МЕМЛЕКЕТТІК АУДИТ
ГОСУДАРСТВЕННЫЙ АУДИТ
GOVERNMENTAL AUDIT

УДК 351.86:004 (574)

Зейнельгабдин А.Б.
д. э. н., профессор
Академии государственного
управления при Президенте
Республики Казахстан, г.Нур-Султан, Казахстан
email: A.Zeinelgabdin@apa.kz;

Исабаева С.Б.
главный эксперт Академии
правоохранительных органов при Генеральной
прокуратуре Республики Казахстан,
докторант 3 курса АГУ при Президенте
Республики Казахстан, г.Нур-Султан, Казахстан
email: S.Issabayeva@apa.kz;

КИБЕРБЕЗОПАСНОСТЬ КАЗАХСТАНА В ПЕРИОД ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Аннотация: *На сегодняшний день Казахстан переживает период цифровой трансформации. Данный этап предусматривает реализации новых проектов в сфере цифровизации в целях создания благоприятного условия для граждан страны. Обеспечение безопасности в киберпространстве в период такой трансформации является одним из важных вопросов. Данное исследование проведено в целях определения уровня качества цифровых услуг, получаемых гражданами Республики Казахстан, а также степени осведомленности и готовности общественности к проводимой политике в области цифровизации и кибербезопасности в стране. В качестве источников в статье использованы международные показатели в области кибербезопасности, проведен теоретический и эмпирический анализ. Одновременно изучен опыт успешных стран. Вместе с тем, в данной статье применен качественный метод исследования путем проведения онлайн опроса граждан Казахстана.*

Авторами предложены комплексные меры по реализации цифровых проектов, обеспечивающие вопросы их защиты и безопасности. Предложенные практические и методические рекомендации по дальнейшему совершенствованию политики кибербезопасности могут быть полезными не только Казахстану, но и другим государствам, которые проходят период трансформации в области цифровизации.

Ключевые слова: *кибербезопасность, цифровизация, международные рейтинги, электронное правительство, государственная политика.*

Введение

Тема кибербезопасности является актуальной как для академиков и государственных управленцев, так и для бизнес-сектора. Удобство информационно цифровых технологий способствует их широкому применению и использованию в сегодняшнем быстро меняющемся мире. Происходящие изменения одновременно повышают риски уязвимости получателей цифровых услуг. С каждым годом уровень угроз кибератак приносит колоссальный финансовый ущерб государственному и бизнес секторам. К примеру, согласно некоторым данным, Steve Wozniak и Steve Jobs в 1970 году взломав телефонную систему, смогли совершать бесплатные звонки, как в ближние, так и дальние зарубежные страны. Также можно отметить, что в 1990 году в истории хакерства основное место занял Kevin Mitnick, который сумел взломать систему безопасности и имел доступ к компьютерам корпорации. Другим примером можно отметить вирус Stuxnet, разработанный в 2009 году. Целью данного вируса было повреждение иранского завода по обогащению урана [19]. Таким образом, обеспечение кибербезопасности в цифровом пространстве является одним из критически важных вопросов любого государства.

Вместе с тем, в связи с проводимыми межсистемными интеграционными работами между разными государствами, в глобальном мире практически смываются границы, что усложняет обеспечение кибербезопасности в онлайн пространстве.

В данной статье опыт и рейтинговый показатель Эстонии и России в области кибербезопасности рассматривается в качестве флагмана передовых технологий. Также необходимо отметить, что Казахстанская политика государственного управления во многом схожа с политикой Российской Федерации. После распада СССР Казахстану необходимо было построить свою суверенную независимость, как и другим государствам, которые были в составе СССР. Одновременно если рассмотреть индексные показатели Эстонии, то они удивляют своими достижениями не только в области цифровизации, но и в кибербезопасности, учитывая, что Эстония также была в составе постсоветских стран.

В результате проведенный обзорный анализ показывает, что большинство научных работ, посвященных развитию цифровизации постсоветских стран, рассматривает электронное правительство, как основной показатель цифрового общества [17]. К сожалению, в Казахстане развитие цифровизации в большей степени понимается также. По результатам проведенных научных исследований, основными барьерами для улучшения цифрового и инновационного общества являются невысокий уровень экономических показателей [9], а также недостаточная степень демократии.

Таким образом, данная статья организована следующим образом. В разделе о результатах исследования рассматривается нынешнее положение Казахстана в области кибербезопасности и цифровизации. В последующем рассмотрен успешный опыт зарубежных стран согласно показателю Global Cybersecurity Index (GCI). Проведен анализ кибербезопасности Эстонии и России. Также проанализированы результаты проведенного онлайн опроса среди пользователей онлайн услуг в Казахстане. В заключении, авторами предложены практические рекомендации в целях обеспечения кибербезопасности страны. Предполагается, что результаты исследования будут представлять интерес для постсоветских стран, поскольку эти страны имеют общую историю становления независимости.

