Научная статья/ Research article

Внешнеполитический аспект в обеспечении безопасности и противодействия угрозам кибертерроризма в Республике Казахстан и Кыргызской Республике

А. А. Абасова
Российский университет дружбы народов им. П. Лумумбы, Москва, Россия
e-mail: 1032229852@rudn.ru

М. А. Абек
Российский университет дружбы народов им. П. Лумумбы, Москва, Россия
e-mail: 1032229815@rudn.ru

Н. Имаралиев
Российский университет дружбы народов им. П. Лумумбы, Москва, Россия
e-mail: 1032225423@rudn.ru

Аннотация. Особенностью информационного терроризма является большой географический охват. У виртуального терроризма отсутствуют явно очерченные границы, и имеются связи и взаимодействия с международными террористическими центрами и организациями, которые сами по себе являются довольно гибкой структурой. Благодаря и технологических достижений в области IT-технологий: информационно-пропагандистская работа ведется террористами с предельной эффективностью. Данная работа включает в себя подбор и подготовку сторонников, активных функционеров и бойцов с целью их практического использования в кризисных зонах. Киберпреступность является одной из важных проблем XXI века. Многие страны подвергаются нападениям в виртуальном мире теряя важные данные. Потери от кибератак с каждым годом растут всё больше, а пандемия, которая ускорила цифровизацию по всему миру лишь увеличила риск. Происходит атака на мышление людей, обладевание личными данными и государственно важной информацией. Кибертерроризм является растущей угрозой во всём мире. В странах Центральной Азии заметен рост данной угрозы информационной безопасности. Это связано с тем, что в странах региона возрастает зависимость от технологий и глобальной сети для связи. Это вкдючает еще торговлю и государственные услуги. Угроза кибератак и утечек данных является серьезной проблемой для правительств, предприятий и частных лиц в регионе. В данной статье рассмотрены вызовы и возможности кибертерроризма в странах региона, а именно в Кыргызстане и Казахстане. Будут разобраны меры, которые могут быть приняты для решения этой проблемы. В данной статье рассмотрены нормативно-правовые акты Республики Казахстан и Кыргызской Республики, методы борьбы против киберпреступности, сотрудничетсво против кибертерроризма в рамках международных организаций.

Ключевые слова: информационный терроризм, кибертерроризм, информационная безопасность, Казахстан, Кыргызстан, кибербезопасность.

Для цитирования: Абасова А. А., Абек М. А., Имаралиев Н. Внешнеполитический аспект в обеспечении безопасности и противодействия угрозам кибертерроризма в Республике Казахстан и Кыргызской Республике // Постсоветские исследования. 2023;6(6):639-650.

Foreign policy aspect in ensuring security and countering cyberterrorism threats in the Republic of Kazakhstan and the Kyrgyz Republic

Altynai A. Abasova
RUDN University named after P. Lumumba, Moscow, Russia
e-mail: 1032229852@rudn.ru

Malika Abek
RUDN University named after P. Lumumba, Moscow, Russia

e-mail: 1032229815@rudn.ru
Nurislam Imaraliev
RUDN University named after P. Lumumba, Moscow, Russia
e-mail: 1032225423@rudn.ru

Abstract. A feature of information terrorism is its large geographical coverage. Virtual terrorism has no clearly defined borders, and there are connections and interactions with international terrorist centers and organizations, which in themselves are a fairly flexible structure. Thanks to the use of technological advances in the field of IT technologies: information and propaganda work is carried out by terrorists with the utmost efficiency. This work includes the selection and training of supporters, active functionaries and fighters with a view to their practical use in crisis zones. Cybercrime is one of the important problems of the XXI century. Many countries are being attacked in the virtual world losing important data. Losses from cyberattacks are growing more and more every year, and the pandemic, which has accelerated digitalization around the world, has only increased the risk. There is an attack on people's thinking, possession of personal data and state-important information. Cyberterrorism is a growing threat worldwide. The growth of this threat to information security is noticeable in the countries of Central Asia. This is due to the fact that the countries of the region are increasingly dependent on technology and a global network for communication. This will also include trade and public services. The threat of cyber-attacks and data leaks is a serious problem for governments, businesses and individuals in the region. This article discusses the challenges and opportunities of cyberterrorism in the countries of the region, namely in Kyrgyzstan and Kazakhstan. The measures that can be taken to solve this problem will be analyzed. This article discusses the regulatory legal acts of the Republic of Kazakhstan and the Kyrgyz Republic, methods of combating cybercrime, cooperation against cyberterrorism within the framework of international organizations.

Key words: information terrorism, cyberterrorism, information security, Kazakhstan, Kyrgyzstan, cybersecurity.

For citation: Abasova A.A., Abek M.A., Imaraliev N. Foreign policy aspect in ensuring security and countering cyberterrorism threats in the Republic of Kazakhstan and the Kyrgyz Republic // Postsovetskie issledovaniya = Post-Soviet Studies. 2023;6(6):639-650. (In Russ.).

