Академия государственного управления при Президенте Республики Казахстан

УДК 451.86:004(574)

на правах рукописи

ИСАБАЕВА СЫМБАТ БОЛАТОВНА

Обеспечение кибербезопасности Казахстана в условиях глобальной цифровизации

6D051000 – Государственное и местное управление

Диссертация на соискание степени
доктора по профилю

Научные консультанты
доктор экономических
наук, профессор,
А.Б. Зейнельгабдин

кандидат физико-
математических наук,
Е.Н. Сейткулов

Республика Казахстан
Нур-Султан, 2020

СОДЕРЖАНИЕ

НОРМАТИВНЫЕ ССЫЛКИ

В настоящей диссертации использованы ссылки на следующие стандарты:

Уголовный кодекс Республики Казахстан: принят 3 июля 2014 года, №226-V ЗРК.

Закон Республики Казахстан. Об электронном документе и электронной цифровой подписи: принят 7 января 2003 года, № 370.

Закон Республики Казахстан. О связи: принят 5 июля 2004 года, №567.

Закон Республики Казахстан. Об образовании: принят 27 июля 2007 года № 319-III.

Закон Республики Казахстан. О национальной безопасности Республики Казахстан: принят 6 января 2012 года, № 527-IV.

Закон Республики Казахстан. О персональных данных и их защите: принят 21 мая 2013 года, № 94-V.

Закон Республики Казахстан. Об информатизации: принят 24 ноября 2015 года, № 418-V ЗРК.

Закон Республики Казахстан. О государственных закупках: принят 4 декабря 2015 года, № 434-V ЗРК.

Постановление Правительства Республики Казахстан. Об утверждении Правил и критериев отнесения объектов информационно-коммуникационной инфраструктуры к критически важным объектам информационно-коммуникационной инфраструктуры: утв. 8 сентября 2016 года, № 529.

Постановление Правительства Республики Казахстан. Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности: утв. 20 декабря 2016 года, №832.

Постановление Правительства Республики Казахстан. Об утверждении Концепции кибербезопасности («Киберщит Казахстана»): утв. 30 июня 2017 года, № 407.

Постановление Правительства Республики Казахстан. Об утверждении Плана мероприятий по реализации Концепции кибербезопасности («Киберщит Казахстана») до 2022 года: утв. 28 октября 2017 года, № 676.

Постановление Правительства Республики Казахстан. Об утверждении Государственной программы «Цифровой Казахстан»: утв. 12 декабря 2017 года № 827.

Послание Президента Республики Казахстан. «Третья модернизация Казахстана: глобальная конкурентоспособность»: принят 31 января 2017 года.

Послание Президента Республики Казахстан - Лидера Нации Н.А. Назарбаева народу Казахстана. Стратегия «Казахстан-2050»: новый политический курс состоявшегося государства: принят 14 декабря 2012 года.

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АО «ГТС»	-	Акционерное общество «Государственная техническая служба»
ВУЗ	-	Высшее учебное заведение
ГО	-	Государственный орган
ГП ЦК	-	Государственная программа «Цифровой Казахстан»
ГУ	-	Государственное учреждение
ИБ	-	Информационная безопасность
ИКТ	-	Информационно-коммуникационные технологии
ИС	-	Информационная система
ИТ	-	Информационные технологии
КВОИКИ	-	Критически важные объекты информационно-коммуникационной инфраструктуры
КИБ	-	Комитет по информационной безопасности
КНБ РК	-	Комитет национальной безопасности Республики Казахстан
МВД РК	-	Министерство внутренних дел Республики Казахстан
МИД РК	-	Министерство иностранных дел Республики Казахстан
МИОР РК	-	Министерство информации и общественного развития Республики Казахстан;
МОН РК	-	Министерство образования и науки Республики Казахстан
МПТ (TAM)	-	Модель Принятия Технологий (Technology Acceptance Model)
МЦРИАП РК	-	Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан
НИОКР	-	Научно-исследовательские и опытно-конструкторские работы
НКЦИБ	-	Национальный координационный центр информационной безопасности
НПА	-	Нормативно правовой акт
НСБ	-	Национальный сертификат безопасности
ООН	-	Организация Объединенных Наций
ПО	-	Программное обеспечение
ППРК	-	Постановление Правительства Республики Казахстан
СМИ	-	Средства массовой информации
СНБ	-	Сертификат национальной безопасности
ЦАРКА	-	Центр анализа и расследования кибератак
ЦМБЭП	-	Центр мониторинга безопасности электронного

		правительства
ЦОД	-	Центр обработки данных
ЭП	-	Электронное правительство
Denial of Service (DoS) атака	-	Отказ в обслуживании
Distributed Denial of Service (DDoS) атака	-	Распределенный отказ в обслуживании
General Data Protection Regulatory (GDPR)	-	Общий Регламент по Защите Данных
Global Cybersecurity Index (GCI)	-	Глобальный индекс кибербезопасности
IMD World Digital Competitiveness ranking (IMD WDC)	-	Рейтинг Мировой Цифровой Конкурентоспособности
KZ-CERT	-	Служба реагирования на компьютерные инциденты
National cyber security index (NCSI)	-	Национальный Индекс Кибербезопасности
PEST	-	Анализ политических, экономических, социальных и технологических факторов
Presidential Policy Directive 20 (PPD – 20)	-	Директива Президентской Политики
SWOT	-	Анализ сильных, слабых сторон, потенциальных возможностей и угроз
The International Telecommunication Union (ITU)	-	Международный Союз Электросвязи

ВВЕДЕНИЕ

Актуальность темы исследования. Вопросы кибербезопасности имеют прямую связь с вопросами национальной безопасности государства. Интернет и социальные сети могут использоваться для управления общественным сознанием, влияния на определенные социальные группы. Полномасштабное применение цифровых технологий в внастоящее время является одной из неотъемлемых частей в удовлетворении ежедневных потребностей граждан. Посредством цифровых услуг осуществляются покупка билетов в кинотеатры, заказ на дом товаров, продуктов, готовой еды и многое другое. Информационные технологии применяются практически во всех сферах государственного управления, экономических, социально-культурных, а также в административно-политических сферах. В связи с таким стремительным развитием цифровизации, обеспечение кибербезопасности больших данных является одной из критических проблем не только в государственном управлении, но и в частном секторе. Многие страны сегодня сосредоточены на вопросах обеспечения кибербезопасности в государственном управлении. Кибератаки могут повредить не только военную или экономическую системы, но и негативно повлиять на политические процессы, дестабилизируя внешнюю и внутреннюю безопасность в стране. Таким образом, большинство стран начали уделять значительное внимание защите особо важных цифровых и информационных систем и технологий.

Как ранее отмечалось сегодня люди, и компании больше зависят от Интернета практически во всех аспектах своего существования. Согласно исследованию McKinsey во всем мире каждую секунду к Интернету подключается около 127 новых цифровых устройств. Любое нарушение цифровой связи считается препятствием на пути к прогрессу экономики. Более того, из-за пандемии COVID-19 зависимость от цифровых технологий резко возросла, поскольку удаленная работа стала неотъемлемой частью экономики, образования, медицинской помощи и др. Растущая зависимость граждан и бизнеса от цифровых технологий в будущем только будет продолжаться. С каждым новым устройством, пользователем и бизнесом, подключающимся к Интернету, угроза кибератак возрастает. McKinsey в своем исследовании также отмечает, что если правительство не будет обеспечивать безопасную и надежную цифровую связь, экономика не сможет процветать [1].

В 2016 году на Всемирном Экономическом форуме отметили, что кибербезопасность является проблемой, которая требует участия на самом высоком уровне правительства [2].

Казахстан, как и другие страны, на правительственном уровне обсуждает вопросы кибербезопасности наравне с цифровизацией. Так, в 2017 году была принята Государственная программа «Цифровой Казахстан» [3] и Концепция Кибербезопасности [4].

В Казахстане с 2010 по 2016 годы количество пользователей Интернет возросло с 36,1% до 75%, одновременно увеличились пользователи мобильного

Интернета с 3,7 миллионов до 10,5 миллионов [4]. Данный показатель является сигналом, так как с каждым годом все больше людей находятся в киберпространстве и используют онлайн услуги, что в свою очередь повышает уязвимость пользователей Интернет к кибератакам.

Многие страны в нормативно-правовых актах определили понятие «кибербезопасность» раньше, чем Казахстан. Предполагается, что это связано с тем, что данные страны столкнулись с проблемами кибератак намного раньше, чем Казахстан, что являлось основанием внедрения политики обеспечения кибербезопасности в стране. К примеру, в 2007 году в Эстонии в течение трех недель были парализованы офис главы государства станы, правительства, парламента, а также другие коммуникации и связи с DDoS атаками [5]. С преодолением этих последствий связана лидирующая позиция Эстонии среди постсоветских стран в области цифровизации и кибербезопасности. Так, Эстония согласно Индексу глобальной кибербезопасности 2018 (Global Cybersecurity Index GCI) заняла 5 позицию [6] и 25 позицию Мирового Рейтинга Цифровой Конкурентоспособности 2018 (IMD World Digital Competitiveness ranking IMD WDC) [7; 8]. С аналогичными крупномасштабными кибератаками сталкивались Индия и Пакистан в 2010 году, Канада в 2011 году и многие другие страны [3]. В XXI веке взгляд цифрового общества на риски изменился, и один из глобальных рисков воспринимает инциденты, которые происходят в киберпространстве. В своем исследовании Карпова Д.Н. отмечает, что ежесекундно 12 Интернет-пользователей подвергаются кибератакам, и каждый год происходит более 500 млн. киберинцидентов, ущерб от которых приравнивается к $100 миллиардов долларов США [9]. Происходящие изменения в глобальном мире подтверждают актуальность вопроса обеспечения кибербезопасности в Казахстане на правительственном уровне.

Таким образом, в данной диссертационной работе будут рассматриваться механизмы государственного управления в целях повышения обеспечения кибербезопасности в Республике Казахстан путем изучения научно-теоретических основ обеспечения кибербезопасности передового международного опыта в сфере защиты цифровых данных, совершенствования защиты персональных данных пользователей, сайтов государственных органов от киберугроз через совершенствование законодательства, подготовку и повышение квалификации специалистов в сфере обеспечения кибербезопасности.

Степень изученности проблемы. В рамках исследовательской работы изучены теоретические и практические проблемы кибербезопасности в трудах зарубежных и отечественных ученых. Стратегии и законодательство кибербезопасности изучены в трудах Шафкад Н., Масуд А. [78]; Ли Ж. [87]; Парасол М. [88]; Ян Ф., Сюй Ж. [89]; Шемчук В. [124]. Понятийный аппарат термина «кибербезопасность» рассматривался такими учеными, как Татаринова Л. [50] и Эфтимиопулос М. [51]. Механизм, политика, а также вопросы рисков обеспечения кибербезопасности исследовали Абучакра Р. Хури М. [5]; Карпова

Д. [9]; Зейнелгабдин А., Исабаева С. [10]; Варнес, К. [11]; Сзакос Ж., Садецкий Т.[12]; Драге-Адриансон К., Крауч Д. [21]; Темз Л., Шефер Д. [23]; Ле, Д. Н., Кумар, Р., Мишра, Б. К., Чаттерджи, Дж. М., и Хари, М. [24]; Амос Н. [28]; Альперен М. [30]; Ллойд Г.[31]; Крейген Д. [40]; Мосчовитис С.[48]; Татаринова Л. [50]; Эфтимиопулос М. [51]; Кен Икс [52]; Жумагалиев А. [59]; Фурье Л., Панг С., Кингстон Т., Хеттема Х., Уоттерс П., Саррафзаде Х. [61]; Колдуэлл Т. [62]; Марр С.[66]; Валиахметова Г. [68]; Хараста Ж. [101]; Андрью Т. [120]; Сейткулов Е. [166]. Вопросы элетронного правительства, цифровизации и кибербезопасности изучали Губайдуллина М.[15]; Элин В. [16]; Исабаева С., Кармыс Г., Бексултанов А., Жусупова Г. [19]; Мишра А., Гош С., Мишра Б. [22]; Беатриз Н., Кутберто В., Сесар Л. [29]; Карасев П.[32]; Емли А.[105]; Клименко, П., Клименко И. [139]; Мусабаев Р., Касымжанов, Б., Калиева, Г., Ибраева В., [149], Головенчик Г., [148]; Бершадская Л., Чугунов А., Джусупова З., [155]. Модель принятии технологий электронного правительства и цифровых сервисов изучали Исаак О. [156]; Вангпипатвонг С., Чутимаскул В., Папасраторн Б., [157], Аль-Адави З., Юсафзай С., Паллистер Ж., [158]; Колеска С., Добрица Л., [159]; Джегер П., [160] и др.

Вместе с тем, изучены отчеты Всемирного Банка, а также ежегодные отчеты Глобального Индекса Кибербезопасности, Национального Индекса Кибербезопасности и Мирового Рейтинга Цифровой Конкурентоспособности, Законы РК «Об информатизации», «О национальной безопасности Республики Казахстан» и «О персональных данных и их защите», а также другие нормативно-правовые акты.

Объектом исследования являются органы, обеспечивающие кибербезопасность в условиях глобальной цифровизации.

Предметом диссертационной работы является взаимодействие управленческих отношений государственных органов по обеспечению кибербезопасности в условиях глобальной цифровизации.

Целью исследования является выработка рекомендаций по совершенствованию обеспечения кибербезопасности Казахстана.

Для достижения цели исследования были поставлены следующие задачи:

– изучить теоретические, методологические и практические аспекты обеспечения кибербезопасности с учетом передового зарубежного опыта;

– проанализировать действующий механизм обеспечения кибербезопасности Республики Казахстан;

– провести анализ степени готовности населения, государства к цифровизации;

– провести SWOT и PEST анализ кибербезопасности Казахстана в условиях глобальной цифровизации;

– определить ключевые направления по совершенствованию системы обеспечения кибербезопасности в Казахстане.

Методы исследования. В рамках исследования среди 182 респондентов-пользователей цифровых услуг Казахстана проведен онлайн-опрос в целях

определения готовности населения к применению онлайн-сервисов. 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. Также в ходе исследование проведено анкетирование по вопросам кибербезопасности среди 357 респондентов и фокус-группы среди 20 сотрудников АО «ГТС» КНБ РК. Итоговое количество респондентов - 539. Результаты анкетирования в Приложении А.

Данное исследование проводилось в целях раскрытия компьютерной и киберграмотности граждан, определения степени доверия к реализации государственной программы «Цифровой Казахстан» и Концепции кибербезопасности.

В исследовании применены качественные и количественные методы анализа, модель принятия технологий Девиса (Technology Acceptance Model), а также методы PEST, SWOT и Case study. Источником проведенного анализа являются нормативные правовые акты, стратегические и статистические материалы государственного управления по обеспечению кибербезопасности.

Научная новизна результатов исследования. Научная новизна исследования заключается в том, что на основе проведенного теоретико-аналитического исследования:

- в целях четкого понимания и единой трактовки уточнено определение понятия «Кибербезопасность»;
- с помощью модели принятия технологий Девиса и по результатам анализа онлайн-опроса респондентов определено отношение готовности населения использовать цифровые сервисы Казахстана;
- по результатам проведенного PEST и SWOT анализа предложены практические рекомендации по совершенствованию системы кибербезопасности в Республике Казахстан, включающие вопросы законодательно-методического и кадрового обеспечения;
- предложен проект управленческой структуры государственного аппарата по совершенствованию системы обеспечения кибербезопасности в Республике Казахстан;
- даны научно-методические рекомендации для Академии государственного управления при Президенте Республики Казахстан в части разработки краткосрочных спецкурсов по кибербезопасности для действующих государственных служащих.

Научные положения диссертации, выносимые на защиту.

1. По результатам проведенного анализа, выявлено, что в концепции кибербезопасности Казахстана дано определение термину «кибербезопасность» и Законе РК «Об информатизации» понятию «Информационная безопасность в сфере информатизации», представленные формулировки нетривиальны и существенно разнятся. В связи с этим, в целях единого и четкого понимания и правоприменения сформулировано авторское

определение понятию «кибербезопасность», под которым следует понимать «комплекс организационно-правовых, экономических и технических процедур в целях защиты от несанкционированного использования информационных ресурсов в киберпространстве». Данное определение представлено на основе изученного материала ближнего и дальнего зарубежья.

2. Обоснована необходимость разработки Национальной стратегии кибербезопасности Казахстана, которая предусматривала бы следующие аспекты:

– укрепление кибербезопасности страны и развитие потенциала киберзащиты, борьбу с киберпреступностью;

– обеспечение предупреждения и расследования уголовных преступлений в киберпространстве, соблюдение баланса между безопасностью и конфиденциальностью;

– продвижение культуры кибербезопасности;

– укрепление международного сотрудничества и обеспечение выполнения международных обязательств в области кибербезопасности.

3. Изучив передовой опыт обеспечения кибербезопасности таких стран, как Сингапур, Китай, Великобритания, а также, проанализировав предпринимаемые государством меры по защите цифровых данных Казахстана, установлена необходимость совершенствования законодательной базы посредством принятия закона по обеспечению кибербезопасности страны. В данном законе одним из направлений необходимо предусмотреть нормы по защите, обработке, приеме и передаче биометрических данных при оказании государственных услуг.

4. На основе анализа деятельности уполномоченных государственных органов по обеспечению кибербезопасности страны, а также с целью эффективной реализации политики по обеспечению кибербезопасности предложено создание нового государственного учреждения с передачей ему функций КИБ МЦРИАП и АО «ГТС» при КНБ РК.

5. В рамках государственно-частного партнёрства предлагается разработать платформу для безопасного и оперативного обмена информацией между государственными и частными структурами в целях минимизации и предотвращении возможных киберинциндентов в цифровом пространстве Казахстана. Данная платформа бизнес сообщества позволит заинтересованным сторонам обмениваться опытом, находить необходимую информацию по обеспечению кибербезопасности.

Теоретическая и практическая значимость исследования состоит в возможности применения результатов данной работы при разработке стратегии кибербезопасности Казахстана. Вместе с тем, разработанные рекомендации могут широко применяться государственным и частным секторами, ответственными за эффективный механизм обеспечения кибербезопасности в стране.

Результаты исследования также могут использоваться в ВУЗах и в других научно-образовательных организациях для составления программ спецкурсов

по предметам «Основы кибербезопасности», «Кибербезопасность» и «Информационная и Кибербезопасность». Более того, в рамках исследовательской работы разработаны четырех и шестичасовые (офлайн) обучающие программы, а также трехнедельные дистанционные курсы по темам «Кибербезопасность» и «Информационная и Кибербезопасность» для Академии государственного управления при Президенте Республики Казахстан. Таким образом, полученные результаты применимы не только в науке, но и в практике.

Ожидаемые результаты. Выявление и определение успешного опыта среди развитых и развивающихся стран по обеспечению кибербезопасности путем эмпирического и теоретического анализа. Предложить оптимальные рекомендации по обеспечению и развитию кибербезопасности Казахстана в условиях цифровизации.

Апробация результатов исследования. Результаты основных положений исследования были апробированы на 5 международной научно-практической конференции «Национальная правовая система Республики Таджикистан и стран СНГ: анализ тенденций и перспектив развития»; на 14 международной научно-практической конференции студентов, магистрантов и аспирантов «Цифровые технологии в экономике и управлении: научный взгляд молодых», организованной Челябинским филиалом Финансового университета при Правительстве Российской Федерации; на 5 международной научно-практической Интернет-конференции «Организационно-правовые аспекты государственного управления в Украине»; на международной конференции BASIQ «New Trends in Sustainable Business and Consumption»; на международной научно-практической конференции «Тенденции мировых интеграционных процессов: вызовы и возможности», проведенной в ЕНУ им. Л.Н. Гумилева.

В целом, по диссертации опубликованы одиннадцать научных работ: 2 – в журнале, индексируемом в базе данных Web of Science Core Collection, Clarivate Analitics и Scopus, 4 – в журналах, рекомендованных ККСОН МОН РК, 5 – в материалах международных конференций.

Апробация результатов исследования прошла в рамках различных международных и отечественных тренингов и проектах: сертификат 2017 года за участие в проекте «Научно-обоснованная база и Интернет-технологии для системного повышения потенциала гражданского сектора» (Казахстан), сертификат 2018 года за участие в Сингапурском корпоративном курсе «Лидерство в электронном правительстве E-government leadership» (Сингапур), сертификат 2018 года за участие в научно-практическом тренинге по повышению роли молодежи из стран СНГ в секторе безопасности «Актуальные вопросы безопасности в условиях глобализации» (Кыргызстан), сертификат 2019 года за участие в семинаре «Экспертный контроль» (Казахстан), и онлайн-курсы «Введение в Кибербезопасность» и «KPI» совместно с Cisco Networking Academy (Украина). Результаты исследования также апробированы в Научно-исследовательском институте информационной безопасности и криптологии

Евразийского национального университета им. Л.Н. Гумилева в рамках проведенного совещания с участием экспертами по обсуждению вопросов кибербезопасности Республики Казахстан (Приложение Б).

Разработанные в рамках исследовательской работы четырех и шестичасовые (офлайн) обучающие программы для Академии государственного управления при Президенте Республики Казахстан, были апробированы в 2019-2020 учебном году в ходе повышения квалификации более 200 действующих государственных служащих. Результаты входного и выходного тестирования показали значительное улучшение уровня киберграмотности слушателей (Приложение В). Акт оказанных услуг в Приложении В.

Структура и объем диссертационного исследования. Диссертационная работа состоит из введения, трех разделов, восьми подразделов, заключения, списка использованной литературы (217 источников) и приложений. Работа в себе включает 23 - рисунка и 11 - таблиц, Основная часть исследовательской работы состоит из 123 страниц.

1 ОСНОВЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ В УСЛОВИЯХ ГЛОБАЛЬНОЙ ЦИФРОВИЗАЦИИ

1.1 Теоретические аспекты кибербезопасности, история их развития

Тема кибербезопасность является одним из актуальных вопросов, как для академиков, государственных управленцев, так и для бизнес-сектора. Исследования данной отрасли обусловлена активным внедрением цифровых технологий во все сферы жизнедеятельности казахстанского общества, в том числе в государственное управление, и необходимостью обеспечения защиты персональных данных увеличивающегося числа пользователей, а также цифровых данных, используемых государственными органами. 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 государственным и бизнес секторам. К примеру, согласно некоторым данным Стив Возняк и Стив Джобс в 1970 году взломав телефонную систему, смогли совершать бесплатные звонки, как в ближние, так и в дальние зарубежные страны. Вместе с тем, можно отметить, что в 1990 году в истории хакерства основное место занял Кевин Митник, который сумел взломать систему безопасности и имел доступ к компьютерам корпорации [10, с. 47]. Другим примером можно отметить вирус Stuxnet, разработанный в 2009 году. Целью данного вируса было повреждение иранского завода по обогащению урана [11]. Таким образом, обеспечение кибербезопасности в цифровом пространстве является одним из критически важных вопросов любого государства [12, с. 195].

Адмирал Джеймс Дж. Ставридис, бывший командующий НАТО, в своем выступлении отметил важность вопроса кибербезопасности и выразил это следующим образом - «Единственное, что не давало мне спать по ночам (как командующему войсками НАТО) - это кибербезопасность. Кибербезопасность исходит из самых высоких уровней наших национальных интересов… через нашу медицину, наше образование, наши личные финансы (системы)» [13].

К концу 1990-х годов Интернет доминировал в глобальной коммуникационной среде. В 1993 году только около 1% телекоммуникационных сетей отправляли информацию через Интернет, но к 2000 году показатель превысил 51%. К 2007 году через Интернет передавалось более 97% информации. Потребность в использовании Интернет продолжает расти, так как данный инструмент на сегодняшний день является одним из двигателей прогресса. Онлайн услуги также важную роль сыграли в торговле (электронная коммерция), развлечений и социальных сетях для общения и обмена информациями [11; 14, с. 35]. Тема цифровизации актуальна не только для развитых государств, но и для развивающихся стран. Казахстан, как и другие страны, переживает период трансформации в области цифровизации. Правительством принят ряд НПА в целях развития цифровизации в стране. В

связи с экспоненциальным использованием цифровых технологий в частном и государственном секторах вопросы кибербезопасности становятся актуальными.

В своем исследовании Губайдуллина М. отметила, что цифровизация подразумевает транспарентность и незащищенность [15, с. 17]. По ее мнению, на международной арене в рамках дипломатических отношений цифровизация несет угрозы национальной безопасности страны. Однако, Вильборг Э., Хедстрем К., и Ларссон Х. [16] отмечают, что «электронное правительство», то есть внедрение цифровизации повышает производительность и транспарентность при оказании госуслуг. Таким образом, нельзя забывать, что цифровизация для населения является инструментом для быстрого общения, передачи информации и удобства для оплаты услуг. Люди ежедневно получают различные электронные справки, распечатку своих кредиторских задолженностей, проверяют баланс и производят покупки благодаря электронной коммерции. Цифровизация подразумевает прозрачность и доступность услуг для населения, что несет за собой положительную тенденцию в работе государственного управления и внедрения политики на местном уровне.

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% опрошенных отметили, что безопасность цифровых данных является важным аспектом в успешности организации [17].

Компания Lloyd при исследовании рассчитала, что киберугроза может обойтись экономике в глобальном масштабе 120 млрд. фунтов стерлингов [18; 19, с. 30]. 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 [20].

Вместе с тем, внедряя цифровые технологии, необходимо помнить о рисках в киберпространстве. Согласно докладу о глобальных рисках Всемирного экономического форума 2018 года (www.weforum.org) кибербезопасность является третьим по величине риском, с которым сталкиваются предприятия [21, с. 65]. Труды Цзин Ч. и Юшин К., [22, с. 215] отличают некоторые проблемные вопросы в области цифровизации. Например, отсутствие четкого решения при возможных кибер угрозах. Всем известный факт, что неразрешенные проблемы несут негативные последствия при внедрении инновационных идей в сфере цифровизации.

Промышленная индустрия 4.0 и связанные с ней технологии, такие как облачные системы проектирования и производства, «Интернет вещей» и «Разработка социальных продуктов» в настоящее время движимы прорывными инновациями, которые обещают предоставить бесчисленные новые возможности во всех секторах рынка. Однако, эти интернет технологии имеют проблемы с кибербезопасностью и конфиденциальностью данных, которые

представляют серьезные проблемы и будут препятствовать для внедрения технологической индустрии 4.0 [23, с.1-2; 12, с. 197].

История развития кибератак показывает, что с каждым годом разновидность киберугроз приобретает новые формы (рисунок 1).

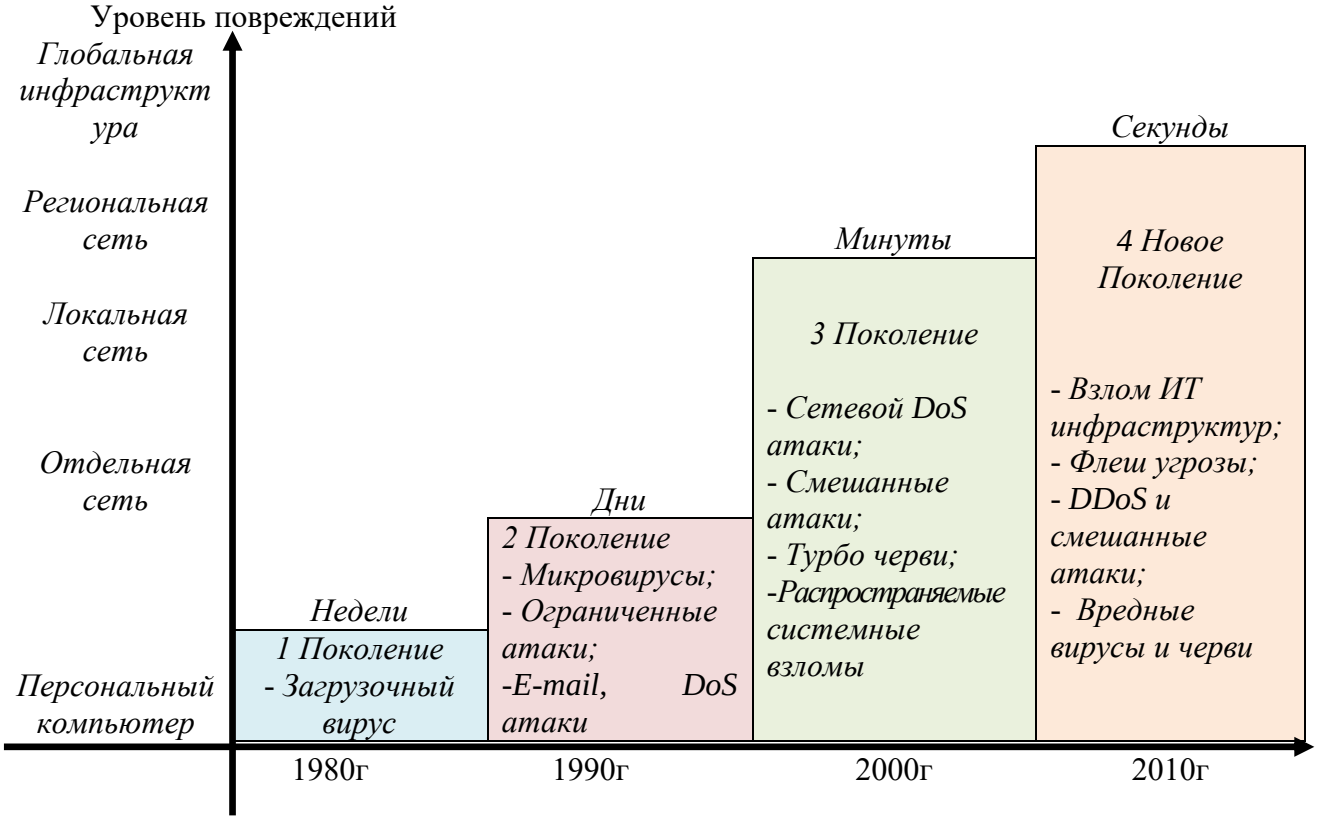

Рисунок 1 – Кибератаки и их развитие в разные годы

Примечание – Составлено по источнику [24]

История развития кибератак отражает реалии развития возможных киберугроз, то есть на сегодняшний день пользователи глобальной сети высоко уязвимы, и их могут атаковать в киберпространстве ежесекундно.

Cybint - это образовательная компания по кибербезопасности, занимающаяся защитой от возникающих киберугроз, отмечает, что средняя стоимость нарушения данных в 2020 году превысит $ 150 млн. Более того, в 2018 году хакеры украли полмиллиарда личных записей, это был скачок на 126% по сравнению с 2017 годом. С 2013 года каждый день похищается около 3 809 448 записей, то есть 158 727 в час, 2 645 в минуту и 44 ежесекундно, сообщает в своем ежедневном отчете Cybersecurity Ventures. Согласно предварительным данным ожидается, что к 2021 году на кибербезопасность в мире будет потрачено около $6 трлн. В нынешнее время необходимо кардинально изменить свой подход к кибербезопасности и расставить приоритеты в бюджетах, чтобы привести их в соответствие с этой новой реальностью нашего современного общества [25].

Исследование школы Кларка показало, что в среднем каждые 39 секунд зарегистрированы хакерские атаки на компьютеры, которые подключены к интернету из-за небезопасного имени пользователя и пароля, которые используют пользователи. Данное исследование проводилось под руководством доцента механического факультета Школы Кларка Мишель Кукье, он отметил, что «Наши данные дают количественные доказательства того, что атаки происходят все время на компьютеры с подключением к интернету», компьютеры в их исследовании подвергались атакам в среднем 2 444 раза в день [26].

Основы обеспечения кибербезопасности заключаются в следующих трех аспектах:

- доступность;
- целостность, которая может включать аутентичность;
- конфиденциальность [27; 23, с. 60].

Мишра А., Гош С., Мишра Б. [22, с. 207] обозначают, что обеспечение конфиденциальности, доступности и целостности данных в мобильных устройствах, электронных почтах, онлайн банках, электронных карточках пациентов является одним из приоритетных задач. Они обращают внимание на готовность стратегических, управленческих механизмов, сервисов, планов и программ риск менеджмента в целях минимизации возможных киберинцидентов.

В области кибербезопасности можно отметить труды Амос Н. Гиора, профессора права в Юридическом колледже им. С. Дж. Куинни Университета штата Юта. В 2017 году он написал книгу «Cybersecurity: Geopolitics, law, and policy», где преподносит новый взгляд на «киберпространство» приводя примеры из жизни. Всем известно, что Интернет больше не является личным или национальным пространством. Интернет объединяет всех с помощью социальных сетей, что несет ряд угроз персональным данным пользователей глобальной сети [28].

Вместе с тем, Беатрис Н., Катберто В., Сезар Л., в своем исследовании отмечают о необходимости установлении связи между государственным управлением и электронным правительством, так как электронное правительство – это «киберпространство», которое ассоциируется с глобализацией [29, с. 85] и не имеет границ [13, с. 14]. Таким образом, в связи с проводимыми межсистемными интеграционными работами между разными государствами, в глобальном мире практически смываются границы, что усложняет обеспечение кибербезопасности в онлайн пространстве.

Известный факт, что нарушение системы управления информационных ресурсов, в свою очередь приводит к неэффективной системе управления экономикой, то есть, стагнация рынка, возможно банкротство хозяйствующих субъектов, которые могут привести к кризису национальной экономики страны. Данное явление заставляет всерьез задуматься государственных политиков о кибербезопасности в цифровом пространстве. Идея о негативных финансовых последствиях от кибератак также поддерживается Алперен М. [30, с. 60-66].

Вместе с тем, Ллойд Г. и Карасев П. отмечают, что эффективная кибербезопасность позволяет компаниям вводить новшества, что ведет к росту доходов и прибыли, защита от киберпреступности может принести реальные выгоды малым и средним предприятиям и привести к созданию более ценных организаций [31, с. 14; 32, с. 53]. Согласно подсчетам компании IBM средняя общая стоимость нарушения данных обходится в $ 3,92 млн [33].

Boston Consulting Group отмечает, что кибератаки являются барьером для достижения стратегических целей и наносит колоссальный ущерб обществу. Их исследование показывает, что к 2021 году затраты на кибератаки в глобальном масштабе могут составить больше чем 6 триллионов долларов в год [34].

В нижеприведенной таблице 1 можно увидеть фактические расходы на кибербезопасность в мировом сегменте с 2017 по 2019гг.

Таблица 1 – Расходы на безопасность в мире по сегментам, 2017–2019годы

(в миллионах долларов США)

Сегмент рынка	2017	2018	2019
Безопасность приложений	2,434	2,742	3,003
Облачная безопасность	185	304	459
Безопасность данных	2,563	3,063	3,524
Управление доступом к удостоверениям	8,823	9,768	10,578
Защита инфраструктуры	12,583	14,106	15,337
Интегрированное управление рисками	3,949	4,347	4,712
Оборудование для сетевой безопасности	10,911	12,427	13,321
Другое ПО информационной безопасности	1,832	2,079	2,285
Охранные услуги	52,315	58,920	64,237
ПО для защиты прав потребителей	5,948	6,395	6,661
ИТОГО	101,544	114,152	124,116
Примечание – Составлено по источнику Gartner (August 2018) [35]			

Согласно последнему прогнозу Gartner, в 2020 году мировые расходы на ИТ составят $3,9 трлн, что на 3,4% больше, чем в 2019 году. Ожидается, что в 2020 году глобальные расходы на ИТ достигнут около 4 трлн долл. США (таблица 2).

Таблица 2 – Мировой прогноз расходов на ИТ

(миллиарды долларов США)

Наименование	Расходы 2019	Рост (%) 2019	Расходы 2020	Рост (%) 2020	Расходы 2021	Рост (%) 2021
1	2	3	4	5	6	7
Системы ЦОД	205	-2.7	208	1.9	212	1.5
Корпоративное ПО	456	8.5	503	10.5	556	10.5
Устройства	682	-4.3	688	0.8	685	-0.3
ИТ-услуги	1,030	3.6	1,081	5.0	1,140	5.5

Продолжение таблицы 2

1	2	3	4	5	6	7
Услуги связи	1,364	-1.1	1,384	1.5	1,413	2.1
В целом ИТ	3,737	0.5	3,865	3.4	4,007	3.7
Примечание – Составлено по источнику Gartner (January 2020) [36]						

По предварительным подсчетам компании Juniper Research, проведенным в 2018 году, киберпреступники к 2023 году украдут около 33 миллиардов записей. Записи включают личную информацию о пользователях (имя, адрес, данные кредитной карты или номер социального страхования), которые интегрируются с различными организациями. Почти 60 миллионов американцев пострадали от кражи личных данных, согласно онлайн-опросу Harris Poll в 2018 году, также данный опрос показывает, что почти 15 миллионов потребителей столкнулись с кражей личных данных в 2017 году.

По прогнозам, в 2022 году мировые расходы на кибербезопасность достигнут $133,7 млрд. 100 000 групп, по меньшей мере, в 150 странах и более 400 000 компьютеров были заражены вирусом WannaCry в 2017 году на общую сумму около 4 миллиардов долларов [37]. Атака WannaCry нарушила критически важную и стратегическую инфраструктуру по всему миру, включая правительства, железные дороги, банки, поставщиков телекоммуникационных услуг, энергетические компании, автопроизводителей и больницы. Можно также отметить NotPetya, который нанес убытки в размере около 300 миллионов долларов в третьем квартале 2017 года [38, с.4].

Термин «кибербезопасность» был и остается одним из обсуждаемых предметов исследователей. В целях понимания и поддержки данного феномена в 2013 году в Оксфордский словарь было добавлено слово «Cybersecurity / Кибербезопасность» [39, с. 1-5]. Основываясь на обзоре литературы, было выявлено, что данный термин широко используется, и его определения различаются. Отсутствие краткого, широко приемлемого определения кибербезопасности запутывает, и порой может быть барьером технологическим и научным достижениям, укрепляя преимущественно технический взгляд на кибербезопасность. Крейген Д., Диакун-Тибо Н., и Персе Р., поддерживают данный подход [40, с. 13].

Кибербезопасность - это широко используемый термин, определения которого сильно различаются. Они порой субъективны и неинформативны. Отсутствие четкого и широко применяемого определения вводят людей в заблуждение. В целях конкретизации и четкого понимания для Казахстанских граждан был проведен обзор международных литератур, а также анализ действующих нормативно-правовых актов РК (таблица 3).

Таблица 3 – Международный и отечественный обзор термина «Кибербезопасность»

Автор / ресурс	Определение
1	2
Закон РК «Об информатизации»	«Информационная безопасность в сфере информатизации (информационная безопасность) – состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз» [41].
Концепция Киберщит Казахстана	«Кибербезопасность – это «состояние защищенности информации в электронной форме и среды ее обработки, хранения, передачи (электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры) от внешних и внутренних угроз, то есть информационная безопасность в сфере информатизации» [4].
Lexico Оксфордский словарь	«Кибербезопасность – это состояние защищенности от преступного или несанкционированного использования электронных данных или меры, принятые для достижения этой цели» [42].
Кембриджский словарь	«Кибербезопасность - это способы защиты компьютерных систем от таких угроз, как вирусы» [43].
Компания Cisco	«Кибербезопасность – это реализация мер по защите систем, сетей и программных приложений от цифровых атак» [44].
Национальный центр кибербезопасности Великобритании	«Кибербезопасность - это то, как отдельные лица и организации снижают риск кибератак» [45].
IT Gartner	«Кибербезопасность - это совокупность людей, политик, процессов и технологий, используемых предприятием для защиты своих киберактивов» [46].
Закон (акт) кибербезопасности Сингапурской Республики 2018	«Кибербезопасность - это состояние, в котором компьютер или компьютерная система защищена от несанкционированного доступа или атаки…» [47].

Продолжение таблицы 3

1	2
Мосчовитс С. Cybersecurity Program Development for Business: The Essential Planning Guide.	«Кибербезопасность - это постоянное применение передового опыта, предназначенного для обеспечения и сохранения конфиденциальности, целостности и доступности цифровой информации, а также безопасности людей и окружающей среды» [48, с 13].
Национальный институт стандартов и технологий	«Кибербезопасность - это процесс защиты информации путем предотвращения, обнаружения и реагирования на атаки» [49].
Примечание – Составлено автором источноку [4; 41–49]	

В целях четкого понимания граждан Казахстана о кибербезопасности предлагается использовать единое определение для всех нормативно правовых актов касательно термина «кибербезопасность». Во многих странах есть закон о кибербезопасности, который четко определяет понимание «кибербезопасность».

Ранее данный аспект в Республике исследовала Татаринова Л., которая предлагала внести на законодательной основе понятие «Кибербезопасность» [50, с. 60]. Она также отметила об отсутствии четкого определения термина «защита информации». Ранее отмечалось, что согласно закону «Об информатизации Республики Казахстан» предусмотрено определение «информационная безопасность в сфере информатизации / информационная безопасность» по смыслу родственное с понятием «кибербезопасность», определенное в Концепции кибербезопасности Республики Казахстан [4].

В соответствии с пунктом 5 статьи 4 Закона «О национальной безопасности Республики Казахстан» предусмотрено понятие «информационная безопасность», которое несет более широкое понимание, чем кибербезопасность.

Изучив и проанализировав выше представленные определения, взятые с НПА Республики Казахстан, а также международные источники, отработанные и утвержденные экспертами в области кибербезопасности, предлагается определить «кибербезопасность» согласно следующего содержания:

«Кибербезопасность - это комплекс организационно-правовых, экономических и технических процедур в целях защиты от несанкционированного использования информационных ресурсов в киберпространстве».

На основании изложенного предлагается внести соответствующие изменения в нормативно-правовые акты Республики, что в свою очередь даст единое понимание «цифровая безопасность», «информационная безопасность в сфере информатизации», а также «кибербезопасность». В результате предлагается внести соответствующее изменение в Закон «Об информатизации

Республики Казахстан» и в другие НПА согласно сравнительной таблицы в Приложении Г. Предполагается, что данное краткое определение будет нести целостное и единое понимание для термина «Информационная безопасность в сфере информатизации» и «Кибербезопасность», что в свою очередь даст возможность эффективного регулирования системы кибербезопасности. Ведь киберугроза всегда может быть внешней и внутренней, как через глобальную сеть Интернет, так и через локальную и индивидуальную сеть посредством накопительных устройств (USB-носители, флеш карты и диски). В этой связи нет необходимости усложнять определение, так как цифровые технологий уязвимы как в онлайн, так и не в сети Интернет. Нынешнее существующее определение на государственном языке очень сложно понять для простых граждан. Правительственные государственные учреждения разрабатывают НПА для всех граждан, а не для экспертов в области кибербезопасности. Определение должно быть кратким, четким и ясным, как это показывают определения развитых зарубежных стран.

Кибербезопасность - это междисциплинарная наука между ИТ и другими ведущими науками, начиная от безопасности до бизнеса, предпринимательства и права. Кибербезопасность определяет стратегический подход правительства и стран к любой возможной угрозе, будучи оборонительным по своему характеру, за счет использования технологий и программного обеспечения, - отмечает Эфтимиопулос М. [51, с. 2]. Таким образом, дисциплины, изучающие вопросы кибербезопасности должны действовать сообща для решения общих проблем. Например, существует ряд технических решений, поддерживающих кибербезопасность, но эти решения не разрешают экономические, политические, организационные и социальные вопросы, связанные с минимизацией кибератак во всех сферах жизнедеятельности граждан. В киберпространстве каждый день происходит немало нарушений, таких как кража интеллектуальной собственности, потери личных данных граждан и множество других киберпреступлений.

Кен Се - основатель, председатель правления и главный исполнительный директор Fortinet 13 января 2020 года отметил 4 основных аспекта, которые необходимо обеспечить:

- обмен информацией в режиме реального времени;
- сотрудничество в области кибербезопасности;
- создание и продвижение общего видения интегрированной кибербезопасности;
- продвижение технологической платформы [52].