Методология исследования

В исследовании использованы как качественные, так и количественные методы анализа. Чтобы определить уровень осведомленности общественности о кибербезопасности и внедрении цифровизации в Казахстане, проведен онлайн опрос. Онлайн-опрос проводился непосредственно среди пользователей цифровых Казахстанских сервисов, с помощью инструмента Google Docs. Опрос проведен в течении месяца и 173 онлайн респондента проявили интерес. Одновременно проведено интервью среди сотрудников РГП «Государственная техническая служба» и KZ-CERT. Количество интервьюированных составило 12.

Вместе с тем проведен эмпирический и теоретический анализ. Рассмотрены вопросы важности доверия населения к реализации Концепции кибербезопасности и Государственной программе «Цифровой Казахстан». Одновременно проанализированы принятые нормативные правовые документы в рамках внедрения кибербезопасности и цифровизации Казахстана и изучен международный опыт успешных стран. В исследовании также использованы и проанализированы первичные и вторичные данные. Первичные данные получены от онлайн опроса, тогда как вторичные получены из GCI.

Информация, полученная от респондентов, является строго конфиденциальной и анонимной. Они использованы только как часть исследования и для публикации научной статьи.

Результаты исследования

Нынешнее положение Казахстана. В стране проводится третья модернизация, целью которой является глобальная конкурентоспособность. Данная мероприятия была объявлена первым Президентом страны Назарбаевым Н. А. в январе 2017 года. [5]. В декабре 2017 года принята государственная программа «Цифровой Казахстан» (сроки реализации 2018-2022 годы), основной целью которой является «повышение качества жизни населения и конкурентоспособности эконо-

мики Казахстана посредством прогрессивного развития цифровой экосистемы».

Так, Казахстан к 2022 году ставит целью повысить уровень цифровой грамотности 83% населения. Основная часть индикаторов программы «Цифровой Казахстан» нацелена на рост производительности труда в приоритетных направлениях экономики, создание рабочих мест и увеличение инвестиций в стартапы. Таким образом, Правительством Казахстана проводится ряд работ, направленных на улучшение оказания государственных услуг, применяя информационно-коммуникационные услуги.

Вместе с тем, согласно информации Комитета по правовой статистике и специальным учётам Генеральной прокуратуры Республики Казахстан, в 2016 году зарегистрировано 106 уголовных дел, предметом которых явились киберпреступления. Более того, Министерство информации и коммуникации Республики Казахстан, за тот же год регистрировано 16576 кибератак [2]. Таким образом, со стороны правительства, при внедрении цифровых технологий одновременно необходимо обеспечить защиту данных в киберпространстве.

Необходимо отметить, что показатель Казахстана в сфере кибербезопасности за 2017 год оставлял желать лучшего по сравнению с цифровизацией. Согласно GCI в 2017 году Казахстан находился на 83 позиции. Если рассмотреть показатель Казахстана в области кибербезопасности за 2017 год среди стран бывшего СССР, то Казахстан опережал только Таджикистан, Узбекистан, Кыргызстан, Армению и Туркменистан. Учитывая экономические и социальные возможности, инвестиционную привлекательность Казахстана, данный показатель являлся одним из худших результатов для страны, и стал сигналом для принятия необходимых мер в целях улучшения уровня киберзащиты. Возможно, отставание Казахстана от ближних соседних стран стало мотивационным фактором для страны. В результате в 2018 году Казахстан показал колоссальный прорыв в области кибербезопасности. Согласно GCI 2018 Казахстан поднял свой рейтинг с 83 на 40 позицию, что является невероятным достижением для страны за такой короткий период времени (см. диаг. 1). В 2017 году Постановлением Правительства Республики Казахстан утверждена Концепция кибербезопасности [6]. В Концепции кибербезопасности рассматривает текущую ситуацию цифровизации государственных органов и госуслуг.

