Положение 3
(к постановлению Правительства
Кыргызской Республики
от 3 мая 2019 года № 209)

КОНЦЕПЦИЯ
информационной безопасности Кыргызской Республики на 2019-2023 годы

1. Общие положения

1. Концепция информационной безопасности Кыргызской Республики (далее - Концепция) представляет собой совокупность официальных взглядов на обеспечение национальной безопасности Кыргызской Республики в информационной сфере.

2. Информационная безопасность Кыргызской Республики является одной из составляющих национальной безопасности Кыргызской Республики и влияет на состояние защиты национальных интересов Кыргызской Республики в различных сферах жизнедеятельности общества и государства.

3. Правовую основу обеспечения информационной безопасности в настоящее время составляют Конституция Кыргызской Республики, Концепция национальной безопасности Кыргызской Республики, законы Кыргызской Республики "О гарантиях и свободе доступа к информации", "О защите государственных секретов Кыргызской Республики", "О средствах массовой информации", "О телевидении и радиовещании", "Об издательском деле", "Об обязательном экземпляре документов", "Об электрической и почтовой связи", "Об электронном управлении", Уголовный кодекс Кыргызской Республики, Гражданский кодекс Кыргызской Республики, Кодекс Кыргызской Республики о нарушениях, Кодекс Кыргызской Республики о проступках, постановление Правительства Кыргызской Республики "Об утверждении Требований к защите информации, содержащейся в базах данных государственных информационных систем" от 21 ноября 2017 года № 762, другие нормативные правовые акты Кыргызской Республики, а также международные договоры, участницей которых является Кыргызская Республика.

2. Определения и термины

4. В настоящей Концепции используются следующие основные термины:

национальные интересы Кыргызской Республики в информационной среде (далее - национальные интересы в информационной среде) - объективно значимые потребности в сохранении системы жизненных устоев и ценностей, обеспечении устойчивого развития и защищенности личности, общества и государства в информационной сфере;

информационная безопасность Кыргызской Республики (далее - информационная безопасность) - состояние защищенности личности, общества и государства от информационных угроз;

угроза информационной безопасности - потенциально возможное событие, действие (воздействие), процесс или явление, которое может привести к нанесению ущерба национальным интересам в информационной сфере в краткосрочной и долгосрочной перспективе;

обеспечение информационной безопасности - осуществление комплекса общегосударственных и отраслевых мер по прогнозированию, выявлению, предупреждению и нейтрализации информационных угроз, а также устранению последствий их проявления;

система обеспечения информационной безопасности - часть системы национальной безопасности, включающая совокупность сил и средств обеспечения информационной безопасности;

силы обеспечения информационной безопасности - государственные органы, органы местного самоуправления и организации, уполномоченные в соответствии с законодательством Кыргызской Республики на участие в обеспечении информационной безопасности;

информационная инфраструктура - совокупность информационных систем, информационно-телекоммуникационных сетей и автоматизированных систем управления технологическими процессами, используемых для формирования, создания, преобразования, передачи, использования и хранения информации, а также для управления технологическими процессами;

информационная сфера - совокупность информации, объектов информатизации, информационных систем, информационно-телекоммуникационных сетей, сетей связи, информационных технологий, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений;

объект информационных отношений - информация, информационные технологии, информационная инфраструктура, информационные ресурсы, информационные процессы, направленные на удовлетворение информационных потребностей общества;

субъект информационных отношений - физические и юридические лица, их объединения, государственные и негосударственные организации, общество в целом, которые являются участниками информационных отношений, наделенные определенными правами и обязанностями в информационной сфере и способные их осуществлять;

информационное воздействие - действия, направленные на изменение восприятия информации субъектом информационной среды;

методы обеспечения информационной безопасности - правовые, организационно-технические и экономические методы, направленные на обеспечение информационной безопасности;

информационное пространство - сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием и хранением информации;

контент - любое информационно-значимое наполнение средств массовой коммуникации. Под средствами массовой коммуникации понимается совокупность средств массовой информации (пресса, радио, телевидение, сеть Интернет) и средств массового воздействия (театр, кино, цирк, литература).

3. Анализ состояния информационного пространства

5. Современный этап развития Кыргызской Республики оказывает непосредственное влияние на состояние ее информационной безопасности. При этом возрастающая роль информационных отношений является ключевым компонентом деятельности органов государственной власти, государственного управления и институтов гражданского общества, связанных с созданием, преобразованием и потреблением информации.

6. Развитие информационно-коммуникационных технологий, обусловленное технологическим прорывом и широким применением инноваций, стало определяющим фактором повсеместного внедрения и использования информационно-коммуникационных технологий во всех сферах жизни людей, что представляет повышенные требования к решению вопросов информационной безопасности.

7. Реальные темпы развития и распространения информационно-коммуникационных технологий во всех сферах жизнедеятельности общества являются факторообразующими элементами, которые необходимо учитывать в процессе определения ключевых проблем в области информационной безопасности.