На сегодняшний день, вопросом исследования по обеспечению кибербезопасности страны заинтересованы на национальном и международном уровне. К примеру, в своем исследовании важность кибербезопасности отмечают Россоу Вон С., Йохан Ван Н., [53, с. 97], Абучакра Р. и Хури М., [5], а также многие другие.

При внедрении политики кибербезопасности необходимо разработать гибкую систему управления, так как рынок цифровых технологий очень быстро

меняется. В своем исследовании Элин Вильборг, Карин Хедстрем и Ханну Ларссон [54, с. 2556] отмечают о гибкости системы при разработке услуг в области кибербезопасности. Они также выделяют важность вопроса нормативных документов, которые используются в сфере услуг электронного правительства.

В своем исследовании Бородакий Ю., Добродеев А. и Бутусов И. отмечают, что на международном уровне имеются определенные соглашения и принципы по применению оружия массового поражения в физических пространствах, тогда как межгосударственные взаимоотношения в киберпространстве остаются открытыми. Во многих странах за последние десятилетия интенсивно проводятся организационно-управленческие работы в области кибербезопасности. Открываются специализированные центры, организации и институты, которые непосредственно занимаются вопросами кибербезопасности в целях защиты государственных цифровых данных.

Международная практика показала актуальность и значимость обеспечения кибербезопасности в стране. В этой связи, на сегодняшний день существуют два научно-исследовательских института, которые непосредственно занимаются оценкой уровня обеспечения кибербезопасности в мире:

1. Глобальный индекс кибербезопасности (GCI) - это совместный проект ITU-ABI research, призванный оценить возможности государств в области кибербезопасности [55, с. 1]. GCI измеряет приверженность стран кибербезопасности на глобальном уровне для повышения осведомленности о важности проблем кибербезопасности [56].
2. Национальный рейтинг кибербезопасности (NCSI) - это глобальный индекс, который измеряет готовность стран предотвращать киберугрозы и управлять киберпреступлениями. NCSI также является базой данных с общедоступными доказательствами, материалами и инструментом для наращивания национального потенциала в области кибербезопасности. NCSI поддерживается и развивается Фондом Академии Электронного Управления [57].

Вышеперечисленные индексы имеют свои методы и индикаторы оценки, которые будут раскрыты в следующем разделе. Однако, хочется отметить, что данный рейтинг порождает конкуренцию между странами, всем известное явление, там, где конкуренция, там и качество.

Таким образом, обеспечение кибербозопасности в цифровом пространстве является актуальным не только в Казахстане, но и в других странах, так как есть риски возникновения кибервойн на международном уровне. Абучакра Р., Хури М. [5, с. 8] отметили важность и положительный эффект глобализации и технологизации. Однако, они предупреждают о возможных рисках и их негативных последствиях в части национальной безопасности. Согласно их мнению, повсеместное применение цифровизации привело к доступности информации, и граждане желают получить быстрые результаты в государственном управлении. Согласно их заключению «цифровая вселенная»

в период с 2013 по 2020 годы увеличится в десять раз, то есть с 4.4 трлн до 44 трлн гигабайт [5, с. 31]. Предполагается, чем больше цифровых данных, тем больше рисков утечки данных и кибератак со стороны.

Правительству Казахстана необходимо привлечь частный сектор в целях повышения эффективности обеспечения кибербезопасности [58]. В киберпространстве в 2014 году выявлено 1 241 случаев не устраненной уязвимости, в 2015 – 469, в 2016 – 355. Ежегодно фиксируются более 180 млн. кибератак различного типа [1].

Жумагалиев А., [59, с. 17] отмечает, что внедрение цифровизации влияет на рынок труда и требование к качеству образования. Вместе с тем, он отметил, что цифровизация повышает уровень возможных рисков кибератак, однако, вопросы по обеспечению кибербезопасности Республикой Казахстан предусмотрены, но, не смотря на его уверенность необходимо отметить, что Казахстану необходимо развивать нормативно-правовую базу в части кибербезопасности.

Более того, необходимо детально рассмотреть инфраструктуру цифровых технологий. Обеспечение кибербезопасности требует немало финансовых средств, которое включает в себя и инфраструктуру ИКТ. Темы, посвященные кибербезопасности в 2020 году, можно также найти в «Социальном вызове 1», который включает в себя здравоохранение, демографические изменения и благополучие - 4 млн. евро и в «Социальном вызове 7» безопасное общество - 68,8 млн. евро за цифровую безопасность; общий бюджет в 2020 году составил около 120 млн. евро [60, с. 19].

Казахстан должен быть готов к реагированию на любые возможные киберугрозы в целях успешной реализации цифровых услуг. Вопросы киберугроз охватывают технические, правовые, организационно-управленческие и политические вопросы национальной безопасности.

Необходимо отметить, что область кибербезопасности на стадии развития в Казахстане и в данной сфере отечественных экспертов немного. Однако, это проблема не только Казахстана. На сегодняшний день многие страны испытывают нехватку высококвалифицированных специалистов в области кибербезопасности [61, с. 173]. Исследование электронных навыков CISO с участием 40 работодателей показало, что 85% организаций испытывают проблемы с набором персонала из-за нехватки кандидатов, обладающих необходимыми навыками в области кибербезопасности [62, с. 5].

В этой связи, в первую очередь в Республике необходимо создать эффективную систему обеспечения кибербезопасности, состоящей из следующих элементов: законодательно-методическое, кадровое обеспечение и механизм функционирования этих систем.

В целях обеспечения кибербезопасности необходимо иметь не только материально-техническую, но и нормативно-правовую базу с высококвалифицированными специалистами в данной области. Многие исследователи отмечают, что обеспечение кибербезопасности требует немало

инвестиционных вложений, так как в любой стране необходимо обеспечить сохранность цифровых данных на международном и национальном уровне.

В следующем подразделе более детально будут раскрываться методы, модели, риск менеджмент и стратегии кибербезопасности. Вместе с тем, будет проведен сравнительный анализ между методами и индикаторами Глобального индекса кибербезопасности и Национального рейтинга кибербезопасности.

1.2 Механизм функционирования системы обеспечения кибербезопасности

Обеспечение кибербезопасности и повышение доверия населения в использовании ИКТ является одним из приоритетных направлений в государственной политике. Многими учеными доказано, что использование цифровых технологий повышает эффективность оказываемых государственных услуг [63, с. 23]. Однако, при масштабном внедрении ИТ, политика государства должна предусмотреть и предвидеть возможные риски в области кибербезопасности. Международный союз эклектросвязи - МСЭ (International telecommunication union - ITU) отмечает, что цифровизация и кибербезопасность рассмотрены как приоритетные направления в Буэнос-Айресе на Всемирной конференции по развитию электросвязи в 2017 году [64, с. 182].

Согласно Оксфордскому словарю под словом «механизм» понимается «метод или система для достижения чего-либо» [65]. В данном исследовании слово «механизм» мы определяем совокупность методы, системы, инструменты и способы управление кибербезопасности в Республике.

В условиях глобальной цифровизации предугадать самый надежный механизм обеспечения кибербезопасности практически невозможно из-за быстро меняющегося прогресса в области ИКТ. Многим странам приходится менять ИТ инфраструктуру, порой и политику в области цифровизации в целях обеспечения кибербезопасности в стране. Таким образом, механизм обеспечения кибербезопасности в государственном управлении должен быть гибким и адаптивным. На сегодняшний день, киберпространство не имеет границ и ограничений, то есть определить географические и юрисдикционные рамки практически невозможно. Тому ярким примером является кибервойна между Америкой и Ираном в 2010 году. По данному case study некоторые академики предполагают, что за этим стоит США и Израиль [66 с. 7; 67, с. 22]. Ярким примером является сетевой червь Stuxnet, который был запущен против ядерного проекта Ирана. В данном случае географические границы не были барьерами для запуска вредоносного Stuxnet [21; 68, с. 71], который вывел из строя около 1000 центрифуг ядерного завода. Вместе с тем, данный вирус заразил около 45 000 компьютеров [21, с. 83]. Позже кроме Stuxnet были выявлены другие вирусы, как Дуку и Флейм [21, с. 84; 71, с. 71], предназначенные для кражи информации. Исследователи отметили, что данные вирусы имеют длительный период реализации от 5 лет и выше [69, с. 122]. Другой яркий пример в рамках кибервойны можно отметить случай

повсеместного отключения электроэнергии в штатах Огайо, Нью-Йорк, Мичиган и некоторых регионах Канады. Вместе с тем можно отметить случай по взлому паролей электронных почтовых адресов Gmail чиновников США. Согласно данным некоторых ученных американцы в данных инцидентах обвиняют Китай [71, с. 70]. Таким образом, кибервойны подтолкнули политиков к разработке международных требований в целях защиты цифровых данных своих граждан. Одним из весомых международных регулирующих документов в области защиты персональных данных можно отметить документ принятый Европейским Союзом в 2018 году - GDPR.

GDPR - это законодательный акт, который предоставляет людям, живущим в Европе новые полномочия в отношении собираемых о них данных. Например, личные данные граждан Европы должны обрабатываться и использоваться только по их согласию [70]. При нарушении данных требовании или утечки информации о персональных данных граждан Европы организации привлекаются к ответственности. Согласно официальным данным Европейского Совета по Защите Данных (European Data protection board - EDPB), общая сумма штрафов, выписанных в рамках GDPR с момента принятия, составила - 55 955 871 евро, и почти 90% этой суммы приходится копанию Google (50 миллионов евро) выставленный французским Агентством по защите данных - CNIL [71, 72]. Данный пример показывает, что Интернет пользователи должны соблюдать кибергигиену, так как соблюдение базовых методов безопасности повышает возможность избежать ответственности на персональном, корпоративном, порой и на международном уровне. На персональном уровне из-за незнания человек может быть оштрафован и освобожден от должности, в то время как на корпоративном и международном уровне может быть оштрафован, освобожден и более того осужден за свои действия или бездействия.

В эпоху цифровых технологий многие аспекты жизни зависят от ИТ инфраструктуры, и такая зависимость является уязвимой к киберугрозам. Правительству целесообразно рассмотреть разработку план управления инфраструктурой ИКТ на национальном, региональном и международном уровнях. Как отмечает Валиахметова Г. [68, с. 69] экспоненциальное развитие ИКТ создает проблему безопасности на международном и национальном масштабе.

В настоящее время, согласно проведенному обзорному анализу, можно заметить, что на глобальном уровне вопрос кибербезопасности рассматривается более активно. Вместе с тем, несмотря на актуальность данного вопроса, необходимо систематически проводить работу среди населения в целях повышения не только компьютерной, но и киберграмотности. В глобальном мире ежедневно разрабатываются инновационные ИКТ решения. Более того, мы проживаем период активной разработки различных ПО и мобильных приложений, которые заставляют политиков менять и улучшать требования и стандарты к новым технологиям. Игнорирование внешних и внутренних

изменений в киберпространстве приводит к серьезным, а порой и катастрофическим последствиям для страны на национальном масштабе.

В этой связи, политикам необходимо пересматривать существующие НПА, а также программные и стратегические документы для обеспечения устойчивого развития кибербезопасности. Более того, странам необходимо развивать дипломатические взаимоотношения на постоянной основе и проводить мероприятия по их улучшению. Вместе с тем, разрабатывать ИКТ проекты в сотрудничестве с другими странами. Однако, необходимо отметить, что обеспечение кибербезопасности требует немало финансовых вложений. Согласно данным Большой 7 (G7) риски кибербезопасности для мировой финансовой системы имеют первостепенное значение. IBM X-Force Research выявило, что сектор финансовых услуг подвергся киберугрозе в большей степени, чем любая другая отрасль в 2016 году. При этом среднее финансовые учреждения отслеживаемое IBM Security Services испытало на 65% больше атак, чем средняя клиентская организация во всех отраслях [73, с. 1]. Таким образом, обеспечение кибербезопасности и защита критически важных информационных ИТ инфраструктур имеет один из важнейших значении для безопасности и экономического благополучия страны.

Согласно даным АО «ГТС» КНБ РК только за октябрь 2020г. В Казахстанском киберпространстве было заблокировано около 600 миллионов кибератак. Таким образом, сотрудниками АО «ГТС» КНБ РК были защещены инфраструктуры ИС государственных и квазигосударственных организации. Необходимо отметить, что фишинговая атака по сравнению с 2019 годом возросла на 91% [74].

Учитывая происходящие изменения, в киберпространстве на сегодняшний день функционируют специальные институты, где оценивают готовность и уровень развития кибербезопасности страны. К данным институтам относятся Глобальный Индекс Кибербезопасности (Global Cybersecuriy Index - GCI) и Национальный Индекс Кибербезопасности (Natinal Cyber Securiy Index - NCSI). Ниже в таблице 4 приведен сравнительный анализ в целях понимания методов оценки рейтингов GCI и NCSI.

Таблица 4 – Сравнительный анализ методов оценивания GCI и NCSI

Наименование	Глобальный индекс кибербезопасности [77]	Национальный индекс кибербезопасности [57]
1	2	3
Цель исследования	GCI измеряет приверженность стран кибербезопасности на глобальном уровне – для повышения осведомленности о важности и различных аспектах этой проблемы	NCSI измеряет готовность стран к предотвращению киберугроз и управлению киберинцидентами. Ресурсы базы данных могут использоваться для наращивания потенциала национальной кибербезопасности.

Продолжение таблицы 4

1	2	3
Основной метод	Онлайн-опрос* с анализом подтверждающих документов (сайты)	Сбор данных (факты, НПА, официальные документы и сайты)
Основные показатели/ параметры	- развитие потенциала; - правовые меры; - технические; - показатели; - организационные меры; - сотрудничество.	- действующее законодательство; - созданные подразделения (организации); - форматы сотрудничества.
Количество индикаторов	25 к ним сформулированы 157 вопросов	46 (3 категории и 12 характеристики)
* - если страна не отвечает на онлайн-опрос, то исследование проводится независимо Центром на основании открытых онлайн-ресурсов страны Примечание – Составлено автором по источнику [77, с. 27; 57]		

Изучив Глобальный и Национальный Индекс кибербезопасности можно отметить, что факторы (индикаторы) оценивания являются одним из ключевых институциональных направлений для разработки механизма обеспечения кибербезопасности для любой страны. Необходимо отметить, что на 05 марта 2020 года NCSI собирают данные (факты и материалы) самостоятельно по всем 152 странам [75]. Возникает вопрос, насколько достоверны собираемые им данные, так как есть вероятность риска, что они могут пропустить важную информацию, которая доступна только на местном (национальном) уровне. Однако, преимущества NCSI в том, что их рейтинг параллельно отражает показатель цифрового развития страны, где можно увидеть есть ли разрыв между цифровизацией и кибербезопасностью. Это дает возможность задуматься и провести соответствующие работы для достижения баланса между двумя показателями. Если в стране неразвита цифровые сервисы, соответственно, нечего защищать.

На основании изложенного, предполагается, что странам целесообразно участвовать в онлайн-опросах, приложив свои подтверждающие материалы, так как эти данные проверяются и оцениваются экспертами, которые формируют рейтинг GCI. Основные факторы, такие как: Правовые; Технические; Организационные; Наращивание потенциала и Сотрудничество рассмотреть возможность при разработке национальной стратегии кибербезопасности страны. Именно эти направления являются ключевыми показателями при оценке кибербезопасности страны. Результаты GCI и NCSI отражают уровень развития, и степень готовности государства к возможным киберугрозам. Предполагается, что страны, которые не имеют собственной стратегии кибербезопасности могут использовать показатели и индикаторы GCI и NCSI для разработки собственной стратегии. Вместе с тем, можно изучить стратегии кибербезопасности преуспевающих стран, которые успешно реализовали на

практике свои национальные стратегии кибербезопасности согласно показателям GCI и NCSI. Многие страны в национальной стратегии кибербезопасности указывают государственные органы, отвечающие за установление минимальных стандартов и реагирование на киберинциденты. Например, упоминание на банковскую безопасность уже можно найти в следующих стратегиях стран как: Австралия, Австрия, Бангладеш, Бруней-Даруссалам, Канада, Китай, Колумбия, Арабская Республика Египет, Франция, Гана, Ирландия, Италия, Япония, Иордания, Кения, Малайзия, Микронезия, Нигерия, Катар, Сингапур, Англия и Америка [78, с. 5]. Всемирный Банк отмечает, что национальные стратегии и другие правовые документы в области кибербезопасности должны четко определять соответствующие обязанности финансового сектора и национальной безопасности, без четкой ясности юрисдикционные конфликты неизбежно возникнут при издании новых правил кибербезопасности или что еще хуже, при обработке киберинцидентов в финансовом секторе [78, с. 5]. Когда речь заходит о стратегии кибербезопасности, страны и организации должны применять подход основанный на глубоком изучении международного опыта. Внедрение и применение многоуровневых механизмов безопасности для защиты ключевых данных организации. Например, случай со взломом системы SingHealth и кражи данных 1,5 млн. пациентов показало о необходимости сокращении разрыва между политикой и практикой применения и внедрения кибербезопасности в стране. Общественность была проинформирована о краже их данных спустя 10 дней после инцидента. [76, с. 1]. Однако, в таких киберинцидентах безотлагательное информирование общества является критический важным вопросом в целях минимизации возможных киберугрозах в финансовом секторе, так как хакеры могут использовать украденные данные граждан.

Анализ стратегии кибербезопасности успешных стран согласно GCI. Согласно показателям GCI 2017 года, только 38% стран официально опубликовали стратегию кибербезопасности, в то время как 12% стран на стадии разработки, 11% из них имеют специальную отдельную стратегию. Анализ глобального индекса кибербезопасности проведен среди 193 стран [77, с. 5]. Однако, Нармин Шафкат, Ашраф Масуд [78, с. 129] в своем исследовании отметили, что более 50 стран имеют сформулированную стратегию кибербезопасности.

Нами рассмотрены и анализированы ряд стратегий кибербезопасности стран, которые согласно GCI заняли лидирующую позицию 2017-2018 годы (рисунок 2). Это Сингапур, Соединенные Штаты Америки (США), Великобритания и другие страны [79, с. 59]. Основной задачей исследования является обзорный и сравнительный анализы действующих стратегий кибербезопасности. По результатам проведенного анализа предложены теоретические и практические рекомендации для стран, которые на сегодняшний день не имеют стратегии кибербезопасности.

Также предложенные рекомендации могут быть полезными странам, которые хотят улучшить инфраструктуру кибербезопасности. Нами определены основные критерии для проведения сравнительного анализа. Целью разработки стратегии кибербезопасности в странах в основном направлено на обеспечение сохранности и безопасности информационного потока в киберпространстве. Вместе с тем, стратегии кибербезопасности стран можно различать по истории развития, осведомленности граждан о кибербезопасности, понимании важности инфраструктуры, разработке нормативно-правовых документов. Таким образом, в целях проведения анализа определены следующие основные критерии:

- дата принятия документов;
- страна, принявшая стратегию;
- их цель и задача.

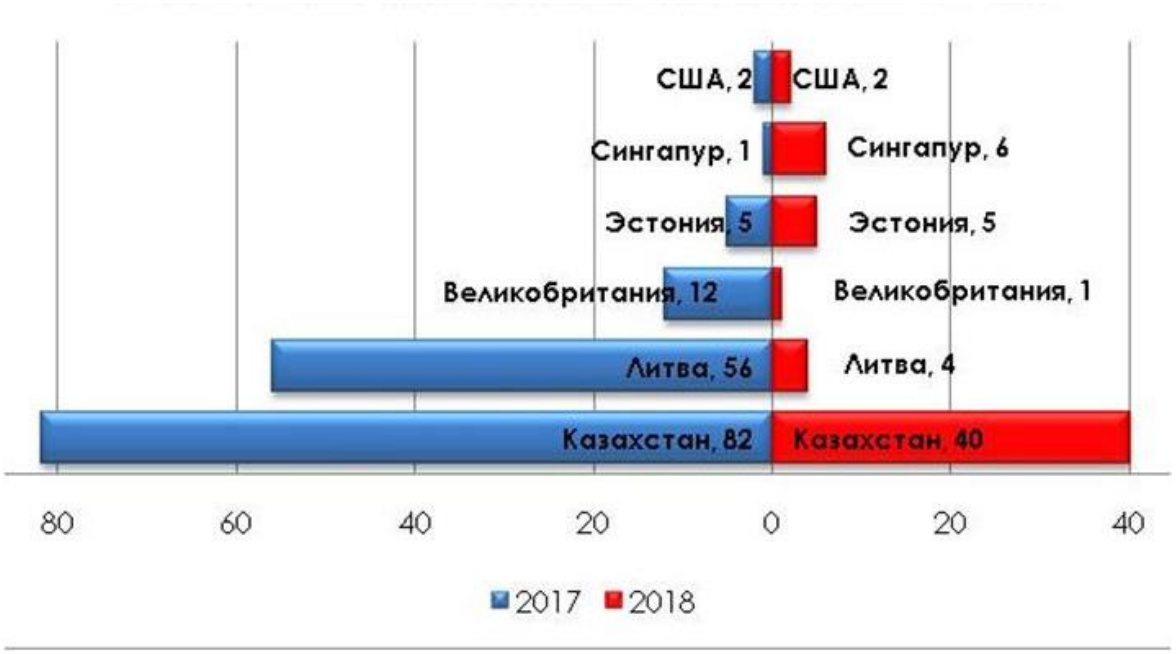

Рисунок 2 – Показатель успешных стран согласно Глобальному индексу кибербезопасности 2017-2018гг.

Примечание – Составлено автором по источнику [6; 77]

В своем исследовании Нармин Шафкат, Ашраф Масуд (2016) отмечают, что стратегия США носит наступательные и оборонительные планы действий. Ранее было отмечено, что выбор страны определен согласно показателям GCI за 2017-2018 годы. Эстония выбрана исходя из показателей, а также учитывая то, что страна в свое время входила в состав СССР, как и Казахстан. Несмотря на общее постсоветское прошлое за последние 2 года показатели Эстонии в области кибербезопасности превосходят показатель Казахстана. Эстония страна, которая в 2008 году разработала стратегию кибербезопасности. Эстонская ассоциация информационной безопасности (The Estonian Information Security Association - EISA) была официально основана в январе 2018 года.

EISA является частью стратегии следующего поколения - «Эстонской Стратегии кибербезопасности на 2019-2022 годы» [135, с. 48].

Стратегические цели кибербезопасности США в 2003 году заключались в предотвращении кибератак против критических инфраструктур; снижении национальной уязвимости к кибератакам, а также в минимизации вреда и времени для восстановления от происходящих кибератак [79, с. 8].

Стратегия кибербезопасности Великобритании 2011 года стала мотивом разработки программы кибербезопасности стоимостью 860 млн. фунтов, что существенно повлияло на уровень кибербезопасности страны в 2018 году [80, с. 9]. Вместе с тем, необходимо отметить, что на сайте Правительства Великобритании размещен перевод стратегии кибербезопасности на шести языках мира. Великобритания в 2018 году заняла первое место с самым высоким баллом в юридической и организационной составляющей. Страна имеет ряд правовых инструментов, позволяющих ей бороться с киберпреступностью, в том числе Закон о неправомерном использовании компьютеров [135, с. 30]. В целом США, также как и Великобритания, имеет ряд нормативно-правовых документов в целях обеспечения кибербезопасности в стране. Однако, лидирует в области кибербезопасности нормотворческая деятельность Сингапура. Сингапурский закон о кибербезопасности устанавливает правовые рамки для контроля и поддержки национальной кибербезопасности [120, с. 28]. Исходя из показателей, можно отметить, что огромное внимание на обеспечение безопасности в киберпространстве уделяют Великобритания, США, Литва, Сингапур и Эстония (таблица 5).

Таблица 5 – Принятые стратегии успешных стран согласно показателям GCI за 2017-2018гг.

Страна	Наименование стратегии	Дата принятия
1	2	3
США	Национальная Кибер Стратегия США принятая в 2018 году (Департамент Внутренней Безопасности) нацелена [81 с.3]: «(1) защищать Родину, сети, системы, функции и данные; (2) содействовать процветанию Америки путем создания защищенной, преуспевающей цифровой экономики и форсирования отечественных инноваций; (3) сохранению безопасности США совместно с партнерами — удерживать и при необходимости привлекать к ответственности тех, кто использует киберинструменты в незаконных целях; (4) расширить влияние США за рубежом для развития защищенного Интернета».	Сентябрь, 2018

Продолжение таблицы 5

1	2	3
Англия	Национальная стратегия кибербезопасности 2016-2021, которая предусматривает следующие цели [80]: – борьба с киберпреступностью; – осведомленность граждан; – защита критически важной информационной инфраструктуры; – участвовать в международном сотрудничестве; – установить государственно-частное партнерство; – обеспечить возможность реагирования на инциденты; – создать институционализированную форму сотрудничества между государственными органами; – установить базовые требования безопасности; – создать механизмы сообщения об инцидентах; – фостер НИОКР; – организация учений по кибербезопасности; – улучшить учебные и образовательные программы. В течение пятилетней стратегии инвестируется 1,9 миллиарда фунтов стерлингов в защиту систем и инфраструктуры Великобритании.	Ноябрь, 2016
Литва	Национальная стратегия кибербезопасности Литвы (Министерство национальной обороны Литовской Республики) [82 с.4] Первая цель стратегии – укрепление кибербезопасности страны и развитие потенциала киберзащиты. Вторая цель стратегии – обеспечение предупреждения и расследования уголовных преступлений в киберпространстве. Третья цель стратегии - продвижение культуры кибербезопасности и развитие инноваций. Четвертая цель стратегии - укрепление тесного сотрудничества между частным и государственным секторами. Пятая цель стратегии – укрепление международного сотрудничества и обеспечение выполнения международных обязательств в области кибербезопасности.	Август, 2018

Продолжение таблицы 5

1	2	3
Эстония	Стратегия кибербезопасности Эстонии 2019-2022. Стратегия Эстонии имеет идентичные цели, как у Великобритании и Литвы [83]. Основные задачи стратегии [84]: −устойчивое цифровое общество; −индустрия кибербезопасности, исследование и развитие; −ведущий международный вклад; −киберграмотное общество.	Сентябрь, 2014
Сингапур	Стратегия кибербезопасности Сингапура. Стратегия кибербезопасности Сингапура направлена на создание надежной киберсреды в целях обеспечения лучшего будущего своего народа. Министерство связи и информации (MCI) и Агентство кибербезопасности (CSA) работают с государственными и частными организациями над созданием устойчивой инфраструктуры, развитием динамичной киберэкосистемы и укреплением международных партнерств [85, с. 4].	10/10/2016
Примечание – Составлено автором по источнику [80-85]		

Азми Р., Тиббен В., Вин К., в своей работе отметили, что страны принимают Национальную стратегию кибербезопасности в целях снижения киберугроз, защиты государственной тайны, повышения национальной устойчивости и экономической безопасности. Вместе с тем они отмечают о необходимости создания надежной правовой основы для работы в киберпространстве. По их мнению, правоохранительные органы должны устранять действия, наносящие ущерб интересам страны, посредством использования международных судов. Они в своем исследовании также отмечают важность политического аспекта, который направлена на укрепление дипломатии и продвижения имиджа страны на международной арене. [86].

На основании изложенного, нами предлагается начать работу в правовой деятельности кибербезопасности, разработать собственную стратегию, где четко будут определены стратегические цели и задачи на краткосрочный, среднесрочный и долгосрочный перспективы. На основании изученного опыта успешных стран нами определенные основные заинтересованные стороны, и предлагается рассмотреть следующие основные аспекты при разработке национальной стратегии кибербезопасности Казахстана (рисунок 3):

- борьба с киберпреступностью;
- баланс безопасности с конфиденциальностью;

Рисунок 3 – Основные аспекты и заинтересованные стороны Национальной стратегии кибербезопасности Казахстана.

Примечание – Составлено автором по источнику [82 с.3-5; 83 с.4-10; 86 с.4-7]

– осведомленность граждан;
– защита критически важной информационной инфраструктуры;
– оценка риска;
– участвовать в международном сотрудничестве;
– установить базовые требования кибербезопасности;
– установить институционализированную форму сотрудничества между государственными органами;
– совершенствовать стандарты информационной безопасности;
– совершенствовать учебные и образовательные программы;
– фостер НИОКР.

Вместе с тем, согласно анализу индекса глобальной кибербезопасности на 2018 год, Казахстану необходимо развивать и работать в сотрудничестве с другими странами [135, с. 29]. Можно отметить, что на правительственном уровне вопрос кибербезопасности, как на более высоком, начал рассматриваться с момента принятия Концепции кибербезопасности Казахстана в 2017 году, но данная концепция до 2022 года [4]. В этой связи до 2022 года необходимо разработать свою Национальную стратегию Кибербезопасности. Более того, большинство развитых стран на сегодня имеют нормативно-правовую базу в области кибербезопасности, где четко определены понятие «кибербезопасность», методы и механизмы управления, а также ответственность за использование цифровых ресурсов противозаконным и несанкционированным методом. Например, в Китае в 2017 году в рамках

обеспечения цифровой безопасности в силу вступил закон о кибербезопасности [87, с. 57; 88, с. 67]. Однако, на данном этапе существует определенные недоработки. Так, Ян Ф., Сюй Дж. [89, с. 533] в своем исследовании отражают проблемные аспекты в части конфиденциальности персональных данных граждан в реализации проекта «Умный город». Согласно их мнению, закон о кибербезопасности не рассматривает защиты больших данных, собираемых ИТ инфраструктурой умного города. Закон о кибербезопасности также принят в странах, которые имеют успешный опыт. К ним можно отнести опыт США принятый Закон об обмене информацией в области кибербезопасности в 2014 году [90], и Закон кибербезопасности Сингапура подписанный в 2018 году [49]. Закон устанавливает правовые рамки для надзора и поддержания национальной кибербезопасности в Сингапуре [91].

В связи с быстро меняющимися тенденциями в цифровизации в глобальном мире нам предстоит разработать аналогичный закон в ближайшем будущем. Это требование быстро меняющего мира и Казахстан не может игнорировать изменения в период глобализации и условиях цифровой трансформации. Более того, необходимо отметить, что с момента принятия закона «Об информатизации» (2015г.) были внесены изменения и дополнения более 15 раз, в закон «О национальной безопасности РК» (2012г.) более 30, и в закон «О персональных данных и их защите» (2013г) боле 5 раз. Исходя из этого, можно прийти к выводу, что большинство государственных служащих заняты только внесением изменений и дополнений в НПА Республики. Казахстан в целях совершенствования обеспечении кибербезопасности может рассмотреть опыт Сингапура, который внедрил единую Правительственную сеть, чтобы выявить возможные угрозы в киберпространстве. Данный механизм помог им разработать стратегию и законодательную базу по предотвращению рисков кибератак [3, с. 91]. Таким образом, основываясь на опыте Сингапура по разработке законопроекта в области кибербезопасности Казахстану необходимо разработать свою национальную стратегию Кибербезопасности. Таким образом, в законопроекте кибербезопасности Казахстана предлагаем охватить следующие основные 4 направления:

1. Усилить защиту критически важные информационные инфраструктуры от кибератак. Критически важная информационная инфраструктура (КВИИ) - это компьютерные системы, непосредственно участвующие в предоставлении основных услуг. Кибератаки на КВИИ могут оказать разрушительное воздействие на экономику и общество. Закон должен обеспечивать основу для назначения КВИИ и предоставляет владельцам КВИИ ясность в отношении их обязательств по защите КВИИ от кибератак. Это создаст устойчивость в КВИИ, защищая экономику Казахстана. Секторами КВИИ являются: энергетика, водоснабжение, банковское дело, финансы, здравоохранение, образования, транспортные инфраструктуры (включая наземные, морские и авиационные), инфокоммуникационные, СМИ (медиа), службы безопасности и экстренные службы, а также правительство.

2. *Готовность предотвращения и реагирования на угрозы и инциденты кибербезопасности.* В соответствии с законом уполномоченный орган по кибербезопасности расследует угрозы и инциденты в области кибербезопасности, определяет их воздействие и предотвращает возникновение дальнейших инцидентов связанных с кибербезопасностью. Таким образом, правительство гарантирует гражданам Казахстана, что они могут эффективно реагировать на киберугрозы и обеспечивать безопасность Казахстана и их граждан.

3. *Создать основу для обмена информацией о киберинцидентах.* Закон также будет облегчать обмен информацией, что крайне важно, поскольку своевременная информация помогает правительству и владельцам ИКТ систем выявлять уязвимости и более эффективно предотвращать киберинциденты. Закон будет обеспечивать основу для уполномоченного органа по кибербезопасности для запроса информации, а также для защиты и обмена такой информацией.

4. *Создать клиентоориентированную систему лицензирования для поставщиков услуг кибербезопасности в целях мотивации и поддержки отечественного бизнеса.* А также внедрить легкий подход к лицензированию поставщиков услуг в области тестирования на проникновение и мониторинг центра управляемых операций безопасности. Полагается, что эти две направления имеют приоритет, поскольку поставщики таких услуг имеют доступ к конфиденциальной информации от своих клиентов.

Таким образом, создание надежной и эффективной правовой базы в области кибербезопасности является одним из нелегких задач. Разработка национальной стратегии кибербезопасности и правовой основы, повышения уровня и требования в системе образования. А также приведения работ в рамках построения партнерских отношении ближними и дальними за рубежными странами в области кибербезопасности является основополагающим управленческим направлением для правительства в целях совершенствования обеспечения кибербезопасности в стране. Как отмечает всемирный банк, правительство несет ответственность за реализацию политики кибербезопасности [92, с. 25].

Вместе с тем, ключевым компонентом Национальной политики кибербезопасности является развитие ГЧП для улучшения системы кибербезопасности. Ю и Цюй отмечает, что ГЧП особенно хорошо подходят для областей, где требуются различные виды опыта и знаний для решения сложных проблем, включая кибербезопасность [93, с. 2-3] Например, в Индии кибербезопасность не так развита из-за слабо развитых процедур взаимодействия между государственным и частным сектором. В этой связи правительство Индии предоставил финансовую помощь индийским фирмам для приобретения иностранных фирм с передовыми технологиями кибербезопасности, так как правительственные учреждения Индии подвергались кибератакам со стороны иностранных правительств, и это послужило для принятия такого характера решении. При этом Индийская

компания владеющая технологиями полученные благодаря правительственной помощью должны предоставить государственным органам доступ к правам интеллектуальной собственности данной компании [98, с. 10].

М. Карр подчеркивает рыночного подхода к сотрудничеству в сфере ГЧП в области кибербезопасности, которая является частью национальной безопасности. Например, в Соединенных Штатах и Соединенном Королевстве государственно-частное партнерство выступает как «центр» стратегии кибербезопасности, поскольку большая часть критической инфраструктуры в США и Великобритании находится в частной собственности [94, с. 43-45]. Их опыт и цифровая глобализация показывает, что с каждым днем все больше критический важные информации переходят в частные руки, так как государство в целях предоставления качественных услуг прибегают к услугам аутсорсинга.

Вопросы кражи личных данных в Интернете, промышленной кибершпионажа, защиты критической инфраструктуры и ботнеты могут быть сферами совместной деятельности государства и частных лиц. Использование ГЧП может включать проекты кибербезопасности связанные с использованием ИКТ в сферах госуправления, местного самоуправления, учитывая определение зон безопасности [95, с. 4].

Например, Министерство внутренней безопасности США (DHS) создало автоматизированную программу киберугроз для облегчения быстрого и своевременного обмена информацией об угрозах между государственным и частным секторами. DHS представило автоматизированный обмен показателями (AIS) для автоматического обмена метриками между государственным и частным сектором [96, с. 25]. Более того, в своем исследование Mckinsey выделяет модель «*Множественного источника информации об угрозах».* То есть создание правительством дополнительных каналов для отслеживания угроз. К примеру, в 2013 году Великобритания запустила Партнерство по обмену информацией в области кибербезопасности, которое представляет собой платформу, на которой правительство и частный сектор могут быстро и конфиденциально обмениваться данными об угрозах [1]. Аналогичную платформу необходимо разработать в Казахстане в целях оперативного информирования участников государственного и частного сектора включая пользователей цифровых услуг.

В процессе управления процедурами киберзащиты необходимо исследовать угрозы и их эволюцию, искать уязвимости, определять перенос и включение целей и приоритетов; на аутсорсинг; предотвращать и поддерживать, реагировать на атаки; для проверки эффективности действий. Учитывая сложность вопроса, реализация кибербезопасности за счет использования ГЧП предусматривает привлечение хозяйствующих субъектов использующих критически важные элементы инфраструктуры. Существующие методы государственного регулирования сектора безопасности стремительно теряют актуальность, учитывая их низкую эффективность. Современный

подход к решениям в области кибербезопасности, основанный на моделях государственно-частного партнерства - это новая форма управления.

Например, Агентство Европейского Союза по кибербезопасности (ENISA) предлагает рекомендации для эффективной работы ГЧП в области кибербезопасности [97, с. 36-37]:

1. Мотивация частного сектора в кибербезопасности. Для создания успешного и эффективного ГЧП необходимы ресурсы. Инвестирование их недостаточно, нужны люди, которые будут взаимодействовать с каждым членом партнерства, организовать встречи и сохранять стратегическую перспективу. В ГЧП нужны люди, которые готовят планы действий и тесно сотрудничают как с государственным, так и частным управлением.

2. Участники единогласно должны определить правовую базу при создании платформы на базе ГЧП, так как отсутствие правовой основы является сдерживающим фактором развития совместной деятельности ГЧП с заинтересованными участниками работ. Правовой основой может быть национальный правовой акт о взаимопонимании, так как каждый член должен знать, какой вклад они должны внести и какие выгоды они могут ожидать от деятельности платформы.

3. Государственным учреждениям предлагается рассмотреть и разработать национальный план действий по обеспечению кибербезопасности. Правительство четко и честно информировать частный сектор о своих потребностях, целях и ограничениях. Таким образом, государственные структуры должны выработать стратегию с четкими целями и задачами перед тем, как приглашать частный сектор к сотрудничеству.

4. Участники ГЧП должны быть открыты и прагматичны. Если члены ГЧП не открыты и честны, то они могут стать жертвами своих ожиданий, которые не смогут удовлетворить ни частный и государственный сектор.

5. Представителям правительства должно быть разрешено участие во встречах. Государственные служащие должны не только участвовать во встречах, но и делиться своими знаниями и опытом, открыто участвовать в обсуждениях и мероприятиях.

6. Малые и средние предприятия также должны быть вовлечены по вопросам кибербезопасности и тесно участвовать в деятельности ГЧП.

Международный опыт показывает, что механизмы ГЧП дают надежду на успех стратегий сотрудничества государственного и частного секторов в области кибербезопасности. При разработке стратегии кибербезопасности необходимо предусмотреть внедрение механизмов ГЧП, как один из приоритетных направлении в развитии кибербезопасности страны.

Многие киберинциденты происходят из-за незнания, неосведомленности граждан, то есть человеческий фактор, и низкий уровень киберграмотности несет за собой негативные последствия. Более 90% проблем кибербезопасности возникают из-за человеческой ошибки, утверждает Алекс А., [98]. Более тревожно, что могут потребоваться годы, чтобы обнаружить внутренние угрозы, то есть ошибки своих сотрудников, потому что их нелегко обнаружить,

и многие из них происходят из-за отсутствия киберграмотности. Киберинциденты неизбежны в период глобализации, так как ежегодно растет количество Интернет пользователей [99].

В целях повышения кибербезопасности в стране необходимо систематически проводить работы по повышению квалификации специалистов в области кибербезопасности. Организовать курсы по подготовке и переподготовке кадров в области кибербезопасности действующих специалистов организации, деятельность которых непосредственно связанны с цифровыми технологиями и большими данными. На сегодня для действующих государственных служащих в Академии государственного управления при Президенте Республики Казахстан успешно проводятся 4 и 6 часовые курсы по основам кибербезопасности.

В этой связи, часто правительство при внедрении новых технологий параллельно проводит образовательные курсы по использованию электронных государственных услуг. Но данные курсы рассматривают обучение только по применению внедренных государственных услуг, и вопрос как обезопасить себя в киберпространстве от возможных киберугроз остается открытым. На сегодня многие страны начали проводить краткосрочные онлайн и офлайн курсы в целях повышения киберграмотности населения. Самое важное, что эти курсы можно пройти бесплатно. К примеру, на сайте Cisco Networking Academy (https://www.netacad.com/ru/courses/security/cybersecurity-essentials) на безвозмездной основе можно пройти курс «Основы кибербезопасности». Аналогичный образовательный ресурс необходимо разработать для Казахстанцев на государственном и русском языках доступным для всех на безвозмездной основе, как это практикуется в Европе и Великобритании.

На основании изложенного, считаем целесообразным выстроить работающую законодательную систему в области кибербезопасности, то есть, правительству Казахстана изучив опыт успешных зарубежных стран, таких как Сингапур, США, Великобритания, Китай, а также учитывая требования GDPR Европейского Союза необходимо рассмотреть вопрос разработки закона кибербезопасности страны. Нормативная база кибербезопасности страны соответствующие отечественным и международным стандартам, требованиям и соглашениям является один из основополагающих механизмов государственного управления в обеспечении кибербезопасности Казахстана в условиях глобальной цифровизации. Предполагается, что реализация эффективной политики государственного управления в обеспечении кибербезопасности даст мультипликативный эффект во все отраслях цифровой экономики Казахстана.

Таким образом, разработка нормативно-правовых документов является одним из ключевых аспектов при проведении политики обеспечения кибербезопасности в стране. Вместе с тем, считаем целесообразным выстроить эффективное взаимоотношение с частным сектором в рамках оперативного выявления и блокировании кибератак. Механизм взаимоотношения можно улучшить путем разработки специальной платформы безопасного обмена

информации. Разработать данной платформу совместно с ГЧП, как это успешно используется в странах США и Великобритании. Детальный механизм функционирования можно рассмотреть в стратегии кибербезопасности Казахстана, которую также необходимо разработать в ближайшем будущем. Разработанная в 2017 году Концепция Кибербезопасности Казахстана на сегодняшний день теряет свою актуальность из-за быстроменяющегося цифровых технологий на глобальном рынке.

В следующем подразделе рассмотрим опыт успешных стран согласно показателям GCI. По результатам проведенного анализа будут предложены практические рекомендации в целях совершенствования обеспечения кибербезопасности в Казахстане.

1.3 Международный опыт в области обеспечения кибербезопасности

В рамках исследования рассматривался опыт ряда успешных стран согласно международному рейтингу в сфере кибербезопасности и цифровизации. Согласно GCI Великобритания, США, Сингапур, Эстония и Литва, являются лидирующими странами в области кибербезопасности.

На национальном уровне кибербезопасность является общей ответственностью, которая требует скоординированных действий по предотвращению, подготовке, реагированию и восстановлению после киберинцидентов. Для обеспечения бесперебойной работы и обеспечения безопасной, надежной и отказоустойчивой цифровой сферы необходима всеобъемлющая стратегия, которая должна разрабатываться и внедряться с участием заинтересованных сторон. Эта стратегия часто упоминается как Национальная стратегия кибербезопасности (NCS) - и является критическим важным документом для социально-экономической безопасности любой страны [100].

Опыт Великобритании. Правительство Великобритании ежегодно проводит обзор нарушений кибербезопасности. Цифровая экономика становится все более важной частью экономики Великобритании. Цифровая стратегия Великобритании 2015 года гласила, что экономика Великобритании стимулируется примерно на 145 миллиардов фунтов стерлингов в год благодаря цифровым технологиям. Компания Fujitsu заявляет, что Великобритания обладает самой большой интернет - экономикой среди G20.

В «Обзоре стратегической обороны и безопасности Великобритании» уточняются некоторые другие угрозы, их характер и возможные контрмеры. Этот документ тесно связан с вышеупомянутой стратегией безопасности. За 4 года было выделено 650 миллионов фунтов стерлингов на создание новой национальной программы кибербезопасности. Стратегия кибербезопасности Великобритании: защита и продвижение Великобритании в цифровом мире, первоначально запланированная на весну 2011 года, была опубликована осенью 2011 года и содержит описание необходимых мер [101, с.1461-1462]. Ключевой частью гибридной войны является информационная война, где пропаганда

наряду с дезинформационными действиями создает хаос в обществе, а кибератаки играют решающую роль [102, с. 58].