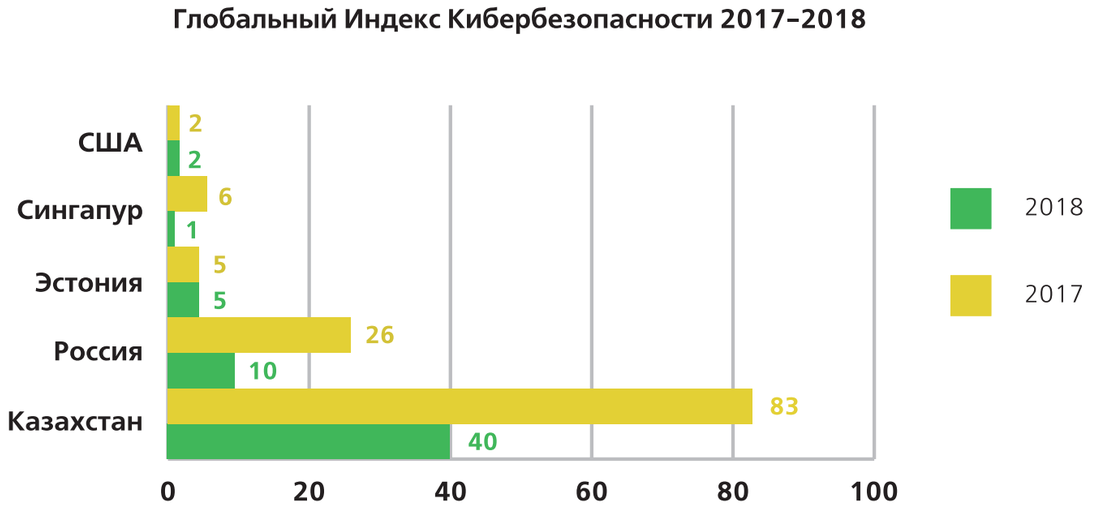

Диаграмма 1. Составлена авторами согласно показателям, GCI за 2017–2018гг.

Согласно Концепции кибербезопасности перед Казахстаном была поставлена задача довести показатель кибербезопасности к 2018 году - 0,300, к 2019 году – 0,400, к 2020 году – 0,500, к 2021 году – 0,550, к 2022 году – 0,600. Однако, как видно Казахстан в 2018 году добился отметки – 0,778. То есть на сегодня перевыполнил поставленные цели. В этой связи необходимо обновить Концепцию кибербезопасности, внося новые приоритетные цели и задачи, а также соответствовать требованиям глобального рынка ИКТ. Вместе с тем, создан национальный институт безопасности, автором идей является Ержан Сейткулов, директор научно-исследовательского института информационной безопасности и криптологии ЕНУ им. Л.Н. Гумилева. Предполагается, что головной институт обеспечит научно-аналитическую базу осуществляемой политики государства в сфере информационной безопасности [7].

Также в 2017 году РГП на ПХВ «Государственная техническая служба» (ГТС) передана в Комитет национальной безопасности Республики Казахстан. Его основной целью деятельности является обеспечение информационной безопасности, а также обеспечение безопасности киберпространства и инфраструктуры связи Республики Казахстан [4]. Также при ГТС была создана служба реагирования на компьютерные инциденты.

Однако есть вероятность, что происходящие политические и управленческие изменения в стране отрицательно влияют на ее развитие, так как это снижает интерес иностранных инвесторов. Зарубежными инвесторами частые изменения понимаются нестабильностью и неустойчивостью политической деятельности государства. Так, за всю историю независимости Казахстана не раз были приняты решения о роспуске Правительства. Например, в феврале 2019 года Указом Президента страны было принято решение об отставке Правительства Республики Казахстан [8]. Позже, 20 марта этого же года Президент страны объявил о своем досрочном прекращении полномочий [3]. Есть вероятность, что эти изменения непосредственно влияют на уровень безопасности страны. Более того, утверждение нового состава Правительства займет немало времени. Эти происходящие изменения влияют на деятельность отраслевых исполнительных органов, в том числе, в области развития и применения ИКТ в стране.

Таким образом, в государственном управлении в целях реализации эффективных результатов и достижении долгосрочных задач необходимо формировать устойчивую структуру правительства и принять все необходимые меры по минимизации утечки (умов) квалифицированных кадров.

Президент Центра анализа и расследования кибератак О. Сатиев отмечает, что на рынке труда в Казахстане имеется высокий спрос на высококвалифицированные кадры в области кибербезопасности [1]. В связи с этим, необходима организация и проведение курсов по повышению компьютерной грамотности, а именно в сфере кирбербезопасности. В рамках Концепции Киберщит Казахстана за счет бюджетных средств запланирована подготовка молодых кадров в области кибербезопасности на 2018-2020 годы [6].

Несомненно, что намеченный путь цифровизации Казахстана является амбициозным, и результаты, достигнутые государством за годы независимости, говорят сами за себя! Однако, необходимо работать усердно и сплоченно над успешной реализацией стратегических государственных задач.

Результаты онлайн опроса. В рамках исследования среди пользователей цифровых услуг Казахстана проведен онлайн опрос. Опрос проводился посредством использования социальной сети Facebook, образовательного портала Академии государственного управления при Президенте Республики Казахстан – Platonus (http://platonus.apa.kz/), а также мобильных приложений What's app и Telegram. В течении месяца активность проявили 173 респондента: из них основную долю составили граждане в возрасте 31 - 40 лет (42 %). Интересный факт, что большинство респондентов, проявивших интерес являются – женщины (88), а мужчин – 85.

