УДК 327.090

ОСОБЕННОСТИ И ПРОБЛЕМЫ РЕАЛИЗАЦИИ ПОЛИТИКИ РЕСПУБЛИКИ КАЗАХСТАН В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Нұрғазиева Диана Азизбекқызы
diananurgazieva4@gmail.com
ЕНУ им. Л.Н. Гумилева, Нур-Султан, Казахстан
Научный руководитель – Алькеев А.К.

В современной стратегии национальной безопасности Республики Казахстана имеют место ряд важных приоритетов, соответствующих современным вызовам.

Один из таковых приоритетов заключается в увеличении угроз информационной безопасности, усиливающиеся с расширением глобализационных тенденций и активизацией Казахстана в системе региональной безопасности.

Кроме того, в Стратегии Казахстан- 2030, отмечается, что национальная безопасность существенным образом зависит от информационной безопасности и с техническим развитием эта зависимость будет только усиливаться.

Прежде всего необходимо констатировать, что на сегодняшний день большинство частных компаний и государственных учреждений нашей страны, все шире применяют технологии ИКТ и вместе с тем увеличивают риски и угрозы безопасности.

Так, в 2013 году был зафиксирован один из активных периодов кибернетических атак в Казахстане, был атакован сайт учреждения «Казкосмос», в том же году атаке подверглись 92 % частных компаний, в 2014 году атаке подверглись около 80% компаний, а в 2020 году, произошла мощная кибератака на сайт государственных закупок РК 2020, и т.д. [1]. Сегодня в условиях пандемии мы наблюдаем за учащением подобных кибератак и активности.

Например, согласно данным информационного портала Tengrinews по сравнению с 2019 г., в 2020 г. было совершено в 2.7 раз больше кибератак [2]. Самым резонансным оказался случай утечки персональных данных в июле 2021 года, когда персональные данные около 30 тысяч казахстанских пользователей Telegram утекли в сеть (согласно мониторинга Служба реагирования на компьютерные инциденты KZ-CERT) [3]. Такие безпрецендентные факты усиливают риски и угрозы исходящие из незащищенного киберпространства.

Примечательно, что Казахстан стал одной из первых стран СНГ, где были приняты специальные нормативно-правовые акты, абсолютно регулирующие деятельность участников интернета. Так, нормативно-правовая база РК в сфере ИБ состоит из Конституции РК, Законов «Об информатизации», «О защите персональных данных», «О противодействии экстремизму», «Об электронном документу и электронной цифровой подписи», «О национальной безопасности РК», Концепции кибербезопасности 2017-2022, Стратегии национальной безопасности 2021-2025, Соглашении СНГ в сфере ИБ, Соглашение между правительствами государств-членов ШОС о сотрудничестве в области международной информационной безопасности и т д.

В Стратегии национальной безопасности РК 2021-2025 приоритетными направлениями работы помимо экономической, продовольственной, водной безопасности выделяется информационная безопасность. В этой же Стратегии отмечается важность «противодействия растущим киберугрозам, защите персональных данных казахстанцев,

информационной инфраструктуры, стратегических объектов, и, в целом, улучшение защищенности национального информационного пространства» [4].

В 2016 году Казахстан первым из стран СНГ создал Министерство цифрового развития, инноваций, аэрокосмической промышленности. В полномочия данного министерства входила в том числе «безопасность в сфере информатизации и связи [5]». Комитет информационной безопасности данного министерства в настоящий момент осуществляет такие проекты как «Киберщит Казахстан», критически важные объекты ИКТ, WEBTOTEAM, система TLAB и т.д.

Сегодня, программа «Киберщит» реализуется в рамках Концепции кибербезопасности 2017-2022 годов.

Целью программы является достижение и поддержание уровня защищенности электронных информационных ресурсов, информационных систем и структуры ИКТ от внешних и внутренних угроз, чтобы обеспечить устойчивое развитие РК в условиях глобальной конкуренции.

