ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2023»
XVIII Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XVIII Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2023»

PROCEEDINGS
of the XVIII International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2023»

2023
Астана

УДК 001+37
ББК 72+74
G99

«ǴYLYM JÁNE BILIM – 2023» студенттер мен жас ғалымдардың XVIII Халықаралық ғылыми конференциясы = XVIII Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2023» = The XVIII International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2023». – Астана: – 6865 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-337-871-8

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001+37
ББК 72+74

ISBN 978-601-337-871-8

Қолданылған әдебиеттер тізімі

1. Independent media are under great pressure in Kazakhstan // Free Press Unlimited. 2020. Режим доступа: https://www.freepressunlimited.org/en/countries/kazakhstan (қаралу күні: 15.03.2023)
2. Reporters without borders // Kazakhstan. 2021. Режим доступа: https://rsf.org/en/country/kazakhstan#all-posts (қаралу күні: 15.03.2023)
3. Nothing new in the 'New Kazakhstan' as attacks on social media freedom continue // Global Voices. 2022. Режим доступа: https://globalvoices.org/2022/05/06/new-kazakhstan-world-press-freedom-day-and-attacks-on-social-media-freedom/ (қаралу күні: 17.03.2023)
4. Khashimov Sh. As press freedom shrinks in Kazakhstan, journalists are standing up for civil liberties // Waging Nonviolence. 2021. Режим доступа: https://wagingnonviolence.org/2021/11/press-freedom-shrinks-kazakhstan-journalists-stand-up/ (қаралу күні: 17.03.2023)
5. Право на свободу слова: в Казахстане разработали новый законопроект о СМИ // Kazakhstan Today. 2023. Режим доступа: https://www.kt.kz/rus/state/pravo_na_svobodu_slova_v_kazahstane_razrabotali_novyy_1377945280.html (қаралу күні: 19.03.2023)
6. Kazakhstan's Media, Journalists Under Pressure // The Diplomat. 2023. Режим доступа: https://thediplomat.com/2023/01/kazakhstans-media-journalists-under-pressure/#:~:text=Reporters%20Without%20Borders%2C%20a%20media,country%20report's%20summary%20said. (қаралу күні: 20.03.2023)

УДК 327(4/9)

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕР ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЕС И КАЗАХСТАНЕ

Дмитриева Алёна Сергеевна
dmitriyeva.alyona@gmail.com
Докторант факультета международных отношений, кафедры «Регионоведение»,
ЕНУ им. Л.Н. Гумилева, Астана, Казахстан
Научный руководитель – А.Н. Жолдасбекова

В современном мире информационная безопасность стала одной из ключевых проблем общества в области глобальной безопасности. Исторически сложилось, что информация всегда была объектом борьбы между странами и чем больше информационных возможностей имело государство, тем легче ему было достигать геополитических преимуществ. В связи с этим, многие страны и объединения рассматривают информацию как стратегически важный ресурс. Однако с каждым годом угрозы для информационной безопасности становятся все более разнообразными и усовершенствованными, в результате чего государства по всему миру стараются отслеживать основные тренды в обеспечении информационной безопасности, чтобы защитить государственные интересы, экономику, инфраструктуру и частную жизнь граждан. Вследствие этого, Европейский Союз и Казахстан активно занимаются вопросами обеспечения информационной безопасности в своих регионах, придавая этому аспекту особое значение.

Стоит отметить, что в научной литературе до сих пор отсутствует однозначное определение понятия «информационная безопасность». В контексте международных отношений, понятие «информационной безопасности» относится к защите государственных интересов от угроз, связанных с использованием информационных технологий и средств в политических и военных целях. Информационная безопасность может включать в себя защиту государственных тайн, конфиденциальной информации, интеллектуальной собственности, а также обеспечение доступности, целостности и конфиденциальности информации.

Одним из ведущих экспертов в области информационной безопасности является Адам Сигал, который работает в Исследовательском центре кибербезопасности при Университете Джонса Хопкинса и является автором множества статей и книг по этой тематике. Согласно его определению, информационная безопасность - это состояние, когда защита информации обеспечивает конфиденциальность, целостность и доступность данных, а также защиту от несанкционированного доступа и использования. Он также отмечает, что информационная безопасность не ограничивается только техническими аспектами, но также включает в себя культурные, политические и организационные факторы. [1].