В целях определения активности граждан в использовании онлайн услуг, был сформулирован вопрос, наглядно показанный на диаграмме 2. Анализ ответов показал, что казахстанские граждане не активны в использовании онлайн услуг ежедневно: из 173 респондентов, только 8 человек каждый день используют услуги онлайн, а 78 человек используют раз в квартал. Очевидно, что данный показатель является сигналом, как государству, так и частному сектору задуматься о мотивации граждан получать и использовать онлайн услуги.

МЕМЛЕКЕТТІК АУДИТ
ГОСУДАРСТВЕННЫЙ АУДИТ
GOVERNMENTAL AUDIT

Как часто Вы используете услуги онлайн (включая государственные услуги Egov)

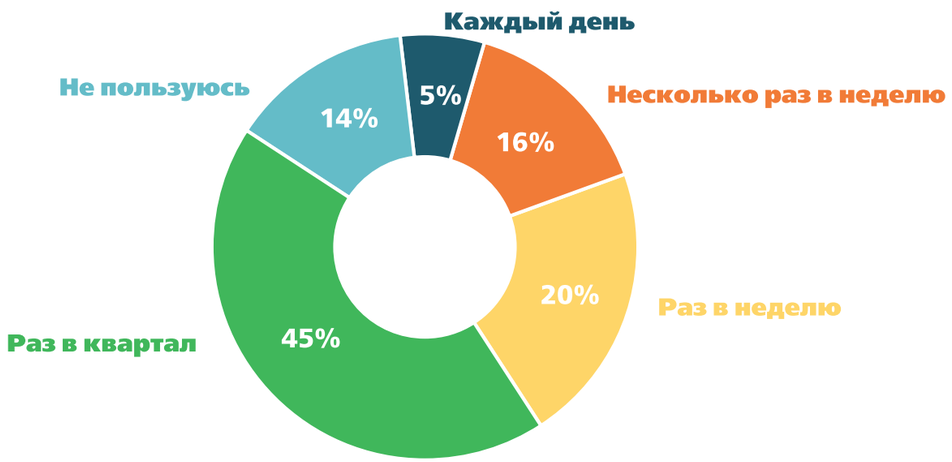

Диаграмма 2. Составлена авторами по результатам опроса, «Как часто Вы используете услуги онлайн (включая государственные услуги Egov)?»

Какие из следующих рисков, по Вашему мнению, могут препятствовать пользователям в использовании онлайн услуг?

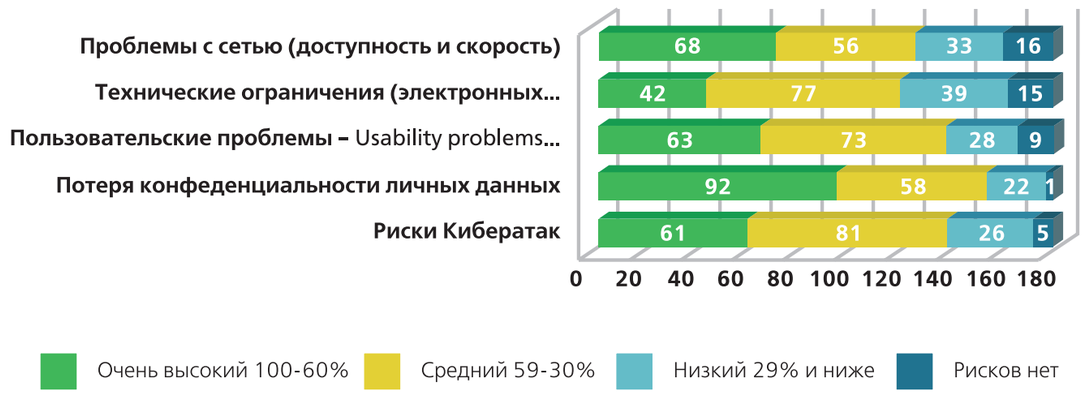

Диаграмма 3. Составлена авторами по результатам опроса. Анализ рисков кибербезопасности

В целях выявления причин пассивности граждан был сформулирован вопрос по выявлению качества и стоимости оказываемых онлайн услуг. Отвечая на вопрос «Как Вы оцениваете онлайн услуги в Республике Казахстан, учитывая их стоимость и качество?», в целом большинство казахстанцев считают, что онлайн услуги хорошие (71), 64 респондента удовлетворены качеством и стоимостью, в то время как 22 респондента дают очень хорошую оценку, и только 16 респондента отметили низкое качество услуг. Резюмируя, можно отметить, что казахстанские онлайн сервисы в целом по качеству и стоимости имеют положительные динамику.