TechUK подчеркнул, цифровая экономика растет, увеличивается риск киберпреступности, и задача сделать Великобританию безопасным местом для ведения бизнеса становится все более важной задачей. По оценкам TechUK, киберпреступность обходится экономике Великобритании в 34 млрд. фунтов стерлингов в год, увеличившись с 27 млрд фунтов стерлингов в 2010 году [103, с. 16]. Согласно проведенному опросу в Великобритании за 12 месяцев более четырех из десяти предприятий (43%) и две из десяти благотворительных организаций (19%) сталкивались с нарушениями или кибератаками. Этот показатель возрастает до семи из десяти (72%) среди крупных предприятий и аналогичной доли (73%) среди крупнейших благотворительных организаций с доходом в 5 миллионов фунтов стерлингов и больше. Кибератаки чаще выявлялись в организациях, в которых хранятся персональные данные граждан [104].

Вместе с тем, Институт для государства – 2016 в своем исследовании обозначил, что Правительственная цифровая служба Великобритании (The Government Digital Service - GDS) должна устанавливать и обеспечивать выполнение центральных стандартов для взаимодействия с пользователем государственных услуг. Институт для государства – 2016 обращает внимание на растущий риск кибератак, тем самым, подчеркивает о соблюдении стандартов безопасности, и это является приоритетной задачей для государства [105, с. 5]. Чем больше государственных услуг оказывается в цифровом формате, тем больше правительство обменивается количеством цифровых данных. Происходящие изменения повышают риск несанкционированного доступа.

В 2015 году в Великобритании произошло 200 инцидентов, связанных с кибербезопасностью, на 100 раз больше, чем в 2014 году [11, с. 30]. После таких инцидентов в Управлении её Величества (Her Majesty's Revenue and Customs - HMRC) по налогам и таможенным пошлинам есть должность «директора по кибербезопасности и информационным рискам». С 30 ноября 2015 года по 5 февраля 2016 года был проведен репрезентативный телефонный опрос среди 1 008 британских предприятий, а также 30 углубленных интервью в январе и феврале 2016 года [106, с. 3]. Согласно обзору нужно отметить, что кибербезопасность - это проблема, которая затрагивает практически все предприятия в Великобритании. В результате проведенного опроса малые предприятия узнали о государственной поддержке в области кибербезопасности, такой как руководство для малого бизнеса, бесплатное онлайн-обучение [109, с. 5].

Необходимо отметить, что правительство Великобритании на официальном сайте в помощь бизнесу опубликовало руководство для малого бизнеса [107], а также бесплатные онлайн курсы [108] для защиты бизнес сектора от киберугроз и онлайн-мошенничества [115]. Бесплатные онлайн курсы на выбор и некоторые из них длятся не больше 30 минут. Таким образом,

рынок Великобритании совершенно бесплатно может узнать, как избежать кибератаки на рабочем месте. Бесплатно представлены онлайн курсы для специалистов по закупкам. Исследовательский институт спроса и предложения (Chartered Institute of Procurement & Supply) помог разработать данный бесплатный онлайн-курс, который показывает, как сотрудники и организации могут противостоять киберугрозам. В своем исследовании Исабаева С. Есениязова Б. отмечают, что в Казахстане необходимо больше внимание уделить по вопросам обеспечения кибербезопасности в государственных закупках [109, с. 74]

Вместе с тем, на сайте Великобритании доступно упражнение в коробке - это новый онлайн-инструмент от Национального центра кибербезопасности Великобритании, который помогает организациям проверить и отработать свои ответы на кибератаки. Дополнительно на официальном сайте Национального центра кибербезопасности можно ознакомиться с руководством, где организации могут защитить себя в киберпространстве. Изначально документ был опубликован в 2012 году [110]. Руководство содержит ряд технических советов, таких как:

- режим управления рисками;
- дом и мобильная работа (работа в удаленной сети);
- управление происшествиями;
- предотвращение вредоносных программ;
- управление пользовательскими привилегиями;
- сетевая безопасность;
- съемные средства управления мультимедиа;
- обучение пользователей и осведомленность.

Вместе с тем, Национальным центром кибербезопасности разработана веб страница «Cyber Essentials – Кибер основы», данный проект также поддерживается правительством. Этот ресурс помогает организациям защитить себя от распространенных онлайн-угроз [111]. Данный сайт содержит несколько секций, разработанных для: индивидуумов и семьи [112]; самозанятых и индивидуальных предпринимателей [113]; малых и средних организации, где количество сотрудников до 250 человек [114]; крупных организации (более чем 250 сотрудников) [115]; государственных секторов [116]. Сайт кибер основы также содержит руководство для экспертов в области кибербезопасности [117].

Более того, необходимо отметить, что на сайте офиса комиссара по информации (Information commissioner's office) размещено руководство, которое охватывает закон о защите данных 2018 (Data Protection Act 2018) и общие правила защиты данных (General Data Protection Regulation) [118].

Рассмотрим обзор нарушений кибербезопасности Великобритании за 2019 год. Согласно данному обзору около трети (32%) предприятий и две из десяти благотворительных организаций (22%) сообщают о нарушениях или атаках кибербезопасности за последние 12 месяцев, это значительно выше, особенно среди среднего бизнеса (60%), крупного бизнеса (61%) и благотворительных

организаций с высоким доходом (52%). Результаты также свидетельствуют о том, что там, где предприятия потеряли данные или активы в результате нарушений кибербезопасности, финансовые расходы от таких инцидентов постоянно увеличивались с 2017 года. Среди благотворительных организаций, регистрирующих нарушения или нападения, это происходило в 21% случаев. В компаниях, которые имели подобные отрицательные результаты, средняя (средняя) стоимость бизнеса составляла 4 180 фунтов стерлингов в 2019 году. Это выше, чем в 2018 году (3 160 фунтов стерлингов) и 2017 году (2 450 фунтов стерлингов). В 2019 году больше предприятий и благотворительных организаций предприняли соответствующие меры для улучшения кибербезопасности, эти меры частично связаны с введением правил GDPR [119, с. 2-3].

По мнению из-за более дорогостоящих наносящих ущерб репутации хакерских атак компании и правительства все больше заботятся о кибербезопасности. Это привело к росту сектора кибербезопасности в Великобритании, который оценивается в более чем 6 млрд. фунтов стерлингов и в котором занято около 40 000 человек [120, с. 5].

Вместе с тем, в 2011 году правительство Великобритании приняла национальную стратегию кибербезопасности (Правительство Великобритании, 2011) [121, с. 27]. Таким образом, неотъемлемым компонентом любой национальной стратегии кибербезопасности является принятие соответствующего законодательства против неправомерного использования ИКТ в преступных целях, которое согласуется с региональной и международной политикой и практикой.

Опыт США. Результаты исследования Рай С., Варма А. К. [122, с. 1] показали, что США имеет больше всего публикаций в области исследований кибербезопасности, за которыми следуют Великобритания, Китай и Индия.

Правительство США на 2019 финансовый год выделил 15 миллиардов долларов на деятельность, связанную с кибербезопасностью. Это на 4 % больше, чем в 2018 году. Наибольшее финансирование получает Министерство обороны, бюджет которого составляет почти 8,5 миллиарда долларов, затем национальная безопасность - примерно 1,7 миллиарда долларов США [123].

Национальная стратегия кибербезопасности США с 2018 года направлена на сохранение лидерства, усиление влияния и продвижение США, интересы на международной арене. Безопасность киберпространства является частью их национальной безопасности. Развитие и устойчивость цифровой экономики рассматривается как основа американского процветания:

- развитие инноваций и инвестирование в ИТ инфраструктуру с привлечением частного сектора и гражданского общества;

- развитие международного сотрудничества, а также создание кадрового резерва, повышение потенциала специалистов в области киберзащиты. Соединенные Штаты были одним из первых, кто осознал стратегическую важность безопасности в киберпространстве. Развитие информационной сферы, ее возрастающая роль в жизни общества, государства и связанный с этим

ростом угроз во все более зависимой экономике от ИКТ и террористических актов 2001 года привели к принятию Национальной Стратегии безопасного киберпространства 2003 года. [124, с. 119].

Обновленная стратегия кибербезопасности - 2018 направлена на поддержание лидерства, использование и продвижение интересов США на международной арене. Защита онлайн-пространства в Соединенных Штатах основана на принципах свободы интернета. В этом аспекте разработка и внедрение многосторонней модели управления интернетом является приоритетной задачей. США для себя определил следующие приоритетные направления: развитие инноваций и инвестиций в ИТ инфраструктуру с привлечением частного сектора и гражданского общества; развитие международного сотрудничества; создание кадрового резерва; развитие, повышение потенциала специалистов в области кибербезопасности. Важным моментом также является то, что именно высококвалифицированный персонал в области кибербезопасности признается США в качестве стратегического актива для национальной безопасности, поэтому поиск молодых талантов и специалистов осуществляется правительством во всем мире посредством различных специальных правительственных программ [121, с. 123].

Американские военные создали ПО «Cyber Command» для защиты внутренней интернет - инфраструктуры и организации военных операций в киберпространстве [121, с. 3]. Вместе с тем, исследователи из университетов Торонто и Кембриджа обнаружили изощренное шпионское кольцо, нацеленное на тибетское правительство в изгнании (монитор информационной войны, Нагараджа и Андерсон 2009). Сотрудникам посольств по всему миру были отправлены электронные письма, якобы имевшие отношение к тибетцам. Когда сотрудники открыли вложение электронной почты, их компьютеры были заражены вредоносным ПО, которое украло документы и сообщения. Согласно свидетельству, представленному перед Конгрессом США 20 марта 2009 года, главный специалист по безопасности AT&T Эдвард Аморосо подсчитал, что годовая прибыль киберпреступников превышает 1 триллион долларов [121, с. 5-8].

Из опыта США для Казахстана очень примечателен, то, что они разработали официальный вебсайт Savvy Cyber Kids (https://savvycyberkids.org/) для детей, где они могут повысить свои знания по компьютерной грамотности. Данный проект функционирует с 2007 года и помогает родителям и учителям обучать детей кибербезопасности, кибер-этике и другим аспектам их повседневной технической жизни. Savvy Cyber Kids предлагает платформу бесплатных образовательных ресурсов в двух направлениях: для семьи и педагогов.

Вместе с тем, необходимо отметить, что правительство Великобритания и США при разрешении киберугроз применяют стандарты риск менеджмента. Более того, эти государство тесно взаимодействуют с честным сектором в рамках оперативного обмена информации о возможных киберугрозах. В целях успешной взаимовыгодной связи между государственным и частным секторам

Великобритания и США привлекли ГЧП. Разрешения и реализации проектов в области кибербезопасности без привлечения частного сектора в настоящее время практически не возможно [125, с. 38]. В результате США и Великобритания в части взаимодействия с частным сектором при решении вопросов обеспечения кибербезопасности привлекли ГЧП. Полагается, что данный опыт для Казахстана также будет полезным.

Опыт Эстонии. Эстония небольшое государство, которое имеет очень зрелое законодательство и подход к кибербезопасности. На сегодняшний день в Эстонии [126]:

– 67% эстонцев регулярно используют электронную ID-карту;
– 99% онлайн государственных услуг;
– 99% жителей Эстонии имеют электронное удостоверение личности;
– 5.9% рабочие в ИТ секторе;

В апреле 2007 года Эстония подверглась крупнейшей организованной кибератаке. В результате на сегодняшний день Эстония стала одной из ведущих стран в области кибербезопасности.

Стратегия кибербезопасности 2008 года была первым документом Эстонии в области кибербезопасности. После кибератак Эстония стала воспринимать кибербезопасность как неотъемлемую часть национальной безопасности [127, с. 7].

В 2015 году 30% интернет - пользователей Эстонии сталкивались киберинцидентами. В Эстонии противостоять атакам отражается в низкой осведомленности внедряемых проектов. 17% всех эстонских компаний внедрили политики безопасности и это показатель 2015 года [135, с. 64].

В 2018 году вступил в силу Закон о кибербезопасности, в котором требования GDPR перенесены в национальное законодательство [135, с. 41]. Закон о кибербезопасности предусматривает требования к содержанию сетевых и ИС. Закон о кибербезопасности не применяется к поставщикам цифровых услуг, в которых в течение финансового года занято в среднем менее 50 человек и чей годовой оборот не превышает 10 миллионов евро с учетом определений малых предприятий [128].

В августе 2018 года Эстония также создала киберкомандование. Основная миссия киберкомандования – это проведения операции в целях обеспечения безопасности цифрового пространства Эстонии [129; 130].

Можно также отметить опыт Израиля как один из ярких примеров в области кибербезопасности. Израиль, начиная с 1990-х годов начал заниматься обеспечением кибербезопасности, и они достигли хороших результатов. В 1993 году была образована компания CheckPoint, которая разрабатывала брандмауэры. Уже к 2013 году в Израиле в области кибербезопасности функционировало более 220 компаний, и их экспорт составил 5% от мирового рынка, то есть $3 млрд. США. Изначально данная отрасль в Израиле финансировалась из местного фонда, то к 2013 году основные средства (58%) привлекались из зарубежных стран [131, с. 95].

Опыт Литвы. Первый закон о кибербезопасности в стране был принят в декабре 2014 года. С 2015 года Министерство внутренних дел уполномочено формировать политику в области обеспечения безопасности общественных информационных ресурсов вместе с Национальным центром кибербезопасности, Органом регулирования связи, Государственной инспекцией по защите данных и Департаментом полиции для реализации политики кибербезопасности. Стратегия кибербезопасности Литвы была принята в 2011 году на 2011–2019 годы. Стратегия включала оценку потенциала Литвы в области кибербезопасности и ряд четко сформулированных целей с графиком их реализации [132]:

Второй раз Национальная стратегия кибербезопасности Литвы была принята в 2018г., который определил основные направления национальной политики в области кибербезопасности в государственном и частном секторах. Реализация Стратегии направлена на укрепление кибербезопасности государства, обеспечение, предотвращения и расследования уголовных преступлений, совершенных с использованием объектов кибербезопасности, а также на продвижение культуры кибербезопасности, развитие инноваций, и укрепление тесного сотрудничества между государственным и частным секторами. Кроме того стратегия Литвы направлена на международное сотрудничество и обеспечение выполнения международных обязательств в области кибербезопасности до 2023 года [133].

Согласно статистическим данным в Литве на данном этапе насчитывается [134]:

– 38 000 специалистов по ИКТ;
– 10 600 студентов IT;
– 2000 выпускников IT в 2018 году;
– 50% увеличение финансирования исследований области ИТ в 2018 году.

В Литве ежемесячная заработная плата ИТ специалиста включая все налоги составляет:

– 1600 евро младший инженер-программист;
– 2,480 евро инженер-программист среднего уровня;
– 3400 евро старший инженер-программист;
– 1,430 евро специалист по контролю качества;
– 2 020 евро специалист среднего уровня по обеспечению качества;
– 2700 евро старший специалист по обеспечению качества;
– 2000 EUR администратор базы данных;
– 3100 евро менеджер по ИТ-проектам.

Сайт CYBERWISER.eu - это европейская инициатива, направленная на необходимость создания эффективных, удобных для пользователя сред, предназначенных для обучения специалистов в области кибербезопасности. В течение всего срока реализации проекта CYBERWISER.eu схема Open Pilot открыта для любой европейской организации, стремящейся повысить уровень навыков сотрудников в области кибербезопасности. CYBERWISER.eu Open

Pilot планирует индивидуальный цикл обучения с продолжительностью от трех до шести месяцев на платформе CYBERWISER.eu. Обучение проводится онлайн включая теоретических и практических работ [135].

LITNET CERT - группа реагирования на компьютерные инциденты в сетях LITNET. Основной целью команды является решение проблем компьютерных атак [136].

Литва подходит к вопросу кибербезопасности более серьезно по сравнению с Чешской Республикой, и возможно это из-за географической близости к Эстонии, а также киберинциденту 2008 года, о чем свидетельствует, например, ее участие в Центре передового опыта совместной киберзащиты НАТО [104, с.1471].

Кроме того в 2018 году Литва утвердила Национальный план управления киберинцидентами. Национальный центр кибербезопасности при Министерстве национальной обороны отвечает за организацию, мониторинг и анализ управления киберинцидентами на национальном уровне. Государственная инспекция по защите данных, литовская полиция и другие учреждения, чьи функции связаны с кибербезопасностью в рамках компетенции, закреплены в Законе о кибербезопасности, и они расследуют и участвуют в управлении и решении киберинцидентов [137].

Опыт Сингапура. *Как и другие страны, в Правительстве Сингапура есть уполномоченный орган, который непосредственно занимается вопросами кибербезопасности - Агентство кибербезопасности.*

Агентство кибербезопасности Сингапура (The Cyber Security Agency of Singapore – CSA / https://www.csa.gov.sg/) является ответственным по надзору и исполнению национальной стратегии кибербезопасности. Закон кибербезопасности Сингапура принят в 2018 году. Закон предусматривает принятие мер по предотвращению, управлению и реагированию на угрозы и инциденты кибербезопасности, регулирование владельцев критически важной информационной инфраструктуры, регулирование поставщиков услуг кибербезопасности [85]. Закон также устанавливает правовую основу для надзора и поддержания национальной кибербезопасности в Сингапуре [101].

Основной деятельностью CSA является взаимодействие и информационно - пропагандистская деятельность, развитие связей с местными и мировыми лидерами, повышение осведомленности о кибербезопасности с помощью общественных информационно-пропагандистских программ, а также содействие разработке концепции безопасности. CSA также несет ответственность за развитие и создание надежной экосистемы в области кибербезопасности. CSA принимаются все необходимые меры для реагирования на кибератаки и смягчения их последствий. На постоянной основе защищают критические сектора, такие как энергетика, водоснабжение и банковское дело.

Миссией CSA является сохранение киберпространства Сингапура в безопасности, чтобы поддерживать цифровую экономику, национальную

безопасность и защищать социальное благополучие граждан страны. CSA определил три основные ценности (рисунок 4).

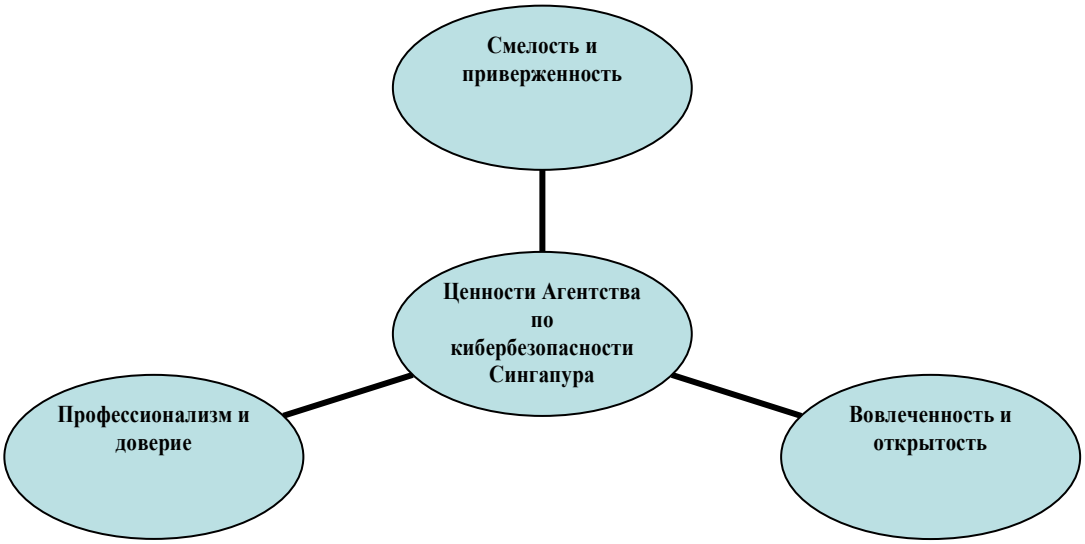

Рисунок 4 – Основные ценности Агентства по кибербезопасности Сингапура.

Примечание – Составлено автором по источнику [86]

В Сингапуре с 2013 по 2020 годы предусмотрено 190 миллионов долларов США для поддержки исследований как технологических, так и гуманитарных аспектов кибербезопасности страны [91, с. 40].

Рассмотрев опыт успешных стран, Казахстану целесообразно принят опыт сфере организации образовательных программ для действующих специалистов. Разработка и принятий национальной стратегии кибербезопасности, а также закона о кибербезопасности, как ранее отмечено. Утвердить план управления киберинцидентами критический важных ИКТ инфраструктур страны. Кроме того, необходимо рассмотреть возможность о повышении заработной платы для ИТ специалистов принимая опыт Литвы.

В следующей главе проведен анализ действующих механизмов использования и внедрения кибербезопасности в Республике Казахстан в условиях глобальной цифровизации.

2 АНАЛИЗ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ В РЕСПУБЛИКЕ КАЗАХСТАН

2.1 Анализ результатов использования цифровых технологий

В настоящее время вопрос обеспечения кибербезопасности требует внимания политиков на национальном уровне. Многие страны внедряют и продвигают цифровые технологии [138, с.197], оказывая свои услуги через электронное правительство. Эти происходящие изменения заставляют политиков задуматься и принимать решения в обеспечении безопасности в киберпространстве. Масштабное применение инновационных ИКТ повышает риск уязвимости цифровых данных к кибератакам. Обеспечение киберпрбезопасности является одним из приоритетных направлений в государственном управлении влияющих на национальную и экономическую безопасность страны. На данном этапе Казахстан, как и многие другие страны, переживает период цифровой трансформации, переводя традиционные государственные услуги на цифровые через портал электронного правительства.

В данном разделе проведен анализ действующего механизма обеспечения кибербезопасности согласно официальным нормативно-правовым и управленческим документам Казахстана. Необходимо отметить, что данный анализ проведен через призму государственной программы цифровой Казахстан, так как без цифровизации вопросы обеспечения цифровых технологии не актуальна. Цифровые технологии на сегодня интенсивно применяются не только правительственными органами для оказания государственных услуг, но и частным сектором. С каждым днем внедрение новых технологий в области цифровизации развивается прогрессивными темпами, и игнорировать происходящий феномен невозможно. Сегодня цифровизация охватывает все аспекты бизнеса и общества. Внедрение и применение ИКТ стало неотъемлемой частью жизни многомиллионных людей. Несомненно, технологии улучшили условия жизни благодаря новым цифровым сервисам в сфере образования, здравоохранения, финансов, торговли и в других областях жизнедеятельности общества. В период глобализации многие страны активно внедряют цифровые технологий. Казахстан также в патоке глобализации применяет инновационные технологии. Показателем является принятая в конце 2017 года Государственная Программа «Цифровой Казахстан» (ГП «ЦК») сроком реализации на 2018 - 2022 годы [3].

Ключевой целью ГП «ЦК» является «повышение качества жизни населения и конкурентоспособности экономики страны посредством прогрессивного развития цифровой экосистемы» [3]. В ГП «ЦК» обозначены 17 задач, одной из которых является обеспечение ИБ в области ИКТ, а также повышение цифровой грамотности населения путем подготовки специалистов в ВУЗах, а также переподготовки и повышения квалификации [3]. В целях достижения обозначенных 17 задач Правительством Республики проводится ряд работ, направленных на улучшение оказания государственных услуг,

применяя информационно-коммуникационные услуги. Вместе с тем, целю Казахстана является повышение уровня цифровой грамотности населения на 83% к 2022 году. Однако, в ГП «ЦК» не раскрыто, как и каким путем будут достигнуты эти показатели. В своем исследовании Клименко П., и Клименко И. отмечают, что реализации ГП «ЦК» является важным и эффективным решением Казахстана к открытому сотрудничеству с развитыми странами в рамках перехода к цифровой экономике [139, с. 99; 140, с. 50]. Можно отметить, что Казахстан в области цифровизации идет в правильном направлении. Более того, идея внедрения цифровых технологий поддерживается исследованиями Мусабаева Р., Касымжанова Б., Калиевой Г. и Ибраевой В., [141, с. 40]. Согласно мнению вышеперечисленных исследователей применение цифровых технологий улучшит взаимодействие государства с населением.

Вместе с тем, Баймухамедов М., Баймухамедова Г. и Аймурзинов М., подчеркивают, что ГП «ЦК» приведет к сокращению государственных расходов и повышению производительности и качества труда и все предусмотренные мероприятия в программе рассматриваются, как потенциальная возможность войти Казахстан в 30ку конкурентоспособных и успешных стран мира [142, с. 42].

Полагается, что пятилетняя ГП «ЦК - 2020» будет способствовать расширению деловых возможностей на развивающемся рынке и повысит конкурентоспособность экономики в целом, который будет реализован в пяти ключевых областях [3]:

– создание «Цифрового шелкового пути», для оказания поддержки в развитии цифровой инфраструктуры;

– улучшение человеческого капитала. Расширение технических знаний в коммерческих и других секторах экономики в целях повышения конкурентоспособности;

– создание цифрового правительства через усовершенствованные электронные и мобильные правительственные системы;

– «создание инновационной экосистемы». Правительство создаст возможные условия для принятия и применения инноваций;

– «цифровизация экономики». Переход от традиционной к цифровой экономике путем применения инновационных технологий повышающие эффективность труда.

За 2019 год Казахстан согласно всемирной цифровой конкурентоспособности поднялся на три позиции, достигнув 35-й позиции. Положительные результаты является повышением эффективности в нескольких подфакторах, таких как обучение и образование (1 место), нормативно-правовая база (16 место), адаптивное отношение (39 место) и гибкость бизнеса (15 место) [143, с. 19]. Однако, если провести анализ за последние 5 лет, то Казахстан остается на той же позиции, что и в 2015 году.

Согласно официальным данным сайта МЦРИАП РК за 2018-2019 годы из бюджета было выделено 35 млрд.тг., экономический эффект составил 802.5

млрд.тг. На выделенные средства в 2019 году автоматизированы более 80% государственных услуг. В результате более чем на 70 млн. сокращен бумажный (традиционный) документооборот, и в 3 раза сокращен средний срок оказания услуг с 31 до 10 дней. Более того, в течение 2019 года проведены более 320 межсистемных интеграционных работ. Однако не были реализованы некоторые интеграционные работы: МОН РК (7), МНЭ (6), МВД (4), МИИР (8), МЗ (2). До конца 2020 года планируется реализовать единую платформу интернет–ресурсов более 300 сайтов акиматов и центральных государственных органов, что в свою очередь должно привести к сокращению и оптимизации затрат на сопровождение сайтов **до 2 млрд.тг.** [144]. Также намечена задача по вхождению в число 30 конкурентоспособных и успешных стран мира согласно стратегическому плану - 2025 [145].

Таким образом, Казахстан проходит цифровую трансформацию в четвертой промышленной революции, как и многие страны мира. По мнению некоторых ученных применение ИТ существенно влияет на экономику страны [146, с.597], и в будущем будет нелегко найти работу людям с низкой квалификацией [147, с. 212]. К ним можно отнести водителей грузовых автомобилей, такси и авто грузчиков, так как в будущем автомобили будут самоуправляемы, а дроны будут применяться для доставки посылок. Предполагается, что в период глобальной цифровой трансформации спрос снизится на физический труд и повысится на специалистов, которые имеют высокую квалификацию, быстро обучаемы и адаптивны в быстро меняющемся мире цифровизации.

Согласно исследованию Головенчик Г., трансформация цифровой экономики страны должна оцениваться в соответствии с разными международными индексами и индикаторами [148, с. 6]. Можно отметить несколько рейтингов, которые рекомендует Головенчик Г.. Например, согласно Глобальному Индексу Инновации (Global Innovation Index) Казахстан за 2019 год занял 79 позицию. Данный показатель по сравнению с 2018 годом ухудшился на 5 позиций. Таким образом, в Казахстане инновационные проекты реализуется меньше по сравнению с другими странами [149, с. 1]. Вместе с тем, согласно Глобальному Индексу сетевого взаимодействия 2019 (Global Connectivity Index - GCI, Huawei) Казахстан занял 49 позицию из 79 [150]. Сильной стороной Казахстана является наибольшее количество баллов за инвестиции в 4G связь и проникновение подвижной широкополосной связи. Отмечается низкая плотность населения в стане, которые усложняет построения и развития ИКТ инфраструктуры. Однако, GCI, Huawei 2019 отмечает, что с населением в 18 миллионов применение технологий можно добиться положительных результатов в короткие сроки, так как несложно провести образовательные и осведомительные программы в среде немногочисленного населения.

Вместе с тем, согласно Индексу Сетевой Готовности 2019 (Network Readiness Index) Казахстан на 60 позиции из 121. Данный индекс включает в себя дополнительно показатели: технология - 74, люди - 61, управления -66 и

воздействия -39. Самый худший показатель Казахстана по технологиям – 74, и управлению - 66 [151, с 25]. Данный показатель является основанием для дальнейшей работы в целях повышения уровня фактора «технология», а именно подфакторами «контент, будущие технологии и доступность» [159, с. 42]. Сумитра Дутта отмечает, что «… для обеспечения позитивного и инклюзивного воздействия на общество и бизнес необходимо внедрить соответствующие механизмы управления для решения вопросов, связанных с доверием, безопасностью и инклюзивностью» [159, с. 13]. Таким образом, в Казахстане есть необходимость уделить внимание вопросам управленческого механизма связанных с безопасностью и доверием общества и бизнеса.

Вместе с тем, Казахстан в 2018 году по покрытию мобильной сети 4G занял 82 позицию из 120 стран [168, с. 180]. Казахстан демонстрирует хорошие результаты по мобильным тарифом и уровню грамотности среди взрослого населения, тогда как к слабым показателям отнесли экономику включая нормативную среду в области ИКТ, расходы на исследования со стороны правительств и высшего образования, а также расходы на лицензионные ПО для компьютеров [152, с. 4].

По мнению Головенчик Г. вышеперечисленные индексы дают оценку по цифровизации экономики и их интеграции в глобальное сообщество. Согласно статистике Глобальной экономики (The Global Economy), пользователи интернет в стране достигло 78,9% в 2018г., в 2008г. – 11%, и 2000г. – 0,67%. Данная динамика показывает колоссальную разницу и как Казахстанцы прогрессивно использует цифровые сервисы [153].

Проведенный обзорный анализ показывает, что большинство научных работ посвященных развитию цифровизации постсоветских стран рассматривает электронное правительство, как основной показатель цифрового общества [154]. В Казахстане развитие цифровизации в большей степени понимается также. Основными барьерами для улучшения цифрового и инновационного общества являются невысокий уровень экономических показателей [155, с. 88], а также недостаточная степень демократии. Таким образом, нами проведен онлайн анкетирование среди пользователей цифровых услуг и среди ИТ экспертов. Вместе с тем проведено исследование в формате фокус группы среди сотрудников АО «ГТС» КНБ РК (таблица 6).

Таблица 6 – Информация о количестве респондентов

Вид исследования	Количество респондентов
1	2
Вопросы в области цифровизации	
Онлайн опрос среди пользователей цифровых сервисов	182

Продолжение таблицы 6

1	2
Вопросы в области кибербезопасности	
Онлайн опрос среди пользователей цифровых сервисов	357
Онлайн опрос среди экспертов КИБ МЦРИАП РК	12
Фокус группа среди сотрудников АО «ГТС» КНБ РК	20
Всего в исследование были вовлечены	571
Примечание – Составлено автором	

Проанализированы результаты проведенного онлайн опроса среди пользователей цифровых сервисов Казахстана (инициативу проявили 182 респондентов). В ходе опроса была применена основы метода Technology Acceptance Model (TAM) – Модель Принятия Технологий (МПТ). Данная модель ранее применена Исаак О. [156, с. 737], Вангпипатвонг С., Чутимаскул В., Папасраторн Б. [157, с. 55], Аль-Адави З., Юсуфзай С., Паллистер Дж. [158, с. 1], Колеска С. Э., Добрица Л. [159, с. 204] и многими другими учеными, которые непосредственно исследовали вопрос принятия и применения информационных технологий. МПТ используется, как в частном, так и государственном секторе в целях исследования принятия и использования гражданами цифровых услуг. Например, в своем исследовании Джегер П. и Маттесон М., отмечают, что электронное правительство США для многих государственных учреждений является основополагающим инструментом взаимосвязи между правительством и гражданам [160, с. 87]. В этой связи, в целях выявления проблемных аспектов оказываемых США цифровых государственных услуг им был проведен анализ с помощью МПТ. В результате проведенного анализа выявлено насколько оказываемые государственные электронные услуги удовлетворяют потребность своих граждан. На основе МПТ смоделирована новая модель (рисунок 5).

Рисунок 5 – Предлагаемая модель принятия технологий.

Примечание – Составлено автором по источнику [156, с. 740].

Представленная МПТ имеет «независимые», «промежуточные» и «зависимые» переменные. Каждая переменная имеет определенный перечень вопросов, с помощью которых можно выявить качество и доверие пользователей онлайн услуг.

На основе предлагаемой МПТ сформированы нижеследующий перечень вопросов по 6 категориям (таблицу 7):

Таблица 7 – Перечень вопросов по категориям МПТ

Код	Взаимосвязь предлагаемой модели и перечень вопросов по категориям
Н1. Личная инновационность. Результаты личной инновационности влияет на воспринимаемые выгоды (социальные, экономические, образ жизни и наслаждение) (ЛИ)	
ЛИ	Возраст, сфера деятельности и пол. Как Вы относитесь к нововведениям? Считаете ли Вы себя инновационным человеком?
Н2. Осведомленность общественности о цифровизации влияет на стоимость получаемых услуг и минимизацию возможных рисков в киберпространстве (ОО)	
ОО	Мое доверие к реализации программы «Цифровой Казахстан»
ОО	Можете ли вы определить основные угрозы для дальнейшего развития цифровых услуг в Республике Казахстан?
Н3. Воспринимаемые выгоды (социальные, экономические, образ жизни и наслаждение) влияет на намерение использовать цифровые сервисы (ВВ)	
ВВ	Как часто Вы используете услуги онлайн (включая государственные услуги Egov)?
Н4. Предполагаемая стоимость влияет на намерение использовать цифровые сервисы (ПС)	
ПС	Как Вы оцениваете онлайн услуги в Республике Казахстан, учитывая их стоимость и качество?
Н5. Предполагаемый риск влияет на намерение использовать цифровые сервисы (ПР)	
ПР	Какие риски, по Вашему мнению, могут препятствовать пользователям в использовании онлайн услуг? Сталкивались ли вы, с какими либо проблемами в Казахстане связанные с онлайн услугами (включая государственные услуги Egov)?
Примечание – Составлено автором	

Результаты опроса по категориям МПТ.

Н1. Личная инновационность. Возраст и пол респондентов показан в рисунке 6. Среди опрошенных респондентов количество представителей женского пола больше чем мужского. Это можно объяснить тем, что по статистическим данным в Казахстане женщин больше, чем мужчин.

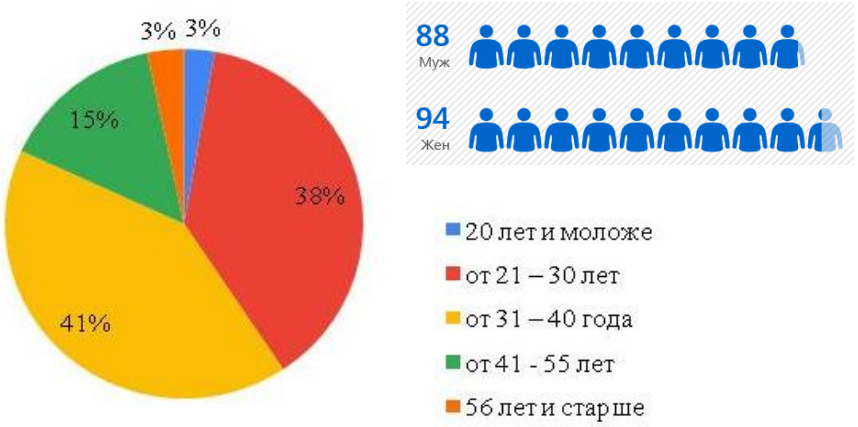

Рисунок 6 – Возраст и пол респондентов

Примечание – Составлено автором

По сферам деятельности необходимо отметить, что большинство респондентов, которые проявили активность - около 40% государственные служащие, 20% из частного сектора, 4% предприниматели и 15% из квазигосударственного сектора

Вместе с тем, 11% опрошенных являются студентами, около 10% люди находящиеся в отпуске по уходу за ребенком, а также среди респондентов оказались временно безработные граждане - 2% (рисунок 7).

ед. измерения: человек

Рисунок 7 – Информация по видам деятельности респондентов

Примечание – Составлено автором

На вопрос «*Как Вы относитесь к нововведениям?»*. Результаты респондентов показывает положительные тенденции. Практически около 95% опрошенных считают себя сторонниками нововведения и положительно относятся к новым изменениям и только больше 5% респондентов не всегда приветствуют нововведения.

Можно отметить, что граждане более адаптивны в использовании новых технологий, то есть не консервативны. Это является ключевым показателем для применения и внедрения новых цифровых сервисов в стране. Чтобы удостовериться в их ответах сформулирован следующий вопрос «*Считаете ли Вы себя инновационным человеком?».* Респонденты практически подтвердили предыдущий результат, так как более 50% считают себя инновационными, около 40% респондентов не всегда и только 5% из них не считают себя таковыми и 3% респондентов затруднились с ответом.

Н2. Осведомленность общественности о цифровизации.

Мое доверие к реализации программы «Цифровой Казахстан». Рисунок 8 показывает, что большинство опрошенных имеют доверительное отношение к реализации ГП «ЦК». Данный показатель является одним из важных факторов в реализации государственной политики в цифровизации. Предполагается, что без доверия населения к проводимой политике государства практически невозможно достичь эффективной реализации новых идей.

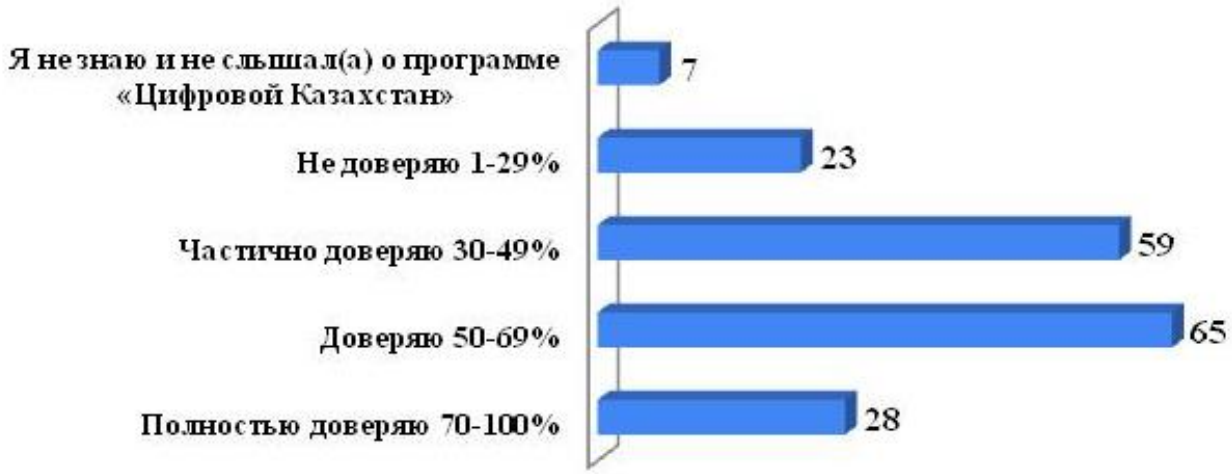

Рисунок 8 – Результаты опрошенных «Мое доверие к реализации программы Цифровой Казахстан»

Примечание – Составлено автором

Более того, результаты респондентов подтверждают *важность доверия казахстанского населения к реализации ГП «ЦК»* более 90% и только 4% из них считают, что это неважно, тогда как 3% из них затруднились с ответами.

На вопрос «*Что бы Вы предложили для повышения доверия к реализации программы «Цифровой Казахстан»?».*

Большинство из респондентов считают, что осуществление подготовки и повышение квалификации специалистов путем изменения образовательных

программ в отечественных ВУЗах с привлечением частного бизнеса, а также развитие политики обеспечения кибербезопасности повысить степень киберграмотности населения. Необходимо отметить, что некоторые из респондентов очень критично отнеслись к данному вопросу в части доверия населения, так как, по их мнению, отсутствует прозрачность, доступность и открытость государственной политики в сфере цифровизации. Вместе с тем, они отмечают о коррумпированности чиновников. Однако, согласно Индексу Восприятия Коррупции за 2017 год Казахстан из 180 стран занял 122 позицию. Данный показатель неоптимистичен, однако, Казахстан опережает соседние страны, как Россия, Кыргызстан, Украина, Узбекистан, Таджикистан и др., но отстает от Китая на 45 позиций (https://www.transparency.org – Transparency International) [160].

Вместе с тем, большинство респондентов предлагают проведение массовых ознакомительных работ среди населения, начиная с детских садов, меняя сознание населения и обеспечивая прозрачность и достоверность всех процессов, реализуемых проектов в Казахстане в области цифровизации. Более того, внедряемые новые системы должны быть устойчивыми и соответствовать всем техническим и программным требованиям. Некоторые респонденты считают, что реклама – двигатель процесса, то есть цифровизацию можно продвигать через социальные сети и СМИ, выделяя для этого время в телевидении, создавая обучающие видео ролики, то есть проводить широкую информационно-разъяснительную работу среди населения. Ниже можно ознакомиться с некоторыми комментариями и предложениями респондентов:

Р. «Необходимо организовать открытые дискуссионные площадки с привлечением ИТ экспертов. Открыто обсуждать существующие проблемные вопросы и не принимать решения кулуарно, проводить работы по снижению информационного неравенства населения повсеместно».

Р. ...каждый шаг должен быть своевременно или заранее разъяснен населению. Прозрачность и доступность информации следует обеспечить с подбором профессиональных спикеров из числа авторитетных экспертов. Эту работу следует сочетать с повышением международного имиджа. Синхронизировать программу цифровизации с работой ведущих корпораций в сфере ИТ. Необходим результат цифровизации на национальном уровне, который мог бы конкурировать с существующими брендами в информационных технологиях, но это упирается в кадровый потенциал сферы.

Р. Подключать интернет в селах и обучать в старших классах цифровым технологиям. Провести мероприятия в школах и лекции в вузах по теме «Цифровой Казахстан».

Р. Надо чтобы в первую очередь народ доверял государству. Сейчас нет этого доверия. В этом виноваты наши чиновники, которые думают только о себе. Мы живем в коррумпированной стране, и все прекрасно это знают…».

Детально с предложениями и комментариями респондентов можно ознакомиться в Приложении А.

На вопрос «*Можете ли вы определить основные угрозы для дальнейшего развития цифровых услуг в Республике Казахстан?»* более 130 респондентов считают, что в стране не хватает высококвалифицированных специалистов. На 2 месте вопросы кибератак, незащищенность сетей. Более детально результаты респондентов отражены в таблице 8.

Таблица 8 – Основные угрозы для дальнейшего развития цифровых услуг в Республике Казахстан

Перечень угроз	ед.изм/ респондент
Кибератаки (незащищенность сетей)	89
Нехватка квалифицированных специалистов	133
Слаба развитая система предоставления услуг операторами связи	69
Недостаточность выделенных и привлеченных финансовых ресурсов	48
Угроз на сегодняшний день не имеются	10
Примечание – Составлено автором	

Результат опроса показывает, что большинство респондентов, считают, что основной угрозой для развития цифровизации в стане является нехватка квалифицированных специалистов (133), затем не незащищенность сетей (89), слаба развитая система предоставления услуг операторами связи (69), а также недостаточное выделение и привлечение финансовых средств (48). Таким образом, на правительственном уровне целесообразно рассмотреть возможность разработки дорожной карты совместно с частным сектором в целях удовлетворения спроса отечественного рынка. Предполагается, что данный механизм управления в будущем снизит привлечения международных экспертов, который требует не малых расходов, как для государственных, так и частным организациям и холдингам.

