РЕАКЦИЯ ОТДЕЛЬНЫХ ГОСУДАРСТВ-УЧАСТНИКОВ СНГ НА ЧЕТВЕРТОЕ ИЗДАНИЕ ГЛОБАЛЬНОГО ИНДЕКСА КИБЕРБЕЗОПАСНОСТИ ЗА 2020 ГОД

Эркин Урал углы АБДИСОАТОВ
магистр
Национальный университет Узбекистана
Ташкент, Узбекистан
Abdisoatoverkin0808@mail.ru

Аннотация

В статье анализируются понятие Глобального индекса кибербезопасности (ГИК), критерии, по которым оно формируется, и проблемы, связанные с отношением некоторых стран, входящих в Содружество Независимых Государств (СНГ), к редакции 2020 г. Индекса.

Ключевые слова: Глобальный индекс кибербезопасности, Международный союз электросвязи, кибербезопасность, цифровое развитие, защита критической инфраструктуры, защита персональных данных.

ГЛОБАЛ КИБЕРХАВФСИЗЛИК ИНДЕКСИНИНГ 2020 ЙИЛГИ ТЎРТИНЧИ НАШРИГА МДҲГА АЪЗО БЎЛГАН АЙРИМ ДАВЛАТЛАРНИНГ МУНОСАБАТИ ХУСУСИДА

Эркин Урал ўғли АБДИСОАТОВ
магистр
Ўзбекистон Миллий Университети
Тошкент, Ўзбекистон
Abdisoatoverkin0808@mail.ru

Аннотация

Мақолада Глобал киберхавфсизлик индекси (GCI) ҳақида тушунчалар, унинг қандай мезонлар асосида шакллантирилиши ҳамда мазкур индекснинг 2020 йилги нашрига Мустақил давлатлар ҳамдўстлигига аъзо бўлган айрим давлатларнинг муносабати хусусидаги муаммолар таҳлил этилган.

Таянч сўзлар: Глобал киберхавфсизлик индекси, Халқаро электр алоқа иттифоқи, киберхавфсизлик, рақамли ривожланиш, муҳим инфратузилмани ҳимоя қилиш, шахсий маълумотларни ҳимоя қилиш.

Новый Глобальный индекс кибербезопасности – 2020 (Global Cybersecurity Index – 2020, GCI), распространенный Международным союзом электросвязи (МСЭ), свидетельствует о росте настроений во всем мире, в том числе у государств-участников Содружества Независимых Государств (СНГ), находить решение проблем в сфере обеспечения кибербезопасности и сокращать их масштаб.

Необходимо отметить, что издание Глобального индекса кибербезопасности за 2020 год основано на данных, представленных рекордным уровнем участия государств-членов, от 105 ответов в итерации 2013–2014 гг. до 150 анкет, возвращенных в 2020 году.

Вместе с тем обновление анкеты сыграло роль различия весов от предыдущих итераций, частично отражая изменения в структуре вопросов, а также добавление и удаление вопросов.

На фоне изменений структуры Глобального индекса кибербезопасности некоторые страны отказались проверять собранные данные или участвовать в выпуске. Данные относительно этих стран были собраны посредством онлайн-исследования, отсутствующие элементы интерпретированы как – ненайденные, а не как отсутствующие.

Очередное, четвертое издание Глобального индекса кибербезопасности за 2020 год также подтверждает, что в последнее время большинство стран СНГ совместно с другими государствами мира тесно работают над повышением уровня своей кибербезопасности, несмотря на связанные с COVID-19 проблемы и переход многих сфер деятельности и социально-экономических услуг в цифровой формат.

При этом международными экспертами подтверждено, что стремительное распространение информационно-коммуникационных технологий (ИКТ) за время пандемии COVID-19 выдвинуло кибербезопасность на передний план. В этой связи, по оценкам авторов GCI, некоторые страны, в том числе СНГ, отстают в следующих ключевых областях:

– *обучение навыкам кибербезопасности* (должно быть адаптировано к потребностям малых и средних предприятий);

– *минимизация пробелов в области обеспечения кибербезопасности* (в таких важных отраслях, как банковско-финансовый сегмент, здравоохранение, энергетика и другие сектора экономики, требует специальных мер);

– *защита критической инфраструктуры* (в современных реалиях должна совершенствоваться с целью борьбы с новыми и возникающими киберугрозами);

– *защита персональных данных* (требует усиления по мере распространения онлайновой деятельности).