Киберпреступность является относительно новым видом преступной деятельности, которую используют террористические группировки. Так как действия происходят в «виртуальном мире» понимание их является достаточно сложным, т.к. человек не сразу понимает, что находится в зоне информационной нестабильности.

По мнению экспертов Организации Объединенных Наций, термин «киберпреступность» охватывает любое преступление, которое может быть совершено через компьютерную систему или сеть, внутри компьютерной системы или сети или против компьютерной системы или сети. Таким образом, киберпреступность может быть отнесена к любому преступлению, которое было совершено в электронной среде [Рассолов 2003: 92]. В целом, преступление, совершенное в киберпространстве, может рассматриваться как незаконное вмешательство в работу компьютеров, компьютерных программ и компьютерных сетей, как несанкционированное изменение компьютерных данных, а также другие социально опасные незаконные действия, совершаемые с использованием компьютеров, компьютерных сетей и программ [Десятый Конгресс ООН, 2000].

Одним из опасных видов киберпреступности является кибертерроризм. Термин "кибертерроризм" появился в литературе примерно в 1997 году, когда специальный агент ФБР М. Поллитт определил этот вид терроризма как умеренные и политически мотивированные "преднамеренные" атаки на информационные системы, компьютерные программы и данные, выражающиеся в применении силы против гражданских

объектов субнациональными группами или секретными агентами [Вестник МГЛУ 2018: 215].

Одной из главных проблем кибертерроризма в Центральной Азии является недостаточная осведомленность и понимание рисков и угроз, связанных с технологиями и интернетом. Многие частные лица и организации в регионе не обладают необходимыми знаниями и навыками, чтобы защитить себя от кибератак и утечек данных. Эта ситуация усугубляется нехваткой ресурсов и инфраструктуры для поддержки инициатив в области информационной безопасности.

Другой проблемой является отсутствие сотрудничества и координации между правительственными учреждениями и организациями в регионе. Кибертерроризм — это глобальная проблема, требующая скоординированного реагирования, но многие агентства и организации в Центральной Азии располагают ограниченными ресурсами и возможностями для решения этой проблемы самостоятельно. Существует необходимость в более тесном сотрудничестве и обмене информацией между правительственными учреждениями и организациями региона для противодействия угрозе кибертерроризма.

В Казахстане и Кыргызстане проживает молодое и технически подкованное население, которое все больше подключается к интернету и социальным сетям. Это дает возможность повысить осведомленность и продвигать лучшие практики в области информационной безопасности среди молодого поколения. Существует также возможность использовать технологии и инновации для разработки новых инструментов и решений для борьбы с кибертерроризмом.

Для решения проблемы кибертерроризма в выделенных странах необходим комплексный подход, включающий как превентивные, так и ответные меры. Превентивные меры включают повышение осведомленности и пропаганду передовых методов обеспечения информационной безопасности, разработку политики и нормативных актов для защиты критически важной инфраструктуры, а также инвестиции в исследования и разработку новых инструментов и решений для борьбы с кибертерроризмом.

Ответные меры включают усиление мер безопасности и улучшение сбора разведывательной информации и обмена ею. Правительственные учреждения и организации в регионе должны работать сообща для обмена информацией и координации своих усилий по борьбе с кибертерроризмом. Они также должны сотрудничать с международными организациями, такими как Организация Объединенных Наций и Европейский союз, в разработке скоординированных мер реагирования на угрозу кибертерроризма.

Кибертерроризм в Казахстане

Кибербезопасность является важнейшей проблемой в Казахстане, поскольку, как было отмечено ранее, страна все больше полагается на технологии и инновационные средства связи. Угроза кибератак и утечек данных является одной из важнейших проблем XXI века. Текущее состояние кибербезопасности в Казахстане неоднозначно. За последние годы страна добилась значительного прогресса в развитии своей инфраструктуры информационных технологий и продвижении использования цифровых технологий. Однако, она по-прежнему сталкивается со значительными проблемами с точки зрения информационной и кибербезопасности. Недостаточная осведомленность и понимание рисков и угроз, связанных с технологиями и интернетом, является серьезным вызовом для относительно молодой страны, равно как и нехватка ресурсов и инфраструктуры для поддержки инициатив в области информационной безопасности.

