Анализ действующего законодательства, регулирующего информационную безопасность и выявление ключевых пробелов с рекомендациями:

В рамках проекта завершен правовой анализ действующего законодательства Кыргызской Республики, регулирующего сферу информационной и кибербезопасности, для оценки существующей ситуации с правовым регулированием данной сферы, выявления пробелов в целях выработки рекомендаций по их восполнению.

Изучен опыт зарубежных стран в этой сфере (ЕС, СНГ), сделан обзор международной практики в сфере кибербезопасности, изучены модельные законы стран СНГ (таких как Российская Федерация, Эстония, Молдова, Казахстан, Грузия), документы и стандарты МСКО, в том числе инициативы в сфере информационной безопасности и способов защиты данных.

Проведен подробный анализ и оценка действующих в Кыргызской Республике нормативных правовых актов, необходимых для обеспечения кибербезопасности на предмет выявления упущений, противоречий, в том числе в используемой терминологии, необходимости гармонизации с успешной международной практикой в этой сфере.

Информационно-Коммуникационные Технологии (ИКТ) являются неотъемлемой составной частью экономического и социального развития страны на пути к информационному обществу. Сегодняшний мир живет в эпоху глобальной конвергенцией цифровых, физических и биологических технологий, изменяя мир вокруг и понимание качества жизни. Информационные технологии фундаментально изменили образ нашей повседневной жизни, способы работы и коммуникаций между людьми. Связь уже не просто соединяет людей: становятся реальностью концепции интернета вещей (IoT), больших данных и "умных" сетей.

Активное развитие информационно-коммуникационных технологий и растущее использование сети Интернет, с особой остротой определяет необходимость обеспечения безопасности в информационной среде, составной частью которой является киберпространство, и защиты информационной инфраструктуры, требующей широкого диапазона мер в области сетей связи и их информационной безопасности, борьбы с киберпреступностью.

Транснациональный и трансграничный характер многих продуктов ИКТ и открытая природа Интернета используются международной преступностью в целях совершения противоправных действий с использованием ИКТ, что приводит к росту киберпреступности,

Увеличение числа пользователей Интернета повышает критичность и делает более ощутимыми последствия в случае отказов техники, ведет к увеличению количества атак на абонентские устройства. Пренебрежение требованиями безопасности при использовании интернет-ресурсов и социальных сетей, игнорирование мер «цифровой гигиены» повышает риск неприкосновенности частной жизни, модификации или уничтожению персональных данных. Низкий уровень компьютерной грамотности конечных пользователей при отсутствии базовых знаний по общим методам компьютерных атак приводит к росту фактов кибер-мошенничества, противоправного использования ИКТ.

Меры, связанные с автоматизацией оказания государственных услуг, начавшаяся цифровизация государственных и муниципальных услуг, доступа к информации о деятельности государственных органов, создание государственных информационных ресурсов и систем, аккумулирование в них большого количества данных, в том числе критически важных (биометрика, данные, необходимые для выполнения государственных функций) также несут в себе определенные риски. Объем данных, обрабатываемых в государственном секторе, постоянно растет, что приводит к необходимости выработки новых форм их хранения и обеспечения их безопасности. Защита и безопасность данных, особенно критически важных, имеет сегодня решающее значение.

Беспечность в выборе поставщиков технологий обеспечения информационной и кибербезопасности государственных органов, отсутствие возможностей для аудита исходных кодов программного обеспечения, или непредставление таковых, также ведет к невозможности оценки рисков, связанных с намеренным внедрением в программное обеспечение или телекоммуникационное оборудование не декларируемых функций, которые потенциально могут быть использованы для нанесения ущерба государственным интересам.

Критичной для Кыргызстана является ситуация с отсутствием обязательных для госорганов требований в сфере информационной и кибербезопасности для государственных информационных систем, включая обучение руководителей подразделений и всего задействованного в оказании электронных государственных и муниципальных услуг персонала принципам и технологиям защиты конфиденциальной информации.

В правовом поле, несмотря на обилие нормативных правовых актов в сфере информатизации, отсутствует единая терминология в части базовых терминов информационной и кибербезопасти. В действующем уголовном законодательстве отсутствуют многие составы совершаемых сегодня киберпреступлений, в процессуальном законодательстве – методы фиксации и оценки цифровых доказательств.

Ситуация усугубляется дефицитом доверия общественности к принимаемым государством мерам, направленным на защиту государственных информационных систем, обеспечение кибербезопасности.

При этом частный и финансовый сектор вынужден полагаться исключительно на собственные силы. Недооценена важность совместных усилий по формированию безопасного киберпространства внутри страны. Недостаточная обеспеченность бизнес сектора в технологиях защиты информации, зачастую не желание признавать потребности в защите информации и сетевой безопасности, приводит к большому количеству остающихся латентными инцидентов информационной и кибербезопасности.