8. В настоящее время на государственном уровне проводится поэтапное внедрение проектов и программ цифровой трансформации Кыргызстана.

9. Так, в рамках Концепции Национальной Программы цифровой трансформации "Цифровой Кыргызстан" - 2019-2023", одобренный решением Совета безопасности Кыргызской Республики от 14 декабря 2018 года № 2, планируется реализация следующих направлений:

- развитие национального цифрового контента на государственном языке;
- внедрение проекта "Цифровой парламент";
- цифровизация государственных и муниципальных услуг для граждан и бизнеса;
- разработка проекта "Цифровое правосудие и правопорядок";
- цифровизация сельского хозяйства и стимулирование инноваций;
- цифровизация легкой промышленности;
- цифровая трансформация туризма.

Также в рамках цифровой трансформации реализуются следующие проекты:

- система межведомственного взаимодействия "Тундук";
- проект в рамках государственно-частного партнерства "Безопасный город";
- автоматизированная информационная система "Единый реестр преступлений и проступков";
- автоматизированная информационная система "Единый реестр нарушений";
- программа Министерства образования и науки Кыргызской Республики "Умная школа";
- Программа перехода на цифровое телерадиовещание в Кыргызской Республике, утвержденная постановлением Правительства Кыргызской Республики от 2 ноября 2011 года № 692.

10. Так, Кыргызская Республика занимает 103-е место согласно национальному индексу кибербезопасности - 19% (индекс, публикуемый Академией электронного управления Эстонии), 96-е место согласно Глобальному индексу кибербезопасности - 27% (индекс, публикуемый Международным союзом электросвязи Организации Объединенных Наций), 109-е место согласно Индексу развития информационно-коммуникационных технологий - 44% (индекс, публикуемый Международным союзом электросвязи Организации Объединенных Наций).

Рис. Национальный индекс кибербезопасности

Примечание к диаграмме:

Общие индикаторы кибербезопасности	%	Базовые индикаторы кибербезопасности	%	Индикаторы инцидентного и кризисного управления	%
1. Разработка политики кибербезопасности	0	5. Защита цифровых услуг	20	9. Реагирование на компьютерные инциденты	0
2. Анализ киберугроз	0	6. Защита основных услуг	0	10. Управление киберкризисом	0
3. Образование и профессиональное развитие	44	7. Электронная идентификация и услуги доверия	89	11. Борьба с киберпреступностью	0
4. Вклад в глобальную кибербезопасность	17	8. Защита персональных данных	25	12. Военные кибероперации	0

11. Одновременно с этим в 2018 году разработан проект "Digital CASA - Кыргызская Республика", являющийся региональным проектом по созданию трансграничной телекоммуникационной сети, которая свяжет страны Центральной и Южной Азии в единый цифровой хаб. Одним из главных преимуществ данного проекта станет доступ стран-участников к дешевому и более качественному Интернету.

12. При этом необходимо отметить, что в межгосударственных отношениях нарастает тенденция использования информационного давления как действенного механизма глобальной конкуренции. Использование различных средств информационной пропаганды и информационной экспансии стало неотъемлемым инструментом решения крупных социальных, экономических и политических конфликтов. Развитые страны мира, имеющие возможность осуществления глобального мониторинга распространяемой информации, используют его результаты для получения односторонних преимуществ в политических, экономических, военных, экологических и прочих аспектах межгосударственных отношений.

13. Экстремистскими и террористическими организациями и группами все активнее используются возможности глобальных информационно-коммуникационных сетей для пропаганды своей идеологии, вербовки и обучения единомышленников, поддержания связи и финансирования различных террористических групп. Распространение

радикальных идей различного толка среди молодежи Кыргызстана вызывает озабоченность. Отмечаются случаи, когда граждане под влиянием целенаправленной пропаганды, в том числе посредством сети Интернет, участвуют в незаконных акциях в различных регионах мира.

14. Существенную проблему составляет распространение информационной преступности (киберпреступности), в том числе деятельность организованных транснациональных преступных групп. Борьба с информационной преступностью требует от правоохранительных органов и специальных служб адекватного оперативного реагирования путем проведения совместных скоординированных действий со специальными службами и правоохранительными органами зарубежных стран.

15. Усиливается роль и влияние глобальных средств массовой информации и коммуникационных механизмов на развитие экономической, политической и социальной ситуации в различных странах мира. Фундаментальные перемены, произошедшие в последние годы в странах с различными экономическими и политическими условиями, указывают на ключевую роль в данных процессах новых технологий управления массами, в том числе посредством использования информационно-коммуникационных технологий: сайтов, социальных сетей и мобильных приложений.

16. Широкое использование населением Кыргызстана возможностей сети Интернет создает предпосылки их использования для оказания целенаправленного воздействия на внутриполитическую ситуацию в ущерб национальным интересам республики.

