики "Об электронном документе и электронной цифровой подписи". При этом оговаривается, что оригинал электронного документа существует только на машинном носителе. Все экземпляры электронного документа, подписанные электронной цифровой подписью, зафиксированные на машинном носителе и идентичные один другому, являются оригиналами и имеют одинаковую юридическую силу. Копии электронного документа создаются путем воспроизведения формы внешнего представления электронного документа на бумажном носителе.

Уголовно-процессуальное законодательство КР допускает прослушивание телефонных и иных переговоров, получение информации о соединениях между абонентами, а также снятие информации с компьютеров, серверов и других устройств, предназначенных для сбора, обработки, накопления и хранения информации, только при наличии достаточных на то оснований.

Закон КР «Об электрической и почтовой связи» определяет круг обязанностей операторов связи при проведении оперативно-розыскных мероприятий на сетях связи.

Операторы связи обязаны предоставлять уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность в сетях связи, информацию о пользователях услугами связи, а также иную информацию, необходимую для выполнения возложенных на эти органы задач, обеспечивать им организационные и программно-технические возможности проведения оперативно-розыскных мероприятий во всех сетях и на каналах связи, доступ к базам данных, автоматизированным системам оператора связи в случаях, установленных законодательством Кыргызской Республики.

Операторы связи обязаны обеспечивать реализацию установленных Правительством КР **требований к сетям и средствам связи** для проведения оперативно-розыскных мероприятий, а также принимать меры по недопущению раскрытия организационных и тактических приемов проведения указанных мероприятий.

Операторы сотовой связи обязаны вести **реестр идентификационных кодов абонентских устройств**, работающих в их сети, а также в порядке, определяемом Правительством КР, осуществлять сбор и хранение в течение 3 лет данных об абонентах.

Технические требования к сетям связи, специальным техническим средствам, предназначенным для контроля и фиксации получаемых законным путем сведений/информации, передаваемой по техническим каналам связи, порядку взаимодействия при реализации функций системы оперативно-розыскных мероприятий в сетях связи, включая проработку интерфейса (технического регламента), разработку необходимого программного обеспечения, решение вопроса о соединении и каналах доступа, иные вопросы, связанные с обеспечением законности осуществления оперативно-розыскных мероприятий в сетях связи, комплексного решения всех вопросов и проблем, связанных с внедрением и функционированием системы оперативно-розыскных мероприятий в сетях связи, в соответствии с разработанными в этой сфере международными рекомендациями и техническими концепциями, а также требованиями действующего законодательства Кыргызской Республики устанавливаются Правительством Кыргызской Республики.

Порядок взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность, устанавливается «Инструкцией о порядке взаимодействия операторов электросвязи и операторов мобильной сотовой связи с государственными органами Кыргызской Республики, осуществляющими оперативно-розыскную деятельность», утвержденной постановлением Правительства КР от 30.06.2014года № 360.

Выводы: принятие нового уголовно-процессуального кодекса и введение его в действие лишь с января 2019года не решает имеющиеся проблемы в судопроизводстве в настоящее время.

Введение новых законодательных норм процессуального характера не охватывают должным образом всю деятельность правоохранительных органов, связанную с обеспечением доказательств в суде.

Существует необходимость в развитии цифровой криминалистики в целях организации и проведения криминалистических экспертиз аппаратов и программных обеспечений, анализа вредоносных программ и тому подобных мероприятий, имеющих юридическое значение при обеспечении доказательств в суде.

Проведение военных операций по киберзащите

В мае 2016 года наряду с Россией, Беларусью, Казахстаном и Арменией Кыргызстан стал участником антитеррористических учений «Кибер-Антитеррор-2016», в ходе которых органы безопасности и спецслужбы этих стран при поддержке Антитеррористического центра СНГ провели комплекс мероприятий по выявлению и пресечению актов кибертерроризма.

Стоит отметить, что Кыргызская Республика в недостаточной мере осуществляет мероприятия по защите киберпространства. Учитывая глобальность роста

террористических угроз, к которым отнесен кибертерроризм, в стране должен быть создан орган, специализирующийся на планировании и проведении кибер-операций. Военные учения по кибероборонe должны проводиться не только на международном, но и на местном национальном уровне.

Обеспечение международной кибербезопасности

Согласно Концепции внешней политики, утвержденной указом Президента КР от 10 января 2007 года № 2, выделяются следующие основные приоритеты:

1. Укрепление национальной безопасности внешнеполитическими методами.
2. Формирование благоприятных внешних условий для реализации национальных приоритетов развития.
3. Укрепление положительного международного имиджа Кыргызстана.
4. Формирование эффективной системы внешнеполитической деятельности во главе с Министерством иностранных дел Кыргызской Республики и в партнерстве с другими заинтересованными ведомствами и институтами гражданского общества.

Концепцией отмечено, что Кыргызстан видит значительные возможности обеспечения своего развития и безопасности в укреплении и расширении сотрудничества со странами Антитеррористической коалиции, что гарантирует стремление государства участвовать в международных мероприятиях по защите киберпространства в том числе.

В приоритетах внешней политики Концепции не обозначена кибебезопасность, что свидетельствует о необходимости её переработки с учетом угроз, существующих в настоящее время.