Н3. Воспринимаемые выгоды (социальные, экономические, образ жизни и наслаждение) (ВВ). *Как часто Вы используете услуги онлайн (включая государственные услуги Egov)?* Большинство респондентов используют онлайн услуги: 6% каждый день, 16% несколько раз в неделю, 20% раз в неделю, 45% раз в квартал и более 10% не пользуются онлайн сервисом. В целом результаты опроса показывают положительную динамику: большинство респондентов заинтересованы и пользуются онлайн услугами, включая сервисы электронного правительства.

На вопрос «*Как вы думаете, затрудняют ли такие методы как аутентификация или шифрование финансовой информации /данных развитию цифровых услуг?* Около 50% респондентов считают, что данный метод не затрудняет развитие цифровых услуг, тогда как более 30% из них полагают, что данный метод не удобен, но безопасен, и больше 20% респондентов затруднились ответить.

Н4. Предполагаемая стоимость (ПС). *Как вы оцениваете онлайн услуги в Республике Казахстан, учитывая их стоимость и качество?* Стоимость и качество получаемых услуг - очень важный показатель для дальнейшего продвижения цифровизации в стране. В этой связи, нам очень важно знать, насколько наши услугополучатели удовлетворены получаемыми ими цифровыми сервисами. Таким образом, результаты респондентов обрадовали тем, что меньше 10% респондентов *считают, что качество и стоимость онлайн услуг плохи, тогда как около 55% из них оценивают как «хорошо» и 37% «удовлетворительно».* Полученный результат свидетельствует о возможности рассмотрения улучшение в стране онлайн услуг применив успешный опыт других стран в области цифровизации, чтобы качества оказываемых услуг соответствовало с их стоимостью. Резюмируя, можно отметить, что казахстанские онлайн сервисы в целом по качеству и стоимости имеют положительные динамику, но есть перспективы для дальнейшего развития.

Н5. Предполагаемый риск (ПР). 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.

«Какие риски, по Вашему мнению, могут препятствовать пользователям в использовании онлайн услуг?» Респонденты на первом месте отмечают риски потери конфиденциальности личных данных, проблемы с сетью, то есть доступность и скорость, а также риски кибератак. Они, вместе с тем, обозначают пользовательские проблемы, такие как размер мобильного устройства, неудобства в поиске информации и технические ограничения электронных гаджетов.

«Сталкивались ли вы в Казахстане с проблемами, связанными с онлайн услугами (включая государственные услуги Egov)?» опрос методом мультипликативного выбора, рисунок 9 четко отражает, что респонденты чаше всего сталкиваются с проблемой сетью Интеренет, который предоставляются операторами связи, а также с техническими проблемами устройства. В Казахстанском рынке не много провайдеров, которые представляют Интернет связь. Среде них можно отметить Казахтелеком, который выкупил акции Altel, и Active. На сегодняшний день конкурентом Казахтелекому является Beeline.

Таким образом, можно отметить, что Казахтелеком практически является монополистом в отечественном рынке. Предположительно у данных респондентов нет интереса провайдерам, которые они получают услугу.

Есть ли у Вас идеи по улучшению и внедрению новых цифровых услуг в Республике Казахстан, обеспечивая их Кибербезопасность?

На данный вопрос были представлены не мало комментарии и рекомендации от респондентов. Многие из них считают, что необходимо внедрять приемлемые и проверенные новшества зарубежных стран в сфере кибербезопасности, повышать компьютерной и киберграмотности населения.

Рисунок 9 – Результат респондентов «Сталкивались ли вы в Казахстане с проблемами, связанными с онлайн услугами (включая государственные услуги Egov)?»

Примечание – Составлено автором

Вместе с тем предлагается создать цепцентр, который непосредственно будет заниматься вопросами киберезопасности и многое др. Более детально с рекомендациями респондентов можно ознакомиться в Приложении А.

В целях подтверждения гипотез по результатам проведенного опроса проведен линейный регрессионный анализ (таблица 9). Функция f линейно зависит от показателей W, линейная зависимость от свободной переменной X не предполагается:

$$y = f(w,x) + v = \sum_{j=1}^{w} w_j g_j(x) + v \quad (1)$$

В данном случае линейная регрессия – используется в целях определения зависимость между переменными. Таким образом, линейная регрессия используется, чтобы понять, можно ли прогнозировать, что результаты:

- *H3. воспринимаемые выгоды (BB) (социальные, экономические, образ жизни и наслаждение) влияют на намерение использовать цифровые сервисы;*

личная инавационность ~ возраст + пол

где:

независимая переменная «личная иновационность» = «возраст» + «пол»

- reg1$innovations_feel, промежуточная переменная, ответ на вопрос «Как часто Вы используете услуги онлайн (включая государственные услуги Egov)?»;

- reg1$age и reg1$gender – независимая переменная, пол и возраст (личная инновационность).

- *H4. предполагаемая стоимость (ПС) влияет на намерение использовать цифровые сервисы;*

$$\text{стоимость}_{\text{предполагаемая}} = 0.03\text{Сфера деятельности}_{\text{Работник квазигосударственного сектора}} + 0.04\text{Сфера деятельности}_{\text{Работник частного сектора}}$$

где:

- $Cost_s -$ предполагаемая стоимость, ответ на вопрос «Как Вы оцениваете онлайн услуги в Республике Казахстан, учитывая их стоимость и качество?»;
- $Activity$ независимая переменная, вид деятельности респондента (да, это вид деятельности)

- *H5. предполагаемый риск (ПР) влияет на намерение использовать цифровые сервисы.*

$$\text{problems}_{online\ services} = 0.6Activity$$

где:

- reg1$problems_online_services, $\text{problems}_{online\ services}$ - промежуточная переменная «предполагаемый риск», ответ на вопрос «Сталкивались ли вы, с какими либо проблемами в Казахстане связанные с онлайн услугами»;
- $Activity$ – независимая переменная, вид деятельности респондента.

Таблица 9 – Результаты регрессионного анализа по проведенному онлайн опросу, построенный на основе МПТ.

Гипотеза	Переменные	Коэф-ты	Уровень доверия
1	2	3	4
H1. Личная инновационность (ЛИ). Результаты личной инновационности влияет на воспринимаемые выгоды (социальные, экономические, образ жизни и наслаждение)	Возраст и личная инновационность На личную инновационность влияет гендерная переменная Различия между мужчинами и женщинами при ответе на вопрос «Считаете ли Вы себя инновационным человеком?» существенны, в отличии от различий по возрасту	-0.36112	p-value 0.01, 99% достоверности

Продолжение таблицы 9

1	2	3	4
Н3. Воспринимаемые выгоды (ВВ) (социальные, экономические, образ жизни и наслаждение) влияют на намерение использовать цифровые сервисы	Частота использования услуги онлайн (включая государственные услуги Egov) и вид деятельности Частота использования различается по видам деятельности для «Работник квазигосударственного сектора»	0.4630	p-value 0.1 90% достоверности
Н4. Предполагаемая стоимость (ПС) влияет на намерение использовать цифровые сервисы	Оценка онлайн услуги по стоимости, качеству и виду деятельности для «Работник квазигосударственного сектора» и для «Работник частного сектора»	3.333e-01 4.907e-01	p-value 0.1 90% достоверности p-value 0.01, 99% достоверности
Н5. Предполагаемый риск (ПР) влияет на намерение использовать цифровые сервисы	Предполагаемый риск и вид деятельности для «В отпуске по уходу за ребенком»	1.3824	p-value 0.01, 99% достоверности
Распределение ответов на вопрос Сталкивались ли вы, с какими либо проблемами в Казахстане связанные с онлайн услугами (включая государственные услуги Egov)? От распределения ответов на вопрос Можете ли вы определить основные угрозы для дальнейшего развития цифровых услуг в Республике Казахстан?	Предполагаемый риск влияет на намерение использовать цифровые сервисы	0.636	Уровень доверия 95%.
Примечание – составлено автором. *исходные коды в Приложении Д.			

Применив МПТ, проведенный анализ действующей Казахстанской политики в области цифровизации показывает, что происходящие тенденции в масштабе страны в целом благоприятны. Результаты опроса респондентов показывают намерения использовать цифровые сервисы. Возможно, на это влияет положение, происходящее в мировом масштабе – глобализация и цифровизация. Однако, необходимо обратить внимание на рекомендации респондентов, которые были отмечены в ходе опроса. В рамках правительство необходимо задуматься о принятии ряд мер в целях дальнейшего развития онлайн сервисов в стране:

- формировать нормативно-правовую базу в целях защиты персональных данных, соответствующих международным требованиям (GDPR);
- принять меры по ликвидации компьютерной и кибербезграмотности населения. Организовать специальные курсы киберграмотности, которые будут включены в школьные программы. В рамках обучения предусмотреть привлечение специалистов из частного, квазигосударственного и международных организаций. На постоянной основе повышать квалификацию отечественных специалистов в области цифровизации и кибербезопасности, так как ИТ индустрия меняется экспоненциально;
- проводить все масштабные ознакомительные работы о проводимой цифровой политике в стране посредством СМИ и социальных сетей, что в свою очередь повысит доверие и осведомленность населения, а также покажет транспарентность и доступность проводимой политики правительства. В целях эффективных пропагандных работ предлагается ознакомить население посредством видеозаписей;
- принять политику и опыт успешных стран в рамках реализации цифровых проектов;
- принять меры по развитию отечественного потенциала ИТ экспертов в разработке программных приложений, то есть рассмотреть возможность повышения заработных плат и обеспечения их семей социальным пакетом (медицинская страховка, санаторий раз в год и предоставление жилья под ипотеку с низкими процентными ставками). Возможно, это позволит снизить «утечку мозгов» отток высококвалифицированных кадров;
- рассмотреть повышение статуса и заработной платы преподавательского состава ВУЗов Казахстана, так как на сегодняшний день высококвалифицированные ИТ специалисты не заинтересованы в работе педагога, так как гораздо больше могут заработать в бизнес секторе.

Предполагается, что вышеперечисленные мероприятия позволят повысить эффективность кибербезопасности в Казахстане. За время независимости страны сделано немало, но мир не стоит на месте, на глобальном уровне идет жестокая конкуренция между странами. Для вхождения в тридцатку конкурентоспособных стран мира необходимо развиваться и внедрять цифровые технологии, создавая комфортное и благоприятное положение для граждан страны, так как требования и уровень качества жизни диктуют новые вызовы и возможности для развития.

2.2 Анализ действующих механизмов использования и внедрения кибербезопасности

Согласно GCI в 2017 году Казахстан находился на 83 позиции [84, с. 61]. 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 незамедлительных мер в целях улучшения уровня киберзащиты.

В 2017 году Постановлением Правительства Республики Казахстан утверждена Концепция кибербезопасности [1]. В Концепции рассматривается текущая ситуация цифровизации ГО. Вместе с тем, 29 октября 2018 года Постановлением правления Национального банка Республики Казахстан утверждена Стратегия кибербезопасности финансового сектора Республики Казахстан на 2018-2022 годы [1]. Данная Стратегия утверждена в рамках реализации Концепции кибербезопасности Казахстана. Стратегия разработана в целях эффективного обеспечения кибербезопасности в финансовом секторе Республики Казахстан, и основное внимание уделено на кибербезопасности информационного обмена между участниками в финансовом секторе. Ранее отмечали, что кибербезопасность - это масштабный и растущий глобальный риск во всех отраслях жизнедеятельности человека. В рамках исследования большинство респондентов считают, что Казахстан на сегодняшний день не готов для внедрения и применения криптовалюты на отечественном рынке, но в будущем, возможно, рассмотреть, улучшив обеспечения кибербезопасности в киберпространстве в национальном масштабе [162, с. 135].

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, как отмечалось ранее. Президент Центра анализа и расследования кибератак О. Сатиев отмечает, что на рынке труда в Казахстане имеется высокий спрос на высококвалифицированные кадры в области кибербезопасности [163]. В этой связи, рассмотрение возможности проведения курсов по повышению компьютерной и киберграмотности специалистов государственного и частного сектора является одним из критических вопросов.

В рамках Концепции Киберщит Казахстана за счет бюджетных средств запланирована подготовка молодых кадров в области кибербезопасности на 2018-2020 годы [1]. Необходимо также отметить выступление Президента Республики Казахстан Касым-Жомарт Кемелевича Токаева от 4 марта 2020 года, который поручил увеличить количество государственного гранта на 2 000 единиц и больше для подготовки кадров по специальности «Информационная безопасность». Он также поручил Правительству и правоохранительным

органам обеспечить «цифровой суверенитет» информационных ресурсов страны [164].

Согласно информации Министерства информации и коммуникации Республики Казахстан в 2016 году за 9 месяцев зарегистрировано 16 576 кибератак [165]. Таким образом, со стороны правительства, при внедрении цифровых технологий необходимо одновременно рассмотреть вопрос обеспечения защиты данных в киберпространстве.

Вместе с тем, создан национальный институт безопасности, автором идей является Ержан Сейткулов, директор научно-исследовательского института ИБ и криптологии ЕНУ им. Л.Н. Гумилева. Предполагается, что институт обеспечит научно-аналитическую базу осуществляемой политики государства в сфере ИБ [166].

На сегодня в Казахстане действует ряд НПА, с помощью которых привлекаются лица, нарушившие этику Интернет и ИТ ресурсов в целях извлечения выгоды. Например, согласно статьи 207 главы 7 Уголовного кодекса Республики Казахстан, «Умышленные действия, направленные на нарушение работы ИС или сетей телекоммуникаций, – наказываются штрафом в размере до двух тысяч месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до шестисот часов, либо ограничением свободы на срок до двух лет…»[167].

Вместе с тем, в 2016 году № 832 Постановлением Правительства Республики Казахстан утверждено единое требование в области ИКТ и обеспечения ИБ [168], а также функционируют государственные учреждения и организации, которые проводят мероприятия в целях выявления киберугроз и при необходимости принимают соответствующие меры в целях минимизации негативных последствий. Например, в социальных сетях и в целом в киберпространстве было заблокировано более 620 тыс. материалов касательно пропаганды экстремизма и терроризма [169].

Согласно отчету 1-М «О зарегистрированных уголовных правонарушениях» Комитета по правовой статистике и специальным учётам Генеральной прокуратуры Республики Казахстан:

В 2015 году зарегистрировано - **45** уголовных правонарушений в сфере интернет – мошенничеств, из них: направлено в суд - 6;

В 2016 году зарегистрировано - **1 047** уголовных правонарушений, направлено в суд - 3, прекращено по нереабилитирующим основаниям – 21;

В 2017 году зарегистрировано - **2 047** уголовных правонарушений, направлено в суд - 82, прекращено по нереабилитирующим основаниям - 64;

В 2018 году зарегистрировано - **4356** уголовных правонарушений, 363 - направлено в суд, 111 прекращено по нереабилитирующим основаниям;

За 10 мес. 2019 года зарегистрировано - **6 279** из них, направлено в суд - 516, прекращено по нереабилитирующим основаниям – 540 [170].

В соответствии представленным данным КИБ МЦРИАП РК в целях обеспечения кибербезопасности Казахстана с момента принятия Концепции

кибербезопасности в 2017 году утвержден План мероприятий до 2022 года. В План вошли 41 организационно-правовых, организационно-технических мероприятий, управление человеческим потенциалом и работы по безопасному использованию ИКТ. В 2018 году утверждены 66 национальных стандартов в сфере ИКТ, из них 17 в области ИБ, которые вступили в силу с 1 января 2020 года. Кроме того, в 2018 году на базе АО «ГТС» КНБ РК запущен Национальный координационный центр информационной безопасности (НКЦИБ). Согласно МЦРИАП РК по результатам проведенного в 2019 году социологического исследования, осведомленность населения об угрозах кибербезопасности составила 73%. Вместе с тем, увеличилось количество образовательных грантов в сфере ИБ с 60 до 674. Более того, утвержден отдельный обучающий профессиональный стандарт по ИБ по специальностям: *«Специалист по безопасности сервисов», «Специалист по ИБ», «Специалист по защите информации», «Шифровальщик данных» «Криминалист по цифровым технологиям» и др*.

В 2018 году утвержден Перечень критически важных объектов информационно-коммуникационной инфраструктуры, в который вошли 219 объектов и в 2019 году был расширен до 336 критически важных объектов, которые планируется в будущем подключить к оперативным центрам ИБ. В 2019 году 7 оперативных центров ИБ получили лицензию на выявление каналов утечки цифровых данных.

Бюджет. В целях обеспечения кибербезопасности Казахстана за последние 3 года согласно ГП «ЦК» выделены из государственного бюджета **31 833 977 тысяч тенге.** Эти средства предназначены для оснащения испытательной лаборатории в сфере ИБ, безопасного функционирования «ЭП», защиты критически важных объектов ИКТ, а также для создания НКЦИБ.

На сегодняшний день в Республике принят ряд мер в рамках обеспечения кибербезопасности ИТ архитектур. Однако, нами предполагается, что принятые меры требуют детального анализа и доработки. Таким образом, в целях анализа действующего механизма обеспечения кибербезопасности в Казахстане проведен онлайн опрос 12 респондентов и фокус группы (неструктурированное интервью) 20 сотрудников АО «ГТС» КНБ РК среди экспертов в области кибербезопасности.

Результаты онлайн опроса и фокус группы. В рамках исследований онлайн анкетирование прошли 12 специалистов в области ИТ в возрастной категории от 20 до 55 лет (рисунок 10).

Больше чем 65% ИТ специалистов отмечают, что при реализации цифровых проектов они сталкиваются с административными (организационными) вопросами и больше 40% отметили технические проблемы, меньше всего респондентов сталкиваются с социально – экономическими и нормативно-правовыми вопросами.

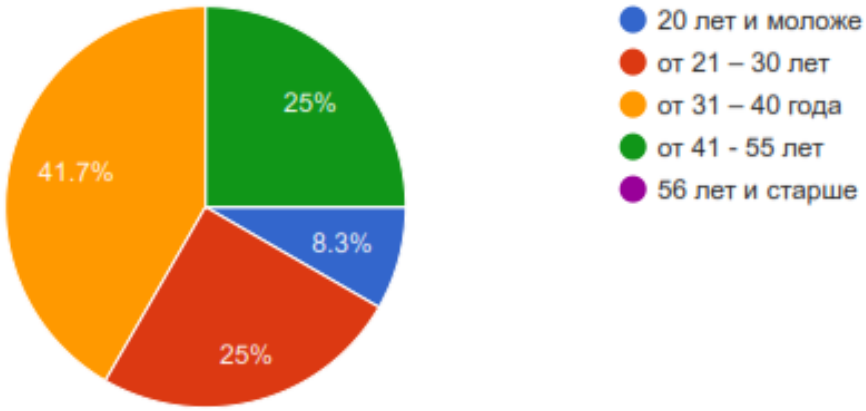

Рисунок 10 – Возраст респондентов.

Примечание – Составлено автором

На вопрос «Объективность и комплексность программы Цифровой Казахстан для достижения поставленных целей и задач» большинство респондентов считают, что такие сферы как образование, медицина и критические инфраструктуры организации требуют внимания экспертов в целях доработки.

Более 80% респондентов отмечают, что доверие казахстанского населения к реализации ГП «ЦК» очень важно и в целях повышения доверия в первую очередь необходимо провести подготовку и повышение квалификации специалистов путем изменения образовательных программ в отечественных ВУЗах с привлечением частного бизнеса (более 90%). Организовать краткосрочные курсы для всех заинтересованных граждан и бизнес сектора по компьютерной грамотности и ИБ в цифровом пространстве, необходимо развивать политику обеспечения кибербезобасности (ИБ в цифровом пространстве), а также повышать государственное регулирование через НПА и технические инструменты.

Важно отметить, что все 12 респондентов указали на недостаточное количество квалифицированных специалистов на рынке Казахстана. По мнению респондентов, второстепенным вопросом для решения является объем выделяемых и привлекаемых инвестиционных средств для развития отечественной индустрии в сфере кибербезопасности. Респонденты также отмечают о необходимости разрешении административных и организационных барьеров. 5 респондентов отмечают о недостаточном количестве научно-исследовательских институтов и лабораторий, слабом сотрудничестве с международными организациями, и 4 из них обратили внимание на несовершенство и негармонизированность нормативно-правового обеспечения в ИБ. Согласно их мнению, вышеизложенные критерии являются барьерами для улучшения кибербезопасности в Казахстане.

Эксперты считают, что самые распространенные киберугрозы для Казахстана – это кибератаки на социальный сектор (утечка персональных данных), вирусные атаки, уязвимости государственных ИС, фишинговые атаки,

мошенничество, уязвимости негосударственных ИС, а также атаки на финансовый сектор.

На основании вышеизложенного киберинцидентов государственному и частному сектору, возможно, необходимо разработать проект плана реагирования в целях минимизации ущерба на ИКТ инфраструктуру Казахстана. Вместе с тем, большинство экспертов отметили, что уровень безопасности персональных данных в Казахстане ниже чем 50% из возможных 100%, то есть данный сектор нуждается в развитии. Однако, положительной тенденцией является то, что многие из экспертов осведомлены о Концепции кибербезопасности и политике государства в сфере ИБ.

Более того, в ходе опроса эксперты отметили, что сфера медицины и образования требует доработки в части объективности и комплексности Концепции кибербезопасности. Необходимо также отметить, что 10 из 12 экспертов считают необходимостью изменить существующую организационную структуру взаимодействия ГУ, уполномоченных органов и частного сектора, которые вовлечены в обеспечении вопроса Кибербезопасности страны. Только 2 респондента из 12 удовлетворены нынешней организационной структурой. Результат опроса заставляет задуматься, так как в некоторых странах вопросами кибербезопасности занимаются Министерства внутренних дел, Комитет национальной безопасности или специализированно созданное ГУ. Однако у нас в Казахстане эти функции разделены между КНБ РК и КИБ МЦРИАП РК. Расследованием и статистикой киберинцидентов занимается правоохранительные органы Республики. Возможно, действующая организационная структура государственного управления является менее эффективной и в этой связи Казахстан не демонстрирует устойчивые показатели по сравнению с цифровизацией (рисунок 11).

Вопросы кибербезопасности охватывают исполнение международных требований и соглашений. В этой связи, экспертам был задан вопрос *«Готов ли Казахстанский рынок к реализации требований правил обработки персональных данных, установленные Общим регламентом по защите данных General Data Protection Regulation (GDPR), который вступил в силу 25 мая 2018 года?»*.

Более 65% экспертов указали, что многие о данном правиле не слышали и не знают, то есть Казахстанский рынок практический не готов, и только у одного эксперта был положительный ответ, тогда, когда другие затруднялись ответить. Таким образом, Казахстану необходимо работать тесно и развивать сотрудничество с зарубежными странами оповещая о результатах населения, местных экспертов и хозяйствующих субъектов Республики. Вместе с тем, больше 55% респондентов считают, что риски и угрозы в области кибербезопасности в определенных областях являются барьером для реализации инновационных идей и привлечения инвестиций, 25% затрудняются ответить и около 17% экспертов определенно считают, что данные риски являются барьером. В рамках онлайн анкетирования были

открытые вопросы, где эксперты могли предложить свои идеи по улучшению обеспечения кибербезопасности в Казахстане.

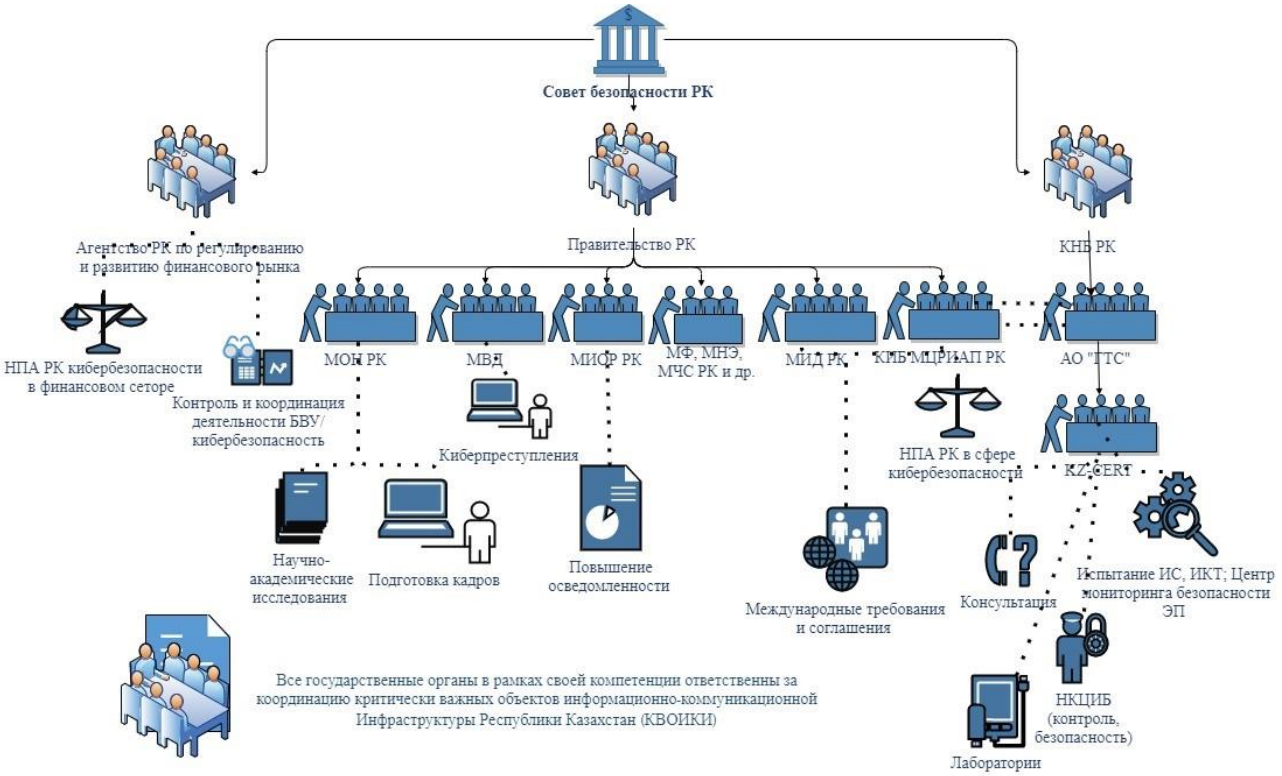

Рисунок 11 – Действующая структура государственного управления в сфере кибербезопасности Республики Казахстан

Примечание – Составлено автором

Рекомендации экспертов: *Р. Изучение международного опыта.*

Р. Подготовка специалистов, искоренить компьютерную безграмотность, ввести понятие «цифровая гигиена».

Р. Совершенствование нормативно-правовых документов, а также необходимо усилить требования к специалистам в данной области.

Р. Закупка технических средств, а также проверка уязвимости ИБ в организациях. Контролировать внутренние и внешние каналы и сети.

Р. Работать и повышать квалификацию экспертов в области кибербезопасности.

Проанализировав предложений экспертов, можно отметить, что на сегодня более актуальным является подготовка кадров и повышение киберграмотности населения. Дефицит кадров в области кибербезопасности также отражена в исследовании Абучакра Р., и Хури М., [5, с. 108]. В 2010 году в США требовалось 20 000 - 30 0000 специалистов в области кибербезопасности, тогда

как фактически число специалистов насчитывалось не больше 1000. Аналогичную ситуацию испытывала Япония, согласно Японскому информационному агентству по продвижению технологий (IPA) 256 000 специалистов были задействованы в работу по обеспечению кибербезопасности, однако из них только 105 000 были специализированы в области кибербезопасности. Более того, им дополнительно в сфере кибербезопасности требовались 80 000 кадров. Япония в целях повышения грамотности в кибербезопасности проводят выездные курсы для молодого поколения - Абучакра Р., и Хури М. [5, с. 133-134]. С кризисом специалистов столкнулись и США. Для решения данной проблемы Департамент внутренней безопасности и Национальный научный фонд организовали программу «CyberCorps: Scholarship for Service». После завершения обучения специалист был обязан работать в государственной службе несколько лет, то есть отрабатывать полученные им знания в госсекторе. Также в США с 2014 года начали практиковать привлечение высококвалифицированных специалистов из частного в государственный сектор. Одним из ярких примеров является привлечение Мики Дикерсона с Google в Белый дом, который успешно усовершенствовал сайт США в области здравоохранения (HealthCare.gov), а также посодействовал улучшению функционала ряда Правительственных сайтов - Абучакра Р., и Хури М. [5, с.135].

Вместе с тем, согласно анализу Абучакра Р. и Хури М., [5, с. 108], в целях привлечения высококвалифицированных экспертов, уполномоченным органам в области кибербезопасности необходимо тесно работать с частным сектором и научными институтами, а также организовать специальные программы в целях повышения цифровой грамотности населения.

Кроме Казахстанских ИТ экспертов онлайн опрос проводился среди пользователей интернет услуг. Инициативу проявили 357 респондентов, из них 186 мужчин, остальные женщины. Возрастные показатели респондентов (рисунок 12).

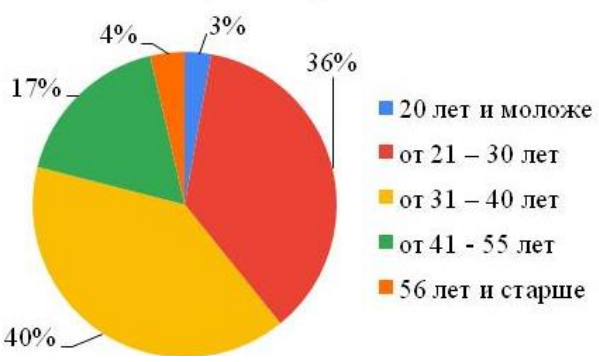

Рисунок 12 – Возрастные показатели респондентов (обычные пользователи интернет)

Примечание – Ссоставно автором

Наибольшее количество респондентов считают, что «отсутствие политики кибербезопасности в стране», «человеческий фактор - самое слабое звено», «финансирование, дефицит талантов и ресурсов», «нет обучения в области кибербезопасности», а также «отсутствие ответственности» могут препятствовать пользователям в использовании государственных онлайн услуг в стране.

58 респондентов отмечают, что кибератаки являются барьером для реализации инновационных идей в государственном управлении, тогда как 137 считают, что риски в области кибербезопасности не всегда являются барьерами и только 90 респондентов думают, что кибер угрозы не являются барьером, 69 респондентов затруднились ответить. Если данный результат сравнить с результатами опрошенных экспертов, то в целом результаты идентичны.

На сегодняшний день перед Правительством Казахстана стоит задача о четком определении приоритетных направлении в области кибербезопасности и избегать нецелесообразные ограничения. Одним из ярких примеров является идея установки на электронных гаджетах «Сертификата Национальной Безопасности». Анализ международного опыта по внедрению и применению сертификата безопасности показал, что среди успешных стран, таких как Великобритания, США, Япония и Сингапур не используют данный метод, как средства защиты цифровых данных на уровне всего государства.

В Казахстане летом 2019 года протестировали данный метод и пришли к выводу, что установка сертификата безопасности будет применена только в случае международных угроз кибератак. Об этом сообщил на своей официальной странице социальной сети Twitter (https://twitter.com/TokayevKZ, рисунок 13) Президент Республики Казахстан Касым-Жомарт Токаев. Комментарии к посту Президента РК не совсем были положительны. Данный факт также подтверждается результатом онлайн опроса, где некоторые респонденты категорически были против установки Национального сертификата безопасности.

На вопрос *«Как Вы смотрите на установку «национального сертификата*

Рисунок 13 – Скриншот с официальной страницы социальной сети Twitter Президента РК Касым-Жомарт Токаева

Примечание – Скриншот. Источник: https://twitter.com/TokayevKZ

безопасности»?» большинство респондентом категорический были против установки сертификата – 122 и 57 респондентов считают, что в этом нет необходимости (рисунок 14).

Рисунок 14 – Результат респондентов на вопрос «Как Вы смотрите на установку национального сертификата безопасности»?
(ед. измерения в количествах респондентов)

Примечание – Составлено автором

Касательно данного вопроса 20 респондентов представили свои комментарии следующим образом:

Р. Необходимо повысить грамотность населения. В связи с последними событиями в Казахстане складывается впечатление, что государство все больше вторгается в личное пространство гражданина. Сертификат безопасности устанавливается с целью слежки и полным контролем населения. На всей планете земля только Казахстану пришло это в голову. США и Европейские страны на такое не решились бы, там засудили всех подряд за нарушение свободы и демократии. Есть множество других способов обеспечить национальную безопасность. Поддержать рождаемость, экологию и начинать уже думать о народе... Использование сертификата это атака MITM («Man In The Middle» – «человек посередине»). Такое нельзя использовать в рамках государства. В рамках компании - да, для государственного органа - да, но не для всего государства, и то, что говорят чиновники о сертификате это - абсолютная некомпетентность. Каждый надёжный ресурс имеет свой сертификат безопасности, который соответствует всем требованиям безопасности и проверяется и выпускается соответствующими доверенными органами. С технической точки зрения промежуточный сертификат «безопасности» не имеет некого смысла. Люди просто перестанут обращать внимание на валидность сертификата и будут передавать свои данные в сети возможным злоумышленникам. Не совершать (применительно к госчиновникам) действий, приводящих к появлению «не приемлемого» контента, а если и были совершены - предпринять все

возможны меры для минимизации ущерба для государства кроме блокирования доступа к информации. Населению не разъяснили для чего, и как работает СНБ.

Р. Национальная безопасность не должна ущемлять права пользователей Интернет.

Р. «Google и Facebook заблокировали казахстанский сертификат безопасности, который крал данные».

Р. Старшему поколению никто не может объяснить и помочь с установкой Сертификата безопасности. В этой связи необходимо искать пути использования Электронно-цифровой подписи без сертификата. Либо проводить масштабную разъяснительную работу гражданам.

Р. Национальный сертификат безопасности - это нарушение права о конфиденциальности персональных данных, так как сертификат собирает всю информацию, включая пароли от аккаунтов, счетов, Pin-коды, пр.

Согласно утвержденной Концепции кибербезопасности [4], а также в пункте 9 Плана мероприятий [171] по реализации данной Концепции отмечено о применении сертификата безопасности со 100% охватом к 2022 году. По факту данное мероприятие не реализуется, что является одним из причин для разработки проекта Стратегии кибербезопасности Казахстана с учетом возможных угроз по неисполнению намеченных задач. Практика показывает, что предусмотренные некоторые задачи в Концепции в каких-то случаях перевыполнены *(достижение показателя 0,600 к 2022 году по ГИК),* а в других *(применение НСБ)* недостижимы, что негативно влияет на качество НПА, а также на доверие граждан страны на проводимую политику Правительством.

Респонденты считают, что в целях улучшения внедряемых новых государственных цифровых услуг в Республике необходимо усилить защиту и конфиденциальность данных в облачных хранилищах, обеспечить бесплатным лицензионным, а также совершенствовать законы в области кибербезопасности. Совершенствовать систему обеспечения цифровых данных в ГО, широко освещать проблематику, создавать платформу для заинтересованных участников для обсуждения проблемных и перспективных вопросов в области цифровизации и кибербезопасности, развивать потенциал отечественных ВУЗ для подготовки высококвалифицированных специалистов. Были представлены другие рекомендации, которые доступны в Приложении А.

Необходимо отметить, тот факт, что большинство опрошенных респондентов в целом имеют доверительное отношение к реализации Концепции кибербезопасности (рисунок 15).

Вместе с тем, в рамках научно-исследовательской работы интервью было проведено и среди работников АО «ГТС» КНБ РК и KZ-CERT.

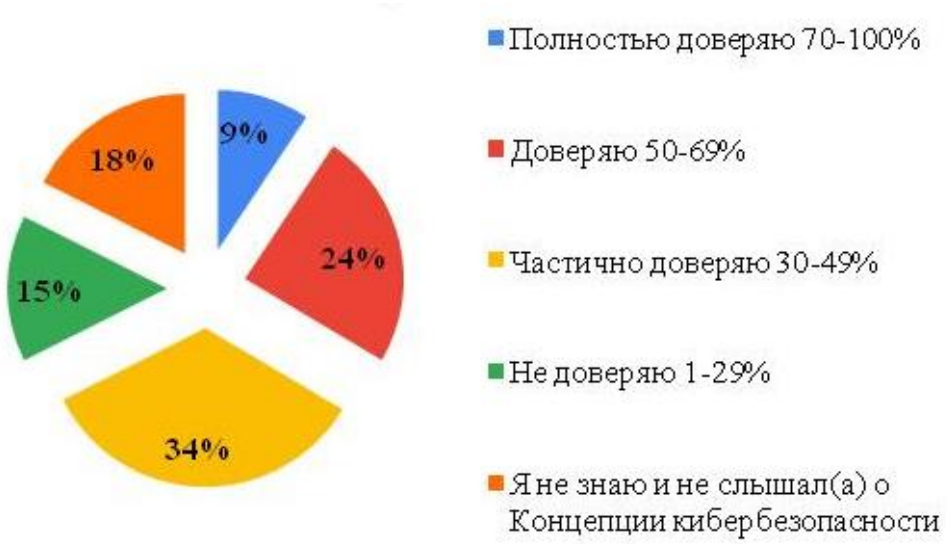

Рисунок 15 – Результат респондентов на вопрос «Мое доверие к реализации Концепции кибербезопасности».

Примечание – Составлено автором

В ходе интервью сотрудники АО «ГТС» КНБ РК отметили, что проводимая государственная реформа в области кибербезопасности передача функций под руководство КНБ РК, значительно повысила эффективность и результативность их работы. Сотрудники также отмечают, что бюрократические барьеры, с которыми ранее сталкивались при Министерстве информации и коммуникаций Республики Казахстан значительно сократились. Однако, они не совсем удовлетворены размером заработной платы. Низкая заработная плата может быть причиной того, что высококвалифицированные специалисты в области кибербезопасности и ИТ покидают и уезжают в другие страны за погоней светлого будущего.

Таким образом, политикам, возможно, следует побеспокоиться о сохранении отечественных квалифицированных сотрудников и сделать Казахстан более привлекательным для других стран. В этом случае следует использовать опыт Сингапура, то есть для высококвалифицированных специалистов имеющие опыт и ученую степень облегчить получения виз.

Резюмируя, полученные результаты опроса говорят о следующем. Правительству РК целесообразно рассмотреть возможность на постоянной основе проводить ознакомительные мероприятия по реализуемым ИТ проектами с населением, организовать работу максимально доступной для народа, улучшить ее качество в целях повышения доверия к реализуемым правительственным инициативам. Респонденты также 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. Организовать обучающие курсы для населения по использованию государственных сервисов

и делать их доступными для масштабного пользования. По возможности на постоянной основе проводить анализ зарубежного опыта и внедрять уже проверенные новшества, повышать сохранность персональных данных граждан и исключать использование их третьими лицами.

Одновременно с наращиванием кадрового потенциала в ИТ сфере, нужно создавать международные хабы, как это практикуется в США и Индии. В этой связи, по необходимости 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.

В целях глубинного понимания системы кибербезопасности Казахстана в следующем разделе проведем SWOT & PEST анализ.

2.3 SWOT и PEST анализ системы кибербезопасности Казахстана

В глобальном мире происходят колоссальные изменения в сфере ИТ индустрии, которые невозможно игнорировать. Многие развивающиеся страны ставят цель войти в число развитых стран, путем применения инновационных технологий, повышая конкурентоспособность страны [171, с.189]. Само понятие «инновационность» по настоящее время изучается академиками разных стран. Например, Джеймс Брайт, под инновационностью подразумевает сам процесс, который связывает предметные области, а именно экономику, науку технику и менеджмент [172]. Всем известный факт, что конкурентоспособность выставляет высокие требования к стандартам во всех отраслях жизнедеятельности населения страны. Данные требования наталкивает как государство, так и бизнес сектор к внедрению и применению новаторских идей в ИТ, что положительно сказывается на жизненно важных аспектах граждан страны [173, с.29].

Необходимо отметить, что в мире угрозы и кибератаки на финансовый сектор растут, и власти пытаются снизить киберриски и повысить их безопасность. Согласно данным Всемирного банка, клиенты финансовых услуг в 2016 году пострадали от кибератак на 65% больше, чем клиенты любой другой отрасли, что на 29% больше, чем в предыдущем году. Всемирный банк считает, что в целях разрешения данного вопроса, необходимо улучшить координацию между органами финансового сектора и другими учреждениями, занимающимися вопросами кибербезопасности [174]. Однако, в сегменте Казахстана нелегко обозначить расходы, которые направлены на обеспечение безопасности в финансовом секторе, так как такие статистические данные в открытом доступе невозможно найти.

Считаем целесообразным рассмотреть случай с компанией Google. Дэйв Дэвис [176] и Кэролайн Форси [177] отмечают, что в мире на сегодняшний день более 70% интернет пользователей используют поисковую систему Google. Эти

показатели также подтверждаются в исследовании Томас Дж. Лоу [178]. Он утверждает, что более 90% мирового рынка пользуется поисковой системой Google. Аналогичный результат показывают статистические показатели Statcounter GlobalStats [179]. Согласно данным Statcounter GlobalStats, с 2019 года по январь 2020 года казахстанцы больше всего прибегают к услугам поисковой системы Google, то есть на январь 2020 года число пользователей поисковой системы Google превысило более 80% [180]. Таким образом, Google, несомненно, является самой популярной поисковой системой в мире. Кроме того, Google захватил почти 85% мобильного трафика. В ходе изучения отчета Google «О Достоверности Сервисов и Данных» с 2015 года 243 информации были удалены с пространства Интернет, касающейся Казахстанского контента. Из них 232 по запросу государственных органов и остальные 11 на основе судебных распоряжений (рисунок 16) [181]. Динамика изменений показывает, что чем больше Казахстан внедряет цифровые технологии и развивает цифровые государственные услуги, тем больше запросов поступают в адрес Google от государственных органов для удаления с пространства Интернет. Статистика показывает, большинство данных удаляются в целях обеспечения национальной безопасности страны. Вместе с тем, компания Google обращает внимание на то, что один из государственных органов Казахстана вышел с просьбой удалить в YouTube оппозиционный канал. Однако, данное требование компанией Google не удовлетворил.

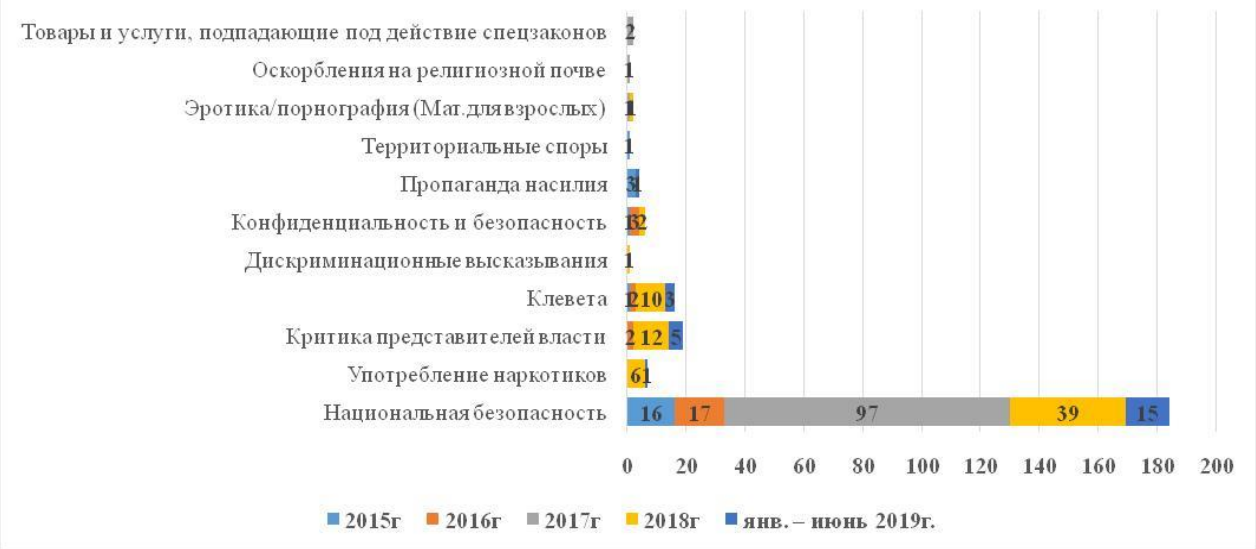

Рисунок 16 – Статистический показатель запросов государственных органов Республики Казахстан на удаление контента с поисковой системы Google с 2015 по июнь 2019г.