Республика Казахстан с момента приобретения независимости (1991 г.) ставит во главу приоритетов свою безопасность и целостность. В более широком смысле здесь подразумевается не только территориальная безопасность, но и безопасность во всех сферах жизнедеятельности казахстанских граждан. Информационная безопасность – состояние защищенности информационного пространства Республики Казахстан, а также прав и интересов человека и гражданина,

общества и государства в информационной сфере от реальных и потенциальных угроз, при котором обеспечивается устойчивое развитие и информационная независимость страны[1]. Большое внимание правительство уделяет безопасности в интернет-пространстве на локальном, региональном и глобальном уровнях. Казахстан активно участвует в глобальном диалоге по противодействию терроризму и экстремизму. Немалое внимание в стране уделяется противодействую терроризма в интернетпространстве. Республика Казахстан также является непосредственным участником контртеррористической деятельности в рамках организаций ОДКБ, ШОС, СВМДА, Антитеррористического центра СНГ, в сотрудничестве с ОБСЕ активно проводит мероприятия обучающего характера, заседания, конференции и тренинги регионального и международного уровня, направленные на противодействие экстремизму и терроризму. [Лагуткина, Мадалимбеков, Омарова, 2022: 8]

В рамках ШОС планируется укрепление международного сотрудничества в вопросах информационной безопасности. Соответственно, и Казахстан и Кыргызстан являясь членами организации, должны содействовать обеспечению развития в области защиты информации и кибертерроризма. В рамках организации уже подписаны такие документы как: «Шанхайская конвенция о борьбе с терроризмом, экстремизмом сепаратизмом» (Шанхай, 2001); «Конвенция Шанхайской организации сотрудничества против терроризма» (Ташкент, 2009); «Московская декларация Совета глав государств-членов Шанхайской организации сотрудничества»; «Заявление Совета глав государств-членов Шанхайской организации сотрудничества о противодействии распространению террористической, сепаратистской и экстремистской идеологии, в том числе в сети Интернет» (Москва, 2020). В документах ШОС очень ясно изложены положения и описаны методы противодействия, которые не вызывают сомнения у стран-участниц. [Румянцева, Рахимов 2022: 5]

Также Казахстан следует глобальной антитеррористической стратегии Совета Безопасности ООН, и каждый год предоставляет отчеты о проделанной работе в сфере информационной безопасности. [Лагуткина, Мадалимбеков, Омарова, 2022: 8]

Одной из главных проблем кибербезопасности в Казахстане является отсутствие сотрудничества и координации между государственными органами и организациями. Кибербезопасность - это глобальная проблема, требующая скоординированного реагирования, но многие ведомства и организации в Казахстане обладают ограниченными ресурсами и возможностями для решения этой проблемы самостоятельно. Существует необходимость в более тесном сотрудничестве и обмене информацией между правительственными учреждениями и организациями в стране для устранения угрозы кибератак и утечки данных.

В Казахстане действует несколько нормативно-правовых актов, связанных с кибербезопасностью. Некоторые из ключевых законов и подзаконных актов, связанных с кибербезопасностью в Казахстане:

1. Закон об информатизации: Настоящий закон, принятый в 2015 году, регулирует использование информационно-коммуникационных технологий в Казахстане. Он устанавливает правовую базу для развития информационных систем и защиты информации[2].

2. Закон о персональных данных и их защите: Этот закон, принятый в 2013 году, регулирует сбор, хранение и использование

[1] Закон Республики Казахстан о национальной безопасности Республики Казахстан URL: https://www.akorda.kz/ru/security_council/national_security/zakon-respubliki-kazahstan-o-nacionalnoy-bezopasnosti-respubliki-kazahstan (дата обращения: 01.06.2023)

[2] Закон Ресублики Казахстан об информатизации// URL: https://online.zakon.kz/Document/?doc_id=33885902 (дата обращения: 01.06.2023)

персональных данных в Казахстане. Он устанавливает правовую базу для защиты персональных данных и прав физических лиц на доступ к своим персональным данным и контроль над ними[3].

3. Закон о связи: Этот закон, принятый в 2004 году, регулирует телекоммуникационную отрасль в Казахстане. Он устанавливает правовую базу для предоставления телекоммуникационных услуг и защиты телекоммуникационной инфраструктуры[4].

4. Концепция кибербезопасности: «Киберщит Казахстана». Этот закон, принятый в 2017 году, регулирует кибербезопасность в Казахстане. Он устанавливает правовую базу для защиты критически важной информационной инфраструктуры и предотвращения кибератак и утечек данных[5].

В стране действует несколько законов, которые связаны или имеют отношение к кибербезопасности. В целом, в Республике Казахстан принято около 30 проектов и законодательных актов, нацеленных на борьбу и противодействие информационному терроризму. Эти законы и нормативные акты устанавливают правовую базу для защиты критически важной информационной инфраструктуры и предотвращения кибератак и утечек данных.

Стоит отметить, что особое внимание уделено информационной безопасности в учебных заведениях РК. Ведется контроль над учебными сайтами и порталами. Спецслужбы следят за сохранностью и безопасностью личной информации обучающихся, а также за распространением сомнительного контента в интернет платформах и на различных сайтах. В основном, террористические группировки целятся для привлечения в свои ряды, в молодежь, которой легко манипулировать. А потому, данному вопросу уделяется и должно уделяться гораздо большее внимание.