Во избежание возможных киберугроз проведен анализ рисков, с которыми чаще всего сталкиваются Казахстанские Интернет-пользователи. В рамках опроса нами был составлен перечень угроз, которые могут быть барьерами для пользования онлайн услугами. В результате, 92 респондента считают, что очень высока вероятность потери личных данных. Также у респондентов возникают проблемы с сетью (68) и пользовательские проблемы (63). Вместе с тем, 81 респондент отметили риски кибератак. Одним из респондентов был приведен пример кибер-инцидента, произошедшего в 2016 году в одной из крупных нефтегазовых компаний «North Caspian operation company». По представленным данным респондента, сеть компании была взломана и в течении двух месяцев ее сотрудники не могли пользоваться компьютерами на рабочем месте, несмотря на то, что в компании выделяются не мало финансовых средств на зарубежные, лицензионные информационные технологии и программные обеспечения.

Таким образом, учитывая, показатели, представленные на диаграмме 3, необходимо уделить огромное внимание мерам по защите от возможных кибератак, улучшению системы по обеспечению безопасности персональных данных, а также на работу провайдеров по обеспечению высокоскоростного доступа к сети интернет.

На вопрос «Можете ли вы определить основные угрозы для дальнейшего развития цифровых услуг в Республике Казахстан?», большинство респондентов отметили дефицит квалифицированных специалистов (126). Следующей угрозой для 86 респондентов являются кибератаки, то есть незащищенность сетей. Низкий уровень цифровой грамотности населения отметили – 66, слабо развитую систему предоставления услуг операторами связи – 45, и только 10 респондентов отметили, что на сегодняшний день никаких угроз не имеется.

Также необходимо отметить, что доверие населения к осуществляемой правительственной политике является одой из важных и приоритетных задач любого государства. В этой связи, в рамках опроса предусмотрено узнать мнение респондентов касательно их доверия к реализации Концепции кибербезопасности. В результате, большинство участников опроса отметили положительную тенденцию в реализации Концепции кибербезопасности Казахстана. Однако 31 респондент из 173 вообще не осведомлены о существовании данной концепции, а 26 относятся с пессимизмом в ее реализации.

По мнению респондентов (R), нижеследующие мероприятия позволят минимизировать кибер-угрозы, которые могут возникнуть в будущем:

R. Организовать открытые дискуссионные площадки с привлечением ИТ экспертов. Открыто обсуждать существующие проблемные вопросы. Не принимать решений кулуарно. Выделить время в эфире отечественным ТВ каналам.

R. Доступно разъяснять информацию, показывать конкретные мероприятия по реализации программы и ожидаемые по ним результаты, повысить качество оказываемых услуг сотрудниками для населения (улучшить сервис, простое отношение к человеку должно быть приятным).

R. Надо проводить работы по снижению информационного неравенства населения повсеместно.

R. Просто улучшать и модернизировать существующие и развивать новые системы.

R. Создать платформу в рамках egov.kz для сбора предложений (обратной связи) с населения по доработке программы в части реализации новых инициатив, не вошедших в 1 редакцию государственной программы Цифровой Казахстан.

R. В целях привлечения и формирования высококвалифицированных специалистов безотлагательно необходимо предусмотреть в ВУЗах, Академиях Комитета национальной безопасности Республики Казахстан и Министерства Внутренних дел Республики

Казахстан подготовку специалистов в области кибербезопасности, а также стимулировать преподавателей, систематически направляя на тренинги и обучение.

R. Требуется проработка нормативных правовых актов в сфере обеспечения кибербезопасности с применением технологии блокчейн (blockchain); расширять использование мобильных гаджетов с использованием протоколов безопасности.

R. Современная кибербезопасность - это командная работа. Исходя из плана «Киберщит», государство не должен закрыться от всего мира и делать в закрытом виде - это утопия. Поэтому нужно построить работу с другими странами и компаниями в рамках сотрудничества. Как пример, можно и следует использовать облачные сервисы, такие как Amazon Web Service, Microsoft Azure и др., так как эти компании более компетентны и обеспечивают безопасность своих серверов на высоком уровне.

R. Заменить ИНН на штрих код. А также необходимо повысить общее доверие к власти. Правительству и частным компаниям организовывать курсы по обучению граждан Казахстана

Некоторые респонденты в ходе опроса не смогли предложить какие-либо идеи, однако они считают, что кибербезопасность крайне важна в национальном масштабе.

Вместе с тем, в рамках научно-исследовательской работы среди работников республиканского государственного предприятия «Государственная техническая служба» Комитета национальной безопасности Республики Казахстан (РГП «ГТС») и KZ-CERT проведено интервью.