Примечание – Составлено автором по источнику [181]

Кибератаки представляют большую угрозу правительству, субъектам экономики и физическим лицам. В целях четкого понимания системы обеспечения кибербезопасности Республики Казахстан проведен PEST и SWOT методы анализа. По результатам проведенного анализа выработаны

практические рекомендации для улучшения обеспечения кибербезопасности в Республике. Выбор данных методов обосновывается тем, что SWOT метод анализа предусматривает сильные, слабые стороны, а также возможности и угрозы существующего механизма обеспечения кибербезопасности в стране. В то время, когда метод PEST рассматривает такие факторы как политические, экономические, социально-культурные и технологические. Важность социально-экономического, политического, морально-идеологического, культурного и других аспектов отметила в своем исследовании вопроса киберпреступности в Российской Федерации, Карпова Д. [9, с. 47].

SWOT и PEST анализ являются одним из популярных методов в части исследования вопросов кибербезопасности и ИТ. Например, в академической поисковой системе в Google Scholar ввести на английском запрос слова «*SWOT & PEST analysis & cyber security»,* указав фильтр срок поиска с 2015 года (за последние 5 лет), то поисковая система выдаст более 3 000 академических материалов. Однако, по аналогичному запросу на русском языке «*SWOT и PEST анализ & кибербезопасность»* поисковая система Google Scholar выдает всего 24 материалов, а на государственном языке «SWOT и PEST талдау & киберқауіпсіздік» ни одного материала. Данный результат показывает, насколько мало заинтересованных экспертов в академическом мире изучающие вопросы кибербезопасности, которые имеют свои труды на казахском и русском языках с применением SWOT и PEST анализа.

PEST анализ. Сильные стороны:

Политические факторы. В целом Казахстан по сравнению с соседними странами демонстрирует положительную динамику в части политической стабильности. Согласно индексу Политической стабильности (TheGlobalEconomy.com) Казахстан за 2018 год занял 101 позицию из 195 стран, тогда как соседние страны, как Китай-119, Узбекистан-122, Россия -136, Кыргызстан - 144 значительно отстают в данном рейтинге [182]. Необходимо также отметить, что с момента утверждения Концепции кибербезопасности Казахстана был проведен ряд управленческих реформ в стране. В результате реформы на сегодняшний день вопросами Киберщит Казахстана непосредственно занимается КНБ РК. Ранее в параграфе 2.1 результаты интервью сотрудников АО «ГТС» КНБ РК положительно отозвались на проведенные реформы, и вопросы киберинцидентов в Республике разрешаются более оперативно и эффективно из-за снижения бюрократических барьеров. В то же время КИБ МЦРИАП РК уполномочен по обеспечению ИБ от киберугроз, поддержке защиты государственных баз данных и ИС. КИБ МЦРИАП РК также ведет политику кибербезопасности в целях защиты страны и их граждан от киберугроз [183].

Вместе с тем, Казахстан не имеет каких-либо внешних и внутренних ограничительных мер на глобальном рынке в целях решения ИКТ задач. То есть для Казахстана при финансовой возможности доступны новые технологические решения. Казахстан также может применить практику

Сингапура по привлечению новых инновационных идей в глобальном масштабе.

Казахстан географически расположен между Россией и Китаем. Эти страны по численности населения и территории на много больше по сравнению с Казахстаном. Майкл Портер и Скотт Стерн отмечают, что инновация является вызовом в глобальном масштабе, и чтобы управлять ими, организации должны воспользоваться географическим расположением в коммерциализации нововведений. Чтобы управлять ими хорошо, компании должны использовать преимущество географического месторасположения в создании и коммерциализации новых идей [184]. Таким образом, учитывая географическое расположение между Россией и Китаем, Казахстану необходимо воспользоваться с такой возможностью и развивать национальную рыночную экономику среди двух держав, развивая собственную ИТ инфраструктуру и индустрию.

Экономические факторы. Казахстан, как и многие страны, проходит период цифровой трансформации. В рамках концепции Киберщит Правительством освоено **31 833 977 тыс. тенге из государственного бюджета.** Таким образом, правительством развитие кибербезопасности в стране поддерживается, и выделяются средства из государственного бюджета. Предполагается, что основные задачи, которые предусмотрены в концепции исполнены. Однако, из-за происходящей в мире пандемии COVID-19 нелегко предопределить устойчивое экономическое развитие страны в ИТ индустрии в целом. Практика показывает, что в период пандемии использовании онлайн сервисов возросло и это в большей степени взаимосвязано с работой и учебой на удаленном доступе.

Социально-культурные факторы. Граждане Казахстана показывают положительные тенденции в использовании цифровых технологий, а именно онлайн государственных услуг на портале электронного правительства. Население Казахстана на практике показало, что оно гибкое и обучаемо касательно применения цифровых услуг. Более того, согласно показателю всемирной цифровой конкурентоспособности 2019 года Казахстан поднялся на три позиции, достигнув 35-й позиции. Повышение эффективности является результатом положительных сдвигов таких подфакторов, как обучение и образование (1-е место), нормативно-правовая база (16-е место), адаптивное отношение (39-е место) и гибкость бизнеса (15-е место) [155 с. 19]. Вместе с тем, в рамках развития цифровизации правительством планируется увеличение выделяемых государственных грантов для получения технического высшего образования в отечественных и зарубежных ВУЗах. Президент страны Касым-Жомарт Кемелевич Токаев 4 марта 2020 года на совещании «Цифровой Казахстан» отметил о необходимости увеличения количества государственного гранта по специализации «информационная безопасность» не менее чем 2 000 ед. [141]. Данные изменения свидетельствуют, что Казахстан двигается в правильном направлении.

Технологические факторы. Согласно действующего нормативно-правового акта банк данных ИС государственных органов должен находиться на территории Казахстана. Таким образом, оцифрованные персональные данные граждан Казахстана в обязательном порядке хранятся в Центрах Обработки Данных (ЦОД) Республики Казахстан. Данный метод хранения данных в первую очередь снижает риск кибервойны. Кибервойна – целенаправленная военная атака в целях уничтожения цифровых данных и ИК инфраструктур. Вместе с тем, хранение данных на территории Республики также снижает риски физического воздействия, как целенаправленная порча ЦОД.

PEST анализ. Слабые стороны:

Политические факторы. В целом в Республике сохраняется стабильная динамика в политической сфере. Однако, как показывает мировая практика в период пандемии COVID – 19 в некоторых станах происходят дестабилизационные ситуации из-за введенного карантина. Согласно Закону Республики Казахстан «О чрезвычайном положении» Президентом страны К. Токаевым на территории страны с 16 марта 2020 года введено чрезвычайное положение [185]. Чрезвычайное положение в стране продлен до 11 мая текущего года [186; 187]. В Казахстане более одного месяца люди находились на карантине и есть возможные риски возобновлении чрезвычайного положения, в случае если количество заболевших будет расти высокими темпами. Ким С., и Куан-Рин С., освещение в СМИ выдвигает на первый план COVID-19 как уникальную угрозу, которая еще больше усиливает панику, стресс и вероятность истерии [188, с 2]. В этой связи, не исключено, что могут возникнуть митинги и повлиять на политическую стабильность страны, которые в свою очередь могут негативно повлиять на все аспекты жизнедеятельности населения в целом.

Необходимо также отметить, что Казахстан не имеет отдельного законодательного акта в части кибербезопасности, если сравнить с успешными странами в области цифровизации и кибербезопасности согласно Индексу глобальной кибербезопасности. Важность вопроса об отсутствии законодательной базы в области кибербезопасности также отметили в своем исследовании Кармыс Г., Бастаубаева, А. [189, с. 155]. Губайдуллина М., в своем исследовании отмечает, что глобальное информационное пространство не имеет границ, однако, имеет риски в политической арене из-за конкуренции и недоброжелательности других стран в целях ослабления конкурентов [13, с. 14]. Вместе с тем, негибкий подход в разработке и реализации ИТ решения может не учесть желание услугополучателей, который негативно повлияет на пользовательский интерес получателей онлайн сервисов.

Экономические факторы. Происходящая в мире пандемия COVID-19 затрудняет предопределить устойчивое экономическое развитие страны как в целом, так и в ИТ индустрии. К большому сожалению, Казахстан зависимая страна от сырьевой (нефть, газ, уголь и мазут) индустрии. В период пандемии спрос на нефть упал. Таким образом, нынешнее положение Казахстана не

совсем утешительное и вероятность рисков инфляции и девальвации высоки. Однако, предполагается, что уполномоченные органы, как Национальный банк РК, Министерство финансов РК, Агентства РК по регулированию и развитию финансового рынка и Министерство национальной экономики РК будут применять регуляторные действия в целях снижения инфляционных и девальвационных рисков. Необходимо отметить, что кризисное явление происходит не только в Казахстане, но и во многих других странах, и прогнозировать резкое светлое будущее в сфере ИТ задача не из простых. 9 марта 2020года Президент страны Касым-Жомарт Токаев провел совещание по экономической ситуации в Республике, где отметил о необходимости разработки антикризисной программы и пересмотра государственного бюджета на 2020-2022 годы [190]. Принимаемые меры Президентом Республики очень своевременны, однако, результативность покажет время. В период происходящего глобального кризиса из-за пандемии экономическую стабильность предсказать практический не возможно.

Во всемирном экономическом форуме ежегодно презентуется отчет по индексу среди конкурентоспособных стран мира (далее - Индекс). Согласно Индексу в 2008 и 2019 годы уровень конкурентоспособности Казахстана поднялся с 61 места всего на 6 позиций [191, с. 10]. То есть в 2019 году Казахстан занял 55 позицию, тогда как Сингапур на 1, США на 2, Великобритания на 9, Эстония на 31, Литва на 39, а также соседние страны как Китай на 28 и Россия на 43 позиции [192, с. 13]. Страны с показателем высокой конкурентоспособностью как ранее отмечалось, занимают лидирующие позиции как в цифровизации, так и в кибербезопасности.

Социально-культурные факторы. Происходящее в стране политическое и экономическое явление влияет на социально-культурные факторы. Однако, необходимо отметить, что эти изменения не сильно повлияют на образовательно-культурные программы и процессы страны. Результаты опроса респондентов показали, что в Казахстане необходимо улучшать компьютерную и киберграмотность населения. Данный показатель на сегодняшний день является слабым фактором. Вместе с тем, Глава государства Касым-Жомарт Токаев 4 марта 2020 года в своем выступлении отметил о необходимости проведении работы по «цифровому неравенству», так как цифровое неравенство является социальным неравенством общества страны [141].

Технологические факторы. Казахстан с технологической стороны имеет ряд уязвимости. Во-первых, Казахстан является потребителем аппаратного и программного обеспечения, закупает готовые решения и продукты в ИТ сфере. Например, соседняя страна Россия имеет свой отечественный антивирус «Касперский», и Казахстан ежегодно покупает данный лицензионный продукт для обеспечения безопасности компьютерных систем государственных учреждений. Казахстан также из ближнего и дальнего зарубежья закупает компьютеры и другие инновационные цифровые технологии, то есть Казахстан – технологический зависимая страна. Тамез Л., [23, с. 132] в своей

исследовательской теме «4 промышленная революция» обозначили внутренние и внешние нужды, и одним из пунктов было снижение расходов на техническое обслуживание. Однако, на сегодняшний день для Казахстана сократить расходы на данное мероприятие практически невозможно, так как все расходные материалы и технические решения закупаются из ближнего и дальнего зарубежья. Более того, многие пользователи устанавливают на своих компьютерах не лицензионные (пиратские) программные обеспечения, такие как Microsoft Office и другие, так как лицензионные стоят недешево.

SWOT-анализ. Сильные стороны. Казахстан - страна с небольшой численностью населения. Согласно последним данным Комитета статистики Министерства национальной экономики Республики Казахстан в стране более 18 600 000 человек [193]. Обучение и ознакомление населения с происходящими изменениями в ИТ индустрии намного легче, так как пользователей IoT (The Internet of Things) - устройств не так много по сравнению со странами, где численность населения намного выше. Более того, в стране принята Концепция кибербезопасности, а также план реализации данной концепции по 2022 годы. Вместе с тем, была принята ГП «ЦК» на 2018-2022 годы. В рамках развития цифровых технологий в стране необходимо рассмотреть возможность выхода на мировой рынок по разработке программного обеспечения.

Слабые стороны. Использование готовых ИТ решений, производимые зарубежными странами. Отсутствие собственного антивирусного программного обеспечения. Вместе с тем, дефицит высококвалифицированных сотрудников с техническим образованием, а также специалистов в области кибербезопасности. Низкая культура компьютерной киберграмотности населения. Таким образом, Казахстан является технологически зависимой страной, который не имеет большого и богатого опыта в ИТ индустрии по сравнению с другими странами. Также необходимо отметить, что с каждым годом на рынке выходят инновационные ИТ решения, тогда как в стране устаревают имеющиеся ИТ инфраструктуры и технологии. Существует нехватка выделяемых бюджетных средств. Так, Кармыс Г., Бастаубаева, А. отмечают, что в Республике финансирование проектов цифровизации недостаточно [187, с. 155].

Возможности. Возможность развивать и поддерживать отечественные ИТ решения, рассмотрев данный вопрос на законодательном уровне. Данную возможность озвучил Глава Государства Касым-Жомарт Токаев 4 марта 2020 года [141]. Можно рассмотреть возможность запуска пилотных проектов по развитию облачных хранилищ отечественного производства. Предполагается, что развитие облачного хранилища даст возможность использования и хранения больших банк данных в отечественных хранилищах, тем самым повышая их безопасность. Из-за пандемии COVID-19 популярность использования онлайн сервисов повысилась. Соответственно есть высокая вероятность возможных киберугроз. Пандемия, несомненно, внес свои коррективы в изменении стиля и образа жизни общества. Например, изменился

покупательские привычки людей, больше онлайн покупки, а также отношение к обслуживанию клиентов. «Образ жизни радикально меняется, и эффект пандемии COVID-19 проникает во все аспекты повседневной жизни», отмечают в своем исследовании Ким С., и Куан-Pin С [188, с. 2].

Угрозы. В Казахстане большинство используемых компьютерных систем отработали уже более чем 3 года. Старые системы могут замедлить производительность и привести к ненужному простою. Например, компания Microsoft с 14 января 2020 года остановила поддержку операционных систем Windows XP [194] и Windows 7 [195], так как они заинтересованы в поддержке и инвестировании новых технологий. Таким образом, Microsoft перестал обновлять и исправлять выявленные ошибки в системе безопасности данных ПО, тем самым они призывают всех пользователей обновить операционные системы на более новую версию Windows 10 и выше. Однако, необходимо отметить, что некоторые компьютеры по техническим требованиям не соответствуют для обновления операционной системы, что в свою очередь требует приобретения компьютера нового поколения с более высокими мощностями и оперативной памятью.

Следующим аспектом является - расстояние расположенности районов от больших центральных городов. Привлечение высококвалифицированных экспертов в отделенные регионы - задача не из простых и это является одним из уязвимостей отдаленных регионов в Казахстане. Казахстан занимает 9 позицию по величине, тогда как численность населения чуть больше 18 500 000 человек. Более того, Казахстану нелегко конкурировать с соседними странами, как Китай и Россия, которые имеют более мощную ИКТ базу. Существует также вероятность киберугроз касательно взлома ИС Казахстана от конкурирующих стран, которые имеют финансовый интерес. Взломав государственные критически важные ИС, они могут предложить свои недешевые услуги для восстановления их. Вместе с тем, есть угроза по снижению доверия населения к государственным цифровым сервисам (утечка конфиденциальных данных физических и юридических лиц). Например, в период пандемии государством выплаты пособий в размере 42 500 тг. наблюдались технические проблемы, как на портале электронного правительства, так и в БОТ-телеграмм канале. Данные проблемы обосновывались большим количеством заявок, и электронный портал не выдержал данную нагрузку [196], однако, еще раз необходимо отметить, что Казахстан - страна с небольшим населением сравнительно с другими странами. Таким образом, можно отметить о низком качестве оказываемых государственных онлайн услуг. Существуют также риски природных катаклизм техногенного характера, которые физически могут навредить техническим средствам (ЦОД).

Сводные результаты PEST и SWOT данных представлены в таблице 10. SWOT анализ представляет сильные и слабые стороны, а также потенциальные возможности и угрозы. Факторами PEST анализа является политические, экономические, социальные и технологические показатели.

Таблица 10 – Перекрестная таблица результатов проведенного PEST и SWOT анализа

SWOT/PEST	Сильные стороны /S	Слабые стороны /W	Потенциальные возможности /O	Потенциальные угрозы /T
1	2	3	4	5
ПОЛИТИЧЕСКИЕ /P	- политическая стабильность в стране согласно данным TheGlobalEconomy .com - политика международной торговли - Концепция кибербезопасности - план реализации Концепции кибербезопасности - государственная программа «Цифровой Казахстан»	- государственное регулирование (отсутствие закона о Кибербезопасности) - возможная политическая нестабильность в связи с пандемией COVID-19 - негибкий подход в разработке и реализации ИТ решений может не учесть желание услугополучателей	- возможность развивать и поддерживать отечественные ИТ решения на законодательном уровне - возможность реализации пилотных ИТ проектов и развивать отечественное облачное хранилище - применение новых технологий, разработанные отечественными ИТ экспертами	- снижение доверия населения к государственным цифровым сервисам (утечка конфиденциальных данных физических и юридических лиц) - низкое качество оказываемых государственных онлайн услуг - «цифровое неравенство» в обществе
ЭКОНОМИЧЕСКИЕ /E	- возможный темп роста экономики при реализации востребованных и конкурентоспособных ИТ решений отечественными разработчиками программного обеспечения	- возможная девальвация национальной валюты и инфляция - высокая конкуренция стран в разработке ИКТ решений	- выход на мировой рынок по разработке программного обеспечения	- недобросовестная конкуренция внутренних и внешних игроков ИТ рынка

Продолжение таблицы 10

1	2	3	4	5
СОЦИАЛЬНЫЕ /S	- увеличение выделяемых государственных грантов для получения технического высшего образования в отечественных и зарубежных ВУЗах - возможное повышение компьютерной и киберграмотности населения	- низкий уровень компьютерной и киберграмотности населения - ограниченные трудовые ресурсы высококвалифицированных ИТ специалистов - вопросы привлечения квалифицированных специалистов в отдаленные регионы Казахстана	- возможные изменения стиля, образа жизни населения после пандемии COVID-19 - повышение осведомленности потребителей цифровых услуг - привлечение талантов	- потеря и взлом государственных критически важных информационных систем, банк данных, риски хакерских атак
ТЕХНОЛОГИЧЕСКИЕ /T	- доступность новых технологических решений - возможность привлечения инновационных идей в глобальном масштабе	- зависимость от ближнего и дальнего зарубежья ИТ решений - низкий уровень ИТ инфраструктур	- продвижение и производство отечественных ИТ решений	- устаревшая техника и ИТ инфраструктура - использование нелицензионных программ (пиратские ПО)
Примечание – Составлено автором				

Итоги PEST и SWOT анализа. В настоящее время, Казахстан, как и многие другие страны, осуществляет свое развитие с акцентом на внедрение передовых технологий, стремясь повысить эффективность государственного управления.

На основании проведенного PEST и SWOT анализа, нами предлагается конкретный перечень мероприятий в целях повышения обеспечения кибербезопасности в Республике Казахстан (таблица 11).

Таблица 11 – Перечень мероприятий по повышению обеспечения кибербезопасности в Республике Казахстан

Цель	Мероприятие	Необхо-е ресурсы
1	2	3
Разработать национальную стратегию кибербезопасности Казахстана	Уполномоченному органу совместно с заинтересованными сторонами (КНБ, НБ, МФ, МНЭ, общественные объединения и др.) определить четкие цели и задачи по обеспечению безопасности киберпространства Казахстана (разработать проект стратегии на основе изученного международного опыта с привлечением отечественных независимых экспертов)	Финансо-вых затрат не требует
Разработать Закон «О Кибербезопасности»	Уполномоченному органу совместно с заинтересованными сторонами (КНБ, НБ, МФ, МНЭ и др.) разработать проект Закона на основе опыта успешных стран в области кибербезопасности, как США, Сингапур, Великобритания, Эстония, Литва. (разработать проект Закона на основе изученного международного опыта с привлечением отечественных независимых экспертов)	Финансо-вых затрат не требует
Искоренить недобросовестную конкуренцию внутренних и внешних игроков в ИТ рынке	Агенству по защите и развитию конкуренции РК совместно с уполномоченным органом координировать и пересекать деятельность недобросовестных конкурентов в внутреннем рынке РК. На законодательной основе предусмотреть поддержку и продвижения отечественных ИТ решении.	Финансо-вых затрат не требует
Быть конкурентоспособным в разработке ИКТ решений	Всем государственным органам в рамках своей специфики мониторить внешний рынок касающихся их деятельности и проводить мероприятия в целях выявления инновационных идей среди молодежи. Мониторить комментарии пользователей государственных онлайн сервисов	В рамках предусмот ренного годового бюджета органи-зации

Продолжение таблицы 11

1	2	3
Искоренить «цифровое неравенство» в обществе	Уполномоченному органу совместно с МИОР РК, МОН РК проводить пропаганду и образовательные мероприятия посредствам СМИ и социальных сетей в целях ознакомления всех слоев населения происходящими изменениями и новшествами в рамках реализации ГП «Цифровой Казахстан» и Концепции кибербезопасности	Финансовых затрат не требует.
Приоритизировать государственные критически важные ИС в целях распределения финансовых средств в рамках сопровождения данных систем	В целях совершенствования системы кибербезопасности предлагается внести дополнение в ПП РК от 8 сентября 2016 года № 529 «Об утверждении Правил и критериев отнесения объектов информационно-коммуникационной инфраструктуры к критически важным объектам информационно-коммуникационной инфраструктуры» определить критически важные объекты информационно-коммуникационной инфраструктуры принимая во внимание показатели классификации объектов информатизации согласно Приказа и.о. Министра по инвестициям и развитию РК от 28 января 2016 года № 135 «Об утверждении Правил классификации объектов информатизации и классификатор объектов информатизации». Таким образом, приоритизировать государственные критически важные ИС согласно нижеследующих критериев от 5 до 1: – Критичный -5; – Серьезный – 4; – Высокий – 3; – Средний – 2; – Низкий – 1.	Финансовых затрат не требует

Продолжение таблицы 11

1	2	3
Обеспечить защиту государственных критически важных ИС и минимизировать риски хакерских атак	АО «ГТС» КНБ совместно KZ-CERT разработать план реагирования на возможные киберугрозы и на постоянной основе обновлять план реагирования, так как технологии и их возможности меняются очень быстро. Тестировать и проверять уровень безопасности государственных критически важных ИС.	В рамках предусмот-ренного годового бюджета организации
Использовать лицензионные программы, а также обновлять ИТ инфраструктуру	Организовать доступные образовательные онлайн курсы, объясняющее важность использования лицензионных ПО. Каждые 3 года проводить инвентарные работы и другие мероприятия в целях обновления ИТ инфраструктур организации	В рамках предусмотре нного годового бюджета организации
Повысить уровень компьютерной и киберграмотности населения	МОН РК совместно ВУЗами РК привлекая высококвалифицированных экспертов в области ИТ и кибербезопасности разработать программы для программ подготовки бакалавр, магистратура и докторантура по специальности ИТ и информационная безопасность	В рамках предусмотре нного годового бюджета организации
Повысить уровень компьютерной и киберграмотности действующих государственных служащих в РК	Академии государственного управления при Президенте РК разработать обучающие специализированные краткосрочные курсы для действующих государственных служащих по следующим уровням: *1этап. для вновь поступающих на госслужбу – «Основы кибербезопасности»;* *2 этап. для всех действующих госслужащих – «Базовый курс кибербезопасности»;* *3 этап. по выбору – «Специалист аналитик по кибербезопасности».*	В рамках предусмотре нного годового бюджета организации

Продолжение таблицы 11

1	2	3
Привлечь высококвалифицированных ИТ специалистов в отдаленные регионы	Министерству труда и социальной защиты населения РК совместно с МИО предусмотреть и обеспечить социальными пакетами (жилье, достойная заработная плата, санаторно-курортные расходы, медицинская страховка и др.) высококвалифицирован-ных ИТ специалистов	За счет приглашающей организации и МИО
Упростить реализацию ИТ проектов и выделяемых финансовых средств, повышая персональную ответственность проектных менеджеров и балансосодержателя	На законодательном уровне обоснованно определить приоритетные инвестиционные проекты в разработке и реализации ИТ проектов, включая проекты информационной безопасности с учетом экономической ситуации в Республике Казахстан	В рамках предусмотренного годового бюджета организации
Примечание – Составлено автором		

На основании вышеизложенного, предполагается, что проведение системных работ в рамках реализации вышеуказанных мероприятий обеспечит:

- во-первых, последовательное решение проблем, которые сегодня существуют в Республике Казахстан в области информационных технологий;

- во-вторых, совершенствование механизма системы кибербезопасности в Республике.

В этой связи, нами предполагается, что в целях качественной реализации вышеназванных мероприятий по обеспечению кибербезопасности, проблема должна рассматриваться правительством, с привлечением научных институтов, частных секторов, общественных объединений, гражданского общества и независимых экспертов, как это практикует Великобритания.

3 ПУТИ ПОВЫШЕНИЯ КИБЕРБЕЗОПАСНОСТИ В РЕСПУБЛИКЕ КАЗАХСТАН

3.1 Совершенствование системы управления обеспечения кибербезопасности в Республике Казахстан

Вопросы кибербезопасности в настоящее время являются одними из злободневных проблем в государственном управлении, и многие политики предлагают и пытаются внедрить инновационные идеи в целях защиты информации в киберпространстве. Необходимо отметить, что развитые и развивающиеся страны заинтересованы и активно внедряют цифровые технологии. Многие страны стремиться конкурентоспособными и создавать безопасные и благоприятные условия своим гражданам. Согласно стратегии «Казахстан-2050» целью, которой является вхождение в первую 30-ку конкурентоспособных стран мира [56]. Седьмым вызовом данной стратегии предусмотрено использование инновационных технологий. Применение цифровых технологий способствует транспарентности и гибкости оказываемых государственных услуг. Ранее отмечалось, что цифровизация несет за собой риски и угрозы в киберпространстве. Обеспечение кибербезопасности требует широкого спектра действий от международного до индивидуального уровня. Необходимо рассмотреть вопрос тесного сотрудничество с международными странами по борьбе с киберпреступниками, так как это повлияет на рейтинг страны в конкурентном рынке. Анализируя состояние кибербезопасности Казахстана через призму цифровизации выявлены ряд преимуществ и недостатков благодаря комментариям респондентов – 539, которые проявили интерес.

Таким образом, проведенный анализ показал, что обеспечение кибербезопасности на национальном и местном уровнях Республики имеет положительные тенденции на социально-экономическое развитие страны в условиях глобальной цифровизации. На сегодня в Казахстане большинство государственных услуг оказывается в режиме онлайн, и персональные данные граждан страны с момента рождения находятся в цифровом пространстве, и за их безопасность ответственны правительственные и квазигосударственные организации.

Проведенное исследование показало, что обеспечение кибербезопасности требует комплексного организационно-управленческого подхода. Так, кибербезопасность - это командная работа, и у каждого есть своя роль. Правительству необходимо рассмотреть возможность инициации по развитию кибербезопасности в Казахстане с привлечением общественности, квазигосударственного и частного сектора при реализации ИТ решении. В целях достижения эффективного результата потребуется построить доверительное сотрудничество между всеми заинтересованными сторонами, такими как: интернет – провайдеры, научные институты и независимые эксперты, правоохранительные органы, квазигосударственные и частные учреждения, СМИ, граждане, ГЧП, отраслевая группа реагирования на

инциденты компьютерной безопасности (ЦАРКА и др.). Кибербезопасность является ответственностью государства и индивида с вышеперечисленными заинтересованными сторонами в команде. В соответствии многочисленным комментариям респондентов в рамках реализации Концепции кибербезопасности в первую очередь необходимо просвещать общественность о происходящих изменениях в киберпространстве. Полагается, что это один из наиболее эффективных методов предотвращения возможных неудач. Вместе с тем, необходимо усилить работу правительства по борьбе с киберпреступностью с учетом ее транснационального характера. В последующем считаем целесообразным рассмотреть нормы законодательства и деятельность правоохранительных органов и судов в Республике в части касающихся вопросов кибербезопасности. Считаем, что вышеназванные мероприятия также будут способствовать повышению статуса и стабильности Казахстана на международной арене как надежного хаб - центра в ИТ индустрии. Однако, для достижения этих целей необходимо тесно работать с партнерами дальнего и ближнего зарубежья, научными институтами, правительствами и неправительственными отраслевыми партнерами, а также интернет-провайдерами.

На основании изложенного и изученного опыта международных стран определены следующие системы государственного управления по совершенствованию вопросов кибербезопасности в РК:

1. управление, решение непредвиденных кризисных ситуаций с заинтересованными сторонами;
2. нормотворчество, нормативно - регуляторные системы, учитывая международные требования и стандарты, такие как GDPR и пр.;
3. технологии (контрольные и координационные меры для выявления, управления и устранения возможных кибер рисков);
4. человеческий фактор (развитие культуры безопасности в обществе, который включает знания, навыки и коммуникации);
5. бизнес-процессы, управление кризисом (разработка плана реагирования на компьютерные инциденты);
6. разработка специальной платформы совместно с ГЧП, где оперативно и в безопасном режиме будут обмениваться информациями государственные и частные сектора о возможных киберугрозах на цифровом пространстве Республики, что в свою очередь минимизирует катастрофических последствии от киберинцидентов;
7. использовать инструменты краудфандинга в инвестировании проектов в области цифровизации для поддержки малого и среднего бизнеса. Вместе с тем краудфандинг целесообразно рассмотреть для закупа лицензионных ПО для малого и среднего бизнеса в целях снижения использования пиратских ПО, то есть рассмотреть корпоративный метод закупа лицензионных ПО. Данный метод является более рентабельным для малого и среднего бизнеса. Более того, это повысит рейтинг страны в использовании лицензионных ПО, так как на сегодняшний день более 73% Казахстанцев используют пиратские ПО, что в

свою очередь повышает риск киберугрозам [220, с. 15]. Рассмотрим некоторые вышеперечисленные направления по отдельности.

Управление. В своем послании народу Казахстана от 2 сентября 2019 года Президент страны Касым-Жомарт Токаев подчеркнул, что благополучные экономические реформы, возможно достичь путем модернизации общественного и политического сознания людей [197]. Вместе с тем, Президент призывает граждан Казахстана двигаться ускоренными темпами. Его посыл понятен, так как в период глобальной цифровизации общественное сознание и методы решения проблем меняются прогрессивными темпами, и нам необходимо быть в потоке быстро меняющегося мира, что поможет сохранить и приумножить нашу конкурентоспособность Казахстана среди других успешных стран мира.

Вместе с тем, 10 апреля 2020 года Касым-Жомарт Токаев отметил о проблемных аспектах реализации программы «Цифровой Казахстан». Обратил внимание о неготовности Правительства к вызовам, причиненной пандемией COVID-19. Например, проблемы по выдаче социальных выплат, по его мнению, ответственными лицами в недостаточной степени были отработаны механизмы выплат в целом, которые включают в себя технические, технологические проблемы, а также нормативно-правового характера и неотработанный бизнес-процесс государственных органов. За получением социальных выплат в размере 42 500 тенге всего обратилось около 2 миллиона граждан Казахстана и большинство из них свои обращения оставили в электронном формате. Он также отметил о неготовности системы образования к дистанционному формату обучения, как в школах, так и в ВУЗах, что привело к прохождению уроков посредством телевидения. Президент страны также отметил о системных недоработках образовательной платформы e-Learning и электронного правительства E-gov. Однако, в рамках реализации данных проектов было выделено немало средств из казны государства. В заключении своего выступления он поручил разработать план действий по улучшению качества и повышению эффективности ИТ инфраструктуры страны без привлечения дополнительных затрат [198].

В связи с этим, считаем целесообразным рассмотреть возможность использования всех инструменты государственного управления в целях снижения внешних и внутренних киберугроз. Лидеры нации несут ответственность за безопасность свих граждан, а также за разработку стратегии кибербезопасности и содействие развитию местного, национального и глобального меж секторального сотрудничества. Международный опыт и результаты исследования показывают, что Казахстану необходимо рассмотреть вопрос разработки Национальной стратегии кибербезопасности, которая включает в себя следующие приоритетные направления:

- конфиденциальность;
- гражданская осведомленность;
- защита критически важной информационной инфраструктуры;
- оценка риска;

- улучшить учебные и образовательные программы;
- установить базовые требования к цифровой безопасности;
- установить возможность реагирования на инциденты;
- установить институционализированную форму сотрудничества между государственными органами;
- участвовать в международном сотрудничестве;
- НИОКР (исследование и развитие);

В настоящее время в Республике политикой обеспечения кибербезопасности занимается КИБ МЦРИАП РК, тогда как вопросами формирования, обеспечения и развития ИБ информационного пространства и инфраструктуры связи РК непосредственно занимается АО «ГТС» КНБ РК. Необходимо отметить, что деятельность КИБ МЦРИАП РК направлена не только на политику обеспечения кибербезопасности, но и на вопросы телекоммуникации и связи, электронного правительства, государственные онлайн услуги, электронной промышленности, инноваций. В ходе онлайн опроса респондентам был задан вопрос: *«Есть ли необходимость изменения существующей организационной структуры взаимодействия государственных учреждений и уполномоченных органов, которые обеспечивают процессы политики кибербезопасности?».* В рисунке 17. результат опроса показывает, что около 85% респондентов за изменение существующей организационной структуры взаимодействия государственных учреждений, обеспечивающее процессы политики кибербезопасности и это вполне объяснимо. Государственные учреждения, которые занимаются вопросами электронного правительства (цифровизация государственных услуг) одновременно занимаются сопровождением законодательной политики обеспечения кибербезопасности. Предполагается, что в ходе деятельности МЦРИАП РК могут возникнуть внутренние конфликты интересов. Например, автор книги «Cybersecurity Program Development for Business: The Essential Planning Guide» Московит С., отмечает, что организация, который занимается вопросами цифровизации недолжен заниматься одновременно обеспечением вопросов кибербезопасности. Для полного понимания он это объясняет следующим образом: *«Проведение клинического исследования (тестирования) препарата, финансируемого производителем самого препарата».* Таким образом, он обозначает, что организация, которая занимается вопросами цифровизации недолжна отвечать за безопасность в киберпространстве.

На основании изложенного, считаем целесообразным рассмотреть вопрос выведении функции касающейся деятельности кибербезопасности из МЦРИАП РК в целях предотвращения конфликта интересов внутри одного государственного учреждения. Вместе с тем, предлагаемая идея возможно повысит качество разрабатываемых нормативно-правовых, стратегических и программных документов в сфере обеспечения кибербезопасности в стране. Например, Концепция кибербезопасности Республики, в которой больше всего рассматривается международный опыт и ключевые проблемы кибербезопасности, период реализации разделен на 2 этапа:

- 2017-2018 годы в 1ом этапе;
- 2019-2022 годы во 2ом этапе.

Необходимо отметить, что в Концепции предусмотрено перечень мероприятий в рамках первого этапа, тогда как перечень мероприятии на второй этап не предусмотрен. Таким образом, по факту Концепция разработана для реализации работ на 2017-2018 годы, при этом некоторые показатели, которые предусмотрены достичь в 2022 году были перевыполнены в 2018 году.

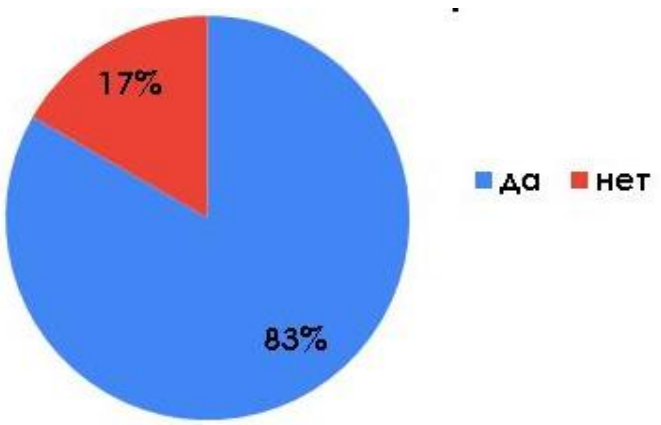

Рисунок 17 – Результат онлайн опроса на вопрос «Есть ли необходимость изменения существующей организационной структуры взаимодействия государственных учреждений и уполномоченных органов, которые обеспечивают процессы политики обеспечения кибербезопасности в РК?»

Примечание – Составлено автором

Необходимо также отметить, что данный документ на 02 ноября 2020 года не обновлялся, то есть новых задач и изменений не вносилось. В этой связи, можно полагать о низком качестве разработанного правительственного документа. Действующая структура государственного управления Казахстана отражена в подразделе 2.2 Анализ действующих механизмов использования и внедрения кибербезопасности данной диссертационной работы.

Например, если рассмотреть Агентство кибербезопасности и инфраструктурной безопасности США (CISA), то данное Агентство является национальным консультантом по рискам, работающим с партнерами для защиты от кибер угроз и сотрудничающим в создании более безопасной и устойчивой инфраструктуры для будущего [199]. Национальное агентство кибербезопасности (NACSA) Малайзии было официально создано в феврале 2017 года в качестве национального ведущего агентства по вопросам кибербезопасности с целью обеспечения и укрепления устойчивости к угрозам путем координации и консолидации лучших национальных экспертов и ресурсов в области кибербезопасности [200].

Таким образом, на основании изученного международного опыта, а также согласно рекомендациям опрошенных респондентов предлагается передача функции деятельности, касающейся обеспечения кибербезопасности полностью

на вновь созданную независимую специальную службу - Агентство по кибербезопасности РК. Предполагается, что предложенное Агентство повысит эффективность и качество проводимой политики кибербезопасности в стране путем независимого и оперативного исполнения возложенных на них функциональных обязанностей.

Предлагаемое изменение в организационную структуру уполномоченных органов по вопросам кибербезопасности повысит значимость и важность цифровой безопасности, персональную ответственность руководителей и исполнителей данного подразделения, которые будут отвечать за качество разрабатываемых НПА Республики Казахстан в сфере кибербезопасности и своевременно вносить соответствующие изменения и дополнения (рисунок 18). Развивать международное сотрудничество непосредственно правительственными и неправительственными организациями касательно вопросов обеспечения кибербезопасности.

Нормотворчество. Нормотворческая деятельность является одним из важных направлений в совершенствовании обеспечения кибербезопасности. Проведенное исследование показало, что успешные страны в области кибербезопасности имеют свою Национальную стратегию, а также Закон о кибербезопасности. На сегодняшний день обеспечение кибербезопасности Казахстана осуществляется в рамках Концепции киберщит Казахстана, а также непосредственно согласно плану реализации данной Концепции на 2018 – 2022 годы Тенденции в период глобальной цифровизации меняются. Казахстан, как и другие страны, внедряет технологии «Умного города – Smart cities», применяют большие данные – big data, рассматривают новые технологии, как блокчейн (blockchain) и пр.. Вместе с тем, есть и международные соглашения и требования, которые необходимо соблюдать. Одно из последних требований – это документ, принятый Европейским Союзом, где рассматривается обеспечение безопасности персональных данных граждан Европы.

В целях соблюдения и защиты интересов граждан страны в будущем необходимо разработать закон о кибербезопасности.

В настоящее время разработка законопроекта о кибербезопасности необходимая мера, которая будет обеспечивать безопасность интересов граждан в киберпространстве, а также повысит их ответственность за действия, направленные на дестабилизацию жизненно важных цифровых инфраструктур страны. Законопроект также предназначен для надзора и поддержания национальной кибербезопасности Казахстана, а также соответствовать международным стандартам, соглашениям и требованиям, как GDPR. Более того, в законопроекте необходимо предусмотреть понятие «киберстрахование» и дать четкое определение термину «кибербезопасность», а также защите, приему и передаче биометрических персональных данных при получении онлайн государственных услуг.

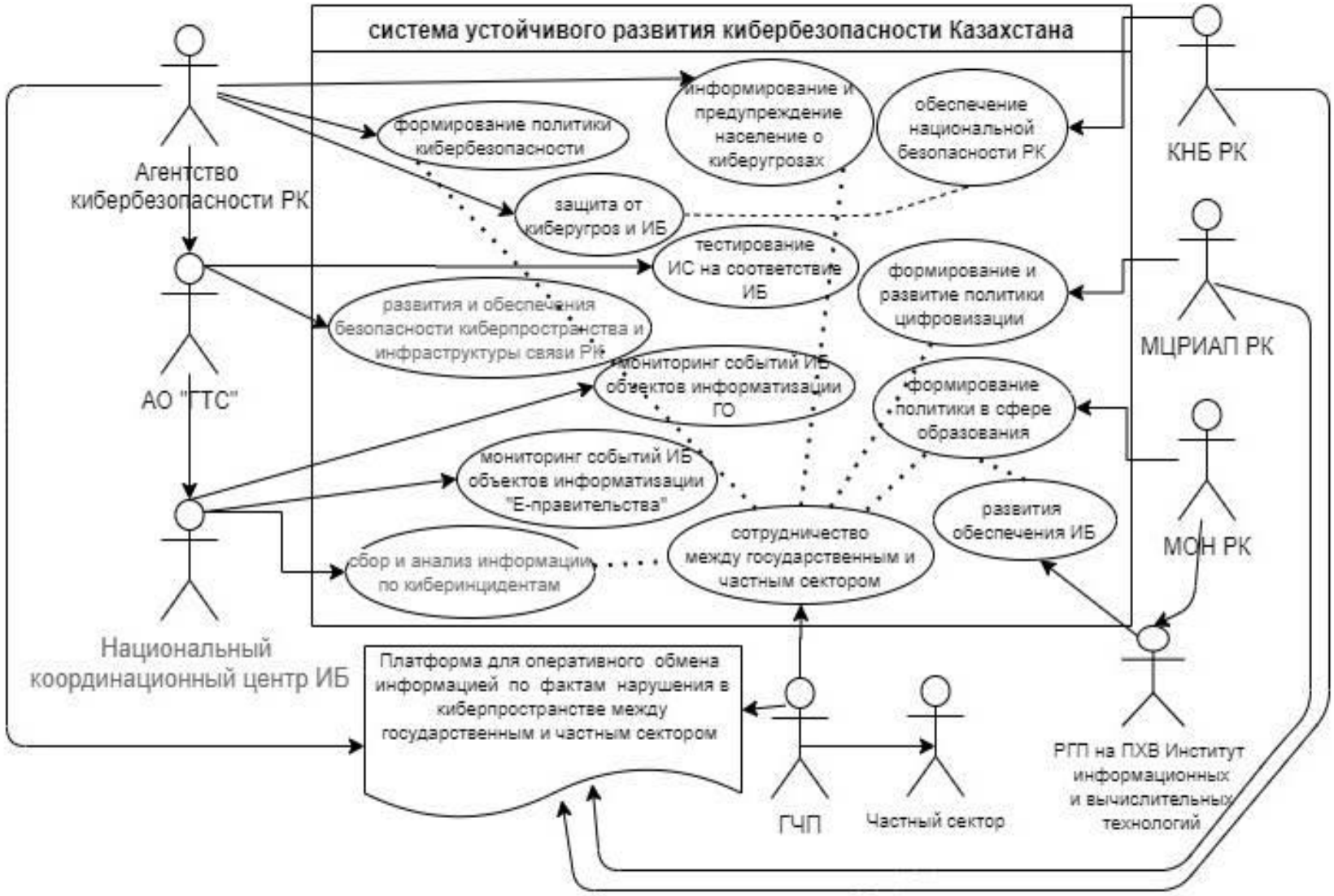

Рисунок 18 – Предлагаемая архитектура системы государственного управления кибербезопасности Казахстана

Примечание – Составлено автором

.