Остро ощущается общая нехватка экспертов по информационной и кибербезопасности, особенно в государственном секторе. Программы обучения и подготовки специалистов в этой сфере, не в полной мере отвечают сегодняшним тенденциям и реалиям.

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

- представляет собой устаревшую нормативную базу, большинство законов были сформированы в принципиально иной технологической и социальной среде, и в силу этого не учитывают современных трендов в сфере кибербезопасности;
- не содержит терминов и определений информационной безопасности, кибербезопасности, киберпространства, кибергигиены, нет понятий критической информационной инфраструктуры и т.п.;
- в определенной степени остается противоречивым, не подкреплено реальными ресурсами;
- не обеспечивает эффективный контроль обеспечения прав субъектов правовых отношений в сере информационной и кибербезопасности.

Проблемой является отсутствие в Кыргызской Республике единой концепции информационной и кибербезопасности в качестве комплексного рамочного документа, определяющего государственную политику в этой сфере.

Вместе с тем, оперативное, проактивное и эффективное противодействие киберугрозам, киберпреступности требует принятия адекватных мер реагирования на уровне государственных органов, и прежде всего - концептуального закрепления необходимых мер на доктринальном и нормативно-правовом уровне, создания государственной политики в области обеспечения информационной и кибербезопасности с вовлечением всех заинтересованных сторон.

Создание единого концептуального документа должно прояснить суть многих терминов в сфере информатизации, упорядочить роли и задачи субъектов информационной деятельности и определить методы обеспечения безопасности киберсферы. Вопросы кибербезопасности следует решать, принимая во внимание глобальный, транснациональный характер киберугроз.

Концепция кибербезопасности должна обеспечить единство подходов к формированию и реализации общенациональной политики обеспечения безопасности защищаемых законом видов информации, защиты электронных информационных ресурсов и систем, информационно-коммуникационной инфраструктуры, а также методологической базы и нормативных правовых актов, регулирующих сферу безопасного использования ИКТ.

Необходимой мерой является и создание организационных киберструктур, специальных подразделений в правоохранительных органах, развитие сети центров реагирования на компьютерные инциденты (CERT) для определения киберугроз, управления операциями и

реагирования на них, а также участия в механизмах сотрудничества на внутригосударственном, региональном и международном уровнях, привлечение технического и экспертного сообщества по вопросам потенциальных решений в сфере кибербезопасности.

Общая цель таких мер должна состоять в создании и постоянном поддержании системы управления кибербезопасностью, обеспечивающей устойчивое развитие Кыргызской Республики при использовании информационно-коммуникационных технологий.

Необходимо развитие национального потенциала в области кибербезопасности, обмен информацией о передовом опыте, привлечение всего сообщества в целом. Формирование культуры кибербезопасности путем распространения передового опыта, повышение уровня осведомленности по вопросам кибербезопасности, создании необходимого потенциала, совершенствования средств кибербезопасности, укрепление и поддержание согласованности усилий в сфере кибербезопасности;

Вопросы кибербезопасности должны включать состояние защищенности средств телекоммуникаций (средств связи), цифровых (электронных) информационных ресурсов информационных систем, информационно-коммуникационной инфраструктуры от внешних и внутренних угроз.

Основными направлениями обеспечения кибербезопасности должны стать:

- правовое обеспечение (принятие и применение правовых норм в сфере 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).

Принятие подобного концептуального документа будет означать значимый шаг в признании проблемы уязвимого киберпространства, выстраивании адекватных сегодняшнему дню методов и способов его защиты.

По результатам разработки и принятия концепции кибербезопасности необходимо разработать план мероприятий, направленный на реализацию стратегических целей по повышению институционального и человеческого потенциала обеспечения кибербезопасности, созданию и защите кибер-физических систем, информационных ресурсов, критической инфраструктуры от киберугроз. В Плане мероприятий должны быть четко определены органы/организации, ответственные за осуществление мер, сроки выполнения мероприятий. Все это должно быть подкреплено прописанными финансовыми ресурсами с четким распределением на каждое конкретное мероприятие.

В стране не выстроена четким образом и нормативно не закреплена иерархия государственных структур, задействованных в сфере обеспечения кибербезопасности с четким распределением задач и функций в данной сфере. Не создан уполномоченный государственный орган по реагированию на возникающие угрозы и киберинциденты (CERT).