В ходе интервью сотрудники KZ-CERT и РГП «ГТС» Комитета национальной безопасности Республики Казахстан отметили, что проводимая государственная реформа в области кибербезопасности, передача функций под руководство Комитета национальной безопасности Республики Казахстан, значительно повысила эффективность и результативность их работы. Сотрудники также отмечают, что бюрократические барьеры, которые ранее испытывались при Министерстве информации и коммуникаций Республики Казахстан, значительно уменьшились. Однако они не совсем удовлетворены размером заработной платы. Низкая зарплата может быть причиной того, что высококвалифицированные специалисты в области ИТ, и сертифицированные эксперты в области кибербезопасности покидают и уезжают в другие страны.

Таким образом, политикам следует беспокоиться о сохранении собственных квалифицированных сотрудников и сделать Казахстан более привлекательным для других стран. В этом случае следует использовать опыт Сингапура. Сделать границу открытой для высококвалифицированных специалистов.

В целом резюмируя, полученные результаты опроса говорят о следующем.

Правительству РК необходимо на постоянной основе проводить ознакомительные мероприятия с населением, сделать информацию максимально доступной для народа, улучшить ее качество в целях повышения доверия к реализуемым правительственным проектам и инициативам. Так, респонденты считают, что необходимо пропагандировать среди населения внедрение новых технологий и их влияние на проводимые реформы как в области кибербезопасности, так и в цифровизации. Вместе с тем, повышать компьютерную и правовую грамотность населения в отдаленных, сельских местностях, то есть организовать обучающие курсы для населения по использованию государственных услуг, и делать их доступными для масштабного пользования.

На постоянной основе необходимо проводить анализ зарубежного опыта и внедрять уже проверенные новшества, повышать сохранность персональных данных граждан и исключать использование их третьими лицами. В этой связи обосновывается необходимость создания Центра по кибербезопасности с привлечением высококвалифицированных специалистов в IT сфере с глубокими знания менеджмента.

Одновременно с наращиванием кадрового потенциала в ИТ сфере, нужно создавать крупные международные хабы, как это практикуется в Соединенных Штатах Америки и Индии. В этой связи, по необходимости нужно рассмотреть возможность увеличения количества серверов, находящихся на территории Республики Казахстан постепенно отказываясь от зарубежных услуг, что стимулирует развитие отечественного ИТ рынка и повысит его безопасность. Максимальное использование отечественных программных решений и продуктов позволит повысить конкурентоспособность Казахстанского ИТ рынка и выйти на международный уровень.

Обсуждение результатов

Elin Wihlborg Karin Hedstrom and Hannu Larsson [11] отмечают, что «электронное правительство» повышает производительность и транспарентность при оказании госуслуг. Тем не менее, несмотря на преимущества, внедрение цифровых услуг несет такие риски как взлом систем и кража данных из-за атак в киберпространстве. Например, согласно данным Global Data Protection Index, 72% опрощенных отметили, что безопасность цифровых данных является важным аспектом в успешности организации [12].

Компания Lloyd при исследовании рассчитали, что киберугроза может обойтись экономике в глобальном масштабе 120 млрд. фунтов стерлингов [18]. Вместе с тем, другие исследования показали, что расходы организации на ИКТ составляют 211 000 000 $ США, и большая часть из ресурсов распределяются на защиту данных [16].

GCI рассчитывается ежегодно. GCI впервые проведен в 2013-2014 годах. В данном рейтинге Казахстан находятся на этапе созревания, а такие страны как США, Сингапур и Швеция находятся на лидирующих позициях [13, с.15]. Например, на сегодня Сингапур вошел в первую десятку стран по использованию ИКТ и обеспечению их защиты согласно IMD WDCR за 2017 год [14, с. 2] и GCI [13, с. 59].

В 2018 году Сингапуром предусмотрены финансовые средства на реализацию образовательных проектов в области цифрового здравоохранения и компьютерной грамотности населения. Вместе с тем, военнослужащие Сингапура будут обучаться по специализациям в области кибербезопасности и цифровизации [10].

Jing Zhanga, and Yushim Kimb [15, с. 215] отличают некоторые проблемные вопросы в области цифровизации. Например, отсутствие четкого решения при возможных киберугроз. Всем известный факт, что неразрешенные проблемы несут негативные последствия при внедрении инновационных идей в сфере цифровизации.

Итоги обзорного исследования показали, что Казахстан за 2018 год достиг достаточно хороших результатов в области кибербезопасности, тогда как показатель по цифровизации сохранил свою позицию предыдущего года – 38.

Выводы и рекомендации

В статье рассматривались вопросы кибербезопасности и цифровизации Казахстана и частично опыт успешных стран, которые были определены согласно показателям рейтингов, GCI и IMD WDC. Россия и Эстония выбраны с учетом того, что эти страны, как и Казахстан входили в состав бывшего СССР. Авторами статьи также описаны нынешнее положение Казахстана в области кибербезопасности и цифровизации. Проведен онлайн опрос с участием 173 респондентов. Одновременно проведено интервью с 12 сотрудниками РГП «ГТС» и KZ-CERT.