Вместе с тем известный британский ученый Томас Рид соотносит понятие «информационной безопасности» с «концепцией информационной войны», объясняющей использование информационных технологий и средств для достижения политических и военных целей [2].

Данные два взгляда на понятие информационной безопасности отражают разные аспекты проблемы, а именно: защиту государственных интересов от угроз, связанных с использованием информационных технологий и средств, а также использование информационных технологий и средств для достижения политических и военных целей. Тем не менее, эти аспекты тесно связаны и взаимодействуют друг с другом.

Согласно Алиевой М.Ф. проблемы информационной безопасности можно условно разделить на три крупные группы, которые имеют свои особенности и влияют на различные аспекты жизни общества [3].

Первая группа – это проблемы гуманитарного характера, которые связаны с несанкционированным использованием и распространением персональных данных граждан, нарушением их частной жизни, клеветой и кражами личности.

Вторая группа проблем – это экономические и юридические проблемы информационной безопасности. Они возникают из-за утечек, искажений и потерь коммерческой и финансовой информации, краж брендов и интеллектуальной собственности, раскрытия информации о материальном положении граждан, промышленного шпионажа и распространения материалов, которые наносят ущерб репутации компаний.

Третья группа – это проблемы политического характера. Они возникают в связи с информационными войнами, кибервойнами и электронной разведкой, осуществляемыми в интересах политических групп. К таким проблемам относятся компрометация государственной тайны, атаки на информационные системы важных оборонных, транспортных и промышленных объектов, а также неполное информирование и дезинформация руководителей крупных учреждений.

Таким образом, проблема информационной безопасности касается всех сфер общественной и государственной жизни и влияет на реализацию национальных интересов каждой страны.

Что касается развития информационной безопасности в Европейском Союзе и Казахстане, то можно отметить, что между государствами существуют схожие подходы к обеспечению информационной безопасности. Страны используют различные технические, организационные и правовые меры для защиты информационных ресурсов. Например, в Европейском Союзе существуют различные органы, такие как Европейский центр кибербезопасности (ENISA), которое было создано в 2004 году. Главной задачей агентства является содействие развитию единой стратегии по кибербезопасности в ЕС и укреплению ее позиций в этой области в международном сообществе.

ENISA занимается проведением исследований и анализом киберугроз, разработкой рекомендаций и стандартов в области кибербезопасности, а также содействием в развитии компетенций и навыков в области кибербезопасности. Оно также предоставляет экспертную поддержку и консультации Европейской комиссии, другим органам ЕС и государствам-членам по вопросам кибербезопасности [4].

В Казахстане также существуют подобные организации, В июне 2017 года была утверждена концепция кибербезопасности «Киберщит Казахстана», которая определила ключевые направления государственной политики в области информационных технологий и телекоммуникаций. Она предусматривает защиту электронных информационных ресурсов, повышение цифровой грамотности населения и бизнеса, а также обеспечение безопасности использования информационно-коммуникационных технологий.

В рамках реализации концепции «Киберщит Казахстана» с 2018 года функционирует национальный координационный центр информационной безопасности (НКЦИБ), который занимается защитой информационных ресурсов государственных органов и критически важной информационной инфраструктуры республики от кибератак и киберинцидентов.

Кроме того, в Казахстане создана частная платформа выявления уязвимостей BugBounty, которая является механизмом общественного и профессионального контроля информационной безопасности на объектах информатизации. За 2022 год на платформе BugBounty зарегистрировано более 690 независимых экспертов по кибербезопасности, от которых получено более 1000 отчетов с сообщениями об уязвимостях [5].

ЕС и Казахстан сотрудничают в области информационной безопасности в рамках Соглашения о партнерстве и сотрудничестве между ЕС и Казахстаном, которое было подписано в 2015 году и вступило в силу в 2020 году. Соглашение предусматривает создание механизма регулярного диалога между ЕС и Казахстаном по вопросам информационной безопасности.

В рамках этого диалога ЕС и Казахстан обмениваются опытом и лучшими практиками в области кибербезопасности и борьбы с киберпреступлениями. Кроме того, они сотрудничают в развитии и применении современных технологий для защиты информации, а также в укреплении инфраструктуры связи и информационных систем.