17. По данным Государственного агентства связи при Государственном комитете информационных технологий и связи Кыргызской Республики, в 2014 году количество пользователей Интернет-услуг составило всего 4147148, в 2015 году - 4754601, в 2016 году - 5240801, в 2017 году - 4802937 (данное снижение объясняется увеличением пользователей Интернет в период проведения Всемирных игр кочевников, прошедших в сентябре 2016 года, а также изменением метода учета абонентов некоторых операторов связи в 2017 году), на конец III квартала 2018 года - 5028889.

18. Уровень проникновения сети Интернет среди населения республики, по состоянию на конец III квартала 2018 года, составил около 80,4%, в 2017 году - 75,8%.

19. В связи с открытостью национального информационного пространства и популярностью зарубежных средств массовой информации, в том числе телевидения и интернет-ресурсов (почтовых служб, социальных сетей, блогов и видеопорталов), возникает реальная угроза информационного влияния на общественное сознание населения. Информационное влияние может выражаться как в виде прямого навязывания идей, противоречащих национальным интересам Кыргызской Республики, так и в виде создания определенного информационного фона, искусственно поддерживаемого путем манипулирования информацией или ее тенденциозным комментированием.

20. Для противодействия подобному манипулированию общественным сознанием требуется серьезно улучшить эффективность государственной информационной политики, увеличить открытость государственных органов, повысить обеспеченность права граждан на информацию.

21. Серьезные угрозы несет в себе проблема неконкурентоспособности отечественного контента. Его качество остается недостаточным для полноценной конкуренции с иностранным информационным продуктом. В условиях открытости национального информационного пространства это приводит к непопулярности отечественного продукта. В свою очередь, низкая популярность не позволяет привлечь значимые инвестиции в его производство, что приводит к крайней недостаточности производства отечественного контента.

22. Согласно данным Государственного агентства связи при Государственном комитете информационных технологий и связи Кыргызской Республики, число абонентов технологии IPTV на конец III квартала 2018 года составил - 26588, в 2017 году - 24188, в 2016 году - 16120.

23. При этом, согласно данным Министерства культуры, информации и туризма Кыргызской Республики на 2018 год, на территории республики на 80 отечественных телеканалов приходится 449 зарубежных телерадиоканалов.

24. Все более остро встает вопрос о совершенствовании программ по подготовке квалифицированных кадров в сфере информационной безопасности. Требуется дальнейшее совершенствование процессов и подходов к обучению, повышение квалификации специалистов государственных органов, организаций, занятых в сфере обеспечения информационной безопасности.

25. Существенно отстает от потребностей текущего дня правовое обеспечение информационной сферы. Недостаточно проработаны правовые механизмы, регулирующие информационные правоотношения, возникающие при осуществлении поиска, получении и потреблении различной категории информации, информационных ресурсов, информационных продуктов, информационных услуг. Нуждаются в улучшении и актуализации правовые механизмы, регулирующие процессы производства, передачи и распространения информации, информационных ресурсов, информационных продуктов, информационных услуг. Особо остро стоит вопрос с регулированием информационных правоотношений, возникающих при создании и применении информационных систем, их сетей, средств обеспечения, телекоммуникационной инфраструктуры. Современное состояние правового обеспечения противодействия информационным преступлениям также характеризуется недостаточной согласованностью используемых правовых механизмов, фрагментарностью деятельности субъектов законодательной инициативы по их развитию и совершенствованию, недостаточной эффективностью, противоречивостью правовых норм.

26. Согласно Национальной стратегии развития Кыргызской Республики на 2018-2040 годы, утвержденной Указом Президента Кыргызской Республики от 31 октября 2018 года № 221, в сфере информационной безопасности государство будет фокусироваться на критически важных направлениях, таких как обеспечение кибербезопасности информационно-коммуникационных технологий и информационных систем, создание системы реагирования на киберугрозы и киберинциденты, а также профилактика всех видов экстремизма и терроризма.

27. Вместе с тем необходимо формирование отечественного медиаконтента, способного конкурировать в необходимых сферах.

28. Согласно Концепции национальной безопасности Кыргызской Республики, утвержденной Указом Президента Кыргызской Республики от 9 июня 2012 года № 120, в связи с растущим использованием сети Интернет с особой остротой встает вопрос защиты информационной инфраструктуры, требующей широкого диапазона мер в области сетей связи и их информационной безопасности, борьбы с киберпреступностью.

4. Основные проблемы и угрозы информационной безопасности

29. Ключевыми проблемами состояния информационной безопасности являются:

- незащищенность, неконтролируемость и недостаточность правового и технического регулирования информационного пространства;
- распространение киберпреступности;
- отсутствие эффективного противодействия трансграничной информационной преступности в современных условиях, сложность контроля за деятельностью интернет-ресурсов;
- незащищенность индивидуального и массового сознания граждан от вредного и опасного контента в ходе информационного взаимодействия субъектов, манипуляция мнением пользователей сети Интернет представителями террористических и экстремистских организаций;
- слаборазвитый отечественный контент средств массовой коммуникации;
- недостаточное финансирование государственных инициатив в области обеспечения информационной безопасности Кыргызской Республики;
- недостаточный уровень подготовки квалифицированных кадров в сфере информационной безопасности, информационной политики и защиты государственных секретов.