На сегодня Казахстан, как и другие страны, осуществляет свое развитие с акцентом на внедрение передовых технологий, стремясь повысить эффективность государственного управления.

На основании результатов исследования, необходимо отметить об отсутствии стратегии кибербезопасности Казахстана, которая будет определять траекторию стратегического плана кибербезопасности. Вместе с тем, наблюдается потребность квалифицированных специалистов в сфере кибербезопасности.

На основании изложенного, авторы статьи предлагают следующие мероприятия в целях развития цифровизации и кибербезопасности.

1. В целях минимизации негативных последствий от кибератак, необходимо проводить работы по повышению компьютерной грамотности населения;

2. Необходимо рассмотреть возможность снижения тарифов за услуги мобильной связи и интернет с крупными провайдерами как АО «Казахтелеком» и Beeline (ТОО «KaP-Тел»);

3. Рассмотреть возможность привлечения зарубежных экспертов, и подготовка отечественных квалифицированных кадров в области кибербезопасности;

Несомненно, Казахстан за годы независимости сделал немало на пути кибербезопасности и цифровизации, однако впереди еще долгий путь. Авторами предполагается, что данная работа должна проводиться не только правительством, но и частным сектором с привлечением гражданского общества.

Список литературы

1. Асланова Н., Олжас Сатиев, ЦАРКА: более 90% казахстанских ресурсов подвержены уязвимостям «Белые хакеры» рассказали о состоянии информационной безопасности в Казахстане, 10.02.2016, http://profit.kz/articles/7223/Olzhas-Satiev-CARKA-bolee-90-kazahstanskih-resursov-podverzheni-uyazvimostyam/ (дата обращения: 23.08.2019г.).

2. Маулетбай С, Как «вирус от Генпрокуратуры» помог разбогатеть хакерам, https://informburo.kz/stati/kak-virus-ot-

genprokuratury-pomog-razbogatet-hakeram.html, 2016 (дата обращения: 23.07.2019г.).

3. Официальный сайт Президента Республики Казахстан, Указ Президента Республики Казахстан от 19 марта 2019г. «Об исполнении полномочий Президента Республики Казахстан» 2019 год, http://www.akorda.kz/ru/legal_acts/decrees/ob-ispolnenii-polnomochii-prezidenta-respubliki-kazahstan (дата обращения: 23.04.2019г).

4. Официальный сайт РГП «Государственная техническая служба» Комитета национальной безопасности Республики Казахстан, http://sts.kz/ru/organization (дата обращения: 09.09.2019 г.).

5. Послание Президента Республики Казахстан от 31 января 2017 года «Третья модернизация Казахстана: глобальная конкурентоспособность»,. Режим доступа: http://adilet.zan.kz/rus/docs/K1700002017 (дата обращения: 06.02.2019г.).

6. Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407, Об утверждении Концепции кибербезопасности («Киберщит Казахстана»), http://adilet.zan.kz/rus/docs/P1700000407 (дата обращения: 09.07.2019 г.).

7. Сейткулов Е.Н. Информационная безопасность Республики Казахстан: состояние и перспективы. [Электронный ресурс] http://www.enu.kz/ru/info/novosti-enu/novosti-nauki/45582/ 10.10.2016г. (дата обращения: 09.09.2019 г.).

8. Указ Президента Республики Казахстан от 21 февраля 2019 года № 845, О Правительстве Республики Казахстан, http://adilet.zan.kz/rus/docs/U1900000845 (дата обращения: 27.04.2019г.).

9. Bershadskaya L., Chugunov A., Dzhusupova Z. Understanding E-Government Development Barriers in CIS Countries and Exploring Mechanisms for Regional Cooperation // Technology-Enabled Innovation for Democracy, Government and Governance. Springer Edition. – 2013. – P. 87–101.

10. Building an inclusive digital society. 6 марта 2018г. https://www.gov.sg/microsites/budget2018/press-room/news/content/building-an-inclusive-digital-society (дата обращения: 13.01.2019г.).

11. Elin Wihlborg Linkoping University, Sweden, Karin Hedstrom and Hannu Larsson Örebro University, Sweden // Proceedings of the 50th Hawaii International Conference on System Sciences, 2017, e-government for all – Norm-critical perspectives and public values in digitalization / < http://aisel.aisnet.org/hicss-50/eg/government_services/4/> (дата обращения: 02.05.2019г.).

12. EMC Global Data Protection Index - Global Results, https://www.emc.com/infographics/global-data-protection-index-global.htm (дата обращения: 22.05.2019г.).