Результаты проведенного правового анализа позволяют сформулировать следующие общие **выводы и рекомендации**:

1) законодательно установить термины и определения кибербезопасности; **разработать стратегию (концепцию) кибербезопасности,** определить меры для достижения целей в области кибербезопасности на национальном уровне; разработать **план реализации такой стратегии**, в котором определить органы/организации, ответственные за осуществление мер, сроки выполнения поставленных задач, финансовые ресурсы для их выполнения;

выстроить на национальном уроне систему органов государственного управления, задействованных в определении политики кибербезопасности и ее реализации на организационном (управление), нормативно-правовом (доктринальном), инженерно-техническом уровне;

создать уполномоченный государственный орган по реагированию на возникающие угрозы и киберинциденты (CERT) (либо в структуре органов национальной безопасности, либо в структуре Госкомитета информационных технологий и связи); ежегодно публиковать отчеты о

киберугрозах и рисках, информировать общественность в целях повышения осведомленности, в том числе через веб-сайт такого уполномоченного органа (CERT); указанный уполномоченный CERT должен нести ответственность за (обладать следующими функциями):

Предотвращение киберугроз:

- предупреждение организаций и широкой общественности о значимых инцидентах кибербезопасности;
- подготовка аналитических отчетов об известных угрозах;
- отслеживание инцидентов кибербезопасности;

Реагирование на киберугрозы:

-распространение соответствующей информации об инцидентах кибербезопасности;

- гарантировать быстрое реагирование на широкомасштабные национальные кризисные инциденты;
- подготовка отчетов об инцидентах, ежегодно подготавливать, по крайней мере, один публичный отчет;
- выступать в качестве контактного пункта в случае инцидентов кибербезопасности на международном уровне в режиме 24/7;
- обеспечить партнерство отечественных и международных заинтересованных сторон по обмену опытом в области кибербезопасности;
- быть членом признанной международной организации по реагированию на инциденты кибербезопасности;

Прогнозирование киберугроз:

- подготовка и распространение образовательных материалов по повышению потенциала кибербезопасности;
- проведение учений по кибербезопасности;
- подготовка и поддержка руководств по лучшей практике по всем аспектам работы CERT, включая создание, управление, расследование инцидентов и использование форензик инструментов.

Предусмотреть на законодательном уровне, что субъекты государственного сектора и операторы критической информационной инфраструктуры обязаны сообщать об инцидентах кибербезопасности;

В соответствии с правовыми актами установить, что субъекты государственного и частного сектора обмениваются соответствующей информацией о кибреугрозах, киберицидентах.

Рассмотреть вопрос о создании в вооруженных силах страны отделы, ответственные за защиту национальное киберпространства (подразделение по кибероперациям/кибероборону).

4) принять меры **к пересмотру образовательных стандартов от общешкольного до ВУЗовского и послеВУЗОвского образования**, чтобы основные знания в области кибербезопасности приобретались в рамках общего образования; внедрить программы профессионального и высшего образования для подготовки технических, правовых и полиси специалистов по кибербезопасности; в целом принимать регулярные меры к повышению потенциала в сфере кибербезопасности;

создать независимый государственный надзорный орган, который отвечает за защиту персональных данных;

внедрить нормативные правила и принять стандарты для управления безопасностью ИКТ в государственном секторе; в том числе предусмотреть, что до внедрения ИКТ-решений в государственном секторе, при государственных закупках проводился обязательный аудит по безопасности, как программных, так и технических средств (исходных программных кодов, бэк-доров); предусмотреть регулярность такого аудита ИТК-решений в государственном секторе;

пересмотреть законодательство с целью внедрения правовой базы для электронной аутентификации и электронной подписи на принципах технологической нейтральности, универсальности, соответствия требований к шифрованию признанным современным международным принципам; выстроить надлежащую систему сертификации средств

шифрования, в соответствии с которыми требования к цифровой подписи и устройствам электронной подписи соответствуют надлежащим требованиям к безопасности;

8) законодательно **выстроить меры к защите критической информационной инфраструктуры**, пересмотреть законодательство о стратегически объектах; нормативно в правовых актах определить понятия и критерии критически важных секторов и критической информационной инфраструктуры; в структуре Госкомитета информационных технологий и связи **создать отдел, специализирующийся на защите критической информационной инфраструктуры на национальном уровне**; для операторов критической информационной инфраструктуры установить обязательные требования к обработке данных и непрерывности услуг с обязательством назначить сотрудника, ответственного за кибербезопасность;

9) поручить **Правительству разработать план управления в случае кризисной ситуации, связанной с кибербезопасностью**; проводить регулярные учения по управлению в случае кризисной ситуации, связанной с кибербезопасностью, и по возможности обеспечивать участие специалистов в учениях на международном уровне; проводить учения по киберзащите;

в уголовном законодательстве принять меры по криминализации следующих составов уголовных киберпреступлений (в соответствии с международными подходами, в том числе Конвенцией Совета Европы о киберпреступности):

- незаконный доступ к информации, данным, сетям;
- незаконный перехват информации, данных;
- незаконное вмешательство в целостность информации, данных;
- незаконное вмешательство в работу информационных систем;
- ненадлежащее использование компьютерных устройств;

принять меры к законодательному (на уровне процессуального законодательства) закреплению методов и средств цифровой криминалистики (компьютерной форензики), внедрить соответствующие методы и способы фиксации цифровых доказательств в целях расследования, их представления в суде;

12) рассмотреть вопрос об усилении международного сотрудничества, заключению соглашений по вопросам кибербезопасности с другими странами и/или международными организациями.