30. Угрозы информационной безопасности Кыргызской Республики представляют собой совокупность условий и факторов, создающих потенциальную или реально существующую опасность нанесения ущерба объектам и субъектам информационной сферы страны. Такие угрозы могут иметь объективный и субъективный характер, выражаться в явлениях, процессах и действиях/бездействиях (или их совокупности) и исходить от внешних и внутренних источников по отношению к информационной сфере Кыргызской Республики.

31. Внешними угрозами для информационной сферы Кыргызской Республики являются негативные для нее физические явления, политические, экономические и иные мировые процессы, а также любые иные подрывные действия, направленные против интересов Кыргызской Республики. К таким угрозам относятся:

1) рост транснациональной преступности в сфере компьютерных технологий и информации, нарушающей сохранность информационных ресурсов и штатное функционирование государственных информационных систем;

2) увеличение технологического отрыва других государств, усиливающее зависимость Кыргызской Республики от использования зарубежной техники и программного обеспечения для защиты критических информационных инфраструктур;

3) разработка рядом стран программ по ведению информационного воздействия и пропаганды, в целях достижения преимущества в информационной сфере;

4) деятельность международных экстремистских, террористических и других преступных сообществ, организаций и групп в информационной сфере Кыргызской Республики;

5) распространение в информационном пространстве противоправного контента, а также иной идеологии, нарушающих нравственные устои общества;

6) обострение международной конкуренции за обладание стратегически важной информацией, стремление ряда стран к доминированию в информационном пространстве Кыргызской Республики и получению доступа к информации с ограниченным доступом;

7) введение некоторыми государствами на своих информационных рынках всевозможных ограничений, ущемляющих интересы Кыргызской Республики.

32. Внутренними угрозами являются процессы и действия субъектов информационной сферы, осуществляющих свою деятельность на территории Кыргызской Республики. К таким угрозам относятся:

1) эксплуатация устаревших технических устройств и оборудования, приобретение импортных технических и программно-аппаратных средств, а также средств защиты информации при создании и развитии информационной инфраструктуры Кыргызской Республики;

2) отставание Кыргызской Республики от многих стран мира по уровню информатизации деятельности органов государственной власти, местного самоуправления и хозяйствующих субъектов;

3) слабая координация деятельности органов власти и управления Кыргызской Республики по укреплению информационной безопасности и недостаточность финансового обеспечения мероприятий, нацеленных на защиту информационной сферы Кыргызской Республики;

4) несовершенство нормативной правовой базы, регулирующей межведомственные отношения и систему контроля в информационной сфере Кыргызской Республики, а также недостаточная правоприменительная практика в данной области;

5) несовершенство законодательства по своевременному ограничению доступа к материалам деструктивного характера в сети Интернет, а также отсутствие законодательной базы по вопросам регулирования взаимоотношений в сети Интернет, несовершенство правоприменительной практики в отношении распространения противоправной информации;

6) функционирование на приграничных территориях Кыргызской Республики теле- и радиоканалов сопредельных государств;

7) отсутствие государственной системы анализа и мониторинга информационного пространства Кыргызской Республики.

33. По своей общей направленности угрозы информационной безопасности Кыргызской Республики подразделяются на следующие виды:

1) угрозы правам и свободам личности в области информационной деятельности и духовной жизни, индивидуальному, групповому и общественному сознанию, обусловленные:

- сдерживанием процессов развития информационной сферы Кыргызской Республики;
- несоблюдением законных ограничений на создание и распространение в Кыргызской Республике информации, разжигающей расовую, этническую, национальную, религиозную и межрегиональную рознь, а также разрушающей нравственные устои общества;

- широкой пропагандой образцов, так называемой массовой культуры, противоречащей исторически сложившимся менталитету и традициям народа Кыргызской Республики и ведущих к постепенному разрушению норм морали в обществе;

- противоправным применением специальных средств воздействия на индивидуальное, групповое и общественное сознание и, как следствие, усиление зависимости духовной, экономической и политической сфер в общественной жизни Кыргызской Республики от навязываемой извне информации;

- угроза подмены государственной идеологии и мировоззрения посредством навязывания идей через средства массовой коммуникации;

- угроза мобилизации граждан для участия в незаконных акциях, вербовки посредством материалов радикального характера;

2) угрозы информационной поддержке и информационному обеспечению внутренней и внешней политики, реализуемой руководством Кыргызской Республики, обусловленные:

- недостаточным вниманием со стороны государственных органов вопросам своевременной разработки проектов нормативных правовых актов;

- деятельностью в информационном пространстве Кыргызской Республики (включая сеть Интернет) информационных агентств, средств массовой информации и иных информационных структур, искажающих информацию о внутренней и внешней политике Кыргызской Республики;