Вместе с тем в странах СНГ, в частности, у официальных респондентов и экспертного сообщества, вызывают неоднозначность выводы и оценки Индекса – 2020 в условиях тесной взаимосвязи между коммерческой деятельностью и обменом информацией, где риски кибербезопасности все в меньшей степени зависят от границ и ни одно отдельно взятое заинтересованное государство не может гарантировать безопасность национального киберпространства.

Характерно и то, что в четвертом издании GCI приводятся оценки степени выполнения 193 государствами – членами МСЭ обязательств в области кибербезопасности. При этом GCI рекомендован в качестве инструмента, призванного выявить пробелы, стать «дорожной картой» для ориентации национальных стратегий, создать информационную основу для нормативно-правовой базы, развивать потенциал, демонстрировать примеры передового опыта, укреплять международные стандарты и содействовать усилиям в сфере обеспечения кибербезопасности.

Индекс кибербезопасности стран СНГ по классификации GCI

(Уровень развития или участия каждой страны оценивается по пяти направлениям Глобальной программы кибербезопасности МСЭ: правовые меры; технические меры; организационные меры; развитие потенциала и сотрудничество)

Название страны	**Общий уровень**	**Региональный (классификатор)**
Российская Федерация	98,06	1
Казахстан	93,15	2
Азербайджан	89,31	3
Узбекистан	71,11	4
Беларусь	50,57	5
Армения**	50,47	6

Кыргызстан	49,64	7
Таджикистан**	17,1	8
Туркменистан **	14,48	9

** нет данных*

*** нет ответа на анкету / данные, собранные Командой GCI.*

Кыргызстан. Согласно пресс-релизу Министерства цифрового развития Кыргызской Республики (КР), Кыргызстан в период с 2018 по 2020 гг. со 111-й позиции поднялся на 92-ю позицию GCI, где позитивная динамика составила положительный рост на 19 позиций.

При этом среди стран СНГ к концу 2020 года Кыргызстан продемонстрировал рост в области кибербезопасности, оказавшись на 7-м месте (Узбекистан – 4 и Казахстан – 2). Как констатируют кыргызские официальные респонденты, в рамках реализации «дорожной карты» по кибербезопасности в течение двух лет были разработаны и утверждены государственные программы, стратегии и концепции с целью развития сферы информационно-коммуникационных технологий и кибербезопасности.

Так, в рамках правовых инициатив были приняты стратегические документы – концепция информационной безопасности и стратегия кибербезопасности. На сегодняшний день разрабатывается проект закона «О защите критической информационной инфраструктуры КР».

Также известно, что по технической части с 2019 года в госорганах КР устранено 676 тысяч 918 единиц вредоносного программного обеспечения, в том числе 663 тысячи 821 обращение на вредоносные ресурсы, 348 уникальных вредоносных программ (класса APT – развитая устойчивая угроза), не обнаруживающихся стандартными антивирусными средствами и предназначенных для негласного съема персональной информации. В 2020 году начато формирование единой базы данных для повышения эффективности реагирования на инциденты.

В рамках организационных мер в период с 2019 по 2021 гг. в КР были проведены национальные киберучения, в 2019 году в международных киберучениях приняла участие национальная команда реагирования CERT-

KG. В качестве тренеров были приглашены эксперты международных компаний в области кибербезопасности. Задействованы также и киберплатформы, предоставленные Международным союзом электросвязи, компанией Group-IB и «Лабораторией Касперского».

В то же время Бишкеком утверждается, что создана и успешно действует Межведомственная комиссия по информационной и кибербезопасности при Кабинете Министров Кыргызской Республики.

Таким образом, как отмечают зарубежные эксперты, на сегодняшний день с учетом проводимой работы КР поступательно идет к построению национальной системы обеспечения кибербезопасности, стабильно демонстрируя динамику роста.