Важным направлением сотрудничества является также борьба с кибертерроризмом и киберспионажем. ЕС и Казахстан совместно разрабатывают меры по выявлению и предотвращению кибератак на критическую информационную инфраструктуру и организации. Так, сотрудничество между ЕС и Казахстаном в области информационной безопасности является важным фактором для обеспечения кибербезопасности и защиты информации в регионе и способствует укреплению доверия между странами [6].

Несмотря на сходства в подходах, есть и различия между Европейским Союзом и Казахстаном в области информационной безопасности. Одним из главных отличий является разный уровень развития цифровой экономики и использования технологий в этих странах. В Европейском Союзе цифровая экономика является одним из ключевых секторов экономики и сильно влияет на ее развитие. Как следствие, в ЕС существует высокий уровень осведомленности населения в вопросах информационной безопасности и более развитая инфраструктура для защиты информационных ресурсов.

В свою очередь, в Казахстане цифровая экономика только начинает развиваться и находится на начальном этапе. Это означает, что уровень осведомленности населения о вопросах информационной безопасности ниже, чем в ЕС. Кроме того, в Казахстане наблюдается недостаток специалистов в области информационной безопасности и недостаточно развитая инфраструктура для защиты информационных ресурсов. Однако, Казахстан активно работает над улучшением своей инфраструктуры и развитием технологического сектора экономики, что может привести к увеличению уровня осведомленности и развитию специалистов в области информационной безопасности.

Также в Европейском Союзе существуют общеевропейские стандарты и нормы в области информационной безопасности, которые регулируют деятельность компаний и государственных учреждений. Эти нормы и стандарты основываются на таких документах, как Общее положение по защите данных (General Data Protection Regulation, GDPR), которое определяет правила обработки персональных данных граждан ЕС, а также на других директивах и регуляторных актах, регулирующих технические и организационные меры по обеспечению безопасности информации, кибербезопасности и т.д. [7].

В Казахстане таких стандартов нет, и регулирование деятельности в области информационной безопасности осуществляется на уровне законодательства, в частности, Законом РК от 6 января 2012 года №527-IV «О национальной безопасности Республики Казахстан». Закон устанавливает меры по обеспечению информационной безопасности в стране, такие как недопущение информационной зависимости Казахстана, защиту государственных секретов, обеспечение бесперебойной эксплуатации сетей связи, предотвращение информационного воздействия на общественное и индивидуальное сознание и т.д. Закон также устанавливает ответственность за нарушения в области информационной безопасности, включая уголовную ответственность за утечку государственных секретов [8].

Кроме того, в 2023 году Глава государства подписал Указ от 20 марта 2023 года № 145 «Об утверждении Информационной доктрины Республики Казахстан», в рамках которой устанавливаются основные принципы и ценностные установки, определяющие вектор и содержание информационной политики на долгосрочную перспективу в целях консолидации общества и укрепления гражданской идентичности. Реализация доктрины должна способствовать усовершенствованию государственного механизма противодействия дезинформации, созданию эффективной системы коммуникаций между всеми участниками информационного процесса, а также решению задач информационной сферы в рамках курса на построение «Справедливого Казахстана» [9].

Таблица 1. Сравнение сходств и различий между ЕС и Казахстаном в области информационной безопасности

Сходства	Различия
1. Обе стороны придают высокое значение защите конфиденциальности данных и личной информации. 2. Европейский Союз и Казахстан признают необходимость борьбы с киберпреступностью и поддерживают сотрудничество в этой области. 3. Обе стороны стремятся создать эффективные механизмы защиты информационных систем и инфраструктуры связи.	1. В Европейском Союзе существует ряд общеевропейских стандартов и норм в области информационной безопасности, тогда как в Казахстане таких стандартов нет, и регулирование осуществляется на уровне законодательства. 2. В Европейском Союзе существует обязательная процедура уведомления о нарушении данных, которая требует, чтобы компании и организации уведомляли пользователей о любом нарушении их конфиденциальной информации, тогда как в Казахстане это не является обязательным. 3. Европейский Союз активно продвигает идею прозрачности в использовании и обработке данных, в то время как в Казахстане уровень прозрачности и открытости в этой области ниже. 4. В Казахстане существует законодательная база, которая позволяет государству более активно вмешиваться в регулирование информационной безопасности, чем в Европейском Союзе, где более распространен подход к саморегулированию и децентрализации регулирования.