Кыргызстаном подписано Соглашение МЕЖДУ ПРАВИТЕЛЬСТВАМИ ГОСУДАРСТВ—ЧЛЕНОВ ШАНХАЙСКОЙ ОРГАНИЗАЦИИ СОТРУДНИЧЕСТВА О СОТРУДНИЧЕСТВЕ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (16.06.2009года), в котором реализуя сотрудничество в соответствии с настоящим Соглашением, государства - участники исходят из наличия следующих основных угроз в области обеспечения международной информационной безопасности: 1) разработка и применение информационного оружия, подготовка и ведение информационной войны; 2) информационный терроризм; 3) информационная преступность; 4) использование доминирующего положения в информационном пространстве в ущерб интересам и безопасности других государств; 5) распространение информации, наносящей вред общественно- политической и социально-экономической системам, духовной, нравственной и культурной среде других государств; 6) угрозы безопасному, стабильному функционированию глобальных и национальных информационных инфраструктур, имеющие природный и (или) техногенный характер.

Подводя итоги проведенных исследований в области кибербезопасности, проанализировав действующее законодательство Кыргызской Республики в сфере информационной и кибербезопасности, сделаны следующие выводы о том, что:

- законодательство КР не имеет четкого определения таких терминов, как кибербезопасность, киберпространство, кибергигиена, критическая инфраструктура и т.д.;

- не имеется уполномоченного государственного органа для обеспечения кибербезопасности в виде созданной и полноценно функционирующей структуры по реагированию на возникающие угрозы и киберинциденты (CERT), иерархия государственных структур, задействованных в данной сфере (Совета безопасности (обороны), Государственный комитет национальной безопасности, Министерство внутренних дел, Государственный комитет информационных технологий и связи) не выстроена четким образом с точным и ясным распределением задач и функций в информационной сфере;

- Кыргызская Республика достаточно слабо представлена в международных договорах и соглашениях в сфере обеспечения информационной и кибербезопасности (за исключением Соглашения государств-членов Шанхайской организации сотрудничества, в рамках ОДКБ работа только начата);

- хотя во многих учебных заведениях страны имеются программы обучения по вопросам информационной безопасности, при этом подготовка отечественных специалистов в сфере обеспечения и регулирования кибербезопасности не осуществляется, а обучение программам, охватывающим информационную безопасность, оставляет желать лучшего и не отвечает требованиям сегодняшнего дня;

- нет возможностей для защиты критической инфраструктуры, поскольку само понятие «критической информационной инфраструктуры» не содержится в действующем законодательстве (есть фрагментировано урегулированные вопросы стратегических объектов, в том числе телекоммуникационных);

- нет специализированной разработанной архитектуры по уровням кибербезопасности.

Для восполнения имеющихся пробелов, с учетом наилучшей международной практики, следует рассмотреть возможность и организовать следующие мероприятия:

- Нормативно закрепить иерархию государственных структур, задействованных в сфере обеспечения кибербезопасности (Совет безопасности (обороны), Государственный комитет национальной безопасности, Министерство внутренних дел, Государственный комитет информационных технологий и связи), с чётким распределением задач, функций и пределов ответственности.
- Принять меры к созданию специализированного документа, отражающего суть и значение развития кибербезопасности в Кыргызской Республике, такого как Концепция\Стратегия по кибербезопасности, который позволил бы определить конкретные понятия и термины по кибербезопасности, выстроить четкую структуру органов, задействованных в ее обеспечении, расставить акценты по международному взаимодействию и т.п. вопросы.
- После принятия Концепции/Стратегии по кибербезопасности разработать план мероприятий, направленный на реализацию стратегических целей по защите информационных ресурсов, критической инфраструктуры от киберугроз. В Плане мероприятий по её реализации должны быть определены организации, ответственные за осуществление мер, четко обозначенных для каждого государственного органа, принимающего участие в реализации Плана, а также

определены конкретные сроки выполнения мероприятий. Все это должно быть подкреплено прописанными финансовыми ресурсами с четким распределением на каждое конкретное мероприятие Плана.

- Создать государственный центр по реагированию на компьютерные инциденты (CERT), который будет нести ответственность за управление инцидентами в сфере безопасности в кыргызских компьютерных сетях, оказывающий помощь кыргызским пользователям интернета в осуществлении превентивных мер для сокращения возможного ущерба от инцидентов в сфере кибербезопасности и оказание помощи при реагировании на возникающие киберугрозы.
- Пересмотреть образовательные программы с целью введения новых дисциплин для более глубокого изучения информационной и кибербезопасности для средне-специальных и высших учебных заведений страны. Обязательным элементом образовательных программ, включая и школьные образовательные программы, должны стать обучающие практики по защите персональных данных среди несовершеннолетних пользователей интернета и их родителей.
- Создать уполномоченный государственный орган, на который были бы возложены функции по контролю и надзору за работой с персональными данными, согласно требований закона КР «Об информации персонального характера».
- Разработать и законодательно закрепить понятие критической инфраструктуры, а также рассмотреть возможность в создании государственного органа или отдела, специализирующегося на её защите, возложив на него ответственность за разработку надлежащих мер безопасности, а также координацию и контролирование мероприятий по их осуществлению.
- На основе международной практики и опыта зарубежных стран дополнить уголовное законодательство нормами, устанавливающими ответственность за совершение преступлений против конфиденциальности, целостности и доступности компьютерных данных и систем, деяний, связанных с подлогом компьютерных данных и других противоправных действий, способных причинить тяжкие и необратимые последствия.
- Принимать меры к развитию цифровой криминалистики в целях организации и проведения криминалистических экспертиз аппаратов и программных обеспечений, анализа вредоносных программ и тому подобных мероприятий, имеющих юридическое значение при обеспечении доказательств в суде.
- Активизировать работу правоохранительных органов, отвечающих за обеспечение информационной безопасности, по укреплению и расширению сотрудничества со странами Антитеррористической коалиции, увеличив количество участия в международных мероприятиях по защите киберпространства.