Вместе с тем обращают на себя внимание итоги проведенных исследований в области кибербезопасности, где по результатам анализа ситуации в сфере обеспечения информационной и кибербезопасности (по состоянию на 29.06.2019г.) кыргызскими независимыми экспертами Общественного фонда «Гражданская Инициатива Интернет Политики» сделаны следующие выводы о том, что:

– принимая во внимание активное развитие ИКТ и растущее использование сети Интернет, с особой остротой встает вопрос необходимости обеспечения безопасности в информационной среде и защиты информационной инфраструктуры, требующий широкого диапазона мер в области сетей связи и их информационной безопасности, борьбы с киберпреступностью;

– оперативное реагирование и эффективное противодействие киберпреступности требуют создания специальных подразделений в правоохранительных органах и развития сети центров реагирования на компьютерные инциденты и организации их взаимодействия с данными подразделениями;

– не имеется уполномоченного государственного органа для обеспечения кибербезопасности в виде созданной и полноценно

функционирующей структуры по реагированию на возникающие угрозы и киберинциденты (CERT), иерархия государственных структур, задействованных в данной сфере (Совет безопасности (обороны), Государственный комитет национальной безопасности, Министерство внутренних дел, Государственный комитет информационных технологий и связи), не выстроена четким образом с точным и ясным распределением задач и функций в информационной сфере;

– Кыргызская Республика достаточно слабо представлена в международных договорах и соглашениях в сфере обеспечения информационной и кибербезопасности, за исключением Соглашения государств-членов ШОС и в рамках ОДКБ;

– несмотря на то, что во многих учебных заведениях КР имеются программы обучения по вопросам информационной безопасности, подготовка отечественных специалистов в сфере обеспечения и регулирования кибербезопасности не осуществляется, а обучение программам, охватывающим информационную безопасность, оставляет желать лучшего и не отвечает требованиям сегодняшнего дня;

– недостаточно возможностей для защиты критической инфраструктуры КР;

– нет разработанной специализированной архитектуры по уровням кибербезопасности.

Казахстан. В то же время ряд казахстанских СМИ и интернет-изданий позитивно оценивают результаты и достижения Республики Казахстан (РК) в Глобальном индексе кибербезопасности – 2020. Как рапортуют официальные источники РК, в мировом рейтинге GCI Казахстан занял 31-е место, в СНГ – второе, в Центральной Азии – первое.

В 2020 году Казахстан занимал в рейтинге 40-е место, в 2019 году – 83-е место, а еще ранее не входил и в топ-100.

В свою очередь, зарубежные эксперты отмечают сильные стороны киберготовности Казахстана: технические, законодательные, кооперативные меры, нацеленные на создание и укрепление технических институтов.

При этом эксперты, близкие к властным структурам, особо подчеркивают, что Казахстан занял 31-е место, обошел Китай (33-е место) и Израиль (36-е место). По их мнению, Индекс за 2020 год подтверждает, что страна работает над повышением уровня своей кибербезопасности, несмотря на связанные с COVID-19 проблемы и стремительный переход повседневной деятельности и социально-экономических услуг в цифровую сферу.

Стоит отметить, что результаты Глобального индекса кибербезопасности были включены в список целевых показателей концепции «Киберщит Казахстана». Характерно и то, что Астана сразу же продекларировала стремление – «войти в топ-10 стран по данному показателю».

В этом контексте казахстанские аналитики отмечают успехи страны в правовом поле, в частности, упоминается, что Казахстан унифицировал требования в области ИКТ, а также информационной и кибербезопасности. Как подчеркивается, инициатива по цифровизации придает все большее значение эффективной стратегии кибербезопасности РК. Так, за прошедшие два года в стране были выработаны базовые концептуальные подходы к развитию сферы кибербезопасности страны. Была разработана и утверждена концепция кибербезопасности «Киберщит Казахстана», а также целый ряд законодательных актов и большое количество отраслевых приказов. В частности, в рамках программы «Киберщит Казахстана» государство определило 336 критически важных объектов, к которым относятся госструктуры, банковско-финансовый и промышленный сектор. Помимо этого, созданы испытательные лаборатории по исследованию вредоносного кода, запущен национальный координационный центр информационной безопасности, увеличено число грантов в ВУЗы страны по этой специальности и т.д.