В период пандемии коронавируса резко возросла нагрузка на цифровую инфраструктуру республики. Это связано с переходом на онлайн обучение, на дистанционную работу и многое другое. В Казахстане за последние несколько лет произошла цифравизация, которая облегчила жизнь граждан, но увеличила риск кибертерроризма.

Пандемия показала неготовность Казахстанской системы к большой нагрузке на сеть, и были зафиксированы проблемы работы государственных интернетпорталов. С начала 2020 г. в Казахстане зафиксировано порядка 200 кибератак. С целью профилактики кибератак и противодействия киберпреступности, в стране ужесточилось отслеживание переписки сомнительных пользователей сети, а также, по данным Комитета Национальной Безопасности, телефонные разговоры граждан могут быть записаны, если в разговоре звучат так называемые слова-маркеры, такие как: бомба, атака, террор и другие.

Кибертерроризм в Кыргызстане.

Обеспечение информационной безопасности и противодействие кибертерроризму в Кыргызской Республике являются составной частью общей информационной политики Кыргызстана. В праве Кыргызской Республики дано четкое понятие национальной «информационной безопасности», которая определена, как «одна из составляющих национальной безопасности Кыргызстана, влияющая на состояние защиты национальных интересов страны в различных сферах жизнедеятельности общества и государства»[6].

[3] Закон Республики Казахстан о персональных данных и их защите// URL:https://online.zakon.kz/Document/?doc_id=31396226 (дата обращения: 01.06.2023)

[4] Закон Республики Казахстан о связи// URL: https://online.zakon.kz/Document/?doc_id=1049207 (дата обращения: 01.06.2023)

[5] Концепция кибербезопасности: «Киберщит Казахстана»// URL: https://adilet.zan.kz/rus/docs/P1700000407 (дата обращения:01.06.2023)

[6] Концепция информационной безопасности Кыргызской Республики на 2019-2023 годы // Постановление Правительства Кыргызской Республики от 3 мая 2019 года №209. URL: http://cbd.minjust.gov.kg/act/view/ru-ru/13652 (дата обращения: 15.04.2023).

Текущую правовую основу обеспечения информационной безопасности и кибербезопасности составляют следующие правовые акты Кыргызской Республики:

1. Закон Кыргызской Республики «О национальной безопасности Кыргызской Республики» от 26 февраля 2003 года № 44 (В редакции Законов КР от 13 октября 2008 года № 212, 25 ноября 2011 года № 222, 18 марта 2017 года № 46, 1 декабря 2017 года N 197 (2))[7]. Настоящий Закон закрепляет правовые основы обеспечения безопасности личности, общества и государства, определяет систему национальной безопасности и ее функции, устанавливает порядок организации и финансирования органов обеспечения национальной безопасности, а также контроля и надзора за законностью их деятельности, включая информационную безопасность и кибербезопасность.

2. Концепция информационной безопасности Кыргызской Республики на 2019-2023 годы. Данная концепция была принята в 2019 году и представляет собой совокупность официальных взглядов на обеспечение национальной безопасности Кыргызской Республики в информационной сфере.

3. Стратегия кибербезопасности Кыргызской Республики на 2019-2023 годы[8]. Данная стратегия была принята в 2019 году и подчеркивает стратегические направления деятельности по построению национальной системы обеспечения кибербезопасности.

4. Концепция государственной политики Кыргызской Республики в религиозной сфере на 2014-2020 годы. Среди задач данной концепции есть «Разработка методологической базы информационных кампаний по продвижению в СМИ и социальных медиа конструктивного дискурса о религии путем создания альтернативного радикально-экстремистскому дискурсу информационного поля с целью разоблачения манипулятивных методов деструктивной и экстремистской пропаганды»[9]. Следовательно, данная концепция включает в себя принятие мер по противодействию кибертерроризму.

В Кыргызстане регламентированы политические механизмы обеспечения информационной безопасности правового, организационно-технического и экономического характера, с помощью которых обеспечивается информационная безопасность республики.

Правовые способы направлены на разработку новых правовых актов и механизмов, направленных на недопущение противозаконных информационно-психологических воздействий на сознание граждан и общества Кыргызстана; активизацию целенаправленной деятельности правоохранительных органов по предупреждению и пресечению преступлений и правонарушений в информационной сфере.

Организационно-технические способы предполагают непрерывное совершенствование технологий защиты информации и информационных систем от угроз. Для этого в республике создаются и совершенствуются системы и средства предотвращения несанкционированного доступа к информации и предотвращения специальных воздействий, вызывающих искажение информации; разрабатываются средства защиты информации; развиваются защищенные телекоммуникационные системы, повышать надежность программ; выявляются и привлекаются к

[7] Закон Кыргызской Республики «О национальной безопасности Кыргызской Республики» от 26 февраля 2003 года № 44 (В редакции Законов КР от 13 октября 2008 года № 212, 25 ноября 2011 года № 222, 18 марта 2017 года № 46, 1 декабря 2017 года N 197 (2)) // URL: http://cbd.minjust.gov.kg/act/view/ru- ru/1168?cl=ru-ru (дата обращения:26.04.2023).