- недостаточной эффективностью деятельности национальных информационных агентств и средств массовой информации по противодействию негативному информационному воздействию на население Кыргызской Республики;

- недостаточным финансово-техническим обеспечением государственных органов, уполномоченных вести работу в области информационной безопасности и информационной политики;

3) угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории Кыргызской Республики, такие как:

- противоправные сбор и использование информации, нарушения технологии обработки информации;

- несанкционированный доступ к информации, находящейся в банках и базах данных;

- разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;

- уничтожение, повреждение, радиоэлектронное подавление, разрушение или хищение средств и систем обработки информации, телекоммуникации и связи, машинных и других носителей информации;

- воздействие или компрометация на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации, средств криптографической защиты информации;

- утечка информации по техническим каналам;

- внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;

- использование несертифицированных зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи;

- внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;

- нарушение законных ограничений на распространение информации;

- увеличение оттока за рубеж специалистов и правообладателей интеллектуальной собственности.

5. Основные цели, задачи и методы обеспечения информационной безопасности

34. Целью настоящей Концепции является выработка и реализация мер, направленных на защиту интересов личности, общества и государства в информационной сфере и создание эффективной национальной системы обеспечения информационной безопасности Кыргызской Республики, представляющей собой совокупность правовых, организационных и экономических методов по реализации государственной политики в данной сфере.

35. Интересы личности в информационной сфере состоят в обеспеченности ее прав и свобод по доступу к достоверной и полной информации, ее использованию для осуществления не запрещенной законом деятельности, интеллектуального, духовного, нравственного и физического развития, а также в гарантированности прав на защиту информации, обеспечивающей личную безопасность.

36. Интересы общества в информационной сфере заключаются в обеспеченности в ней интересов личности, развитии демократии, сохранении духовных ценностей, создании правовых и иных основ для достижения и поддержания в республике мира, стабильности и общественного согласия.

37. Интересы государства в информационной сфере заключаются в ее гармоничном формировании, наиболее эффективном развитии и использовании в целях реализации прав и свобод личности и общества, соблюдения норм законности и правопорядка, обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности Кыргызской Республики, достижения экономического роста, политической и социальной стабильности.

38. Национальными интересами в сфере информационной безопасности являются:

- соблюдение прав и свобод человека и гражданина в области получения и пользования информации, обеспечение духовного развития народа Кыргызстана, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны;

- информационное обеспечение государственной политики Кыргызской Республики, связанное с доведением до национальной и международной общественности достоверной информации о государственной политике Кыргызской Республики, ее официальной позиции по социально значимым событиям внутригосударственной и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам;

- защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории Кыргызской Республики;

- развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранения и эффективного использования отечественных информационных ресурсов.

39. Основные задачи Концепции:

- выработка предложений по совершенствованию законодательства в сфере обеспечения информационной безопасности Кыргызской Республики;

- координация деятельности органов власти и управления в сфере разработки и реализации мероприятий по комплексному противодействию угрозам информационной безопасности Кыргызской Республики;

- развитие и совершенствование правового, методического, научно-технического и организационного обеспечения работ, относящихся к этой сфере;

- выявление, оценка и прогнозирование угроз информационной безопасности.

40. Методы обеспечения информационной безопасности Кыргызской Республики разделяются на правовые, организационно-технические и экономические:

1) правовые методы обеспечения информационной безопасности Кыргызской Республики включают:

- разработку нормативных правовых актов и нормативно-методических документов, регламентирующих отношения и действия всех субъектов в информационной сфере Кыргызской Республики;

- разработку правовых механизмов, направленных на недопущение в Кыргызской Республике противозаконных информационно-психологических воздействий на сознание личности и общества;

- активизацию целенаправленной деятельности компетентных правоохранительных органов Кыргызской Республики по предупреждению и пресечению правонарушений в информационной сфере государства;

2) организационно-технические методы обеспечения информационной безопасности Кыргызской Республики заключаются в непрерывном совершенствовании технологии защиты информации и государственных информационных систем от потенциальных и реальных угроз.

К таким методам относятся:

- создание и совершенствование системы обеспечения информационной безопасности Кыргызской Республики;

- создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи;

- разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения;

- усиление правоприменительной деятельности органов исполнительной власти Кыргызской Республики, включая предупреждение и пресечение правонарушений в информационной сфере, а также выявление и привлечение к ответственности лиц, совершивших преступления, и другие правонарушения в этой сфере;

- формирование системы мониторинга показателей и характеристик информационной безопасности Кыргызской Республики в наиболее важных сферах жизнедеятельности общества и государства;

- государственная поддержка и координация действий субъектов информационных отношений в подготовке кадров в области обеспечения информационной безопасности;

3) экономические методы включают в себя:

- разработку, соответствующее финансирование и неукоснительное выполнение государственных целевых программ обеспечения информационной безопасности Кыргызской Республики в целом и информационной безопасности в конкретных специфических областях жизнеобеспечения государства (наука, техника, экономика, банковское дело, оборона, правоохранительная деятельность и т.д.).