Между тем, по данным казахстанских специалистов, в 2021 году количество интернет-преступлений в Казахстане выросло на 139 процентов. По заявлению властей РК, в основном такие преступления совершаются из-за рубежа, используются ресурсы иностранных государств и, как правило, злоумышленники имеют своих подельников на территории Казахстана, которые выполняют лишь определенные функции. В целом за 2020 год в РК было зарегистрировано фактов интернет-мошенничества в два раза больше, чем за 2019 год (7,7 тысячи – в 2019 и 14,1 тысячи – в 2020 году).

Об этом также свидетельствует официальная информация АО «Государственная техническая служба» Казахстана (ГТС), согласно которой за 2020 год было отработано более 24 тысяч инцидентов информационной безопасности, 1,5 тысячи обращений граждан, отражено более 594 миллионов атак на государственные органы, а также было направлено свыше 2,2 тысячи исходящих уведомлений и получено более 1,7 тысячи уведомлений от международных партнеров.

В позитивном ключе стоит отметить, что АО «ГТС» выражает благодарность Республике Узбекистан за организацию и проведение Международного экспертного Форума стран СНГ по вопросам обеспечения информационной безопасности в формате онлайн-видеоконференции (29.06.2021г.) и надеется на дальнейшее плодотворное сотрудничество.

Российская Федерация. Россия, получившая 98,06 балла из 100 возможных, делит в таблице пятое место с Объединенными Арабскими Эмиратами и Малайзией. На четвертом месте – Испания, Республика Корея и Сингапур, на третьем – Эстония, на втором – Великобритания и Саудовская Аравия. На первой строчке – США, у которых 100 баллов.

Таким образом, согласно отчету, областью потенциального роста для России являются организационные меры, которые включают в себя, в том числе наличие национальной стратегии кибербезопасности и организаций, функционирующих в этой области.

В блоке стран СНГ Россия уже который год является лидером, 2-е место по итогам 2020 года занял Казахстан, 3-е – Азербайджан, 4-е – Узбекистан и 5-е – Беларусь.

В общем рейтинге за два года Россия поднялась сразу на 21 позицию, и ее показатели достигли максимального значения за все годы публикации Индекса. В 2016-2017 гг. она занимала 10-е место (с показателем 0,788), в 2018-2019 гг. опускалась на 26-е (при этом сам ее показатель стал выше – 0,836). Таким образом, снижение происходило не за счет ослабления по оцениваемым параметрам, а благодаря усилению позиций других государств.

Вместе с тем, согласно отчету британского Международного института стратегических исследований (International Institute for Strategic Studies, IISS) «Кибервозможности и мощь государств: комплексная оценка» (Cyber capabilities and national power: a net assessment), Соединенные Штаты обладают наибольшими возможностями защиты от нападений и ответа на них в киберпространстве, где Россия отнесена к странам «второго уровня» вместе с Австралией, Израилем, Канадой, Китаем, Францией и Великобританией.

Азербайджан. Согласно опубликованному отчету «Глобальный индекс по кибербезопасности – 2020», Азербайджан поднялся на 15 позиций в данном рейтинге, заняв 40-е место, набрав 89,31 балла, и таким образом улучшив свою позицию в международном рейтинге по кибербезопасности.

Азербайджан занимает третье место среди стран СНГ после России и Казахстана, опережает Узбекистан, занимающий 70-е место в мировом рейтинге среди стран СНГ, Беларусь (89-е место), Армению (90-е место) и ряд других стран.

Согласно заявлению советника министра транспорта, связи и высоких технологий Рашада Байрамова – страна получила максимальный балл по правовым мерам и мероприятиям по сотрудничеству, а деятельность по техническим мерам получила высокую оценку. Меры, связанные с присоединением Азербайджанской Республики к соответствующим

международным конвенциям и программам, развитием национальной правовой базы, подготовкой с целью внедрения и государственной регистрацией международных стандартов информационной безопасности в качестве национального стандарта, защитой детей от вредоносной информации в онлайн-среде, информационная и просветительская деятельность CERT по текущим и потенциальным электронным угрозам на национальном уровне, международное сотрудничество в профильной сфере, превентивные меры, осуществленные совместно с национальными интернет-операторами в целях предотвращения глобальных атак на входящий в страну интернет-трафик, и т.д. заложили основу для достижения этих результатов.