[8] Стратегия кибербезопасности Кыргызской Республики на 2019-2023 годы. // Постановление Правительства Кыргызской Республики от 24 июля 2019 года № 369 URL: http://cbd.minjust.gov.kg/act/view/ru-ru/15479 (дата обращения:26.04.2023).

[9] Концепция государственной политики Кыргызской Республики в религиозной сфере на 2014-2020 годы. Утверждена Указом Президента КР от 17 ноябрь, 2014 // Правительство Кыргызской Республики. С. 21. URL: http://www.gov.kg/?p=45807 (дата обращения:27.04.2023).

ответственности лица, совершившие преступления и правонарушения в информационной сфере; создается система мониторинга информационной безопасности; осуществляется подготовка кадров в области обеспечения информационной безопасности.

Государству необходимо разрабатывать, финансировать и выполнять государственные целевые программы обеспечения информационной безопасности внешней и внутренней политики Кыргызстана. Обеспечение их информационной безопасности требует существенного усиления национальных механизмов ее реализации. Это должно быть частью комплексной государственной политики, реализуемой государственными органами, политическими силами и гражданами Кыргызстана.

Международными политическими механизмами обеспечения информационной безопасности Кыргызстана является участие в формирующейся системе международной информационной безопасности на двустороннем, многостороннем, региональном и глобальном уровнях. Особое внимание Кыргызстан уделяет сотрудничеству с государствами-членами СНГ, ЕАЭС, ОДКБ и ШОС. Кыргызстан поддерживает инициативы по установлению международного правового режима нераспространения информационного оружия; созданию механизмов международного сотрудничества в области противодействия угрозам при попытках вмешательства во внутренние дела суверенных государств; организации информационного обмена между евразийскими государствами; обеспечению технологического суверенитета.

Среди таких сотрудничеств в сфере кибербезопасности можно выделить:

1. Меморандум о взаимопонимании между Правительством Кыргызской Республики и корпорацией Майкрософт по сотрудничеству в рамках Программы инновационного правительства Майкрософт(R), который был одобрен Распоряжением Правительства Кыргызской Республики от 18 сентября 2009 года № 525-р. В рамках сотрудничества между Правительством Кыргызской Республики и корпорацией Майкрософт одной из ключевых задач меморандума было «повышение безопасности компьютеризации или кибербезопасности»[10]. Результатом чего явилось повышение уровня реагирования на случаи нарушения информационной безопасности и противодействие кибертерроризму.

2. Соглашение о сотрудничестве между Правительством Кыргызской Республики и Правительством Королевства Саудовской Аравии в области борьбы с преступностью, который был одобрен Распоряжением Правительства Кыргызской Республики от 14 января 2015 года № 3-р. Обе страны усилили дружеские отношения путем сотрудничества в области безопасности и эффективной борьбы с преступностью по 16 пунктам в разных сферах, включая «преступления, связанные с терроризмом (во всех формах – кибертерроризм) и его финансированием; киберпреступность»[11].

Информационная безопасность и противодействие угрозе кибертерроризма является важнейшим направлением системы национальной безопасности. В современных условиях эффективное обеспечение

[10] Меморандум о взаимопонимании между Правительством Кыргызской Республики и корпорацией Майкрософт по сотрудничеству в рамках Программы инновационного правительства Майкрософт(R). // Одобрен Распоряжением Правительства Кыргызской Республики от 18 сентября 2009 года № 525-р. URL: http://cbd.minjust.gov.kg/act/view/ru-ru/211306?ckwds=%25d0%25ba%25d0%25b8%25d0%25b1%25d0%25b5%25d1%2580 (дата обращения: 06.04.2023).

[11] Соглашение о сотрудничестве между Правительством Кыргызской Республики и Правительством Королевства Саудовской Аравии в области борьбы с преступностью, // Одобрен Распоряжением Правительства Кыргызской Республики от 14 января 2015 года № 3-р. URL: http://cbd.minjust.gov.kg/act/view/ru-ru/214239?ckwds=%25d0%25ba%25d0%25b8%25d0%25b1%25d0%25b5%25d1%2580 (дата обращения: 21.04.2023).