В ходе опроса респондентами более часто предлагались следующие идей (рисунок 19).

Рисунок 19 – Часто предлагаемые рекомендации и комментарии респондентов

Примечание – Составлено автором

Технологии. Стандарт ISO / IEC 27000 является наиболее широко признанной системой управления информационной безопасностью ISMS. На основании ISO / IEC 27000 предлагается применить следующий процесс управления рисками (рисунок 20):

Рисунок 20 – ISO/IEC Процесс управления рисками

Примечание – источник [201, с. 78]

Человеческий фактор. В организациях необходимо поощрять и мотивировать коллективную ответственность за кибербезопасность. Действия одного специалиста могут повлиять на коллективную безопасность в организации. На данном этапе правительством выделяются государственные гранты в целях формирования профессиональной рабочей силы, тем не менее, необходимо поощрять действующих специалистов кибербезопасности развивая их квалификацию и определяя им более четкие пути карьерного роста. Предполагается, что данная методика позволит создать сильное и киберграмотное сообщество практиков в стране.

Более того, необходимо рассмотреть возможность увеличения количества грантов по международной программе «Болашак» для перспективных и амбициозных студентов в сфере ИБ и ИТ. Рассмотреть возможность присуждения стипендий для получения сертификатов в международных специализированных научно-исследовательских организациях в области кибербезопасности по программе «Болашак». Обеспечение безопасности в киберпространстве требует высококвалифицированных экспертов в данной сфере. Ранее отмечалось, что не только в Казахстане проблемы с нехваткой высококвалифицированных специалистов области кибербезопасности, но и во всем мире. В нынешнее время квалифицированные эксперты пользуются большим спросом, так как бизнес все больше внимание уделяет киберрискам. Спрос к специалистам в области кибербезопасности будет только расти, так как практически во всех отраслях жизнедеятельности внедряются цифровые технологии. В целях обеспечения Казахстанского рынка специалистами, которые имеют глубокие знания в сфере ИБ, необходимо предусмотреть вышеуказанные мероприятия. Вместе с тем, необходимо установить четкие карьерные траектории и возможность сертифицировать специалистов за счет организации с последующей отработкой в данной организации в зависимости от вложенных финансовых средств.

Вместе с тем, отечественным ВУЗам на постоянной основе необходимо обновлять учебную программу согласно новым трендам и стандартам, происходящим в глобальном цифровом мире, так как профессия кибербезопасность развивается быстрыми темпами. На сегодняшний день специализация в области кибербезопасности включает в себя реагирование на киберинциденты, тестирование на проникновение, оценка и анализ угроз, управление рисками и многие другие сопутствующие специализации.

Бизнес-процесс, управление кризисом. Юридические и физические лица должны быть постоянно информированы и принимать соответствующие меры для обеспечения безопасности своих информационных систем и цифровых устройств. Вместе с тем, необходимо рассмотреть возможность расширения преимущества Казахстана в области кибербезопасности за счет отечественных компаний в сфере ИТ. Необходимо развивать ИТ отрасль, привлекая компании с передовыми возможностями, развивать стартапы, так как это даст возможность развитию отечественного рынка для вывода ИТ решений на мировой уровень под маркой «Сделано в Казахстане». Однако, необходимо

помнить, что в ИТ индустрии уже имеются сильные конкуренты с богатым опытом, чем Казахстан. В этой связи, Казахстану будет нелегко, но несмотря на это необходимо внедрять инновации в целях ускорения роста ИТ отрасли.

Более того, возможно необходимо проанализировать принятие опыта Сингапура в части привлечения молодых высококвалифицированных специалистов с ИТ стартап проектами. Рассмотреть внедрения их опыт по выдаче виз для граждан, имеющих техническое образование с престижных ВУЗах мира.

Кроме того, целесообразно рассмотреть и принять опыт Литвы и Великобритании сфере организации образовательных программ для действующих специалистов. Разработка и принятий национальной стратегии кибербезопасности, а также закона о кибербезопасности. Утвердить свои план управления киберинцидентами, который устанавливает процедуры управления, определяет категорий, расследует и анализирует киберинциденты. Вместе с тем, проанализировав рынок оплаты труда других стран возможно необходимо рассмотреть повышении заработной платы для ИТ специалистов.

3.2 Разработка рекомендации по обеспечению кибербезопасности в Республике Казахстан

Цифровая технология является неотъемлемой частью нашей жизни, однако, на данном этапе, как и многие другие страны, Казахстан переживает нелегкий период из-за пандемии COVID-19. Пока мир нацелен на здоровье своих граждан и экономику, киберпреступники во всем мире, несомненно, извлекают выгоду из этого кризиса и пандемии COVID-19. В период карантина многие люди начали использовать онлайн сервисы. Соответственно за этот период активизировались интернет мошенники, а также хакеры в черных шляпах [202]. Вопросы социальной инженерии стали обсуждаться более активно, чем раньше, так как поток фишинговых атак увеличились. С начала чрезвычайного положения KZ-CERT зарегистрировало более 3 000 киберинцидентов, из них более 400 являются фишинговыми атаками [203; 204]. Под фишингом понимается интернет мошенничество в целях получения идентификационных и персональных данных пользователей Интернет [205]. На сегодняшний день фишинговых атак, а также распространения ложной информации в сети Интернет происходит намного чаще и быстрее, чем распространение вируса COVID-19. Данное явление происходит в масштабе всего мира и в том числе в Казахстане. На своем официальном сайте АО «ГТС» КНБ РК предлагает рекомендации по снижению риска кибератак, так как многие организации и предприятия в период чрезвычайного положения начали работать дистанционно. Однако, не многие знают об этих инструкциях. АО «ГТС» КНБ РК предлагается предусмотреть трансляции своих инструкций во всех социальных сетях, а также через СМИ и телевидение. В результате отдаленные регионы Казахстана могут ознакомиться с этими инструкциями через телевидение. Более того, инструкции должны быть четкими и понятными для всех слоев населения, то есть использовать инструменты визуализации

(видеоролики и инфографики). Некоторые граждане преклонного возраста не имеют возможность читать, но на официальном сайте АО «ГТС» КНБ РК все инструкции доступны только в печатном виде. Более того, у читателей инструкции на сайте АО «ГТС» КНБ РК нет возможности поделиться /распространять данную информацию с коллегами, друзьями и знакомыми в различных социальных сетях. Например, полезная инструкция для пользователей Интернет, опубликованная на сайте АО «ГТС» КНБ РК http://sts.kz/ru/node/391 и http://sts.kz/ru/node/393, невозможно поделиться в социальных сетях, таких как Twitter, Facebook, Instagram, Linkedin и прочее. Считаем в данном направлении АО «ГТС» КНБ РК целесообразно рассмотреть возможность размещения иконок социальных сетей, таких как Facebook, Twitter, Instagram, Linkedin и др. Это даст возможность поделиться важной и востребованной информацией в целях ознакомления и предупреждения граждан Казахстана о возможных и актуальных угрозах в киберпространстве. Данная рекомендация не требует финансовых вложений, так как распространение информации в социальных сетях происходит бесплатно.

На рисунке 21 нижняя часть окна скиншота официального сайта АО «ГТС» КНБ РК, в ней необходимо разместить значки социальных сетей в целях распространения полезной информации среди пользователей сети Интернет.

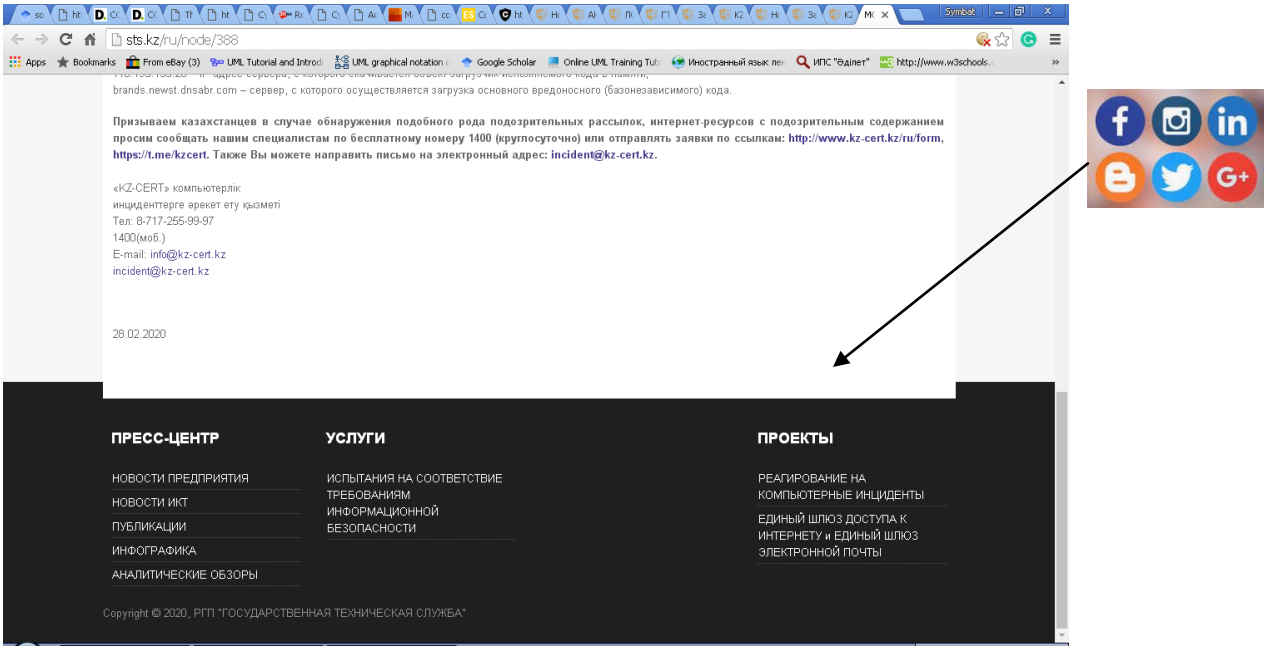

Рисунок 21 – Скриншот официального сайта АО «ГТС» КНБ РК на 25.05.2020г.

Примечание – Источник: http://sts.kz/ru/node/388

Более того, АО «ГТС» КНБ РК в период чрезвычайного положения на официальном сайте опубликовало 5 вредоносных мобильных приложений, более 10 интернет ресурсов и 5 зараженных файлов для ОС Windows [206]. В период чрезвычайного положения у пользователей Интернет появился огромный интерес к вирусу COVID -19. При поиске информации о

коронавирусе пользователи цифровых гаджетов на своих устройствах могли запустить эти вредоносные программные обеспечения сами того не зная. В этой связи, АО «ГТС» КНБ РК предлагается развивать ознакомительно-пропагандную работу с применением инструментов визуализации в целях восприятия информации для разных слоев населения. То есть информация должна быть понятной и доступной как для школьников начальных классов, так и для людей пожилого возраста, которые пользуются смартфонами.

Таким образом, следующей практической рекомендацией для АО «ГТС» КНБ РК является принятие опыта Сингапура и Великобритании, где доступно применяют инструменты визуализации. Возможно, некоторые граждане Казахстана с отдаленных регионов не знают о деятельности данной организации, где они могут ознакомиться о возможных киберугрозах и инцидентах (вирусы, фишинговые атаки, интернет мошенники, подозрительные сайты), которые распространяются по просторам Интернет.

Более того, в первой половине мая месяца 2020 года на сайты государственных органов были направлены DDoS – атаки из 48 стран мира и из ранних IP-адресов. Эти атаки также были зарегистрированы АО «ГТС» КНБ РК [207]. Вместе с тем, за период чрезвычайного положения было много рассылок ложного происхождения. В этой связи, в период пандемии предлагаются следующие меры безопасности в киберпространстве:

- организации должны обеспечить безопасность и надежность услуг VPN (использование virtual private network - виртуальная частная сеть), поскольку этот метод подключения к Интернет более безопасен. Кроме того, сотрудники не должны использовать персональные компьютеры в служебных целях;

- организациям рекомендуется информировать своих сотрудников об ИБ за пределами офиса, и сотрудники не должны подключаться к Интернет незащищённого/открытого доступа;

- организация должна обучать своих сотрудников к возможным киберугрозам, то есть образованность, и осведомленность сотрудников даст возможность максимально избежать киберинциденты. Например, персоналу необходимо помочь определить сомнительные электронные письма с вложениями, который поступают на их электронную почту с ссылками на веб-сайты и файлами, которые могут содержать фишинговые атаки (письма, файлы, ссылки и сообщения), показывая типичные примеры атак и предоставляя советы по распознаванию приманок (рисунок 22). Развивать у сотрудников уверенность, и при возникновении каких-либо проблем они могли открыто сообщать о возникшей проблеме на рабочей станции;

- сотрудники регулярно должны делать резервные копии выполненных им работ, а также всех критических ИС и проверять целостность резервных копий;

- ограничивать сотрудников в использовании не нужных ПО, которые не используются в работе (просмотр фильмов и разного рода игр, использование различного вида видеоконференц связей и прочее);

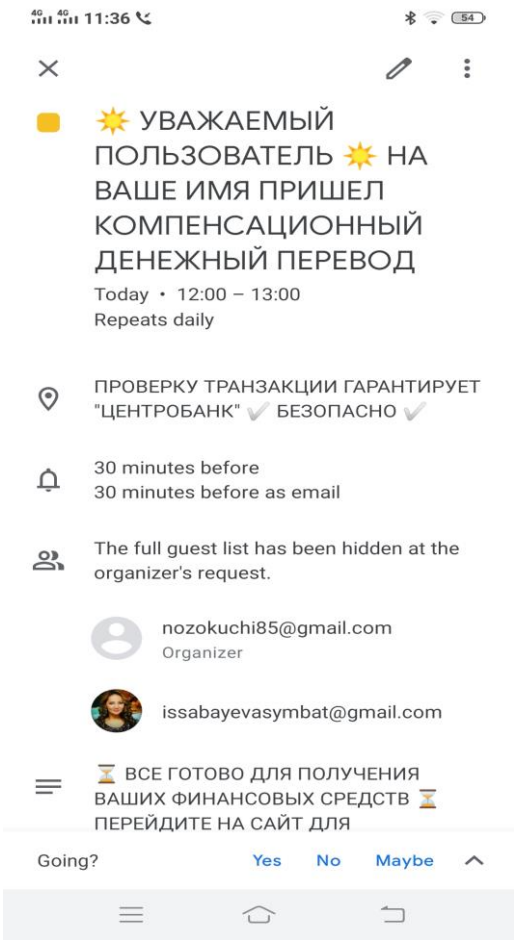

Рисунок 22 – Скриншот программ вымогателей в период пандемии COVID-19

Примечание – Источник: личный опыт.

- самое важное, граждане Казахстана должны быть адаптивными к изменяющимся процессам, что поможет более безболезненно воспринимать происходящие изменения;

- сотрудники организации должны установить надежные пароли и предпочтительно использовать двухфакторную аутентификацию для всех учетных записей удаленного доступа к инструментам Microsoft Office 365;

- отключите USB-накопители, чтобы избежать риска вредоносных программ.

- обеспечить на корпоративных ноутбуках и компьютерах использование лицензионных антивирусных и других ПО с последней версией брандмауэра. Так, использование нелицензионного ПО играет немаловажный фактор в обеспечении кибербезопасности. Использование пиратских ПО по всему миру составляет 37% – это всего на 2% меньше, чем в 2016 году [208, с. 15]. Например, уровень пиратства ПО в Ливане в 2015 году составил 70% согласно данным Business Software Alliance (BSA), базирующегося в США. В глобальном масштабе уровень пиратства ПО в Ливане был таким же, как в

Китае, и был выше, чем в Аргентине (69 %), Таиланде (69 %) и Эквадоре (68 %), и ниже, чем в Албании (73 %). Казахстан (73 %) и Панама (72 %) [208, с.15]. В последние годы правительство Казахстана проводит работу по закрытию веб-сайта, незаконно обменивающиеся материалами, защищенными авторским правом, при условии, что правообладатели регистрируют материалы, защищенные авторским правом. Американские компании утверждают, что 73 % ПО используемые в Казахстане являются пиратскими, в том числе в правительственных министерствах, и критикуют усилия правительства по обеспечению соблюдения [209, с. 61].

Согласно Закону Республики Казахстан «Об авторском праве и смежных правах» правонарушением является распространение, продажа, использование и хранение нелицензионного ПО. С 2015 года за нарушение авторских и смежных прав нарушитель привлекается к уголовной ответственности согласно ст. 198 УК РК. По этой статье нарушитель может наказываться штрафом в зависимости от степени тяжести. Один из известных случаев произошёл в ноябре 2017 года. Алмалинский районный суд Алматы признал предпринимателя Утебекова А.У. виновным в приобретении и хранении контрафактных ПО Microsoft, которые продавал в своей торговой точке. По ст. 198, ч. 2, УК РК его приговорили к выплате штрафа.

По официальным данным Министерства юстиции, за 2017 год по итогам деятельности Службы экономических расследований в производстве находилось 228 уголовных правонарушений по факту изготовления, реализации контрафактной продукции (из них по статье о нарушении авторских прав – 179 дел). Основная доля правонарушений этой категории была связана с распространением (установлением) нелицензионных программных продуктов компаний Microsoft («Windows»), Инфософт («1С: Бухгалтерия») и SonyPlayStation. На предмет использования пиратского софта периодически проверяют и представителей бизнеса.

Борьба с вредоносными программами, связанными с нелицензионным ПО, может стоить более $10 000 США на зараженный компьютер, что в целом составляет более $ 359 миллиардов США [210]. Согласно данным исследователей использование нелицензионных программ повышает риски подери корпоративных и личных данных на 46%, несанкционированного доступа - 40%, программ-вымогателей 30%, системного сбоя на 28%, потеря IP на 24%, репутации организации на 20% [211, с. 6]. В этой связи считаем, целесообразным проводить информационно-образовательную работу в части использования лицензионных ПО. В настоящее время, большинство компании предпочитают использовать пиратские ПО в целях экономии финансовых средств не осознавая о масштабных угрозах на основную деятельность их организации. Вместе с тем, необходимо развивать приобретении корпоративных лицензионных программ на большое количество пользователей компьютера, так как данный метод является выгодным для малого и среднего бизнеса. Для достижения этой цели, малому и среднему бизнесу необходимо скооперироваться, применяя метод краудфандинга, то есть, используя

цифровые технологий. Рассмотреть возможность создания официального канала или группы посредством социальных сетей, где можно найти заинтересованных лиц в приобретении лицензионных ПО. Также на рынке существует более 2000 платформ краудфандинга [212, с. 1]. На сегодняшний день краудфандинг успешно применятся в инвестировании инновационных проектов для поддержки малого и среднего бизнеса, таких странах как США, Белоруссия, Россия и др [213, с. 125]. Под краудфандингом подразумевается инвестирование какого-либо проекта, а также финансирование в поддержку бизнеса и благотворительных стартапов и многое другое. Популярными платформами краудфандинга являются Kickstarter, Indiegogo, CircleUp, Gofundme и многое другое [214, с. 2; 215, с. 22; 216 с. 65]. Таким образом, корпоративный метод закупок лицензионных ПО является рентабельным для малого и среднего бизнеса.

Высокая вероятность, что пандемия COVID-19 изменит нашу жизнь с новыми стилями работы, новыми проблемами кибербезопасности. После COVID-19 многим государственным и частным организациям необходимо будет пересмотреть меры по управлению киберрисками.

Пользователи онлайн сервисов очень уязвимы. Предполагается, что уязвимость пользователей интернет-услуг происходит по нескольким причинам:

- во-первых, большинство пользователей Интернет очень доверчивы и не имеют большого опыта использования онлайн сервисов, так как человеческий фактор очень уязвим, и быстро поддается манипуляциям социальной инженерии;

- во-вторых, из-за незнания граждан о возможных киберугрозах. Данное явление еще раз доказывает, что общество Казахстана нуждается в повышении компьютерной грамотности.

Вместе с тем, эксперты KPMG считает, что в период пандемии люди более привержены к киберугрозам, так как удаленная работа значительно увеличивает риск атаки вымогателей. Это увеличение связано с сочетанием более слабого контроля над домашней ИТ системой и более высокой вероятностью того, что пользователи кликнут на вымогательское программное обеспечение COVID-19 [217]. Рисунок 11. один из примеров программ вымогателей в период чрезвычайного положения в стране.

На основании изложенного, предложенные практические рекомендации применимы не только в период пандемии COVID-19, но и в повседневной жизни даст возможность минимизировать риски киберугроз.

Более того, также хочется отметить, что из-за происходящей пандемии COVID-19 практика показывает, что есть целесообразность усиления роли правительства в деятельности реализуемых проектов в области цифровых технологий и кибербезопасности. Вместе с тем, на сегодня существует проблема участившихся киберинцидентов, таких как фишинговых атак, программ вымогателей, DDoS атак. При этом страдают проводимые ознакомительные работы населения с происходящими изменениями в

киберпространстве. Период экономического кризиса и пандемии COVID-19 создал необходимость в ближайшем будущем рассмотреть создание независимого специального государственного органа в целях усиления роли правительства в сфере кибербезопасности. Вновь созданный правительственный орган непосредственно будет заниматься обеспечением кибербезопасности и своевременно принимать соответствующие меры в целях минимизации киберинцидентов. Иными словами, государственное учреждение по обеспечению кибербезопасности будет:

- обеспечивать защиту и безопасность киберпространства Казахстана;
- повышать национальную безопасность и улучшать цифровую экономику, защищая жизнь граждан в цифровом пространстве;
- постоянно контролировать киберпространство на предмет возможных киберугроз;
- защищать критическую информационную инфраструктуру в целях обеспечения непрерывной работы основных цифровых услуг, включая государственных;
- анализировать риски, которые представляют угрозу и принимать соответствующие меры по их минимизации;
- тесно сотрудничать со всеми заинтересованными сторонами в целях обеспечения кибербезопасности;
- расследовать киберинциденты совместно с правоохранительными органами и судами;
- организовывать и проводить краткосрочные образовательные программы по кибербезопасности в целях повышения компьютерной грамотности;
- гарантировать готовность к критическим ситуациям и эффективно, оперативно реагировать на кибератаки;
- нести ответственность за создание более безопасного киберпространства для корпоративных и индивидуальных конечных пользователей;
- предоставлять консультационные услуги по вопросам обеспечения кибербезопасности другим ГУ и частным секторам;
- сертифицировать продукты и проверять гарантии безопасности ИС;
- создавать динамическую экосистему кибербезопасности в целях стимулирования цифровой экономики Казахстана, привлекая высококвалифицированных специалистов с большим опытом исследований и разработок ПО для удовлетворения потребности Республики Казахстан в области безопасности и экономики;
- тесно сотрудничать с международными странами в сфере кибербезопасности;
- сотрудничать с ВУЗами, отраслевыми партнерами и стимулировать инновации в области кибербезопасности, предлагая готовые решения и создавая рабочие места;
- сотрудничать с ВУЗами, отраслевыми партнерами в целях подготовки востребованных специалистов в области кибербезопасности для удовлетворения растущего спроса на защиту цифровой экономики;

- обеспечивать консультативные услуги заинтересованным сторонам для сотрудничества и защиты их от критических уязвимостей;

- разрабатывать НПА и совершенствовать политику кибербезопасности Казахстана не только на территории страны, но и за ее пределами (развивать сеть международных партнеров);

- изучать и принимать передовые методы в области обеспечения кибербезопасности;

- наращивать партнерские отношения с заинтересованными сторонами, в рамках своей компетенции участвовать в научно-образовательных дискуссиях с целью формирования норм ответственного поведения государства в киберпространстве;

- проводить мероприятия и реализовать программы по совершенствованию потенциала в области кибербезопасности;

- проводить информационно-пропагандистские работы в целях повышения осведомленности граждан;

Безусловно, создание ГУ по кибербезопасности внесет свои коррективы в цифровой Казахстан, а именно в части политики реализации ИТ проектов.

Вместе с тем, в целях выявления Казахстанских пользователей онлайн услуг и их отношения к вопросу кибербезопасности был задан следующий вопрос:

«В связи с применением ИКТ, согласны ли вы, что вопрос кибербезопасности является для Вас приоритетом в рамках работы, учебы и жизнедеятельности?». В рисунке 23 видно, что большинство респондентов осознают важность вопроса кибербезопасности в каждодневном использовании онлайн сервисов.

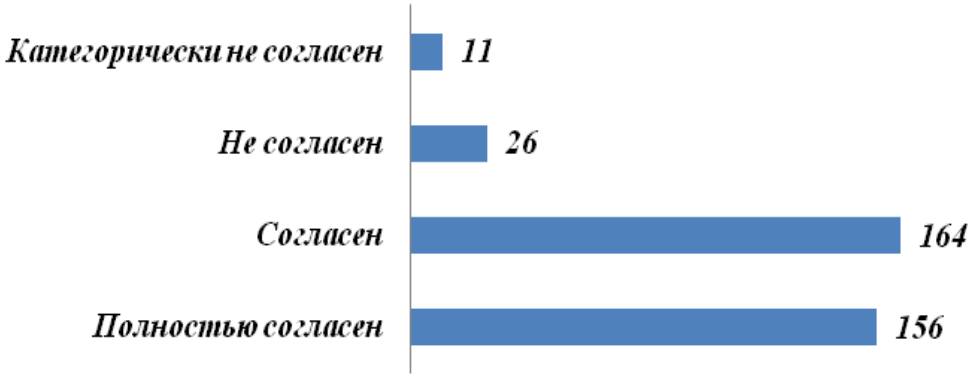

Рисунок 23 – Результат респондентов на вопрос «В связи с применением ИТК, согласны ли вы, что вопрос кибербезопасности является для Вас приоритетом в рамках работы, учебы и жизнедеятельности?»

Примечани – Составлено автором

Однако, необходимо отметить, что большинство респондентов в ходе опроса предлагали ликвидацию киберграмотности и компьютерной грамотности в стране. То есть, по их мнению, большая часть населения не владеет базовыми знаниями и происходящими изменениями в цифровом

пространстве, включая программные проекты, которые реализуются в рамках Цифрового Казахстана. Однако, данное мнение респондентов наталкивает на мысль, что на сегодняшний день в обществе Казахстана стоит проблема цифрового неравенства. В целях решения данной проблемы предполагается, что гражданам Казахстана необходимо владеть знаниями, которые им помогут быстро ориентироваться, быть гибкими и адаптивными в цифровом потоке. Более того, результаты проведенного исследования вселяет надежду на светлое будущее, так как опрошенные респонденты понимают значимость вопроса кибербезопасности, ведь большинство киберинцидентов происходит из-за человеческих ошибок.

ЗАКЛЮЧЕНИЕ

В рамках диссертационной работы изучены методические и практические основы по обеспечению кибербезопасности в Республики Казахстан в сравнении с странами как США, Сингапур, Великобритания, Эстония и Литва. Выбор стран обусловлен успешностью их опыта в соответствии с рейтингом Глобального индекса Кибербезопасности. По результатам проведенного исследования сделаны следующие выводы:

1. Лучшие мировые практики показывают, что государство ежегодно выделяет огромные средства для защиты киберпространства страны. В развитых странах выработаны национальные стратегии кибербезопасности с четким определением цели, задач и оценкой проводимых работ. В то же время Казахстан переживает трансформационный период цифровизации, но, несмотря на это имеет определенный механизм кибербезопасности. Безусловно, принятая Концепция кибербезопасности Казахстана и утвержденный план по реализации данной концепции в 2018 году подняли рейтинг Казахстана в Глобальном индексе кибербезопасности на 40 позицию по сравнению с 2017 годом. Однако, принимаемые меры не являются достаточными. Перед внедрением каких-либо ИТ проектов, в Казахстане необходимо проведение пилотного проекта локально на уровне города или районного центра. Это крайне необходимо для минимизации негативных последствий, как это случилось с установкой национального сертификата безопасности. Анализ ответов опрошенных респондентов показали крайне негативное отношение к использованию сертификата безопасности. Опыт показал, что перед внедрением ИТ проектов предварительно необходимо протестировать пилотный проект в рамках города, районного центра или поселка. Это необходимо в целях минимизации негативных последствий, как это случилось с установкой и применением НСБ.

2. Согласно Концепции кибербезопасности Казахстана ожидаемые результаты по достижению показателя 0,600 по рейтингу Глобального индекса кибербезопасности перевыполнены. В связи с чем, предлагается к окончанию в 2022 году срока реализации Концепции кибербезопасности Казахстана разработать проект Национальной стратегии Кибербезопасности, где четко будут определены цели, задачи и методы оценки реализуемых задач. Необходимо отметить, что в действующей Концепции «Киберщит Казахстана» наибольшее внимание уделено международному опыту и национальным проблемным аспектам, но не их решению. В этой связи, необходимо одой из задач определить развитие международного сотрудничества, что является одним из требований Индекса глобальной кибербезопасности. В соответствии с лучшими мировыми практиками, совершенствование международного сотрудничества благоприятно повлияет на конкурентоспособность Республики Казахстан на мировой арене, что является одним из приоритетных направлений в период глобализации и отражает транспарентность страны. Тогда кибербезопасность Казахстана по своей сущности будет отвечать основным трем требованиям: доступность, целостность и конфиденциальность данных.

Вместе с тем, в рамках исследования и четкого понимания, нами дано определение понятию «кибербезопасность» как комплекс организационно-правовых, экономических и технических процедур в целях защиты от несанкционированного использования информационных ресурсов в киберпространстве.

3. Проанализировав предпринимаемые Казахстаном меры обеспечения кибербезопасности, считаем необходимым совершенствование национальной законодательной базы. После разработки национальной стратегии кибербезопасности Казахстана, необходимо разработать законопроект по обеспечению кибербезопасности страны, где будут рассмотрены защита, обработка, прием и передача биометрических данных при оказании государственных услуг. Вместе с тем, необходимо внедрить систему «киберстрахования» и четко определить данный термин в НПА РК. Аналогичные законы приняты за последние несколько лет в Сингапуре, Китае и в ряде других стран, прогрессивно применяющих цифровые технологии. В Казахстане запланировано повсеместное применение больших данных, внедрение технологий умного города, требующих специфических подходов обеспечения кибербезопасности. Низкий уровень кибербезопасности Казахстана предполагает высокую вероятность уязвимости к хакерским атакам, а также киберпреступлениям. В перспективе использование криптовалют, что приведет к необходимости применения технологии блокчейн. Реализация этого требует значительной подготовительной работы, нормативно-техническую и организационно-управленческую базу. Несомненно, разработка данного законопроекта требует определенных знаний и опыта в области кибербезопасности, цифровизации, менеджменте, управлении рисками и изменениями, в связи с чем необходимо привлечение и подготовка высококвалифицированных специалистов. Более того, практика Казахстана показывает необходимость совершенствования нормотворческой деятельности ввиду часто вносимых изменений и дополнений в законодательство, в том числе Законы РК «Об информатизации», «О национальной безопасности», «О персональных данных и их защите».

4. В целях определения уровня готовности и степени доверия населения к реализуемым программам и проектам в области кибербезопасности и цифровизации проведен онлайн-опрос. Его результаты показали в целом положительную динамику и достаточный уровень готовности восприятия цифровых технологий населением. Это является показателем высокого доверия населения на проводимую политику государством в области цифровизации, кибербезопасности и облегчает работу государственных органов при реализации ИТ решений в Республике. Ярким примером послужил процесс получения гражданами социальных выплат в период чрезвычайного положения в стране. Однако, в ходе использования государственных услуг в режиме онлайн выявлены значительные технические и организационные проблемы. Оказалось, что государственные онлайн-услуги не выдерживали нагрузку на информационную систему, не в должной степени были предусмотрены

организационные моменты. Это показало насколько в Казахстане слабо развита деятельность риск-менеджеров, которые не смогли предугадать возникшие сложности и вовремя принять соответствующие меры для минимизации технических, программных и организационных сбоев. В период пандемии государством совершены те же ошибки, что и при установке сертификата национальной безопасности. Мы пришли к выводу о том, что недостаточно развивать только технические знания у управленцев, а параллельно необходимо развивать навыки в области управления рисками и стратегического мышления, что поможет государственным служащим минимизировать возможные социально-экономические потери.

5. В ходе исследования установлена обеспокоенность большинства респондентов относительно нехватки высококвалифицированных специалистов и существующего цифрового неравенства в обществе. В этой связи, для обеспечения базовыми знаниям и минимизации киберинцидентов в повседневной жизни (на работе, учебе и дома), нами предлагается организовать:

- проверку знаний основ кибербезопасности у молодых специалистов, поступающих на государственную службу, путем проведения комплексного тестирования с последующим обучением в случае необходимости. Предполагается, что данное мероприятие снизит риски киберинцидентов на государственной службе при работе с критически важными ИС;

- дистанционное обучение для всех действующих государственных служащих основам кибербезопасности, форма обучения которого позволит принять участи государственным служащим из отдаленных регионов страны. Организацию данного курса предлагается возложить на Академию государственного управления при Президенте Республики Казахстан, имеющую успешный опыт проведения дистанционного обучения для государственных служащих, в том числе в период пандемии COVID-19. Более того, Академия государственного управления при Президенте Республики Казахстан для проведения дистанционного обучения имеет соответствующую материально-техническую базу и обучающие платформы Moodle и Microsoft Teams;

- бесплатное и доступное обучение всех граждан, имеющих интерес к киберграмотности. Предлагается организовать обучение по успешному опыту Великобритании, доступному всем желающим и на безвозмездной основе. Каждый видео курс организован на 15-20 минут и находится в свободном доступе, однако для самостоятельного прохождения данного обучения необходимо знание английского языка. С учетом того, что не все граждане Казахстана владеют английским, предлагается РГП на ПХВ «ГТС» КНБ РК совместно с образовательными институтами разработать аналогичные короткометражные бесплатные онлайн-курсы на государственном и русском языках.

6. В период экономического кризиса и пандемии COVID-19 правительству необходимо разделить планируемые ИТ проекты и проекты в области

кибербезопасности по приоритетности. Упростить реализацию приоритетных цифровых проектов на основе государственно-частного партнёрства в рамках реализации инвестиционных проектов. Данное мероприятие даст возможность расставить акценты и ускорить реализацию стратегически важных цифровых решений, в том числе выявленных сложностей при получении социальных выплат в условиях пандемии COVID-19.

7. Полагаем необходимым на постоянной основе модернизировать уполномоченные институты и организации в области кибербезопасности, принимать меры по искоренению «информационного неравенства» путем образования и модернизации общественного сознания. Для этого необходимо сформировать четкие функциональные границы уполномоченных органов в области цифровизации и кибербезопасности в целях построения доверительного отношения между заинтересованными сторонами. Вместе с тем, в рамках решения нехватки высококвалифицированных специалистов полагаем целесообразным разработать программу о возврате отечественных экспертов на родину, которые в возрастном эквиваленте не достигли 45 лет, а именно возврат кадров в области кибербезопасности, ИТ, облачного вычисления и искусственного интеллекта.

8. Уполномоченному органу по вопросам обеспечения кибербезопасности в рамках государственно-частного партнёрства предлагается рассмотреть вопрос разработки платформы для безопасного и оперативного обмена информации между государственными и честными секторами о возможных киберинцидентах на Интернет-просторах Казахстана. Для этого необходима разработка национального плана действий по ГЧП с четким информированием частного сектора о государственных целях, потребностях и ограничениях в области кибербезопасности. При этом для определения единой правовой базы при создании ГЧП в данной сфере, предлагается разработка национального нормативного правового акта или Меморандума о взаимопонимании.

Казахстан за годы независимости прошел немало на пути обеспечения кибербезопасности в цифровом пространстве и за последние годы прилагает все больше усилий для создания надежной экосистемы в киберпространстве, укрепляя доверие между организациями и пользователями в использовании онлайн-услуг, однако на наш взгляд впереди ждет еще долгий путь.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Ankit F., Mahir N., John N. Follow the leaders: How governments can combat intensifying cybersecurity risks // https://www.mckinsey.com/industries/public-and-social-sector/our. 20.09.2020.

2 Global Agenda Council on Cybersecurity, World Economic Forum, April 2016, // http://www3.weforum.org/docs/GAC16_Cybersecurity_WhitePaper_.pdf. 22.05.2020.

3 Постановление Правительства Республики Казахстан. Об утверждении Государственной программы «Цифровой Казахстан»: утв. 12 декабря 2017 года. № 827. // http://adilet.zan.kz/rus/docs/P1700000827. 10.03.2020.

4 Постановление Правительства Республики Казахстан. Об утверждении Концепции кибербезопасности («Киберщит Казахстана»): 30 июня 2017 года № 407// http://adilet.zan.kz/rus/docs/P1700000407. 10.03.2020.

5 Абучакра Р., Хури М. Эффективное правительство для нового века. Москва: Олимп-бизнес, 2020. – С. 256.

6 Global Cybersecurity Index – 2018. // https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf. 20.09.2019.

7 Issabayeva S., Yesseniyazova B., Cybersecurity issues in digital Kazakhstan. E-Proceedings of the 27th NISPAcee Annual Conference «From Policy Design to Policy Practice». // https://www.nispa.org/files/conferences/2019/e-proceedings/system_files/papers/cyber-security-issues-issabaeva.pdf. 13.09.2019.

8 The IMD World Digital Competitiveness Ranking 2018 // https://www.imd.org/globalassets/wcc/docs/imd_world_digital_competitiveness_ranking_2018.pdf. 02.07.2020.

9 Карпова Д., Киберпреступность: глобальная проблема и ее решение // Власть. – 2014. - №08. – С. 192.

10 Зейнелгабдин А., Исабаева С., Кибербезопасность Казахстана в период цифровой трансформации // Государственный аудит. - 2019. - №4 (45). – С. 46-55.

11 Warnes, K., Cybersecurity, Salem Press Encyclopedia. 2019 // https://ezproxy.nu.edu.kz/login?url=https://ezproxy.nu.edu.kz:2358/login.aspx?direct=true&db=ers&AN=89677538&site=eds-live&scope=site. 13.03.2019.

12 Szakos J., Szadeczky T., Building a Cybersecurity Ecosystem in a Hungarian City – The Potential for Innovative Growth //The Choice-Architecture behind Policy Designs. – С. 195-202. // https://www.nispa.org/files/publications/PRACTIC-monograph-final.pdf. 25.03.2020.

13 Cybersecurity and Digital Business Risk Management, // https://www.gartner.com/en/information-technology/insights/cybersecurity. 10.03.2020.

14 Исабаева С.Б., Cybersecurity policy development in Kazakhstan: analysis of m-commerce user acceptance // Государственное управление и государственная служба. – 2019. - №1(68). - С 34-49.

15 Губайдуллина М. Внешнеполитическая деятельность и дипломатия в современных условиях транспарентного информационного пространства // International Relations and International Law Journal. – 2018. – Т. 79, №3. – С. 14-22.

16 Wihlborg E., Hedström K., Larsson H. E-government for all–Norm-critical perspectives and public values in digitalization //Proceedings of the 50th Hawaii International Conference on System Sciences. – 2017. – С. 2549-2559.

17 EMC Global Data Protection Index - Global Results, https://www.emc.com/infographics/global-data-protection-index-global.htm. 22.05.2019.

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. 22.03.2019.

19 Исабаева С., Кармыс Г., Бексултанов А., Жусупова Г., Сравнительный анализ рейтинга стран по цифровизации и кибербезопасности: проблемы и возможности // Казахстан – Спектр. – 2018. - №3(85). – С. 23-36.

20 Key findings & Results for Italy // http://www.datamanager.it/wp-content/uploads/2014/12/EMC-Data-Protection-Index-Key-Findings-Italy-FINAL.pdf. 12.03.2019.

21 Drage-Arianson K., Crouch D., Cybersecurity: Building Resilience from the Inside Out // Chemical Engineering. – 2018. – Vol. 125(10). - P. 65–68.

22 Mishra A., Ghosh S., Mishra B. K. Cybersecurity: A Practical Strategy Against Cyber Threats, Risks with Real World Usages //Cyber Security in Parallel and Distributed Computing: Concepts, Techniques, Applications and Case Studies. – 2019. – С. 207-220.

23 Thames L., Schaefer D. Cybersecurity for Industry 4.0 : Analysis for Design and Manufacturing. // https://search.ebscohost.com/login.aspx?direct=true&db=edsebk&AN=1497891&site=eds-live. 12.12.2019

24 Le D., Kumar R., Mishra B., Chatterjee J., Khari M., Cyber Security in Parallel and Distributed Computing: Concepts, Techniques, Applications and Case Studies.// John Wiley & Sons. 2019. 261 P.

25 Milkovich D. Alarming Cyber Security Facts and Stats // https://www.cybintsolutions.com/cyber-security-facts-stats/. 20.08.2020.

26 University of Maryland. Study: Hackers Attack Every 39 Seconds? // https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds. 10.03.2020

27 The International telecommunication unit // https://www.itu.int/search#?q=cyber%20security&fl=0&ex=false. 10.03.2020.

28 Guiora A. N. Cybersecurity: Geopolitics, Law, and Policy. //– CRC Press, 2017. 170 P.

29 Beatriz N., Cutberto V., Cesar L., Electronic government and social satisfaction: analysis of social conditions for Tijuana // Вопросы государственного и муниципального управления. – 2018. – №6. С. 84–97.

30 Alperen M. Foundations of Homeland Security : Law and Policy. // Hoboken, NJ: Wiley. 2017. // https://search.ebscohost.com/login.aspx?direct=true&db=edsebk&AN=1453384&site=eds-live. 20.02.2018

31 Lloyd G. The business benefits of cyber security for SMEs //Computer Fraud & Security. – 2020. – Т. 2020. – №. 2. – P. 14-17.

32 Карасев П. Новые информационные технологии во внешней политике США // Мировая экономика и международные отношения. – 2014. – №5. – С. 53-62.

33 Cost of a Data Breach Report highlights. // https://www.ibm.com/security/data-breach. 14.02.2020.

34 Mastering Cybersecurity with BCG. // https://www.bcg.com/ru-ru/capabilities/technology-digital/mastering-cybersecurity.aspx. 10.03.2020.

35 Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019, 2018, // https://link.ac/5HMP2. 10.03.2020.

36 Gartner Says Global IT Spending to Reach $3.9 Trillion in 2020. // https://www.gartner.com/en/newsroom/press-releases/2020-01-15-gartner-says-global-it-spending-to-reach-3point9-trillion-in-2020. 10.03.2020.

37 Rob S. Must-Know Cybersecurity Statistics for 2020. // https://www.varonis.com/blog/cybersecurity-statistics/. 10.07.2020.

38 Kruhlov V. V. et al. Public-Private Partnership in Cybersecurity //Vcheni zapysky TNU im. VI Vernadskoho. Seriia: Derzhavne upravlinnia. – 2018. – Т. 3. – №. 29. – С. 68.

39 Lin H., Zegart A. Introduction to the special issue on strategic dimensions of offensive cyber operations. // Journal of cybersecurity. – 2017. №3(1). P. 1-5.

40 Craigen D., et al. 2014.Defining Cybersecurity. Technology Innovation Management Review, 4(10): 13-21. // http://doi.org/10.22215/timreview/835. 10.03.2019.

41 Закон Республики Казахстан от 24 ноября 2015 года № 418-V ЗРК «Об информатизации» // http://adilet.zan.kz/rus/docs/Z1500000418. 10.03.2020.