13. Global Cybersecurity Index 2017, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf (дата обращения: 12.03.2019г.).

14. IMD World Digital Competitiveness Ranking, 2017, (дата обращения: 12.03.2019.).

15. Jing Zhanga, and Yushim Kimb, Digital government and wicked problems: Solution or problem?, Information Polity 21 (2016) 215–221 215 DOI 10.3233/IP-160395 IOS Press, Special Issue Editorial, pp. 215-221 https://content.iospress.com/download/information-polity/ip395idinformation-polity2Fip395 (дата обращения: 12.03.2019г.).

16. Key findings & Results for Italy retrieved from http://www.datamanager.it/wp-content/uploads/2014/12/EMC-Data-Protection-Index-Key-Findings-Italy-FINAL.pdf, (дата обращения: 12.03.2019г.).

17. Lagutina M. Eurasian Economic Union Foundation: Issues of Global Regionalization // Eurasia Border Review. – 2014. – №5(1). – P. 102

18. The guardian, Lloyd's says cyber-attack could cost $120bn, same as Hurricane Katrina https://www.theguardian.com/business/2017/jul/17/lloyds-says-cyber-attack-could-cost-120bn-same-as-hurricane-katrina (дата обращения: 22.03. 2019г.).

19. Warnes, K., PhD (2019) 'Cybersecurity', Salem Press Encyclopedia. https://ezproxy.nu.edu.kz/loginurl=https://ezproxy.nu.edu.kz:2358/login.aspxdirect=true&db=ers&AN=89677538&site=eds-live&scope=site (Дата обращения: 13.03.2019г.).

А.Б. Зейнелғабдин
э.ғ.д., Қазақстан Республикасы Президентінің жанындағы Мемлекеттік басқару академиясының Басқару институтының профессоры, Нұр-Сұлтан қ, Қазақстан, email: A.Zeinelgabdin@apa.kz

С.Б. Исабаева
Қазақстан Республикасы Президентінің жанындағы Мемлекеттік басқару академиясының «Мемлекеттік және жергілікті басқару» мамандығы бойынша докторанты; Қазақстан Республикасы Бас прокуратурасының жанындағы Құқық қорғау органдары академиясының бас сарапшысы. Нұр-Сұлтан қ, Қазақстан, email: S.Issabayeva@apa.kz

ТҮЙІН
ЦИФРЛЫҚ ТРАНСФОРМАЦИЯ КЕЗЕҢІНДЕГІ ҚАЗАҚСТАННЫҢ КИБЕРҚАУІПСІЗДІГІ

Мақала Қазақстанның цифрлық трансформациясы кезеңінде киберкеңістіктегі киберқауіпсіздік мәселелерін қарастырады. Онлайн қызметтердің сапа деңгейін анықтау мақсатында авторлар Қазақстандағы цифрлық қызметтерді пайдаланушылар арасында онлайн сауалнама жүргізді. Аталмыш мақалада киберқауіпсіздік саласындағы халықаралық көрсеткіштер қолданылған. Зерттеудің сапалы әдісі қолданылды, сонымен қатар теориялық және эмпирикалық талдау жүргізілді. Мақалада табысты елдердің тәжірибесі де қарастырылған. Зерттеу нәтижелері бойынша мақала авторлары киберқауіпсіздік және цифрландыру саласында ұсыныстар ұсынды. Киберқауіпсіздік саясатын жетілдіру бойынша ұсынылған тәжірбиелік ұсыныстар тек Қазақстанға ғана емес, сандық трансформация кезеңін бастан өткеріп жатқан басқа елдерге де қолдануға болады.

Zeinelgabdin A.B.
Professor of the Institute of Management of the Academy of public administration under the President of the Republic of Kazakhstan, Doctor of Economic Sciences, c. Nur-Sultan, Kazakhstan, email: A.Zeinelgabdin@apa.kz

Issabaeva Symbat
doctoral student of the Academy of public administration under the President of the Republic of Kazakhstan, specialty "Local public administration"; chief expert of the Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan, Nur-Sultan, Kazakhstan, email: S.Issabayeva@apa.kz

SUMMARY
CYBERSECURITY OF KAZAKHSTAN IN THE PERIOD OF DIGITAL TRANSFORMATION

The article considers the issues of cybersecurity in cyberspace in the period of Kazakhstan's digital transformation. In order to determine the level of quality of online services, the authors conducted an online survey among digital services users of Kazakhstan. The international indicators in the field of cybersecurity are used in the article. A qualitative research method was applied, as well as theoretical and empirical analysis. The article also considers the experience of successful countries. Based on the study results, the authors of the article proposed recommendations in the field of cybersecurity and digitalization. The proposed practical recommendations for improving cybersecurity policy are applicable not only to Kazakhstan but also to other countries which are experiencing a period of digital transformation.