информационной безопасности нацелено не решение проблем и вопросов психологической, военной, экономической, экологической и прочих видов национальной безопасности. Информационная безопасность, и противодействие кибертерроризму как составляющие национальной безопасности, обеспечивает защиту информационного пространства суверенных государств; поддерживает справедливое распределение национальных ресурсов и благ; содействует переходу к устойчивому развитию информационной сферы; обеспечивает защиту ментальных основ и культуры народов. Процессы обеспечения национальной информационной безопасности включают правовые, организационно-технические и социально-культурные аспекты. Мировой и отечественный опыт противодействия угрозам национальным интересам в информационной сфере обуславливает потребность в формировании целостной системы безопасности. Информационная безопасность суверенных государств должна взаимно связывать правовые, организационные, идеологические и технические меры защиты и использовать современные методы прогнозирования, анализа и моделирования опасных ситуаций. Внешнеполитический аспект обеспечения информационной безопасности Кыргызской Республики обусловлен проблемами незащищенности, неконтролируемости и недостаточности нормативно-правового регулирования национальной информационной сферы; отсутствием эффективной системы противодействия транснациональной киберпреступности; отсутствием технических возможностей контролировать национальный сегмент Интернета; незащищенностью индивидуального и массового сознания кыргызстанцев от деструктивного информационного взаимодействия внешне-политических игроков, террористических и экстремистских групп; слабо развитостью национального контента и средств массовых коммуникаций; недостаточностью финансирования государственных мероприятий по обеспечению информационной безопасности Кыргызстана; недостаточностью уровня подготовки кадров в сфере информационной безопасности и информационной политики в целом. Внешними угрозами безопасности национальной информационной сферы Кыргызстана являются: рост террористических, экстремистских и международных преступных групп, а так же транснациональной киберпреступности, нарушающих сохранность информационных ресурсов и угрожающей информационно-психологической безопасности общества; технологическое отставание Кыргызстана от других государств, что усиливаете зависимость республики от зарубежного программного обеспечения, сервисов облачного хранения и информационной техники; внешнеполитическое информационное воздействие и пропаганда иностранных игроков, стремящихся получить и сохранить преимущества в информационной сфере Кыргызстана; распространение и пропаганда в национальном ин-формационном пространстве чуждых идеологических установок, нарушающих нравственные устои кыргызского общества; стремление ряда стран к доминированию в информационном пространстве Кыргызстана, получение ими секретной информации, а так же обострение международной конкуренции за обладание такой информацией; введение некоторыми государствами на своих информационно-коммуникативных рынках искусственных ограничений.

Обеспечение кибербезопасности. Обеспечение безопасности от кибертерроризма в Казахстане является критически важным вопросом, поскольку страна все больше полагается на технологии и интернет для связи, торговли и государственных услуг. Угроза кибератак и утечек данных является серьезной проблемой для правительства, бизнеса и частных лиц в стране.

Одной из главных проблем обеспечения безопасности от кибертерроризма в Казахстане является недостаточная осведомленность и понимание рисков и угроз, связанных с технологиями и

интернетом. Многие частные лица и организации в стране не обладают необходимыми знаниями и навыками, чтобы защитить себя от кибератак и утечек данных. Эта ситуация усугубляется нехваткой ресурсов и инфраструктуры для поддержки инициатив в области информационной безопасности.

Другой проблемой является отсутствие сотрудничества и координации между правительственными учреждениями и организациями в стране. Информационная безопасность - это глобальная проблема, требующая скоординированного реагирования, но многие ведомства и организации в Казахстане обладают ограниченными ресурсами и возможностями для решения этой проблемы самостоятельно. Существует необходимость в более тесном сотрудничестве и обмене информацией между правительственными учреждениями и организациями в стране для устранения угрозы кибератак и утечки данных.

Обеспечение безопасности в сфере киберпреступности в Казахстане является важнейшим вопросом. Проблемы информационной безопасности в стране сложны и многогранны, и решение этой проблемы требует скоординированного реагирования со стороны государственных органов и организаций.

Повышение кибербезопасности в Казахстане и Кыргызстане является критически важным вопросом, поскольку современными носителями информации можно управлять издалека и можно получить к ней доступ, не находясь физически рядом. Существуют некоторые меры, которые могут быть приняты для улучшения кибербезопасности в Казахстане и Кыргызстане:

1. Повышение осведомленности: Одним из наиболее важных шагов в улучшении кибербезопасности является повышение осведомленности среди отдельных лиц и организаций в обеих странах. Это может быть сделано с помощью кампаний по информированию общественности, обучающих программ и семинаров. Цель состоит в том, чтобы информировать людей о рисках и угрозах, связанных с технологиями и Интернетом, и продвигать передовые методы обеспечения информационной безопасности.

2. Разработка политики и нормативных актов: Правительствам обеих стран следует разработать политику и нормативные акты для защиты критически важной инфраструктуры и конфиденциальной информации. Эти политики должны включать руководящие принципы по защите данных, реагированию на инциденты и управлению рисками. Они также должны устанавливать наказания за киберпреступления и оказывать поддержку жертвам кибератак.