В настоящее время Азербайджан проводит глобальную работу в направлении кибербезопасности, в частности, в соответствии с международной практикой в стране действуют 3 группы реагирования на компьютерные инциденты: Служба электронной безопасности при Министерстве транспорта, связи и высоких технологий – национальный CERT (cert.az), которая выступает в качестве координирующей структуры, Центр по борьбе с компьютерными инцидентами Государственного агентства специальной связи и информационной безопасности (cert.gov.az), который отвечает за безопасность сети государственных структур, и Центр по борьбе с компьютерными инцидентами Национальной академии наук, отвечающий за безопасность научной компьютерной сети AzScienceCERT (sciencecert.az).

Стоит отметить еще тот факт, что регулярно в рамках международной недели проводятся конференция кибербезопасности, выставка Cyber Village, международные мероприятия «Безопасное правительственное облако», практический семинар по пентестингу для специалистов по кибербезопасности, Cyber4StartUp, «Цифровое право: защита персональных данных», международный сертификационный тренинг по кибербезопасности и т.д.

В 2020 году Министерством транспорта, связи и высоких технологий совместно с соответствующими структурами подготовлены и представлены

на утверждение проекты «Национальной стратегии Азербайджанской Республики по информационной и кибербезопасности на 2021-2025 годы», а также план мероприятий по реализации данной стратегии.

Республика Беларусь. По итогам четвертого выпуска Глобального индекса кибербезопасности спустилась на 20 уровней и занимает 89-ю позицию с 50,57 балла.

Как отмечают эксперты, данное обстоятельство связано с обновлением анкеты, где внесены изменения в структуре, а также добавлением и удалением вопросов.

Несмотря на то, что регулятором обеспечения информационной безопасности Республики Беларусь (Оперативно-аналитический центр при Президенте Республики Беларусь) предпринимаются необходимые меры, генеральный прокурор Беларуси Андрей Швед отмечает следующее: «В Беларуси за 5 лет число преступлений, совершенных с использованием компьютерных систем и сети Интернет, выросло более чем в 10 раз. В прошлом году на их долю пришлось свыше четверти всех преступлений, совершенных в республике. Абсолютное большинство из них составляют хищения путем использования компьютерной техники. От действий преступников страдают не только организации, но и граждане, особенно незащищенные слои населения, пенсионеры. Киберхищения подрывают доверие к банкам и требуют принятия серьезных мер по устранению изъянов в их системах безопасности».

В рамках правовых инициатив принят стратегический документ «Концепция информационной безопасности Республики Беларусь», который также затрагивает вопросы обеспечения кибербезопасности страны.

Украина. Несмотря на то, что Украина является страной СНГ, ее результаты в Глобальном индексе кибербезопасности по политическим соображениям отражаются в разделе региона Европы.

Однако Государственная служба специальной связи и защиты информации Украины отмечает рост уровня обеспечения кибербезопасности,

ссылаясь на отчет редакции Национального индекса кибербезопасности – 2020. Согласно которому, Украина поднялась на четыре позиции по сравнению с предыдущей редакцией Национального индекса кибербезопасности, заняв 25-е место среди 160 стран мира.

Если обратиться к статистическим данным, согласно официальным публикациям с начала 2021 года киберспециалисты СБУ локализовали почти 350 потенциальных угроз информационной безопасности государства, к уголовной ответственности привлечено 35 хакеров и пропагандистов, 14 злоумышленников осуждены.

«СБУ постоянно принимает меры по поиску, выявлению и локализации указанных кибератак и киберинцидентов, а также противодействует киберугрозам в ИТС (информационно-телекоммуникационные системы). Кроме того, киберспециалисты Службы наладили взаимодействие при помощи системы обмена данными о кибератаках на базе платформы MISP-UA и других программно-аппаратных решений», – заявили в спецслужбе.