За периоды реализации программы были достигнуты следующие показатели:

РК поднялся с 83 места на 40-е в глобальном индексе кибербезопасности (согласно отчету Международного союза электросвязи в 2021 году, Казахстан находится на 31 месте в мире и на 2 месте по Региону СНГ после Российской Федерации) [6].

Осведомленность населения о киберугрозах достигла 63%

Количество переподготовленных специалистов в сфере ИБ достигла 700

Увеличилась доля компаний и государственного сектора, использующего национальные IT-продукты-с 9.3% до 21%

Доля использования национального сертификата безопасности с запланированных 20% была достигнута до 25% и т.д.

Программой tlab была эффективно обезврежена кибератаки на сайт электронного правительства в 2020 г. [7].

Следует отметить, что помимо вышеуказанного министерства в РК имеют место и другие органы, обеспечивающие защиту информационного пространства. Это такие как:

Национальный координационный центр по информационной безопасности (НКЦ ИБ) осуществляет проекты по реагированию на компьютерные инциденты KZ-CERT, по испытанию на соотвествие требованиям ИБ, мониторинг обеспечения ИБ объектов информатизации «электронного правительства» и государственных органов и т.д.

Центр анализа и расследования кибератак (ЦАРК) занимается внедрением с системы управления информационной безопасностью (СУИБ), аудитом информационных систем, расследованием инцидентов ИБ и т.д.

Подразделения по обеспечению кибербезопасности национальных министерств, частных компаний и т.д.

В качестве угроз национальной системы на основе мониторинга KZ-CERT можно выделить следующие:

Ботнеты-сеть компьютеров, зараженных вредоносной программой. С помощью ботнет возможно рассылать спам, распространять вирусы и тому подобные действия [8]. За 2019 году совершено 17.7 тысяч инцидентов. Только за III квартал 2021 года в 1.5 раза увеличилось количество инцидентов с распространением ботнетов, сообщает Национальный координационный центр по информационной безопасности [9].

Фишинг - обманным путем вымогание персональных данных пользователя. За 2019 г. зафиксировано 883 случая. В 6.8 раз участились случаи «фишинга» через спам.

Отказ в обслуживании (Ddos-атаки). Согласно отчетам АО «Государственной технической службы» в РК было совершено в 7.3 раза больше Ddos-атак за III квартал этого года, чем за II [9].

Кроме того, необходимо отметить, что большинство киберугроз и рисков информационной системы РК заключается в низкой кибергигиене граждан РК и организаций. Данная проблема была отмечена в программном изложении Концепции Киберщит 2017-2022.

Исследователь же Асадова З.А. в качестве проблем в выстраивании национальной политики ИБ отмечает такие проблемы как кадровый дефицит, «отсутствие условий для развития производства национальных программных и технических средств обеспечения безопасности» [10]. Вместе с тем, на примере достижений программы «Киберщит» мы убедились, что с одной стороны РК делает попытки для разрешения данных проблем, но с другой стороны для устранения «кадрового голода» требуется время, а проблемы требуют незамедлительных решений.

Вместе с тем, в своем докладе Данияр Сабитов «Информационная безопасность Казахстана: защита данных и смыслов», выпущенным Институтом мировой экономики и политики (ИМЭП) поднимает проблемы национальной системы информационной безопасности (ИБ). Наш взгляд, следующие положения, опубликованные в Докладе, являются актуальными и бесспорными:

Служба реагирования на компьютерные инциденты - KZ-CERT занимается только мониторингом, при этом активных практические попыток по нейтрализации и ликвидации угроз применить не в силах. Действительно, на наш взгляд, за период с 2016 по 2021 годы, с их стороны не было предпринято активных усилий по противодействии киберугрозам [11].

Центра анализа и расследования кибератак (ЦАРК) отмечает неэффективность аттестации KZ-CERT. Даже после 2016 года, частный сектор после внедрения сертификата KZ-CERT продолжает подвергаться кибератакам. Таким образом, частный сектор остается уязвимым звеном политики ИБ РК.