41. Противодействие всем видам угроз информационной безопасности Кыргызской Республики осуществляется путем комплексного использования правовых, организационно-технических и экономических методов.

42. Противодействие угрозам, касающимся прав и свобод человека в области информационной деятельности и духовной жизни, индивидуального, группового и общественного сознания, осуществляется преимущественно правовыми методами, а также путем решения органами власти и управления Кыргызской Республики экономических, организационных и технических вопросов, связанных с повышением уровня компьютерного образования населения и с расширением доступа общественности к социально значимой информации.

43. В противодействии угрозам информационной поддержки и информационному обеспечению внешней и внутренней политики, проводимой руководством Кыргызской Республики, а также развитию национальной индустрии технических средств, программного обеспечения информации, информатизации и связи, развития отечественной информационной продукции и услуг используются в основном правовые и экономические методы.

44. Организационно-технические методы являются основными методами для противодействия угрозам функционирования государственных информационных систем, накоплению, сохранности и эффективному использованию их информационных ресурсов.

6. Основные направления в области обеспечения информационной безопасности

45. Основные направления в области обеспечения информационной безопасности:

1) в сфере обеспечения информационной безопасности в информационных и телекоммуникационных системах:

- принятие стратегического документа в области обеспечения кибербезопасности;

- организация единой системы мер обеспечения кибербезопасности;

- определение уполномоченного органа в области обеспечения кибербезопасности;

- определение и категорирование критической информационной инфраструктуры Кыргызской Республики, выработка правовых, организационно-технических мер по обеспечению ее безопасности;

- формирование национальной системы предупреждения, реагирования и управления компьютерными инцидентами;

- криминализация и противодействие компьютерной преступности;

- создание национальной системы защиты информации, включая криптографическую защиту информации;

- определение единого подхода к обеспечению кибербезопасности в государственном секторе Кыргызской Республики;

- техническая стандартизация в области кибербезопасности;

- изучение положительного зарубежного опыта и внедрение механизмов государственно-частного партнерства в области обеспечения кибербезопасности;

2) в сфере внутренней и внешней политики:

- выработка и принятие мер по защите конституционных прав и свобод человека и гражданина в информационной сфере;

- разработка и внедрение правовых и организационно-технических мер по регулированию информационной сферы от негативного ее влияния на стабильность государственной власти, межнациональное, межконфессиональное и межрегиональное согласие, суверенитет и территориальную целостность Кыргызской Республики;

- принятие мер нормативного и административного характера, стимулирующих государственные учреждения и организации к размещению открытой информации о проводимой политике и результатах деятельности на официальных интернет-ресурсах;

- оказание государственного содействия (в т.ч. экономические преференции: налоговые, таможенные и др.) средствам массовой информации и коммуникации, включая интернет-ресурсы, продвигающие положительный имидж государства;

- применение информационных технологий в доведении до общественности страны и международного сообщества достоверной информации о государственной политике Кыргызской Республики и ее официальной позиции по социально значимым событиям в стране и в мире, в целях обеспечения национальной безопасности;

- разработка и реализация основных направлений организационного и технического обеспечения информационного сопровождения внутренней и внешней политики государства;

- активное ведение информационной деятельности с позиции дипломатических представительств по предотвращению информационного вмешательства во внутренние дела государства с использованием возможностей современных информационно-коммуникационных технологий;

- осуществление международного сотрудничества в сфере обеспечения информационной безопасности Кыргызской Республики, представление интересов Кыргызской Республики в соответствующих международных организациях;

3) в сфере образования и науки:

- разработка целевых программ и реализация мероприятий по обучению несовершеннолетних правилам и культуре поведения в информационной сфере;

- информационное обеспечение и внедрение систем исключения доступа к информации, несовместимой с задачами образования и воспитания обучающихся в организациях начального, среднего и высшего образования;

- разработка и реализация мероприятий по организации безопасного доступа образовательных организаций к сети Интернет;

- проведение обучающих мероприятий в образовательных организациях по безопасному использованию сети Интернет;

- разработка нормативного правового акта о защите детей и подростков от информации, причиняющей вред их здоровью и развитию;

- внедрение механизмов защиты детей и подростков от противоправного и социально опасного контента;

- профилактика у детей и подростков Интернет-зависимости и правонарушений с использованием информационно-коммуникационных технологий;

- формирование у несовершеннолетних навыков ответственного и безопасного использования информационно-телекоммуникационных технологий;

- совершенствование подходов в вопросах подготовки высококвалифицированных кадров в области информационной безопасности Кыргызской Республики;

- создание необходимых условий для осуществления и развития прикладных научных исследований и государственная поддержка научной деятельности в области информационной безопасности;

4) в сфере культуры и информации:

- принятие мер нормативного и административного характера по использованию современных информационно-коммуникационных технологий в сфере культуры и искусства;

- использование современных достижений в области информационно-коммуникационных технологий для осуществления творческой деятельности и функционирования учреждений культуры;

- пропаганды культуры и традиций в информационной сфере при помощи современных информационно-коммуникационных технологий, в целях защиты от негативного влияния на общественное сознание;

- формирование и продвижение с помощью современных информационно-коммуникационных технологий общенациональной идеологии;

- использование современных информационно-коммуникационных технологий в сфере туризма в Кыргызской Республике (туристические маршруты с помощью информационных технологий, интернет-экскурсии и т.д.);

- государственное содействие развитию отечественного контента, путем применения налоговых и других стимулирующих преференций;

- выработка предложений по развитию национальных информационных агентств и ресурсов;

- обеспечение онлайн-присутствия телерадиоорганизаций и периодических печатных СМИ в интернет-пространстве, популяризация интернет-версий СМИ, разработка мобильных приложений;

- позиционирование одного из телерадиоорганизаций как поставщика эксклюзивных материалов о масштабных событиях в жизни страны, о важнейших новостях глобального уровня, уникальных материалов зарубежных партнеров, размещение государственного заказа на реализацию социальных телепроектов;

- развитие международного медиа-сотрудничества в наиболее значимых для Кыргызской Республики политических, экономических, культурных, социальных и других информационных сферах;

- формирование системы мониторинга информационного пространства, в целях противодействия распространению противоправного контента в средствах массовой информации и интернет-пространства;

- осуществление мониторинга информационного пространства за соблюдением телерадиоорганизациями производства объемов отечественного контента (национальной аудиовизуальной продукции), предъявляемых нормами действующего законодательства Кыргызской Республики;

- определение юридического статуса интернет-пространства, регламентация взаимоотношений в интернет-пространстве;

5) в религиозной сфере:

- применение современных информационно-коммуникационных технологий в целях проведения мероприятий по агитации о недопущении нарушения общественной стабильности вследствие деятельности религиозных объединений, проповедующих религиозный фундаментализм, а также тоталитарных религиозных сект;

- размещение на официальных интернет-площадках информации о традиционных течениях религии, в целях просвещения населения, а также о запрещенных религиозных организациях;

- выработка мер по повышению религиозной грамотности, профилактика религиозного экстремизма и терроризма среди населения с использованием современных информационно-коммуникационных технологий;

- противодействие негативному информационному воздействию и деструктивному влиянию религиозных организаций в информационной сфере;

6) в сферах обороны и правопорядка:

- совершенствование форм и способов активного противодействия операциям в информационном пространстве, направленным на ослабление обороноспособности государства;

- противодействие использованию информационных технологий для совершения противоправных действий, в том числе для оказания деструктивного информационного воздействия на сознание личного состава вооруженных сил и граждан Кыргызской Республики;

- разработка и совершенствование правовых, организационно-технических механизмов, методов и способов противодействия деструктивному информационному воздействию на индивидуальное, групповое и массовое сознание;

- совершенствование системы органов обеспечения информационной безопасности в военной сфере;

- осуществление систематического анализа применения средств, форм и способов информационного противоборства в военной сфере;

- выработка действенного механизма взаимодействия государственных органов и операторов связи в противодействии распространению противоправной информации в сетях и каналах связи;

- совершенствование правоприменительной практики органов исполнительной власти Кыргызской Республики, включая предупреждение и пресечение правонарушений в информационной сфере, а также выявление и привлечение к ответственности лиц, совершивших преступления, и другие правонарушения в этой сфере.

7. Государственно-частное партнерство в области обеспечения информационной безопасности

46. В настоящее время актуальное значение приобретает развитие механизмов взаимодействия государства, населения, бизнеса и структур гражданского общества посредством развития механизмов государственно-частного партнерства в сфере обеспечения информационной безопасности.

47. В Кыргызской Республике 22 февраля 2012 года был принят Закон "О государственно-частном партнерстве в Кыргызской Республике", который предусматривает взаимодействие государственного и частного партнеров по вопросам привлечения государственным партнером частного партнера к проектированию, финансированию, строительству, восстановлению, реконструкции объектов, а также по управлению существующими или вновь создаваемыми объектами, в том числе инфраструктурными.

48. Анализ состояния в области обеспечения информационной безопасности требует внедрения принципиально новых форм взаимодействия государственного и частного сектора, в целях совместного решения проблем обеспечения информационной безопасности.

49. Основной причиной, сдерживающей развитие государственно-частного партнерства в сфере обеспечения информационной безопасности, является отсутствие в Кыргызской Республике опыта в осуществлении эффективного взаимодействия между государством и бизнесом в данном направлении.