В конце 2018 года Государственной службой специальной связи и защиты информации был представлен план по кибербезопасности на 2019-2020 гг. Целью которого было создание условий для безопасного функционирования киберпространства, его использования в интересах личности, общества и государства.

Таджикистан. Таджикистан занял 138-е место из 193 стран, участвующих в Глобальном индексе кибербезопасности. Как указано в рейтинговой таблице доклада Global Cybersecurity Index, Таджикистан, занявший 138-е место, опередил только своего ближайшего соседа по СНГ – Туркменистан (144), но отстал в Центрально-Азиатском регионе от Казахстана, Узбекистана, Кыргызстана.

Известно, что официальный Душанбе, так же как Армения и Туркменистан, проигнорировал анкету экспертов МСЭ по кибербезопасности. Для стран, не представивших ответы на анкету, было проведено кабинетное исследование с использованием общедоступной

информации на официальных веб-сайтах и других ресурсах, поэтому собранные данные могут неточно отражать состояние кибербезопасности в стране.

Таким образом, по данным МСЭ, с 2007 по 2019 гг. порядка 3,5 миллиарда человек во всем мире (в странах СНГ – порядка 75 процентов населения) имеют доступ к Интернету. В докладе МСЭ подчеркивается, что «цифровой гендерный разрыв» сократился на пространстве СНГ и Европы, однако одновременно он растет в Африке, арабских государствах и Азиатско-Тихоокеанском регионе.

По утверждению экспертов МСЭ, стремительное распространение информационно-коммуникационных технологий за время пандемии COVID-19 выдвинуло кибербезопасность на передний план. Около 64 процентов стран к началу 2021 года приняли национальную стратегию кибербезопасности, и более 70 процентов в 2020 году провели кампании по повышению осведомленности о кибербезопасности, тогда как в 2018 году их было, соответственно, 58 и 66 процентов.

Согласно GCI, примерно половина стран мира заявляет о создании национальной группы реагирования на компьютерные инциденты (CERT), что отражает увеличение их числа на 11 процентов с 2018 года.

Между тем, по прогнозам аналитиков МСЭ, глобальный ущерб, вызванный киберпреступностью, имеет тенденцию к росту. В этой связи они обращают внимание на то, что национальные правительства должны усилить нормы кибербезопасности в целях защиты персональных и финансовых данных. В силу растущей зависимости от цифровых решений требуются более эффективные, но в то же время доступные и удобные для пользователей меры защиты данных.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА:

1. Закон Республики Узбекистан «О кибербезопасности», от 15.04.2022г. № ЗРУ-764. https://lex.uz/uz/docs/5960604

2. Указ Президента Республики Узбекистан от 02.06.2020г. № УП-6003. https://lex.uz/docs/-4838762

3. Глобальный индекс кибербезопасности (GCI) 2020. https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

4. Кыргызстан улучшил позиции в глобальном индексе кибербезопасности. https://economist.kg/novosti/2021/07/02/kyrgyzstan-uluchshil-pozicii-v-globalnom-indekse-kiberbezopasnosti/

5. Казахстан поднялся в мировом рейтинге киберготовности на 31-е место. https://informburo.kz/novosti/kazaxstan-podnyalsya-v-mirovom-reitinge-kibergotovnosti-na-31-e-mesto

6. Россия заняла 5 место в глобальном рейтинге кибербезопасности. https://www.infowatch.ru/analytics/novosti-ib/rossiya-zanyala-5-mesto-v-globalnom-reytinge-kiberbezopasnosti

7. Азербайджан значительно улучшил индекс кибербезопасности в международном рейтинге. https://mincom.gov.az/ru/view/news/1234/

8. Кибербезопасность в Беларуси: подписан новый Указ. https://clevr.by/news/113

9. Украина заняла 25 место среди 160 стран в международном рейтинге кибербезопасности. https://hromadske.ua/ru/posts/ukraina-zanyala-25-mesto-sredi-160-stran-v-mezhdunarodnom-rejtinge-kiberbezopasnosti

10. Таджикистан занял 91-е место из 165 в индексе. https://tajikta.tj