3. Инвестирование в технологии и инфраструктуру: Обе страны должны инвестировать в технологии и инфраструктуру для поддержки инициатив в области информационной безопасности. Это включает в себя разработку защищенных сетей, внедрение технологий шифрования и инвестиции в программное обеспечение и аппаратное обеспечение для кибербезопасности.

4. Укрепление сотрудничества и обмен информацией: Правительства, предприятия и организации в обеих странах должны работать сообща для обмена информацией и координации своих усилий по борьбе с кибератаками и утечками данных.

5. Развитие квалифицированной рабочей силы: Обе страны должны инвестировать в развитие квалифицированной рабочей силы для поддержки инициатив в области информационной безопасности. Для этого необходима профессиональная подготовка кадров. Государство может инвестировать в программы образования и профессиональной подготовки для подготовки квалифицированной рабочей силы в области кибербезопасности. Это включает в себя предоставление учебных программ для лиц, заинтересованных в продолжении карьеры в области кибербезопасности, а также постоянное обучение существующих специалистов в области кибербезопасности. Также сотрудничество с университетами и научно-исследовательскими институтами в разработке исследовательских и учебных программ по кибербезопасности. Это поможет обеспечению того, чтобы

сотрудники были оснащены новейшими знаниями и навыками в области кибербезопасности.

6. Международное сотрудничество: оно является одним из важнейших факторов. Обе страны должны сотрудничать с международными организациями, такими как Организация Объединенных Наций и Европейский союз, для разработки скоординированного реагирования на угрозу кибератак и утечки данных. Это включает в себя участие в международных инициативах по кибербезопасности и обмен информацией с другими странами.

Заключение

Улучшение кибербезопасности в Казахстане и Кыргызстане требует комплексного подхода, который включает в себя как превентивные, так и ответные меры. Правительства, предприятия и организации в обеих странах должны работать сообща над повышением осведомленности, разработкой политики и нормативных актов, инвестированием в технологии и инфраструктуру, укреплением сотрудничества и обмена информацией, подготовкой квалифицированной рабочей силы и участием в международных инициативах по кибербезопасности. Работая сообща, страны могут преодолеть угрозу кибератак и утечек данных и обеспечить безопасность своих граждан и критически важной инфраструктуры.

Что касаемо аспекта внешней политики Кыргызской Республики то она играет решающую роль в обеспечении безопасности и противодействии угрозам кибертерроризма. Кибертерроризм представляет собой серьезную проблему для стабильности и экономического развития страны, требующую комплексного и упреждающего подхода. Кыргызской Республике необходимо более интенсивно участвовать в международном сотрудничестве и партнерствах для эффективного противодействия угрозам кибертерроризма. Сотрудничество с другими странами, региональными организациями и международными организациями может улучшить обмен информацией, сбор разведданных и разработку совместных стратегий по борьбе с киберугрозами. Активно участвуя в глобальных инициативах в области кибербезопасности, Кыргызская Республика может извлечь выгоду из совместного опыта, ресурсов и передовой практики.

Кыргызской Республике следует сосредоточиться на дипломатических усилиях по установлению международных норм и правил, регулирующих киберпространство. Участие в дискуссиях на региональных и международных форумах позволяет стране формировать политику и выступать за усиление мер кибербезопасности. Содействуя развитию международных правовых рамок, таких как Будапештская конвенция о киберпреступности, Кыргызская Республика может укрепить свою правовую базу для противодействия кибертерроризму и облегчить международное сотрудничество в расследовании и судебном преследовании киберпреступников. Также следует отметить о важности Тесного партнерства и сотрудничества с соседней Республикой Казахстан также жизненно важно для кибербезопасности в Кыргызской Республике. Совместные усилия могут включать обмен разведданными, совместные учения и инициативы по наращиванию потенциала. Установление каналов связи с соседними государствами помогает в координации реагирования на киберинциденты, предотвращении распространения атак через границы и укреплении региональной стабильности. активно участвуя в международном сотрудничестве, отстаивая международные нормы, развивая региональные партнерства и расширяя внутренние возможности в области кибербезопасности, Кыргызская Республика может значительно повысить свою безопасность и эффективно противостоять угрозам кибертерроризма. Именно благодаря всеобъемлющему и совместному внешнеполитическому подходу страна может защитить свое киберпространство и обеспечить благополучие своих граждан перед лицом развивающихся киберугроз.

СПИСОК ЛИТЕРАТУРЫ

Абазов К.М. Проблема использования современных информационно-коммуникационных технологий международными террористическими организациями. Вопросы безопасности. Общество с ограниченной ответственностью "НБ-Медиа". – 2018. С. 7.

Бокошев, Ж.Б. Проблемы национальной безопасности Кыргызстана. Бишкек: Ин-т соц.-полит. технологий, 2006. 124 с.