50. В целях выработки и внедрения механизмов государственно-частного партнерства в сфере информационной безопасности необходимо:

- изучить положительный опыт зарубежных стран в реализации проектов государственно-частного партнерства в области обеспечения информационной безопасности;

- стимулировать законодательные инициативы бизнес-сообществ, осуществляющих деятельность в области информационной безопасности;

- оказывать государственную поддержку частным компаниям, задействованным в реализации проектов государственно-частного партнерства в сфере информационной безопасности, в форме налоговых, таможенных и иных преференций.

8. Система и принципы обеспечения информационной безопасности

51. Система обеспечения информационной безопасности строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере.

52. Обеспечение информационной безопасности осуществляется на основе сочетания законодательной, правоприменительной, правоохранительной, судебной, контрольной и других форм деятельности государственных органов во взаимодействии с органами местного самоуправления, организациями и гражданами.

53. Организационную основу системы обеспечения информационной безопасности составляют государственные органы, принимающие в соответствии с законодательством Кыргызской Республики участие в решении задач по обеспечению информационной безопасности.

54. Участниками системы обеспечения информационной безопасности являются: собственники объектов информационной инфраструктуры и организации, эксплуатирующие такие объекты, средства массовой информации и массовых коммуникаций, организации денежно-кредитной, валютной, банковской и иных сфер финансового рынка, операторы связи, операторы информационно-телекоммуникационных систем, организации, осуществляющие деятельность по созданию и эксплуатации информационных систем и сетей связи, организации по разработке, производству и эксплуатации средств обеспечения информационной безопасности, организации по оказанию услуг в области обеспечения информационной безопасности, держатели массивов персональных данных, организации, осуществляющие образовательную деятельность в данной области, общественные объединения, религиозные и иные организации, а также граждане.

55. Деятельность государственных органов по обеспечению информационной безопасности основывается на следующих принципах:

1) соблюдение Конституции Кыргызской Республики, законов и иных нормативных правовых актов Кыргызской Республики, а также общепризнанных принципов и норм международного права;

2) уважение основных прав и свобод граждан, жизненно важных интересов личности, общества и государства в целом;

3) единство, взаимосвязь и адекватность системы мер обеспечения информационной безопасности;

4) приоритет политических и экономических мер обеспечения информационной безопасности;

5) взаимная ответственность личности, общества и государства по обеспечению информационной безопасности;

6) открытость и доступность информации о деятельности органов государственной власти по обеспечению информационной безопасности, за исключением случаев, когда такая открытость и доступность в соответствии с законодательством Кыргызской Республики может нанести ущерб национальной безопасности Кыргызской Республики;

7) эффективное взаимодействие государственных органов, организаций и граждан при решении задач по обеспечению информационной безопасности.

9. Международное сотрудничество в сфере обеспечения информационной безопасности

56. В международных отношениях в области обеспечения информационной безопасности необходимо исходить из своих национальных интересов, действуя в соответствии с общепризнанными принципами и нормами международного права, а также вступившими в установленном законом порядке в силу международными договорами, участницей которых является Кыргызская Республика.

57. Для реализации целей международного сотрудничества в обеспечении информационной безопасности требуется актуализация сотрудничества Кыргызской Республики с международными организациями, занимающимися обеспечением информационной безопасности на мировом и региональном уровнях. Особое внимание следует уделить сотрудничеству со странами СНГ и государствами - членами ЕАЭС, ОДКБ и ШОС.

58. Основные направления международного сотрудничества Кыргызской Республики по вопросам обеспечения информационной безопасности формируют уполномоченные государственные органы.

10. Реализация Концепции

59. Реализация настоящей Концепции осуществляется на основе отраслевых документов стратегического планирования развития Кыргызской Республики. В целях актуализации таких документов Правительством Кыргызской Республики определяется перечень приоритетных направлений обеспечения информационной безопасности на среднесрочную перспективу.

60. В каждой из сфер информационных отношений имеются свои особенности, связанные со спецификой защищаемых объектов и степенью их уязвимости в отношении угроз информационной безопасности. В целях обеспечения информационной безопасности таких объектов должны разрабатываться и реализовываться внутриведомственные специальные концепции, соответствующие программы и планы мероприятий по их реализации.

61. Разработка и рассмотрение концепций, государственных целевых программ, планов мероприятий, направленных на обеспечение информационной безопасности Кыргызской Республики, а также реализация государственной политики в сфере обеспечения информационной безопасности Кыргызской Республики осуществляются государственными органами в рамках полномочий, предоставленных им законодательством Кыргызской Республики.

62. Совершенствование правового обеспечения политики информационной безопасности Кыргызской Республики осуществляется на основе соответствующих планов работы государственных органов, предусматривающих анализ проблем правового регулирования отношений в рассматриваемой области, определение рациональных путей их решения, подготовку проектов нормативных правовых актов по конкретным направлениям этого регулирования. Проведение данных работ может осуществляться на основе соответствующих межведомственных государственных целевых программ.

63. Эффективность реализации настоящей Концепции зависит от уровня консолидации усилий всех заинтересованных государственных органов, частных и общественных организаций, широкой общественности.