42 Lexico powered by Oxford, Оксфордский словарь // https://www.lexico.com/definition/cybersecurity. 10.03.2019.

43 Cambridge dictionary. Cybersecurity. // https://link.ac/5HMO7. 10.03.2019.

44 Что такое кибербезопасность? // https://www.cisco.com/c/ru_ru/products/security/what-is-cybersecurity.html. 10.05.2020.

45 Национальный центр кибербезопасности Великобритании / National cybersecurity centre of the UK, // https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security. 10.03.2020.

46 Information Technology Gartner Glossary, // https://www.gartner.com/en/information-technology/glossary/security-governance. 02.03.2020.

47 Cybersecurity Act 2018 of Republic of Singapore, // https://sso.agc.gov.sg/Acts-Supp/9-2018/. 10.03.2020.

48 Moschovitis C. Cybersecurity Program Development for Business: The Essential Planning Guide. //– John Wiley & Sons. 2018. 224 P.

49 National Institute of Standards and Technology Internal Report. // https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8183.pdf. 10.03.2020.

50 Татаринова Л., Соотношение понятий «информационная безопасность»,«защита информации» и «кибербезопасность»,«киберзащита» по законодательству Республики Казахстан // Вестник КазНУ. Серия юридическая. – 2019. – Т. 67. – №. 3. – С. 60-64.

51 Efthymiopoulos M. A cyber-security framework for development, defense and innovation at NATO // Journal of Innovation and Entrepreneurship. – 2019. – Vol. 8, №1. – P. 1-26.

52 Ken Xie, Founder, Chairman of the Board and Chief Executive Officer. Fortinet. 2020. Four key challenges for cybersecurity leaders. // https://link.ac/5HMU7. 10.03.2020.

53 Von Solms R., Van Niekerk J. From information security to cyber security //computers & security. – 2013. – Т. 38. – С. 97-102.

54 Wihlborg E., Hedström K., Larsson H. E-government for all–Norm-critical perspectives and public values in digitalization //Proceedings of the 50th Hawaii International Conference on System Sciences. – 2017. P. 2549-2558

55 International Telecommunication Union & ABI research. Global Cybersecurity Index & Cyberwellness Profiles. Geneva: ITU. // http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf. 12.12.2019

56 The Global Cybersecurity Index, // https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx. 10.03.2020.

57 The National Cyber Security Index. // https://ncsi.ega.ee/methodology/. 10.03.2020.

58 Послание Президента Республики Казахстан - Лидера Нации Н.А. Назарбаева народу Казахстана. Стратегия «Казахстан-2050»: новый политический курс состоявшегося государства. утв. 14.12.2014года. // http://adilet.zan.kz/rus/docs/K1200002050. 11.03.2020.

59 Жумагалиев А. The Boston Consulting Group review. // Специальный выпуск: Казахстан, обозрение. 2018. С.1-66.

60 European Commission Decision. Horizon 2020, Work Programme 2018 – 2020 // http://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-intro_en.pdf. 11.03.2020.

61 Fourie L, Pang S, Kingston T, Hettema H, Watters P, Sarrafzadeh H. The global cyber security workforce : an ongoing human capital crisis. // https://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.CCF661AB&site=eds-live. 12.07.2018

62 Caldwell T. Plugging the cyber-security skills gap //Computer Fraud & Security. – 2013. – Т. 2013. – №. 7. – С. 5-10.

63 Земскова И. А. Трансформация качества государственных услуг под влиянием цифровизации государственных органов //Вестник Саратовского

государственного социально-экономического университета. – 2018. – №. 3 (72). – С. 23–28.

64 Исабаева С.Б. Стратегии кибербезопасности разных стран в эпоху глобальной цифровизации // Тенденции мировых интеграционных процессов: вызовы и возможности: сб. матер. междунар. науч. конф.. – Нур-Султан, 2019. – С. 182-194.

65 Oxford Learner's Dictionaries, Mechanism // https://www.oxfordlearnersdictionaries.com/definition/english/mechanism?q=mechanism. 27.05.2019.

66 Marr C. Cyberwarfare and Applied Just War Theory: Assessing the Stuxnet Worm through Jus ad Bellum and Jus in Bello //SPICE: Student Perspectives on Institutions, Choices and Ethics. – 2019. – Т. 14. – №. 1. – С. 2.

67 Gokce Y. Güç Kullanımı Olarak Siber Faaliyetler: Uluslararası Hukukun Siber Uzaya Uygulanabilirliği. //Journal of Yeditipe University Faculty of Law. // https://link.ac/5HMY0. 05.03.2020.

68 Валиахметова Г. Проблемы информационной безопасности в Азии //Известия УрФУ. Серия 3. Общественные науки. – 2015. – Т. 10. – №. 1. – С. 128-136.

69 Li Y., Zhang T., Li X., Li T. A Model of APT Attack Defense Based on Cyber Threat Detection //China Cyber Security Annual Conference. – Springer, Singapore, 2018. – С. 122-135.

70 The GDPR Racket: Who's Making Money From This $9bn Business Shakedown, Oliver Smith. 2018. // https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/#26e517e734a2. 27.05.2020.

71 General Data Protection Regulation (GDPR), GDPR fines after one year: Key takeaways for businesses, // https://gdpr.eu/gdpr-fines-so-far/. 27.05.2020.

72 European Data Protection Board // https://link.ac/5HN84.14.02.2020.

73 Finance, Competitiveness & Innovation Insight, Financial Stability & Integrity. 2018. // https://link.ac/5HN90. 02.03.2020.

74 АО «ГТС» КНБ РК, Более 590 миллионов атак отражено инструментарием АО «ГТС». // http://www.sts.kz/ru/node/456. 09.11.2020.

75 Ranking of the National cybersecurity Index // https://ncsi.ega.ee/ncsi-index/. 05.03.2020.

76 Public Sector Data Security Review Committee Report. Existing Government Efforts in Using Data Securit // https://link.ac/5HNa5. 27.05.2020.

77 Global Cybersecurity Index 2017, International Telecommunication Union - ITU, 2017, Geneva // https://link.ac/5HNb5. 27.05.2019.

78 Shafqat N., Masood A. Comparative analysis of various national cyber security strategies //International Journal of Computer Science and Information Security. – 2016. – Т. 14. – №. 1. – С. 129.

79 The National strategy to secure Cyberspace. // https://link.ac/5HNc8. 27.05.2019.

80 Natinal cybersecurity strategy of the UK 2016-2021. // https://link.ac/5HNe8. 27.05.2019

81 National Cyber Strategy of the United States of America. // https:// link.ac/5HNf5. 22.05.2020.

82 Lithuanian National Cybersecurity Strategy, European Union Agency for Cybersecurity // https://link.ac/5HNg9. 20.05.2020

83 Estonian National Cyber Security Strategy. European Union Agency for Cybersecurity, // https://link.ac/5HNh7. 27.05.2020

84 Vision 2022, Estonia is the most resilient digital society, // https://link.ac/5HNj9. 10.03.2020.

85 Singapore's Cybersecurity Strategy, 2016, // https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy. 22.05.2020.

86 Azmi R., Tibben W., Win K. T., Motives behind Cyber Security Strategy Development: A Literature Review of National Cyber Security Strategy. – 2016. // https://ro.uow.edu.au/cgi/viewcontent.cgi?article=1044&context=acis2016. 12.12.2019.

87 Lee J., Hacking into China's Cybersecurity Law //Wake Forest L. Rev. – 2018. – T. 53. – C. 57.

88 Parasol M., The impact of China's 2016 Cyber Security Law on foreign technology firms, and on China's big data and Smart City dreams //Computer law & security review. – 2018. – T. 34. – №. 1. – C. 67-98.

89 Yang F., Xu J. Privacy concerns in China's smart city campaign: The deficit of China's Cybersecurity Law //Asia & the Pacific Policy Studies. – 2018. – T. 5. – №. 3. – C. 533-543.

90 Cybersecurity Information Sharing Act of 2014. // https://www.congress.gov/bill/113th-congress/senate-bill/2588. 27.05.2019.

91 Cybersecurity Act. A Singapore Government Agency Website // https://www.csa.gov.sg/legislation/cybersecurity-act. 22.05.2020.

92 Nations United. Combatting Cybercrime. The World Bank, 2017. // https://econpapers.repec.org/bookchap/wbkwbpubs/30306.htm. 02.03.2020.

93 Kshetri N., Kshetri N. Cybersecurity in India: Regulations, governance, institutional capacity and market mechanisms //Asian Research Policy. – 2017. – T. 8. – №. 1. – C. 64-76.

94 Carr M. Public–private partnerships in national cyber-security strategies //International Affairs. – 2016. – T. 92. – №. 1. – C. 43-62.

95 Moore T. Introducing the economics of cybersecurity: Principles and policy options //Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy. – 2010. – C. 3-23.

96 World Economic Forum, Cyber Resilience Playbook for PublicPrivate Collaboration, Future of Digital Economy and Society System Initiative. January 2018. https://link.ac/5HNk9. 20.04.2020.

97 ENISA. Public Private Partnerships (PPP). Cooperative models. 2017 // https://link.ac/5HNl1. 20.04.2020.

98 Alex A., Why Educating Your Employees on Cyber Intelligence and Security Will Reduce Risk. 2018. // https://link.ac/5HNm10. 11.03.2020.

99 Statistics of the ITU // https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx. 05.03.2020.

100 ITU Committed to connecting the world. Legislation. // https://www.itu.int/en/ITU-D/Cybersecurity/Pages/legislation.aspx. 27.05.2020.

101 Harašta J. Cyber Security in Young Democracies // Jurisprudencija. – 2013. - Vol. 20, №4. - P. 1457-1472.

102 Ižak Š. Using The Topic of Migration by Pro-Kremlin Propaganda: Case Study of Slovakia // Journal of Comparative Politics. – 2019. – Vol. 12, №1. – P. 53-70.

103 House of Commons Culture, Media and Sport Committee, Cyber Security: Protection of Personal Data Online, First Report of Session 2016–17, // https://publications.parliament.uk/pa/cm201617/cmselect/cmcumeds/148/148.pdf. 06.03.2020.

104 Finnerty, K., Motha, H., Shah, J., White, Y., Button, M., & Wang, V. Cyber security breaches survey 2018: Statistical release. // https://link.ac/5HNn03. 19.11.2019.

105 Andrews, E., Thornton, D., Owen, J., Bleasdale, A., Freeguard, G., Stelk, I.. Making a success of digital government Institute for Government. 2016 // https://wdco.ru/OQ3cQ.

106 Klahr, R., Amili, S., Shah, J. N., Button, M., Wang, V. Cyber security breaches survey 2016. *UK Government, Ipsos MORI and University of Portsmouth.*// https://wdco.ru/PmFjA. // https://wdco.ru/F35us. 06.03.2020.

107 Cyber security: advice for small businesses, Official UK Government Website. // https://www.gov.uk/government/publications/cyber-security-what-small-businesses-need-to-know. 06.03.2020.

108 Cyber security training for business. Free online training courses to help business protect against cyber threats and online fraud. // https://link.ac/5HNp10. 24.07.2020.

109 Issabayeva S., Yesseniyazova B., Grega M. Electronic Public Procurement: Process and Cybersecurity Issues //NISPAcee Journal of Public Administration and Policy. – 2019. – Т. 12. – №. 2. – С. 61-79.

110 National Cyber Security Center of the UK, // https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security. 06.03.2020.

111 Cyber Essentials powered by National Cyber Security Center of the UK, // https://www.cyberessentials.ncsc.gov.uk/. 20.05.2020.

112 Individuals & families, National Cyber Security Center of the UK, // https://www.ncsc.gov.uk/section/information-for/individuals-families. 20.05.2020.

113 Self employed & sole traders, National Cyber Security Center of the UK. // https://www.ncsc.gov.uk/section/information-for/self-employed-sole-traders. 20.05.2020.

114 Small & medium sized organisations, National Cyber Security Center of the UK. // https://www.ncsc.gov.uk/section/information-for/small-medium-sized-organisations. 20.05.2020.

115 Large organisations, National Cyber Security Center of the UK. // https://www.ncsc.gov.uk/section/information-for/large-organisations. 207.05.2020.

116 Public sector, National Cyber Security Center of the UK. // https://www.ncsc.gov.uk/section/information-for/public-sector. 20.05.2020.

117 Cyber security professionals, National Cyber Security Center of the UK. // https://www.ncsc.gov.uk/section/information-for/cyber-security-professionals, 20.05.2020.

118 The information commissioner's office. // https://ico.org.uk/for-organisations/guide-to-data-protection/. 20.05.2020.

119 Department for Digital, Culture, Media and Sport, Cyber Security Breaches Survey 2019: Statistical Release. // https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_Breaches_Survey_2019_-_Main_Report.pdf. 06.03.2020.

120 Tyrer A. Can the UK cyber-security industry lead the world? //Computer Fraud & Security. – 2015. – Т. 2015. – №. 2. – P. 5-7.

121 Osborn E., Simpson A. On small-scale IT users' system architectures and cyber security: A UK case study //Computers & Security. – 2017. – Т. 70. – С. 27-50.

122 Rai S., Singh K., Varma A. K. Global research trend on cyber security: A scientometric analysis //Libr. Philos. Pract.(e-journal). – 2019. – Т. 3339.

123 Norton LifeLock Inc. 10 cyber security facts and statistics for 2018 // https://link.ac/5HNq9. 27.05.2020.

124 Шемчук В., National Cyber Strategy of the United States of America: Experience for Ukraine //Науковий вісник Національної академії внутрішніх справ. – 2019. – Т. 113. – №. 4. – С. 119-124.

125 Осипенко А. Л. Государственно-частное партнерство в сфере противодействия киберпреступности //Вестник Воронежского института МВД России. – 2016. – №. 4.

126 E-Estonia. We have built a digital society and we can show you how // https://e-estonia.com/#. 27.05.2020.

127 Cybersecurity stratify Republic of Estonia 2019-2022. // https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf. 25.05.2020.

128 Cybersecurity act of the Republic of Estonia. // https://www.riigiteataja.ee/en/eli/523052018003/consolide. 25.05.2020.

129 Monica M., To Bolster Cybersecurity, the US Should Look to Estonia. // https://link.ac/5HNr4. 27.05.2020.

130 Republic of Estonia Defence Forces, Cyber Command. // https://mil.ee/en/landforces/Cyber-Command/. 27.05.2020.

131 Марьясис Д. А. Сферы инновационного прорыва Израиля //Мировая экономика и международные отношения. – 2016. – Т. 60. – №. 3. – С. 92-100.

132 Natinal Cyber Security Strategy - NIS Capacities // https://www.cyberwiser.eu/lithuania-lt. 27.05.2020.

133 Government of the Republic of Lithuania, Resolution on the Approval of the National Cyber Security Strategy, // https://link.ac/5HNt4. 27.05.2020.

134 Invest Lithuania, Cybersecurity. // https://investlithuania.com/key-sectors/technology/cybersecurity/. 27.05.2020.

135 CYBERWISER.eu Open Pilots. Cyber Range and Capacity Building in Cybersecurity. // https://www.cyberwiser.eu/open-pilots, 27.05.2020.

136 LITNET CERT, The Computer Emergency Response Team of LITNET networks. // https://cert.litnet.lt/about/. 27.05.2020.

137 The National Cyber Incident Management Plan. // https://www.hsdl.org/?view&did=798128. 27.05.2020.

138 Кармыс Г., Бексултанов А., Исабаева С., Джусупова Г.. Сравнительный анализ государственного подхода к цифровизации Казахстана и России //Вестник университета Туран. – 2018. – №. 3. – С. 197-201.

139 Клименко П., Клименко И., Цифровая экономика современного Казахстана: новые вызовы //Черноморская конференция-2019. – 2019. – С. 98-99.

140 Притворова Т., Жашкенова Р., Системообразующие характеристики цифровой экономики // Найновите Постижения на Европейската Наука -2019. – 2019. – С. 50.

141 Мусабаев, Р., Касымжанов, Б., Калиева, Г., & Ибраева, В., Разработка Информационных технологий и систем для стимулирования устойчивого развития личности как одна из основ развития Цифрового Казахстана // Проблемы оптимизации сложных систем. – 2018. – С. 39-46.

142 Баймухамедов М., Баймухамедова Г., Аймурзинов М., Технологическая модернизация экономики страны на основе реализации госпрограммы «Цифровой Казахстан» // Аграрный вестник Урала. – 2019. – №. 2 (181). – С. 42-45.

143 The IMD World Digital Competitiveness Ranking 2019 results. // https://link.ac/5HNu6. 29.02.2020.

144 Официальный сайт Министерства цифрового развития, инновации и аэрокосмической промышленности Республики Казахстан. // https://link.ac/5HNv2. 10.04.2020.

145 Официальный информационный ресурс Премьер-Министра Республики Казахстан, Стратегический план 2025, // https://primeminister.kz/ru/documents/gosprograms/stratplan-2025. 11.04.2020.

146 Бексултанов А., Кармыс Г., Исабаева С., Цифровизация экономики – фактор повышения конкурентоспособности Республики Казахстан. // Сб. 14 междунар. науч.-практ. конф. студентов, аспирантов, магистрантов «Цифровые технологии в экономике и управлении: научный взгляд молодых. 2018. С. 596-599.

147 Краузе Н., Алимбетов У., Битенова Б., Самусенко Е., Цифровизация: формирование и развитие в Республике Казахстан. // Вестник университета Туран. – 2019. - № 4. – С. 211-217.

148 Головенчик Г. Г. Рейтинговый анализ уровня цифровой трансформации экономик стран ЕАЭС и ЕС //Цифровая трансформация. – 2018. – №. 2. – С. 5-18.

149 Global Innovation Index 2019 ranking. // https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2019/kz.pdf, 07.04.2020.

150 Global Connectivity Index – Huawei. 2019. // https://www.huawei.com/minisite/gci/en/country-profile-kz.html. 15.04.2020.

151 The Network Readiness Index 2019: Towards a Future-Ready Society. // https://link.ac/5HNw9. 29.02.2020.

152 Network Readiness Index 2019 Kazakhstan, // https://networkreadinessindex.org/countries/kazakhstan/. 19.04.2020.

153 About TheGlobalEconomy.com, Kazakhstan: Internet users, // https://www.theglobaleconomy.com/kazakhstan/internet_users/. 29.02.2020.

154 Lagutina M. Eurasian Economic Union Foundation: issues of global regionalization //Eurasia Border Review. – 2014. – Т. 5. – №. 1. – С. 95-111.

155 Bershadskaya L., Chugunov A., Dzhusupova Z. Understanding e-government development barriers in CIS countries and exploring mechanisms for regional cooperation //International conference on electronic government and the information systems perspective. – Springer, Berlin, Heidelberg, 2013. – P. 87-101.

156 Isaac, O., Abdullah, Z., Ramayah, T., & Mutahar, A. M.. Internet usage within government institutions in Yemen: An extended technology acceptance model (TAM) with internet self-efficacy and performance impact //Science International. – 2017. – Т. 29. – №. 4. – P. 737-747.

157 Wangpipatwong S., Chutimaskul W., Papasratorn B. Understanding Citizen's Continuance Intention to Use e-Government Website: a Composite View of Technology Acceptance Model and Computer Self-Efficacy //Electronic Journal of e-Government. – 2008. – Т. 6. – №. 1. – P. 55-64

158 Al-Adawi Z., Yousafzai S., Pallister J., Conceptual model of citizen adoption of e-government. //The second international conference on innovations in information technology. – 2005. – С. 1-10.

159 Colesca S. , Dobrica L., Adoption and use of e-government services: The case of Romania. //Journal of applied research and technology. – 2008. – Т. 6. – №. 3. – С. 204-217.

160 Jaeger P., Matteson M. e-Government and Technology Acceptance: The Case of the Implementation of Section 508 Guidelines for Websites //Electronic Journal of E-Government. – 2009. – Т. 7. – №. 1. - P. 87-98.

161 Transparency International. The global coalition against corruption. // https://www.transparency.org. 09.09.2019.

162 Akhmetkerey B, Issabayeva S, Bastaubayeva A., The Formation of the Cryptocurrency Market in the Republic of Kazakhstan: Opportunities and Threats

from the Point of View of Economic Securit. //BASIQ 2019 – International conference. - 2019. – P. 135-142.

163 Асланова Н., Сатиев О., ЦАРКА: более 90% казахстанских ресурсов подвержены уязвимостям «Белые хакеры» рассказали о состоянии информационной безопасности в Казахстане. // https://link.ac/5HNw9. 23.08.2019.

164 Глава государства провел совещание по реализации Государственной программы «Цифровой Казахстан», Касым-Жомарт Токаев, 04 марта 2020г. // https://link.ac/5HNx1. 16.03.2020.

165 Маулетбай С., Как «вирус от Генпрокуратуры» помог разбогатеть хакерам, 2016.// https://informburo.kz/stati/kak-virus-ot-genprokuratury-pomog-razbogatet-hakeram.html. 23.07.2019.

166 Сейткулов Е., Информационная безопасность Республики Казахстан: состояние и перспективы. 2016. // http://www.enu.kz/ru/info/novosti-enu/novosti-nauki/45582/. 09.09.2019.

167 Кодекс Республики Казахстан. Уголовный кодекс Республики Казахстан: утв. 3 июля 2014 года № 226-V ЗРК // http://adilet.zan.kz/rus/docs/K1400000226. 29.02.2020.

168 Постановление Правительства Республики Казахстан. Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности: утв. 20 декабря 2016 года, №832 // http://adilet.zan.kz/rus/docs/P1600000832. 29.02.2020.

169 Постановление Правительства Республики Казахстан. Об утверждении Государственной программы по противодействию религиозному экстремизму и терроризму в Республике Казахстан на 2018 - 2022 годы: утв. 15 марта 2018 года, №124 // http://adilet.zan.kz/rus/docs/P1800000124. 20.03.2020.

170 Письмо ГУ: ответ на запрос / Комитет по правовой статистике и специальным учетам Генеральной Прокуратуры Республики Казахстан. – Нур-Султан, 2019. - №2-20-19-09960 от 13 ноября.

171 Постановление Правительства Республики Казахстан. «Об утверждении Плана мероприятий по реализации Концепции кибербезопасности («Киберщит Казахстана») до 2022 года»: утв. 28 октября 2017 года, №676 // http://adilet.zan.kz/rus/docs/P1700000676. 20.04.2020.

172 Исабаева С. Тенденции инновационной деятельности Казахстана и стран СНГ: сравнительный анализ // Матер. 5-й междунар. науч.-практ. конф. «Национальная правовая система Республики Таджикистан и стран СНГ: анализ тенденций и перспектив развития». – Душанбе, 2017. – С. 187 -192.

173 Бездудный Ф., Смирнова Г., Нечаева О. Сущность понятия инновация и его классификация // Инновации. – 1998. – №2-3. – С. 3-13.

174 Исабаева С. Digitalization as one of the factors of modernizing public administration: Singapore experience // Матер. 5-й междунар. науч.-практ. Интернет-конференции «Организационно-правовые аспекты государственного управления в Украине». Полтава. - 2018. - С. 28-31.

175 Cybersecurity. Cyber Risk and Financial Sector Regulation and Supervision. 2018. // https://link.ac/5HNy8. 20.05.2020.

176 Dave D., Meet the 7 Most Popular Search Engines in the World. 2018. // https://www.searchenginejournal.com/seo-101/meet-search-engines/#close. 29.02.2020.

177 Caroline F., The Top 7 Search Engines. Ranked by Popularity, // https://blog.hubspot.com/marketing/top-search-engines. 29.02.2020.

178 Thomas J., Law, Meet the Top 10 Search Engines in the World in 2019, 2019. // https://www.oberlo.com/blog/top-search-engines-world. 25.03.2020.

179 Statcounter Global Stats, Search Engine Market Share Worldwide, Jan 2019 - Jan 2020, 2019. // https://gs.statcounter.com/search-engine-market-share. 29.02.2020.

180 Statcounter Global Stats. Search Engine Market Share in Kazakhstan. Jan 2019 - Jan 2020. // https://gs.statcounter.com/search-engine-market-share/all/kazakhstan. 25.05.2020.

181 Google Отчет о доступности сервисов и данных. Запросы государственных органов на удаление контента // https://link.ac/5HNz8. 29.02.2020.

182 Business and economic data for 200 countries, TheGlobalEconomy.com, // https://www.theglobaleconomy.com/rankings/wb_political_stability/. 25.05.2020.

183 Сайт Комитета информационной безопасностей Министерства цифрового развития, инновации и аэрокосмической промышленности Республики Казахстан. // https://link.ac/5HNA57. 20.05.2020.

184 Porter M. E., Stern S. Innovation: location matters //MIT Sloan management review. – 2001. – Т. 42. – Vol. 42. - №. 4. – P. 28-36.

185 Указ Президента Республики Казахстан. «О введении чрезвычайного положения в Республике Казахстан»: утв. 15 марта 2020 года № 285 // https://link.ac/5HNB10. 17.04.2019.

186 Указ Президента Республики Казахстан. «О продлении действия чрезвычайного положения в Республике Казахстан»: утв. 14 апреля 2020 года № 306. https://link.ac/5HNC0. 20.05.2020.

187 Заявление Главы государства Касым-Жомарта Токаева. 27 апреля 2020г. // https://link.ac/5HND8. 29.04.2020.

188 Kim S., Su K. Using psychoneuroimmunity against COVID-19 // Brain, behavior, and immunity. – 2020. - Vol. 87, - P 4-5

189 Сагындыккызы К. Г., Бастаубаева А. Ж. Swot и Pest анализ цифровизации HR-процессов госслужбы Казахстана //Вопросы государственного и муниципального управления. – 2018. – №. 1. – С. 140-163

190 Глава государства провел совещание по экономической ситуации в стране, 9.03.2020г. // https://link.ac/5HNF10. 25.03.2020.

191 Porter M. E., Schwab K. The global competitiveness report 2008-2009 //World Economic Forum. – 2008. – С. 472. https://link.ac/5HNG3. 20.09.2017.

192 Schwab, K. The global competitiveness report 2019. // Geneva: World Economic Forum. https://link.ac/5HMx20. 19.05.2020.

193 Комитет статистики Министерства национальной экономики РК, Основные социально-экономические показатели // https://stat.gov.kz/. 07.05.2020.

194 Окончание поддержки Windows XP. Официальный сайт компании Microsoft. // https://link.ac/5HNH010. 13.05.2020.

195 Поддержка Windows 7 окончена. Официальный сайт компании Microsoft. Источник // https://link.ac/5HNI9. 13.05.2020.

196 Ошакбаев Р., Официальный информационный ресурс Премьер-Министра Республики Казахстан. 15 апреля 2020г. «Цифровой Казахстан: нам еще многое нужно оцифровать» // https://link.ac/5HNi7. 19.05.2020.

197 Послание Главы государства Касым-Жомарта Токаева народу Казахстана. 02 сентября 2019г. // https://link.ac/5HNJ24 05.09.2019.

198 Выступление Главы государства на заседании Государственной комиссии по чрезвычайному положению, Официальный сайт Президента Республики Казахстан, 10 апреля 2020г. // https://link.ac/5HNK4 25.05.2020.

199 An official website of the United States government, Cybersecurity & Infrastructure security Agency, About CISA of the USA, https://www.cisa.gov/about-cisa. 10.03.2020.

200 An official portal of National Cyber Security Agency. Malaysia, https://www.nacsa.gov.my/. 25.08.2020.

201 Wamala F. The ITU National Cybersecurity Strategy Guide. 2011. – 2012. // http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf. 13.05.2020.

202 What is a Black-Hat hacker?. Kaspersky. // https://link.ac/5HNL70. 22.05.2020.

203 За период ЧП в Казахстане увеличилось число фишинговых атак, АО «UNC» RY< HR. // http://sts.kz/ru/node/397. 25.05.2020.

204 Турин М., Побочный эффект. // https://time.kz/blogs/hocu-skazat/2020/03/25/medet-turin-pobochnyj-effekt. 25.05.2020.

205 Энциклопедия Касперского. // https://encyclopedia.kaspersky.ru/knowledge/what-is-phishing/. 24.05.2020

206 KZ-CERT выявил ряд «компьютерных вирусов» COVID, АО «Государственная техническая служба» Комитета национальной безопасности Республики Казахстан. // http://sts.kz/ru/node/396. 25.05.2020.

207 ГТС зафиксировал DDoS – атаки на сайты госорганов, АО «Государственная техническая служба» Комитета национальной безопасности Республики Казахстан. // http://sts.kz/ru/node/399. 25.05.2020.

208 Lebanon pirates 70 percent of its software, Compliance Alert. // https://calert.info/details.php?id=1078. 20.06.2020.

209 US Country Commercial Guides, Kazakhstan, 2018. // https://link.ac/5HNM4 . 20.09.2020.

210 Business Software Alliance. Software Management: Security Imperative, Business Opportunity. // https://gss.bsa.org/. 20.09.2020

211 Software management: Security imperative, business opportunity //BSA Global Software Survey. – 2018. // https://gss.bsa.org/wp-content/uploads/2018/05/2018_BSA_GSS_Report_en.pdf. 20.09.2020.

212 Rau P. R. Law, trust, and the development of crowdfunding // Trust, and the Development of Crowdfunding. // https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2989056. 20.04. 2020

213 Малахова М., Левкович В., Бухтик М., Проблемы финансирования социальной сферы в Республике Беларусь // SCI-ARTICLE.RU : электронный периодический рецензируемый научный журнал. – 2018. – № 55. – С. 122-126..

214 Ковнерев М., Правкин С.. Экономико-правовые основы краудфандинга как современного механизма финансирования предпринимательства // Информационно-экономические аспекты стандартизации и технического регулирования. – 2017. – №. 4. – С. 4-4.

215 Shneor R. Crowdfunding models, strategies, and choices between them //Advances in Crowdfunding. – Palgrave Macmillan. Cham. 2020. – P. 21-42.

216 Ziegler T., Shneor R. Lending Crowdfunding: Principles and Market Development // Advances in Crowdfunding. – Palgrave Macmillan. Cham. 2020. – P. 63-92.

217 Ferbrache D., The rise of ransomware during COVID-19, How to adapt to the new threat environment // https://home.kpmg/xx/en/home/insights/2020/05/rise-of-ransomware-during-covid-19.html. 25.05.2020.

ПРИЛОЖЕНИЕ А

Результаты онлайн анкетирования пользователей цифровых услуг

Метод сбора информации: Онлайн анкетирование.
Выборка: 182 респондентов.
География опроса: Казахстан.
Период проведения опроса: дата 12.04.2018 время 10:45:12 – дата 19.02.2020 время 21:20:25.

Уважаемый респондент,

Представляю Вашему вниманию вопросник, который был разработан с целью получения информации о качестве и степени безопасности цифровых услуг в Казахстане, а также о важности доверия населения к реализации государственной программы «Цифровой Казахстан».

Ваши ответы строго конфиденциальны и анонимны, и будет использованы только в рамках данного исследования.

Ваш ответ очень важен и может улучшить систему цифровых услуг и повысить их безопасность. Опрос займет не более 3 минут.

Если у Вас есть какие-либо вопросы по исследованию, пожалуйста, пишите в любое время на адрес: IssabayevaSymbat@gmail.com.

Заранее огромное Вам спасибо.
С уважением,
Сымбат Исабаева

Таблица А.1 – Сколько Вам лет

Варианты ответов	Количество	Проценты
20 лет и моложе	5	3
от 21 – 30 лет	69	38
от 31 – 40 года	75	41
от 41 - 55 лет	27	15
56 лет и старше	6	3
Итого	182	100

Таблица А.2 – Укажите Ваш пол:

Варианты ответов	Количество	Проценты
Муж	88	48
Жен	94	52
Итого	182	100

Таблица А.2 – Укажите сферу деятельности

Варианты ответов	Количество	Проценты
Временно безработный	4	2
Частный предприниматель	5	3
В отпуске по уходу за ребенком	8	4
Студент	19	10
Работник квазигосударственного сектора	27	15
Работник частного сектора	36	20
Государственный служащий	68	37
Другое	15	8
Итого	182	100

Таблица А.4 – Как часто Вы используете услуги онлайн (включая государственные услуги Egov)?

Варианты ответов	Количество	Проценты
Каждый день	10	5
Несколько раз в неделю	29	16
Раз в неделю	37	20
Раз в квартал	82	45
Не пользуюсь	24	13
Итого	182	100

Таблица А.5 – Как Вы оцениваете онлайн услуги в Республике Казахстан, учитывая их стоимость и качество?

Варианты ответов	Количество	Проценты
Очень хорошо	25	14
Хорошо	73	40
Удовлетворительно	67	37
Плохо	17	9
Итого	182	100

Таблица А.6 – Как Вы думаете, затрудняют ли такие методы как аутентификация или шифрование финансовой информации /данных развитию цифровых услуг?

Варианты ответов	Количество	Проценты
Думаю, что нет	86	47
Да, такие методы неудобны, но безопасны	58	32
Затрудняюсь ответить	38	21
Итого	182	100

Таблица А.7 – Как Вы считаете, насколько важно доверие казахстанского населения к реализации государственной программы «Цифровой Казахстан»

Варианты ответов	Количество	Проценты
Очень важно 70-100%	99	54
Важно 50-69%	52	29
Незначительно важно 30-49%	18	10
Неважно 1-29%	8	4
Затрудняюсь ответить	5	3
Итого	182	100

Таблица А.8 – Мое доверие к реализации программы «Цифровой Казахстан»

Варианты ответов	Количество	Проценты
Полностью доверяю 70-100%	28	15
Доверяю 50-69%	65	36
Частично доверяю 30-49%	59	32
Не доверяю 1-29%	23	13
Я не знаю и не слышал(а) о программе «Цифровой Казахстан»	7	4
Итого	182	100

Таблица А.9 – Как Вы относитесь к нововведениям, которые внедряются правительством в сфере государственных услуг?

Варианты ответов	Количество	Проценты
Я сторонник нововведения	73	40
В целом отношусь положительно	99	54
Не всегда приветствую нововведения	10	5
Я консервативен, и отношусь к нововведениям со скептицизмом	0	0
Итого	182	100

Таблица А.10 – Что бы Вы предложили для повышения доверия к реализации программы «Цифровой Казахстан». Выберите предложенные варианты ответов.

Варианты ответов	Количество	Проценты
1	2	3
Необходимо развивать политику обеспечения кибербезобасности (информационной безопасности в цифровом пространстве)	91	26
Повышать государственное регулирование через нормативно-правовые акты и технические инструменты	45	13
Осуществлять подготовку и повышение квалификации специалистов путем изменения образовательных программ в отечественных ВУЗах с привлечением частного бизнеса	108	31

Продолжение таблицы А.10

1	2	3
Организовать краткосрочные курсы для всех заинтересованных граждан и бизнес сектор по компьютерной грамотности и информационной безопасности в цифровом пространстве	87	25
Затрудняюсь выбрать ответ, так как я не эксперт в данной отрасли	18	5
Итого	349	100
Примечание – Возможность выбора нескольких ответов одновременно		

Таблица А.11 – Сталкивались ли Вы с какими либо проблемами в Казахстане, связанными с онлайн услугами (включая государственные услуги Egov)?

Варианты ответов	Количество	Проценты
1	2	3
Кибератаки (потеря личных данных)	8	3
Проблемы с сетью Интернет, ошибки со стороны оператора связи	96	41
Технические проблемы устройств	79	34
Не сталкивалась, так как я не доверяю отечественным цифровым услугам	9	4
Затрудняюсь ответить	43	18
Итого	235	100
Примечание – Возможность выбора нескольких ответов одновременно		

Таблица А.12 – Можете ли Вы определить основные угрозы для дальнейшего развития цифровых услуг в Республике Казахстан?

Варианты ответов	Количество	Проценты
Кибератаки (незащищенность сетей)	89	26
Нехватка квалифицированных специалистов	133	38
Слаба развитая система предоставления услуг операторами связи	69	20
Недостаточность выделенных и привлеченных финансовых ресурсов	48	14
Угроз на сегодняшний день не имеются	10	3
Итого	349	100
Примечание – Возможность выбора нескольких ответов одновременно		

Рисунок А.1 – Какие из следующих рисков, по Вашему мнению, могут препятствовать пользователям в использовании онлайн услуг в Казахстане?

Примечание – Составлено автором

Открытый вопрос. Есть ли у Вас идеи по улучшению и внедрению новых цифровых услуг в Республике Казахстан, обеспечивая их кибербезопасность? *(Для сведения: пройдя по ссылке http://adilet.zan.kz/rus/docs/P1700000407 Вы можете ознакомиться с концепцией «Киберщит Казахстана»).*

Р. Необходимо внедрять приемлемые и проверенные новшества зарубежных стран в сфере кибербезопасности».

Р. «Создать условия, чтобы цифровая цивилизация дошла до сел и аулов».

Р. «Необходимо обеспечить сохранность данных граждан и исключить их использование другими лицами, в т. ч. некоторыми гос.органами.»

Р. «Создание Центра по кибербезопасности с heightek technology и высококвалифицированными специалистами в IT, это позволит предотвратить угрозы, которые могут возникнуть в будущем и расходы будут гораздо выше. Также именно сейчас необходимо предусмотреть в вузах, академиях КНБ и МВД специальность кибербезопасности».

Р. «Повышение правовой, цифровой и киберграмотности населения».

Р. «Сложно сказать, так как, не являясь специалистом, не имею информации даже о применяемых сегодня мерах. Но защита крайне важна в национальном масштабе».

Р. «В 2016 году взломали сеть компаний «North Caspian operation company», 2 мес работники не могли пользоваться компьютерами на рабочем месте. Это в крупной нефтяной компании, в которой выделяются огромные средства на зарубежные технологии и ресурсы, про госсектор боюсь и думать про гарантии, сохранности персональных данных. Коррупция убивает или сводит на нет такие инициативы. Решением было бы развивать кадры ИТ, как в Америке и Индии, где ИТ в почете, и есть крупные международные хабы».

Р. «Возможно необходимо увеличить количество серверов, находящихся на территории РК, также необходимо усилить защиту онлайн платежей, повысить квалификацию кадров».

Р. «… использовать отечественные программные решения и продукты, …открыто с ИТ сообществом обсуждать архитектуру и принимаемые решения».

Р. «Перевести максимум услуг в онлайн, сделайте их быстрыми, а саму систему максимально прозрачной».

Р. «Необходимо взращивать профессиональные кадры, чтобы преподавать в ВУЗе было выгоднее работы в любом ТОО, отправлять программистов на тренинги по кибербезопасности».

Р. «Только хорошо проработанный законопроект - гарантия защиты данных и применять успешный зарубежный опыт».

«Проблема в управлении, как эти услуги и системы разрабатываются - неправильное отношение: разрабатываются, чтобы заработать деньги или чтобы получить галочку «сделано»…, а отношение должно быть «я делаю это для людей, простого населения, поэтому подойду к разработке этой услуги с умом».

Р. «Нужно кардинально упростить механизм ГЧП и сервисной модели информатизации и облегчить процедуры закупа IT услуг для госорганов».

Р. «…ценные кадры уезжают за границу (много друзей и знакомых уехали работать в Канаду, Польшу, США и Германию). Наше электронное правительство должно быть открытым, то есть такие порталы как госзакупки, егов, кабинет налогоплательщика и т. д. должны предоставлять открытые API функции, чтобы любые частные компании, используя их, могли разрабатывать свои ресурсы или интегрировать их со своими сервисами. Сейчас работать со ШЭП'ом могут только «свои конторы»».

Р. Поменьше госрегулирования в области оказания услуг, привлекать частников на основе окупаемости проектов».

Р. «Организовать сотрудничество с ИТ сообществом, проводить семинары по повышению квалификации на несколько дней бесплатно. Приглашать специалистов квазигосударственного и частных секторов. Необходимо подготовить высококвалифицированных специалистов в этом направлении».

Р. «Современная кибербезопасность - это командная работа. Исходя из плана «Киберщит» и из личного опыта, государство пытается закрыться от всего мира и делать все самому. Это утопия, к которой даже Россия не может прийти. Нужно пересмотреть видение в сторону сотрудничества с другими странами и компаниями. Как пример, можно и следует использовать облачные сервисы, такие как Amazon Web Service, Microsoft Azure и др., так как эти компании более компетентны, а также лучше обеспечивают и инвестируют на безопасность своих серверов, чем может позволить себе любой орган государства или нац.компания….»

Открытый вопрос. Что бы Вы предложили, дополнительно, в целях повышения доверия казахстанцев к реализации программы «Цифровой Казахстан». *(Для сведения: пройдя по данной ссылке, Вы можете ознакомиться с государственной программой «Цифровой Казахстан» http://adilet.zan.kz/rus/docs/P1700000827)*

Р. «Необходимо организовать открытые дискуссионные площадки с привлечением ИТ экспертов. Открыто обсуждать существующие проблемные вопросы и не принимать решения кулуарно, проводить работы по снижению информационного неравенства населения повсеместно».

Р. Максимальная прозрачность - публикация подробных, регулярных отчётов о расходовании средств и проведённых мероприятиях простым и понятным для большинства населения языком….

Р. Создать платформу в рамках egov.kz для сбора предложений (обратной связи) с населения по доработке программы в части реализации новых инициатив, не вошедших в первую редакцию ГП ЦК.

Р. Обеспечить конкурентоспособность казахстанских кадров в сфере ИТ. Что в свою очередь обеспечит кибербезопасность страны.

Р. Необходимо детальнее изучать аудитории/пользователей и их ценности.

Р. Подключать интернет в селах и обучать в старших классах цифровым технологиям. Провести мероприятия в школах и лекции в вузах по теме «Цифровой Казахстан».

Р. Распространять лучшие практики и реальные примеры развития цифровой среды, благодаря которым можно будет показать безопасность, простоту, экономичность, удобство и качество использования.

Р. … каждый шаг должен быть своевременно или заранее разъяснен населению. Прозрачность и доступность информации следует обеспечить с подбором профессиональных спикеров из числа авторитетных экспертов. Эту работу следует сочетать с повышением международного имиджа. Синхронизировать программу цифровизации с работой ведущих корпораций в сфере ИТ. Необходим результат цифровизации на национальном уровне, который мог бы конкурировать с существующими брендами в информационных технологиях, но это упирается в кадровый потенциал сферы.

Р. Необходимо демонстрировать надежность ИС, повышать уровень защищённости персональных данных, в первую очередь исключить возможность поиска ИИН граждан по ФИО /номеру мобильного телефона посредством доступных информационных систем (например, база данных налогоплательщиков КГД, в открытом доступе fa-fa.kz и т.д).

Р. Надо чтобы в первую очередь народ доверял государству. Сейчас нет этого доверия. В этом виноваты наши чиновники, которые думают только о себе. Мы живем в коррумпированной стране, и все прекрасно это знают.

Р. Думаю необходимо не только приобретать новые технологии, но и повышать активность в пользовании ими. Например, в школах, особенно сельских, некоторые мультимедийные, интерактивные доски, устройства

могут использоваться не полностью, не применяют все их возможности в учебном процессе, а где-то могут даже не использовать их вообще. Такие прецеденты были, когда проверяющие органы находили оборудование даже нераспакованным.

Р. Необходимо уменьшить суммы оплат за услуги мобильной связи, чтобы с мобильных выходить на интернет.

Р. Продолжение разъяснения посредством массовой информации о государственных услугах, и кроме этого рассказывать населению не только положительные стороны, но и о тех же самых рисках. И оповещать возникновение таких идей цифровизации не только со стороны государства, и подключать непосредственных людей, имеющих больше знаний в данной области …. Например, по иностранному каналу TED проводятся разъяснения различными специалистами по каждой отрасли, которые рассказывают практику, и тем самым вызывая доверие, население понимает, что они специалисты и больше доверяют им.

Р. Народный контроль, но не с целью наказать госслужащих, а чтобы реально выявлять некачественное исполнение. … Кадров нет в регионах. При таких маленьких зарплатах госслужащим тяжело принимать новшества. Высокие риски коррупции и провала программы из-за формальных отчетностей ….