Бурков В.Н., Грацианский Е.В., Дзюбко С.И. Модели и механизмы управле-ния безопасностью. М.: СИНТЕГ, 2017. 160 с.

Галтенко В.А. Основы информационной безопасности / Под ред. Члена-корр. РАН В.В. Бетелина. - М.: Интернет-Университет Информационных технологий, 2013.

Дакка А., Дмитриева М. Роль Центральной Азии в российско-индийском сотрудничестве в области энергетики. Вестник МГИМО-Университета. – 2020. – №13(6). С.208-227.

Комова А.С. Международная информационная безопасность: проблемы и решения / Под. общ. ред. - М., 2018.

Косовец А.А. Терроризм как объект противодействия в системе обеспечения информационной безопасности: международные и организационно-правовые аспекты// Вестник Академии экономической безопасности МВД России, 2011. № 3.

Курылев К.П., Мартыненко Е.В. Российско-китайское экономическое сотрудничество в контексте проекта "один пояс, один путь". Фактор ЕАЭС и ШОС // Вопросы национальных и федеративных отношений. 2019. Т. 9. № 11 (56). С. 1937-1948.

Лагуткина Ю.Н., Мадалимбеков Ж.И., Омарова Д.К., Противодействие Российской Федерации и Республики Казахстан информационному терроризму// Постсоветские исследования. Т.5. № 8 (5) 2022. С.847-860.

Рассолов И.М. Право и Интернет. Теоретические проблемы. - М.: Изд-во НОРМА, 2003. - С. 92.

Румянцева А.К., Рахимов К.Х. Роль ШОС в противодействии терроризму в странах Центральной Азии // Постсоветские исследования. - 2022. №8 (5). С.835-846.

REFERENCES

Abazov K.M. The problem of the use of modern information and communication technologies by international terrorist organizations. Security issues. Limited Liability Company "NB-Media". – 2018. p. 7.

Bokoshev, Zh.B. Problems of national security of Kyrgyzstan. Bishkek: In-t soc.-polit. technologies, 2006. 124 p.

Burkov V.N., Graziansky E.V., Dzyubko S.I. Models and mechanisms of security management. Moscow: SINTEG, 2017. 160 p.

Galtenko V.A. Fundamentals of information security / Ed. Member-correspondent. RAS V.V. Betelina. - M.: Internet University of Information Technologies, 2013.

Dhaka A., Dmitrieva M. The role of Central Asia in Russian-Indian cooperation in the field of energy. Bulletin of MGIMO University. – 2020. – №13(6). Pp.208-227.

Komova A.S. International information security: Problems and solutions / Ed. - M., 2018.

Kosovets A.A. Terrorism as an object of counteraction in the information security system: international and organizational and legal aspects// Bulletin of the Academy of Economic Security of the Ministry of Internal Affairs of Russia – 2011. No. 3.

Kurylev K.P., Martynenko E.V. Rossijsko-kitajskoe ekonomicheskoe sotrudnichestvo v kontekste proekta "odin poyas, odin put'". Faktor EAES i SHOS // Voprosy nacional'nyh i federativnyh otnoshenij. 2019. T. 9. № 11 (56). S. 1937-1948.

Lagutkina Yu.N., Madalimbekov Zh.I., Omarova D.K., Counteraction of the Russian Federation and the Republic of Kazakhstan to information terrorism// Post-Soviet Studies. Vol.5. No. 8 (5) 2022. pp.847-860.

Rassolov I.M. Law and the Internet. Theoretical problems. - M.: Publishing House NORMA, 2003. - p. 92.

Rumyantseva A.K., Rakhimov K.H. The role of the SCO in countering terrorism in Central Asian countries // Post-Soviet Studies. - 2022. No. 8 (5). pp.835-846.

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Абасова Алтынай Абасовна, студент 1 курса магистратуры, направление «международные отношения», Российский университет дружбы народов, Москва, Россия. (E-mail: abasova665@gmail.com)

Абек Малика, студент 1 курса магистратуры, направление «международные отношения», Российский университет дружбы народов, Москва, Россия. (E-mail: m_abek@mail.ru)

Имаралиев Нурислам, студент 1 курса магистратуры, направление «международные отношения», Российский университет дружбы народов, Москва, Россия. (E-mail: 1032225423@rudn.ru)

Altynai A. Abasova, 1st year student of the master's program “International Relations”, Peoples' Friendship University of Russia (RUDN University), Moscow, Russia. (E-mail: abasova665@gmail.com)

Malika Abek, 1st year student of the master's program “International Relations”, Peoples' Friendship University of Russia (RUDN University), Moscow, Russia. (E-mail: m_abek@mail.ru)

Imaraliev Nurislam, 1st year student of the master's program “International Relations”, Peoples' Friendship University of Russia (RUDN University), Moscow, Russia. (E-mail: 1032225423@rudn.ru)