В национальном законодательстве недостаточно освещена защита бизнеса от кибератак. В Концепции 2017 г. говорится о наличии угроз малому и среднему бизнесу. Также в принципах и походах работы программы указывается «обеспечить гражданам и бизнесу к квалифицированным оценкам угроз в сфере информационной безопасности и получение дополнительных знаний о том, как уменьшить негативное влияние от угроз использования уязвимостей в программном обеспечении и ИКТ системах» [12]. То есть предполагаются лишь профилактические меры, в то время как в передовых странах тесное сотрудничество частного сектора с государственным в сфере нейтрализации вышеуказанных рисков является первостепенной задачей. Исходя из вышеуказанных данных считаем, что РК необходимо обеспечить сотрудничество частного сектора с государственным сектором в реализации ИБ. Согласно Д. Сабитову политика ИБ РК зациклена на защите государственных структур. Кроме того, необходимо обеспечить участие частного сектора в политике ИБ: проводить киберучения с компаниями как это делают в странах ЕС (в киберучениях РК участвует лишь государственный сектор), закрепить за частным сектором на национальном уровне ответственность за защиту от киберугроз, данных своих клиентов и т.д.

Заключение. Таким образом, мы констатируем, что национальная политика безопасности основана на таких документах как Концепция «Киберщит», Стратегия

национальной безопасности 2021-2025, законы «О защите персональных данных», «Об информатизации» и т.д. Инструментами реализации политики ИБ являются Министерство, ЦАРК и т.д.

В последние годы реализуется программа «Киберщит», которая достигла таких заметных успехов как выход РК на 31 место в Глобальном индексе кибербезопасности, увеличение осведомленности организаций и населения о киберугрозах, внедрение отечественных разработок в свете кибербезопасности, подготовка кадров и т.д.

Но несмотря на это у данного проекта имеются такие изъяны как необеспеченность включения частного сектора в реализацию политики кибербезопасности РК (например, в странах ЕС проводятся совместные киберучения, деятельность компаний в сфере кибербезопасность регулируется законодательством), дефицит кадров, деятельность Службы реагирования на компьютерные инциденты – «KZ-CERT» только как мониторингового центра, неэффективная аттестация KZ-CERT, которая подвергает частные компании рискам.

Список использованных источников

1 Кибертерроризм набирает популярность в Казахстане Ковалева Т.// https://www.zakon.kz/4722418-kiberterrorizm-nabiraet-populjarnost-v.html.

2 Количество кибератак увеличилось в Казахстане// https://tengrinews.kz/kazakhstan_news/kolichestvo-kiberatak-uvelichilos-v-kazahstane-430369/-

3 Национальный координационный центр информационной безопасности// https://www.sts.kz/ru/nccib

4 Президент РК подписал указ об утверждении Стратегии национальной безопасности РК на 2021-2025 годы//https://online.zakon.kz/Document/? doc_id=35705200

5 Проблемы обеспечения информационной безопасности Республики Казахстан Камбаров А.Н. Тулаганов Н.А.-С.257-262.

6 Опыт РК в эффективной реализации национальной стратегии кибербезопасности. https://www.itu.int/ru/ITU-D/Regional-Presence/CIS/Pages/News/20210810.aspx

7 «Киберщит Казахстана»: первые итоги реализации // https://strategy2050.kz/ru/news/52085/?sphrase_id=25307982.

8 Развитие информационной безопасности в Казахстане Лим В.Б.//Наука, техника, образование. - №4. - 2020. - С.32-34.

9 Национальный координационный центр информационной безопасности// https://www.sts.kz/ru/nccib.

10 Асадова З.А. Состояние и стратегии обеспечения информационной безопасности в странах Центральной Азии на примере Республики Казахстан //Вестник МГИМО. - 2016. - С.92-96.

11 Информационная безопасность Казахстана: защита данных и смыслов Сабитов Д. // https://www.researchgate.net/publication/344726621_Informacionnaa_bezopasnost_Kazahstana_zasita_dannyh_i_smyslov.

12 Об утверждении Концепции кибербезопасности («Киберщит Казахстана») // https://adilet.zan.kz/rus/docs/P1700000407.