Ваш ответ сохранен и учтен.

Если у Вас есть какие-либо вопросы по исследованию или о том, как Ваши ответы будут сохранены, пожалуйста, пишите в любое время на адрес: IssabayevaSymbat@gmail.com.

Спасибо Вам за Ваше время и участие!

Результаты онлайн анкетирования по кибербезопасности

Метод сбора информации: Онлайн анкетирование.
Выборка: 357 респондентов.
География опроса: Казхастан.
Период проведения опроса: дата 12.06.2019 время 02:23:44 – дата 19.02.2020 время 20:10:10 .

Таблица А.13 – Укажите Ваш пол:

Варианты ответов	Количество	Проценты
муж.	186	52
жен	171	48
Итого	357	100

Таблица А.14 – Сколько Вам лет:

Варианты ответов	Количество	Проценты
20 лет и моложе	10	3
от 21 – 30 лет	130	36
от 31 – 40 лет	142	40
от 41 - 55 лет	62	17
56 лет и старше	13	4
Итого	357	100

Таблица А.15 – В связи с применением ИКТ, согласны ли вы, что вопрос кибербезопасности является для Вас приоритетом в рамках работы, учебы и жизнедеятельности?

Варианты ответов	Количество	Проценты
Полностью согласен	156	44
Согласен	164	46
Не согласен	26	7
Категорически не согласен	11	3
Итого	357	100

Таблица А.16 – Какие из следующих причин, по Вашему мнению, могут препятствовать пользователям в использовании государственных онлайн услуг в Казахстане?

Варианты ответов	Количество	Проценты
1	2	3
Отсутствие политики кибербезопасности	134	19
Человеческий фактор - самое слабое звено	139	20
Финансирование, нехватка талантов и ресурсов	78	11

Продолжение таблицы А.16

1	2	3
Нет обучения в области кибербезопасности	130	18
Отсутствие ответственности	101	14
Сложность в интеграции источников данных	77	11
Разрыв между расходами и реализацией проектов	51	7
Отсутствие доверия населения местным онлайн сервисам	2	0
Итого	712	100
Примечание – Возможность выбора нескольких ответов одновременно		

Таблица А.17 – Кибератаки (риски в области кибербезопасности) являются барьером для реализации инновационных идей в государственном управлении

Варианты ответов	Количество	Проценты
Нет, кибер угрозы и риски не являются барьером	90	25
Не всегда, но они являются барьером	137	38
Да, они являются барьером	58	16
Затрудняюсь ответить	69	19
Итого	354	100

Таблица А.18 – Как Вы смотрите на установку «национального сертификата безопасности»?

Варианты ответов	Количество	Проценты
Положительно и не против установить	66	20
Нейтрально, если необходимо, то могу установить	92	27
Отрицательно, нет необходимости устанавливать	57	17
Категорически против установки сертификата	122	36
Другое:	17	5
Итого	354	100

Открытый вопрос. Ваши предложения по улучшению и внедрению новых государственных цифровых услуг в Республике Казахстан в целях обеспечения кибербезопасности?

Р. Необходимо повысить грамотность населения. В связи с последними событиями в Казахстане складывается впечатление, что государство все больше вторгается в личное пространство гражданина. Сертификат безопасности устанавливается с целью слежки и полным контролем населения. На всей планете земля только Казахстану пришло это в голову. США и Европейские страны на такое не решились бы, там засудили всех подряд за нарушение свободы и демократии. Есть множество других способов обеспечить национальную безопасность. Поддержать рождаемость, экологию и начинать уже думать о народе... Использование сертификата это атака MITM («Man In The Middle» – «человек посередине»). Такое нельзя

использовать в рамках государства. В рамках компании - да, для государственного органа - да, но не для всего государства, и то, что говорят чиновники о сертификате это - абсолютная некомпетентность. Каждый надёжный ресурс имеет свой сертификат безопасности, который соответствует всем требованиям безопасности и проверяется и выпускается соответствующими доверенными органами. С технической точки зрения промежуточный сертификат «безопасности» не имеет некого смысла. Люди просто перестанут обращать внимание на валидность сертификата и будут передавать свои данные в сети возможным злоумышленникам. Не совершать (применительно к госчиновникам) действий, приводящих к появлению «не приемлемого» контента, а если и были совершены - предпринять все возможны меры для минимизации ущерба для государства кроме блокирования доступа к информации. Населению не разъяснили для чего, и как работает СНБ.

Р. «Google и Facebook заблокировали казахстанский сертификат безопасности, который крал данные».

Р. Старшему поколению никто не может объяснить и помочь с установкой Сертификата безопасности. В этой связи необходимо искать пути использования Электронно-цифровой подписи без сертификата. Либо проводить масштабную разъяснительную работу гражданам.

Р. Национальный сертификат безопасности - это нарушение права о конфиденциальности персональных данных, так как сертификат собирает всю информацию, включая пароли от аккаунтов, счетов, Pin-коды, пр.

Р. Национальная безопасность не должна ущемлять права пользователей Интернет.

Р. Сертификат это и есть угроза.

Р. Отрицательно, нет необходимости устанавливать.

Р. Повысить грамотность населения.

Р. Стимулирование грантами работников для развития навыков в области кибербезопасности и IT.

Р. Нужно усилить защиту и конфиденциальность данных в облачных хранилищах, так как их у нас недостаточно.

Р. Внедрение всех нововведений в кибербезопасности только после опроса населения и консультаций с техническими специалистами.

Р. Необходимо всю деятельность государства цифровизировать.

Р. Необходимо обеспечить доверие к государственным институтам.

Р. Нужно создать независимую спецслужбу, проводить разъяснения и обучение киберсамообороны еще с детского возраста

Р. Сделать привязку аккаунта в госаккаунтах к номеру мобильного телефона

Р. Обеспечить бесплатным антивирусом.

Р. Чтобы народ не обращался за услугами в госорганы, а получали через портал Egov цифровые государственные услуги

Р. Увеличить финансирование для привлечения узкопрофильных специалистов, проводить качественный отбор для отсеивания профессионально непригодных специалистов.

Р. Создать комиссии с профессионалами по разработке мер и процедур ИБ. Сделать все на основе open source. Пример Италии, где сейчас все сервисы страны начали делать не на основе предложений вендора, а на основе возможности доработки открытого кода всех информационных ресурсов и систем государства.

Р. О своей кибербезопасности каждый должен позаботиться сам: не заходить на подозрительные сайты, не вестись фишингу, фармингу, и др; Ставить сильные пароли в аккаунтах, использовать two factor authentification, как метод защиты своих данных.

Р. Создание собственных поисковых систем (как гугл, яндекс и др.)

Р. Доработать уже имеющиеся приложения. Обновлять своевременно приложения при обновлении операционной системы, постоянно мониторить и вводить новые корректные данные, систематика и стабильность самое важное...

Р. Все ИС отправлять на независимую оценку (пентест и прочие проверки) частным компаниям, а не только АО ГТС КНБ РК.

Р. Хоть это и трудоемко и утопично, есть нужда в обучении населения киберграмотности. Не только так, чтоб бабушки и дяди в Egov умели заходить и билеты онлайн покупали, а вообще, чтобы у них развить навыки саморазвития техграмотности.

Р. Совершенствовать законы в области кибербезопасности, привлекать к ответственности. Внедрение Закона о Кибербезопасности.

Р. Возможность единой базы. Интегрирование данных

Р. Самый важный факт - соблюдение сохранности данных. Наращивание талантов без утечек мозгов. Необходимо дать соответствующее образование по кибербезопасности и постоянно совершенствовать навыки.

Р. Совершенствовать систему обеспечения цифровых данных в ГО, финансовом секторе (пенсионный фонд, социальное страхование, банки). Возникает вопрос, если негосударственная организация в лице палаты предпринимателей Атамекен имеет доступ к информации по поступлениям в пенсионный фонд выпускников ВУЗов, то о какой кибербезопасности можно говорить. Банки как заинтересованные лица должны совершенствовать свои программы, приложения, так как получают за это свои вознаграждения.

Р. Увеличить мощность Egov. Упростить формы всех отчетностей или создать ресурс, который сам будет генерировать декларирование доходов и расходов граждан.

Р. Широко освещать проблематику, обсуждать, создавать поле для заинтересованных участников, пилотные проекты запускать с последующей оценкой экспертов

Р. Выделять финансовые средства, обучать прокуроров, судей и следователей как расследовать киберпреступления, обучение граждан основам кибербезопасности. Создать дата центры.

Р. Необходимо принять Закон о противодействии киберпреступности.

Р. Не стоит устанавливать НСБ.

Р. Прозрачность деятельности в области кибербезопасности

Р. Усовершенствовать ЕТС (скорость передачи данных маленькая)

Р. Максимальная защита персональных данных пользователей, свободный и беспрепятственный доступ к интернету

Р. Не создавать монополиста в этой сфере и максимально просвещать население

Р. Кибербезопасность касается исключительно интересов государства. Граждане и юридические лица должны самостоятельно осуществлять кибербезопасность в зависимости от уровня наличия секретов. Государство, реализуя кибербезопасность не должно затрагивать интересов граждан и юридических лиц, они самостоятельно должны это делать. Лучше бюджет на реализацию киберщита направить на социальные программы

Р. Необходимо повышать компьютерную грамотность и доверие со стороны населения. Привлекать сильных ИТ специалистов.

Р. Обеспечить широким покрытием интернета, особенно в селах. Постоянное совершенствование кибербезопасности через анализ.

Р. Не нарушать свободу граждан в информационном пространстве

Р. Решения принимать в этой сфере после доступного обсуждения среди возможно большего числа пользователей государственных услуг.

Р. Создать новое министерство по кибербезопасности

Р. Сначала прекратите воровать деньги с бюджета

Р. Грамотная политика, ответственность за принимаемые меры, максимальная прозрачность. Законодательные нормы привести в соответствие.

Р. Народ не доверяет правительству, пусть создадут такую программу, где третьему лицу не будут доступны наши данные

Р. Больше специалистов готовить по кибербезопасности. Обучать молодежь зарубежном. Необходимо со школьной скамьи углубленно изучать кибербезопасность и обучать население

Р. Для начала искоренить коррупцию с гос. управления.

Р. Переосмыслить подходы реализации ИБ в стране. Использование мирового опыта, не китайского и российского.

Р. Для начала установить на всех госсайтах ssl сертификат.

Р. Следует регулярно проводить обучение IT специалистов на местах и далее эти специалисты должны обучать личный состав на постоянной основе.

Р. Информирование населения по ИБ и цифровым услугам

Р. Бесплатные обучение населения по кибербезопасности

Р. Нужно улучшать то, что есть, начнём с ЭЦП, был хороший прогресс, который переселился в удостоверения личности. Нужно вводить мобильный

Egov, но если использовать мобильные номера, то и нужно улучшать защиту и ответственность. Нужно давать максимум интернета всем бюджетным и госучреждениям. Также нужно вести какую-то форму отказа от цифровых услуг, потому что есть лица, которые более доверчивы бумажным документам.

Р. Отменить ЭЦП. Ввести возможность входа на портал государственных услуги с помощью своего собственного логина и пароля

Р. Установить ответственность конкретных исполнителей, все технические меры по кибербезопасности не приведут к хорошему результату. Преступники тоже обучаются…

Р. Нет системного подхода. МИО передают информацию по незащищенным каналам.

Р. Государственные услуги необходимо оказывать без утечки персональных данных третьим лицам, усилить кибер информационную безопасность на должном уровне, изучить и перенять опыт преуспевших стран в этой деятельности.

Р. Необходимо к каждой государственной цифровой услуге, иметь свою политику безопасности

Р. Больше уделять внимаю обеспечению ИБ. И больше внести вклад в развитие именно культуре поведения в школьной программе. МОН РК внедряло не только машиностроение, но и как соблюдать ИБ. Привлекали специалистов в области ИБ. В Казахстане есть KZ-CERT надо чтоб они вели несколько часов в неделю уроки по ИБ.

Р. Отсутствие организации, которая ведет и реализует единую политику

Р .Открыть ВУЗ или факультетов в сфере по обучению современных инновационных технологий (в т.ч. IT-программистов-специалистов и др.) в целях обеспечения кибербезопасности. Также рассмотреть вопрос о включении в штатное расписание должность по кибербезопасности.

Ваш ответ сохранен и учтен.

Если у Вас есть какие-либо вопросы по исследованию или о том, как Ваши ответы будут сохранены, пожалуйста, пишите в любое время на адрес: IssabayevaSymbat@gmail.com.

Спасибо Вам за Ваше время и участие!

Результаты онлайн анкетирования экспертов в сфере ИТ

Метод сбора информации: Онлайн анкетирование.
Выборка: 12 экспертов
География опроса: Казхастан.
Период проведения опроса: дата 12.06.2018 время 22:05:53– дата 16.06.2018 время 09:35:06.

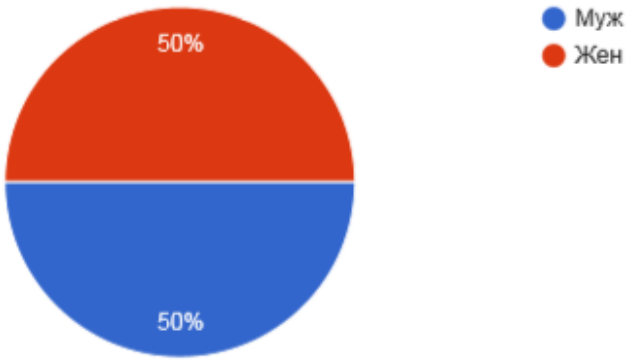

Рисунок А.2 – Укажите Ваш пол

Примечание – Составлено автором

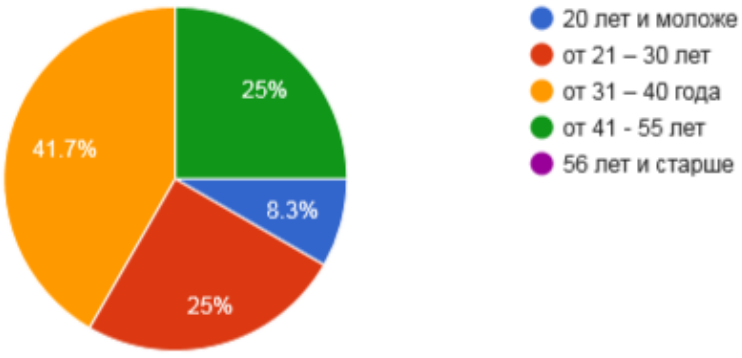

Рисунок А.3 - Сколько Вам лет

Примечание – Составлено автором

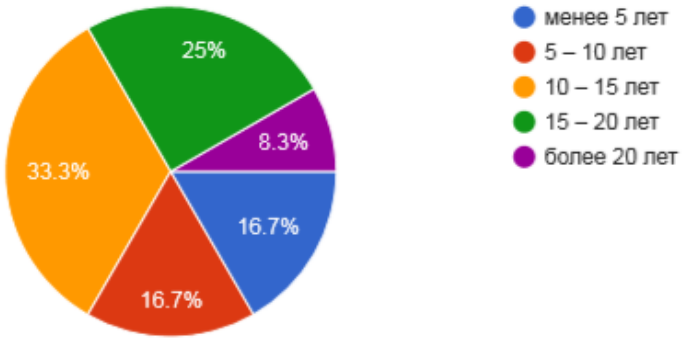

Рисунок А.4 – Укажите Ваш стаж работы

Примечание – Составлено автором

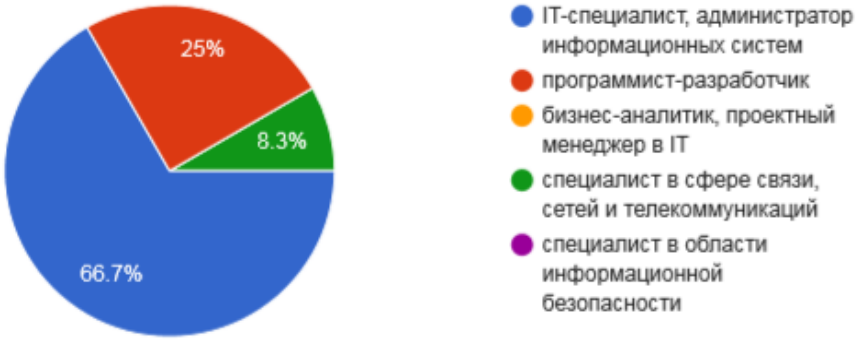

Рисунок А.5 – Укажите Вашу специализацию:

Примечание – Составлено автором

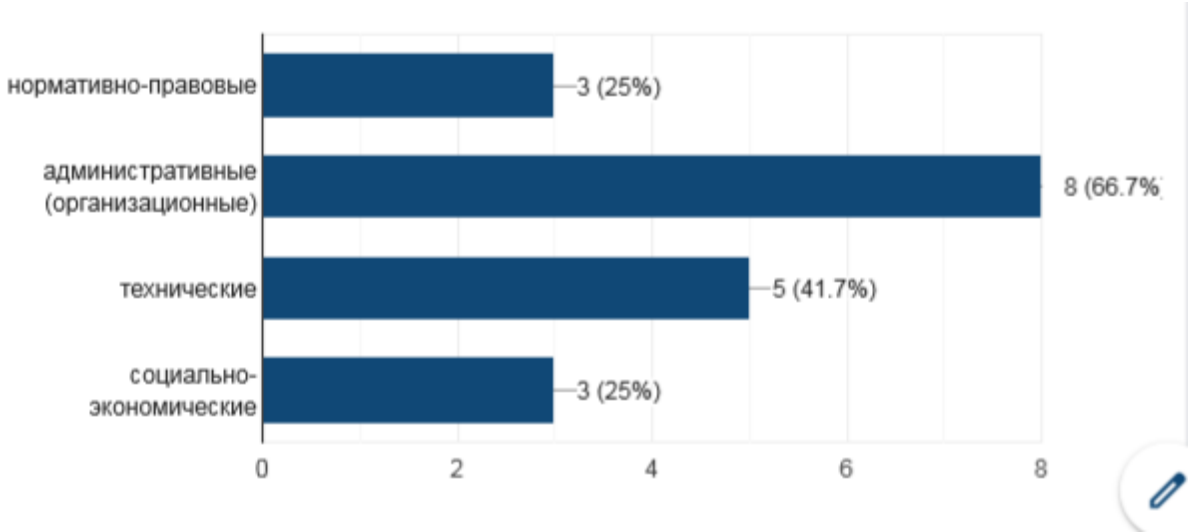

Рисунок А.6 – С какими трудностями Вы и Ваша организация чаще всего сталкиваетесь в процессе работы по проектам информатизации и цифровизации?

Примечание – Составлено автором

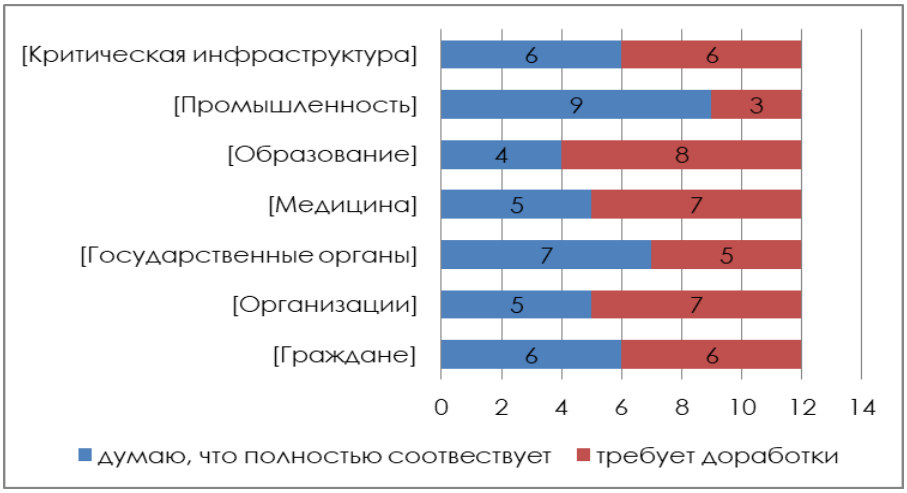

Рисунок А.7 – Имеются ли на Ваш взгляд какие либо ограничения или барьеры на рынке Казахстана для развития и внедрения цифровых технологий?

Примечание – составлено автором

Открытый вопрос. Если да, то можете в деталях описать данную проблему.

Р. Блокировка порталов по хотению не понравившиеся администрации президента, внедрение киберщита и т.д.

Р. Оборудование чаще всего не соответствует современному стандарту

Р. Отсутствие необходимой финансовой поддержки со стороны государства действительно прорывным исследованиям и изобретениям.

Р. Преподавание в учебных заведениях примитивным и не актуальным темам информационных технологий.

Р. Р. Мы не конкурентоспособны в плане цифровой грамотности.

Р. Государственные учреждения тормозят развитие электронной эры.

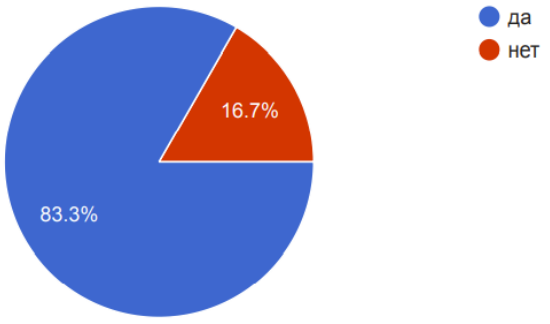

Рисунок А.8 – Есть ли необходимость изменения существующей организационной структуры взаимодействия государственных учреждений и уполномоченных органов, которые обеспечивают процессы политики обеспечения Кибербезопасности

Примечание – Составлено автором

Ваши предложения по улучшению обеспечения кибербезопасности в Казахстане

Р. Изучение международного опыта

Р. Подготовка специалистов

Р. Искоренить компьютерную безграмотность, ввести понятие цифровой гигиены

Р. Совершенствование нормативно правовых документов

Р. Работать и повышать квалификацию.

Ваш ответ сохранен и учтен.

Если у Вас есть какие-либо вопросы по исследованию или о том, как Ваши ответы будут сохранены, пожалуйста, пишите в любое время на адрес: IssabayevaSymbat@gmail.com.

Спасибо Вам за Ваше время и участие!

ПРИЛОЖЕНИЕ Б

Акт о внедрении результатов исследования

Л.Н.Гумилев атындағы ЕҰУ-нің ақпараттық қауіпсіздік және криптология ғылыми-зерттеу институты
010008, Астана қ., К.Сатпаев к-сі, 2, тел.: 8 (7172) 70-95-00, www.iisc.kz

Научно-исследовательский институт информационной безопасности и криптологии ЕНУ им. Л.Н.Гумилева
010008, г. Астана, ул. К.Сатпаева, 2, тел.: 8 (7172) 70-95-00, www.iisc.kz

«27» ноября 2018 г.

Диссертационный совет по специальности «6D051000 – Государственное и местное управление» при Академии государственного управления при Президенте Республики Казахстан

Научно-исследовательский институт информационной безопасности и криптологии Евразийского национального университета им. Л.Н. Гумилева (далее – Институт) подтверждает, что Исабаева Сымбат Болатовна в рамках своей диссертационной работы: *«Обеспечение кибербезопасности Казахстана в условиях глобальной цифровизации»* принимала участие в совещании в качестве независимого научного консультанта по обсуждению вопросов кибербезопасности Республики Казахстан. Совещания проходило с участием экспертами Казахстана в области информационных технологий и кибербезопасности. В ходе совещании комментарии и рекомендации Исабаевой С.Б. были учтены в рамках работы Института.

Кандидат физико-математических наук, директор научно-исследовательского института информационной безопасности и криптологии ЕНУ им. Л.Н. Гумилева **Е. Сейткулов**

Акт оказанных услуг
к договору возмездного оказания услуг
«27» января 2020 года № 25-ИПУ-911

г. Нур-Султан **«28» февраля 2020 года**

РГКП «Академия государственного управления при Президенте Республики Казахстан» (далее – Академия), именуемое в дальнейшем «Заказчик», в лице вице-ректора по учебной работе и академической мобильности Актымбаевой А.С., действующей на основании приказа ректора от 20 декабря 2016 года №677, с одной стороны, и гражданка Республики Казахстан Исабаева Сымбат Болатовна, удостоверение личности № 043687292 выданное МВД РК от 22.12.2017 г., именуемая в дальнейшем «Исполнитель», с другой стороны, далее совместно именуемые «Стороны», составили и подписали Акт оказанных услуг о нижеследующем:

1. «19 - 20» февраля 2020 года Исполнитель по заданию Заказчика оказал образовательные услуги по теме «Основы кибербезопасности» в количестве 6 академических часов на курсах переподготовки государственных служащих, впервые поступивших на административную государственную службу корпуса «Б», проводимые с 10 по 28 февраля 2020 года.

Общая стоимость услуг составляет 90 000 (девяносто тысяч) тенге и включает в себя все налоги и сборы, предусмотренные законодательством Республики Казахстан.

2. Акт оказанных услуг составлен в 2 (двух) экземплярах, на русском языке, по 1 (одному) экземпляру для каждой из Сторон.

Заказчик	**Исполнитель**
РГКП «Академия государственного управления при Президенте Республики Казахстан»	Исабаева Сымбат Болатовна
Вице-ректор по учебной работе и академической мобильности	
_____ **А. Актымбаева**	_____ **С. Исабаева**

ПРИЛОЖЕНИЕ В

Результаты слушателей Академии государственного управления при Президенте РК курса переподготовки по теме: «Основы кибербезопасности»

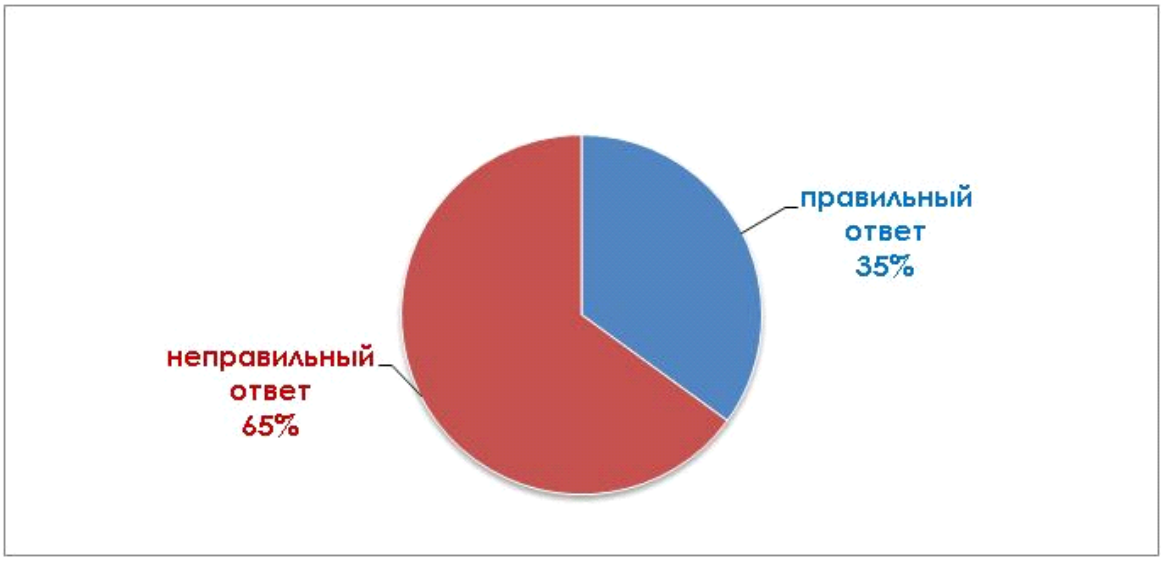

Рисунок С.1 – Результаты слушателей до начала занятий «Основы кибербезопасности»

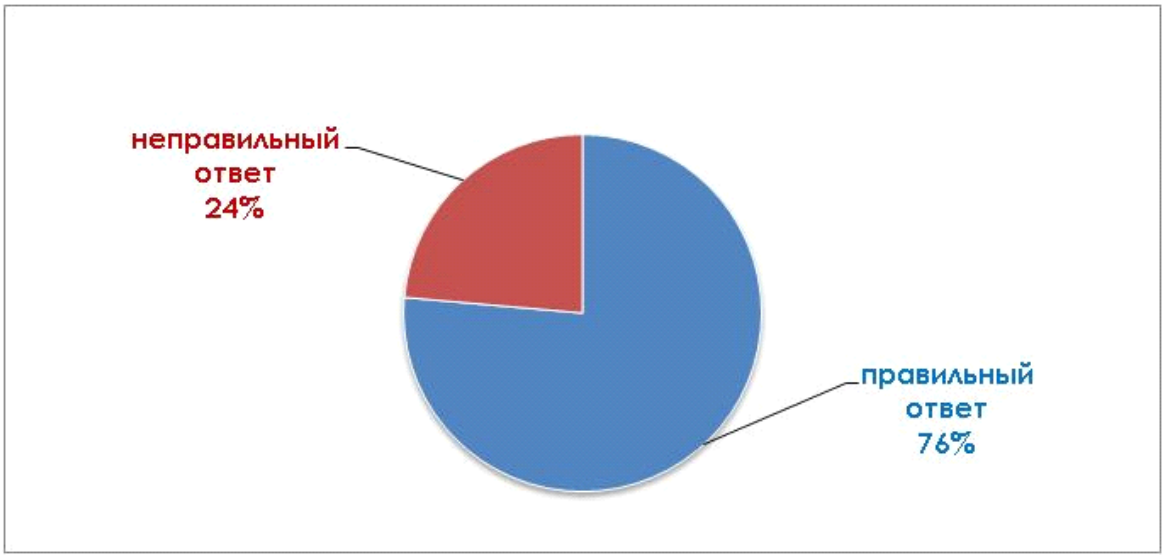

Рисунок С.2 – Результаты слушателей после завершения занятий «Основы кибербезопасности»

ПРИЛОЖЕНИЕ Г

Таблица Г.1 – Сравнительная таблица по внесению изменения в некоторые НПА Казахстана в области кибербезопасности

Нормативно правовой акт	Действующая редакция	Предлагаемая редакция	Примечание
1	2	*3*	4
Закон РК «Об информатизации» от 24 ноября 2015 года № 418-V ЗРК, п. 7. Статьи 1	«Информационная безопасность в сфере информатизации (далее – информационная безопасность) – состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз».	*«Кибербезопасность - это комплекс организационно-правовых, экономических и технических процедур в целях защиты от несанкционированного использования информационных ресурсов в киберпространстве».*	Предлагаемые соответствующие изменения в нормативно-правовые акты Республики даст единое понимание определению «цифровая безопасность», «информационная безопасность в сфере информатизации», а также «кибербезопасность». На сегодня в разных НПА представлены разные оправления, которые несут идентичное понимание «цифровая безопасность», «информационная безопасность в сфере информатизации» и «кибербезопасность».
Концепция кибербезопасности от 30 июня 2017 года № 407, глава 1 «Введение»	Кибербезопасность - это «состояние защищенности информации в электронной форме и среды ее обработки, хранения, передачи (электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры) от внешних и внутренних угроз, то есть информационная безопасность в сфере информатизации».		
Концепция кибербезопасности от 30 июня 2017 года № 407, глава 1 «Введение»	«Защита информации или электронных информационных ресурсов и информационных систем – комплекс физических, технических, программных, криптографических и административных мер, направленных на обеспечение информационной безопасности».		

Продолжение таблицы Г.1

1	2	**3**	4
Концепция кибербезопасности от 30 июня 2017 года № 407, глава 1 «Введение»	«Компьютерная атака – целенаправленная попытка реализации угрозы несанкционированного воздействия на информацию, электронный ресурс, информационную систему или получения доступа к ним с применением программных или программно-аппаратных средств (или протоколов межсетевого взаимодействия)».	*Кибератака - незаконная попытка нанести вред через киберпространство с целью отключения, разрушения, злонамеренного контроля информационной системы, вычислительной среды, инфраструктуры или кражи электронных данных нарушая их целостность.*	Изученный международный опыт, а также их стандарты (NIST SP 800-30 Rev. 1 CNSSI 4009 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf, ISO/IEC 27000) показывают, что слово «компьютерная атака» не раскрывать суть всех атак, которые происходят в киберпространстве, так как атаки бывают не только компьютерные. На сегодняшний день атаки происходят в целом киберпространсте на любые цифровые гаджеты. То есть, это могут быть смартфоны, планшеты, компьютеры, и серверы.
			Более того, проведенный анализ показывает, что всеми известный Оксфордский и Кембриджский словарь не имеет в базе слово «компьютерная атака». В период цифровой глобализации считаем целесообразным применять всеми признанный и общедоступный понятийный аппарат в ИТ. индустрии, так как большинство определении слов в области цифровизации приходят к нам из-за рубежа.

ПРИЛОЖЕНИЕ Д

Таблица Д.1 – Исходные коды

Вид регресии	Код	Результат	Дополнительная информация
1	2	3	4
1 - дисперсионный	disp1 <- aov(reg1$innovative_person ~ reg1$age + reg1$gender, data=reg1) summary(disp1)	Df Sum Sq Mean Sq F value Pr(>F) reg1$age 1 0.59 0.588 0.434 0.5110 reg1$gender 1 5.92 5.924 4.373 0.0379 * Residuals 179 242.48 1.355 --- Signif. codes: 0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1	Различия между мужчинами и женщинами при ответе на вопрос «Считаете ли Вы себя инновационным человеком?» существенны, в отличии от различий по возрасту уровень p-value 0.01 Регрессия: коэффициент регрессии отрицательный, уровень личного восприятия инновационной растёт, по мере уменьшения возраста (-0.36112), уровень p-value 0.01
1 - регрессионный	agegen_in <- lm(reg1$innovative_person~reg1$age+reg1$gender) summary(agegen_in)	Call: lm(formula = reg1$innovative_person ~ reg1$age + reg1$gender) Residuals: Min 1Q Median 3Q Max -1.3030 -0.8795 -0.7548 1.1205 2.8217 Coefficients: Estimate Std. Error t value Pr(>\|t\|) (Intercept) 2.72647 0.39074 6.978 5.62e-11 *** reg1$age -0.06235 0.10163 -0.613 0.5403 reg1$gender -0.36112 0.17268 -2.091 0.0379 * --- Signif. codes: 0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1 Residual standard error: 1.164 on 179 degrees of freedom Multiple R-squared: 0.02615, Adjusted R-squared: 0.01527 F-statistic: 2.404 on 2 and 179 DF, p-value: 0.09331	

Продолжение таблицы Д.1

1	2	3	4
2 - дисперсионный	disp2 <- aov(reg1$innovations_feel ~ reg1$age + reg1$gender, data=reg1) summary(disp2)	Df Sum Sq Mean Sq F value Pr(>F) reg1$age 1 0.04 0.0354 0.104 0.748 reg1$gender 1 0.27 0.2679 0.788 0.376 Residuals 179 60.89 0.3402	Различия между мужчинами и женщинами, а также различия по возрасту при ответе на вопрос «Как Вы относитесь к нововведениям?» не существенны
2 – регрессионный	agegen_infeel <- lm(reg1$innovations_feel~reg1$age+reg1$gender) > summary(agegen_infeel)	Call: lm(formula = reg1$innovations_feel ~ reg1$age + reg1$gender) Residuals: Min 1Q Median 3Q Max -0.7321 -0.6205 0.3027 0.3795 1.3968 Coefficients: Estimate Std. Error t value Pr(>\|t\|) (Intercept) 1.72197 0.19580 8.794 1.18e-15 *** reg1$age 0.01739 0.05093 0.341 0.733 reg1$gender -0.07680 0.08653 -0.887 0.376 --- Signif. codes: 0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1 Residual standard error: 0.5832 on 179 degrees of freedom Multiple R-squared: 0.004956, Adjusted R-squared: -0.006162 F-statistic: 0.4458 on 2 and 179 DF, p-value: 0.641	

Продолжение таблицы Д.1

1	2	3	4
3 - дисперсионный	disp2 <- aov(reg1$confidence_digital_Kazakhstan ~ reg1$threats_digital_services, data=reg1) summary(disp2)	Df Sum Sq Mean Sq F value Pr(>F) reg1$threats_digital_services 16 22.53 1.408 1.394 0.15 Residuals 165 166.70 1.010	Взаимосвязь между ответами на вопросы «Можете ли вы определить основные угрозы для дальнейшего развития цифровых услуг в Республике Казахстан?» и «Моё доверие к реализации программы «Цифровой Казахстан» не существенна
3 – регрессионный	lm <- lm(reg$confidence_digital_Kazakhstan ~ reg$threats_digital_services) summary(lm)	Call: lm(formula = reg$confidence_digital_Kazakhstan ~ reg$threats_digital_services) Residuals: Min 1Q Median 3Q Max -1.9500 -0.6296 0.0000 0.5882 2.5882 Coefficients: Estimate Std. Error t value Pr(>|t|) (Intercept) 2.000e+00 1.005e+00 1.990 0.0483 * reg$threats_digital_services10 -2.000e-01 1.101e+00 -0.182 0.8561 reg$threats_digital_services11 6.000e-01 1.101e+00 0.545 0.5865 reg$threats_digital_services12 4.118e-01 1.020e+00 0.404 0.6869 reg$threats_digital_services13 1.667e-01 1.033e+00 0.161 0.8720 reg$threats_digital_services14 -2.500e-01 1.066e+00 -0.234 0.8149 reg$threats_digital_services15 -2.925e-14 1.421e+00 0.000 1.0000 reg$threats_digital_services16 -3.397e-14 1.421e+00 0.000	

Продолжение таблицы Д.1

1	2	3	4
		1.0000 reg$threats_digital_services2 8.667e-01 1.038e+00 0.835 0.4050 reg$threats_digital_services3 4.545e-01 1.050e+00 0.433 0.6656 reg$threats_digital_services4 1.000e+00 1.054e+00 0.949 0.3442 reg$threats_digital_services4. 14 1.000e+00 1.421e+00 0.703 0.4827 reg$threats_digital_services5 6.000e-01 1.101e+00 0.545 0.5865 reg$threats_digital_services6 1.000e+00 1.050e+00 0.953 0.3422 reg$threats_digital_services7 2.222e-01 1.060e+00 0.210 0.8341 reg$threats_digital_services8 9.500e-01 1.030e+00 0.922 0.3577 reg$threats_digital_services9 6.296e-01 1.024e+00 0.615 0.5393 --- Signif. codes: 0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1 Residual standard error: 1.005 on 165 degrees of freedom (23 observations deleted due to missingness) Multiple R-squared: 0.1191, Adjusted R-squared: 0.03365 F-statistic: 1.394 on 16 and 165 DF, p-value: 0.1501	

Продолжение таблицы Д.1

1	2	3	4
4 - дисперсионный	disp2 <- aov(reg1$often_online_services~reg1$In_activity, data=reg1) summary(disp2)	Df Sum Sq Mean Sq F value Pr(>F) reg1$In_activity 7 11.22 1.603 1.396 0.21 Residuals 174 199.73 1.148	Частота использования онлайн услуг различается в зависимости от вида деятельности только для занятых в области «QPSW» p-value 0.1 Регрессия: коэффициент (0.4630).
4 – регрессионный	reg2 <- lm(reg1$often_online_services~reg1$In_activity, data=reg1) summary(reg2)	Call: lm(formula = reg1$often_online_services ~ reg1$In_activity, data = reg1) Residuals: Min 1Q Median 3Q Max -2.5000 -0.6389 0.3611 0.6382 1.9630 Coefficients: Estimate Std. Error t value Pr(>|t|) (Intercept) 3.5000 0.1299 26.938 <2e-16 *** reg1$In_activityO -0.2333 0.3056 -0.763 0.4462 reg1$In_activityPL 0.3750 0.4005 0.936 0.3504 reg1$In_activityPSW 0.1389 0.2208 0.629 0.5302 reg1$In_activityQPSW -0.4630 0.2437 -1.900 0.0591 . reg1$In_activityS -0.1842 0.2780 -0.663 0.5085 reg1$In_activitySE -0.3000 0.4964 -0.604 0.5464 reg1$In_activityTU 0.7500 0.5512 1.361 0.1754 --- Signif. codes: 0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1 Residual standard error: 1.071 on 174 degrees of freedom Multiple R-squared: 0.05318, Adjusted R-squared: 0.01509 F-statistic: 1.396 on 7 and 174 DF, p-value: 0.2097	

Продолжение таблицы Д.1

1	2	3	4
5 - дисперсионный	disp2 <- aov(reg1$rate_online_services~reg1$activity, data=reg1) summary(disp2)	Df Sum Sq Mean Sq F value Pr(>F) reg1$activity 1 0.01 0.0112 0.016 0.9 Residuals 180 128.25 0.7125	Оцениваете онлайн услуги в Республике Казахстан, учитывая их стоимость и качество различается в зависимости от вида деятельности только для занятых в области «QPSW» PSW p-value 0.1 и p-value 0.01
5 – регрессионный	reg3 <- lm(reg1$rate_online_services~reg1$In_activity, data=reg1) summary(reg3)	Call: lm(formula = reg1$rate_online_services ~ reg1$In_activity, data = reg1) Residuals: Min 1Q Median 3Q Max -1.7407 -0.4737 -0.2500 0.6000 1.7500 Coefficients: Estimate Std. Error t value Pr(>|t|) (Intercept) 2.250e+00 1.013e-01 22.208 <2e-16 *** reg1$In_activityO 1.500e-01 2.383e-01 0.629 0.5299 reg1$In_activityPL -1.250e-01 3.123e-01 -0.400 0.6894 reg1$In_activityPSW 3.333e-01 1.722e-01 1.936 0.0545 . reg1$In_activityQPSW 4.907e-01 1.900e-01 2.582 0.0106 * reg1$In_activityS 2.237e-01 2.168e-01 1.032 0.3036 reg1$In_activitySE -5.000e-02 3.871e-01 -0.129 0.8974 reg1$In_activityTU -7.854e-16 4.298e-01 0.000 1.0000 --- Signif. codes: 0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1 Residual standard error: 0.8354 on 174 degrees of freedom Multiple R-squared: 0.05315, Adjusted R-squared: 0.01505 F-statistic: 1.395 on 7 and 174 DF, p-value: 0.2101	

Продолжение таблицы Д.1

1	2	3	4
6 - дисперсионный	disp2 <- aov(reg1$problems_online_services~reg1$activity, data=reg1) summary(disp2)	Df Sum Sq Mean Sq F value Pr(>F) reg1$activity 1 8.2 8.192 3.812 0.0524 . Residuals 180 386.8 2.149 --- Signif. codes: 0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1	Ответы на вопрос «Сталкивались ли вы, с какими либо проблемами в Казахстане связанные с онлайн услугами (включая государственные услуги Egov)?» различается в зависимости от вида деятельности только для занятых в области «PL» p-value 0.01
6 – регрессионный	reg4 <- lm(reg1$problems_online_services~reg1$In_activity, data=reg1) summary(reg4)	Call: lm(formula = reg1$problems_online_services ~ reg1$In_activity, data = reg1) Residuals: Min 1Q Median 3Q Max -2.3158 -1.0667 -0.0667 1.0875 5.1389 Coefficients: Estimate Std. Error t value Pr(>|t|) (Intercept) 3.6324 0.1771 20.506 <2e-16 *** reg1$In_activityO 0.5657 0.4167 1.358 0.1764 reg1$In_activityPL 1.3824 0.5460 2.532 0.0122 * reg1$In_activityPSW 0.2288 0.3011 0.760 0.4484 reg1$In_activityQPSW 0.1454 0.3323 0.438 0.6622 reg1$In_activityS 0.3166 0.3791 0.835 0.4048 reg1$In_activitySE 0.2324 0.6768 0.343 0.7318 reg1$In_activityTU 0.1176 0.7515 0.157 0.8758 --- Signif. codes: 0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1 Residual standard error: 1.461 on 174 degrees of freedom Multiple R-squared: 0.05996, Adjusted R-squared: 0.02214 F-statistic: 1.585 on 7 and 174 DF, p-value: 0.1425	