Выводы данного сравнительного анализа мер по обеспечению информационной безопасности в ЕС и Казахстане показывают, что в обеих юрисдикциях существуют различные меры для защиты информации, однако они имеют как сходства, так и различия (см. Таблицу 1).

Несмотря на отличия в подходах, важно отметить, что Казахстан принимает на себя большую ответственность в этой области, как это подтверждается созданием новых законодательных актов и введением новых стандартов. Однако, чтобы справиться с быстро развивающейся угрозой кибератак, необходимо усилить международное сотрудничество, особенно между Европейским Союзом и Казахстаном, которое имеет большой потенциал для развития.

Так, на основе анализа подходов к обеспечению информационной безопасности в ЕС и Казахстане можно сделать следующие рекомендации по усилению международного сотрудничества в данной области:

1. Регулярные встречи и консультации между экспертами ЕС и Казахстана по вопросам информационной безопасности. Это позволит обменяться опытом и лучшими практиками в этой области.

2. Совместные исследовательские проекты, направленные на разработку новых технологий и методов защиты информации. Это позволит Казахстану и ЕС получать доступ к передовым знаниям и технологиям в области информационной безопасности.

3. Создание механизмов обмена информацией и общего анализа угроз информационной безопасности. Это поможет Казахстану и ЕС лучше понимать общие угрозы и координировать свои действия для более эффективной борьбы с киберугрозами.

4. Обучение и обмен опытом в области кибербезопасности между учеными и специалистами из ЕС и Казахстана. Это поможет улучшить уровень знаний и компетенций в области информационной безопасности в обеих странах.

5. Создание более жестких стандартов в области информационной безопасности и их применение на международном уровне. Это поможет создать единые правила и требования для защиты информации и обеспечения безопасности на международной арене.

Таким образом, данные рекомендации, включающие обмен опытом и знаниями, укрепление партнерских отношений и совместные проекты помогут обеим сторонам развиваться в данной области, что в свою очередь, сможет привести к повышению уровня информационной безопасности в обществе.

Список использованных источников

1. Segal, A. The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age. – PublicAffairs, 2016, 320 pp.

2. Rid, T. Cyber War Will Not Take Place. – London: C. Hurst, 2013, 256 pp.

3. Алиева М.Ф. Информационная безопасность как элемент информационной культуры // Вестн. Адыг. гос. ун-та. Сер. 1: Регионоведение: философия, история, социология, юриспруденция, политология, культурология. 2012. № 4. С. 97–102.

4. About ENISA // URL: https://www.enisa.europa.eu/about-enisa (дата обращения: 23 марта 2023 года)

5. В 2022 году будет принята новая редакция концепции «Киберщит Казахстана» // Курсив, 2022. URL: https://kz.kursiv.media/2022-03-31/v-2022-godu-budet-prinyata-novaya-redakciya-koncepcii-kibershhit-kazahstana/ (дата обращения: 23 марта 2023 года)

6. Вступило в силу соглашение между Казахстаном и Евросоюзом // Курсив, 2020. URL: https://kz.kursiv.media/2020-03-01/vstupilo-v-silu-soglashenie-mezhdu-kazakhstanom-i-evrosoyuzom/ (дата обращения: 23 марта 2023 года)

7. What is GDPR? // URL: https://gdpr.eu/what-is-gdpr/ (дата обращения: 23 марта 2023 года)

8. Закон Республики Казахстан от 6 января 2012 года № 527-IV «О национальной безопасности Республики Казахстан» // Административно-правовой портал «Adilet», 2012. URL: https://adilet.zan.kz/rus/docs/Z1200000527 (дата обращения: 23 марта 2023 года)

9. Указ Президента Республики Казахстан от 20 марта 2023 года № 145 «Об утверждении Информационной доктрины Республики Казахстан» // Административно-правовой портал «Online.zakon», 2023. URL: https://online.zakon.kz/Document/?doc_id=35286710&pos=174;-50#pos=174;-50 (дата обращения: 23 марта 2023 года)

УДК 327