Л.Н. Гумилев атындағы Еуразия ұлттық университетінің ХАБАРШЫСЫ. ISSN: 2616-6887. eISSN: 2617-605X

САЯСИ ҒЫЛЫМДАР/ POLITICAL SCIENCE / ПОЛИТИЧЕСКИЕ НАУКИ

ГРНТИ 11.01.11
Научная статья

https://doi.org/10.32523/2616-6887/2026-155-2-25-34

ОПЫТ ЕВРОПЕЙСКОГО СОЮЗА В ОБЕСПЕЧЕНИИ КИБЕРБЕЗОПАСНОСТИ: СРАВНИТЕЛЬНЫЙ ПОДХОД И ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ ДЛЯ КАЗАХСТАНА

Б.С. Сегизбаева[1], Р.М. Таштемханова

Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан

E-mail: bbizhanova8@gmail.com, tashtemkhanova@mail.ru

Аннотация. В условиях глобализации и ускоренной цифровизации кибербезопасность превращается в стратегический приоритет, оказывающий непосредственное влияние на национальную безопасность, экономическое развитие и социальную стабильность государств. Киберугрозы приобретают всё более комплексный и транснациональный характер: возрастают масштабы атак на критическую инфраструктуру, государственные учреждения, финансово-экономическую систему, а также на социальные и информационные сети. Эти вызовы обусловливают необходимость формирования целостной и устойчивой системы кибербезопасности, которая должна сочетать правовое регулирование, институциональные механизмы, кадровую подготовку и международное сотрудничество.

Европейский союз выработал целостный подход к кибербезопасности, который основан на стратегических документах и нормативных актах, таких как Общая стратегия ЕС по кибербезопасности, Директива NIS и GDPR. Европейская модель сочетает превентивные меры, институциональную ответственность, защиту персональных данных и соблюдение цифровых прав граждан, а также развитие потенциала специализированных агентств и исследовательских центров. ЕС уделяет особое внимание международному взаимодействию, в том числе с НАТО и ООН, рассматривая киберугрозы как общую глобальную проблему.

Целью статьи является проведение сравнительного анализа европейского опыта и выявление возможностей его адаптации в контексте Казахстана. В исследовании применены методы контент-анализа стратегических документов, сравнительного анализа институциональных моделей, а также SWOT-анализа национальной системы кибербезопасности. Такой подход позволяет выявить сильные и слабые стороны существующей системы Казахстана, определить угрозы и возможности, связанные с её дальнейшим развитием.

Результаты исследования показывают, что Казахстану необходимо сконцентрироваться на институциональной модернизации, повышении межведомственной координации, совершенствовании подготовки специалистов в сфере информационной безопасности и интеграции международных стандартов.

Поступила: 10.05.2025; Принята: 25.06.2026; Доступна онлайн: 30.06.2026

*автор для корреспонденции

Важным направлением становится формирование национальной культуры кибербезопасности, которая предполагает повышение уровня цифровой грамотности населения, вовлечение частного сектора и академического сообщества. Таким образом, опыт Европейского союза может быть использован в качестве модели для создания устойчивой и эффективной киберполитики Казахстана, что позволит повысить национальную устойчивость к глобальным киберугрозам и обеспечить гармоничное развитие в условиях цифровой трансформации.

Ключевые слова: кибербезопасность, цифровая устойчивость, критическая инфраструктура, цифровизация, информационные системы, государственное регулирование, международные стандарты, защита персональных данных, киберугрозы, киберполитика.

Введение

Цифровые технологии становятся неотъемлемым элементом государственного управления, экономики, национальной обороны и социальной инфраструктуры. Расширение цифровых процессов сопровождается ростом количества и сложности киберугроз, что приводит к повышению уязвимости как отдельных информационных систем, так и критически важной инфраструктуры в целом. Эти вызовы требуют от государств выработки целостной и устойчивой политики в сфере кибербезопасности, основанной на международных стандартах, институциональной скоординированности и эффективном государственном регулировании.

Актуальность темы подтверждается и словами Президента Республики Казахстан Касым-Жомарта Токаева, который на встрече с учёными в Алматы в 2024 году отметил: «В эпоху цифровизации данные становятся новым “золотом”, и вопрос их комплексной защиты приобретает критически важное значение. Уже сегодня необходимо начинать подготовку специалистов и проведение передовых исследований в области кибербезопасности» [1]. Данная позиция подчёркивает стратегическую значимость темы и необходимость своевременного научного и институционального ответа на современные вызовы цифровой эпохи.

Одним из наиболее продвинутых примеров успешной реализации киберполитики является Европейский союз (ЕС), который за последние десятилетия разработал и внедрил комплексную модель кибербезопасности. В её основе лежат современные нормативно-правовые акты, требования по защите персональных данных, международные стандарты управления информационной безопасностью, а также функционирование специализированных агентств и стратегий по защите критической цифровой инфраструктуры. Страны ЕС демонстрируют высокий уровень цифровой устойчивости, что делает их опыт релевантным для анализа и возможным для практического применения в других государствах. В этой связи и Казахстан не составляет исключения.

Как было уже сказано выше, цель настоящего исследования заключается в анализе европейского подхода к обеспечению кибербезопасности и выработке практических рекомендаций по его применению в казахстанском контексте. Для достижения указанной цели нами обозначены следующие задачи: изучить нормативно-правовые, институциональные и стратегические механизмы, реализуемые в странах Европейского союза; провести сравнительный анализ с действующей системой кибербезопасности Республики Казахстан; определить возможности применения и интеграции наиболее эффективных элементов европейской модели с учётом приоритетов и национальных особенностей.

Материалы и методы исследования

Кибербезопасность в современном государственном управлении рассматривается как неотъемлемая часть национальной безопасности и цифрового суверенитета. Согласно докладу Международного союза электросвязи, эффективное регулирование в данной сфере требует не только технической оснащённости, но и наличия нормативной базы, институциональной координации и международного взаимодействия [2, 1 с.]. Современная теория кибербезопасности исходит из необходимости защиты конфиденциальности,

целостности и доступности информации, функционирования критической инфраструктуры и обеспечения доверия к цифровой среде. Основу успешных стратегий кибербезопасности составляет использование международных стандартов. Одним из наиболее признанных является стандарт ISO/IEC 27001, определяющий требования к системам управления информационной безопасностью, в том числе в государственных структурах. Важное значение имеет также Общий регламент Европейского союза по защите данных, который ввёл обязательные требования по их защите во всех сферах цифрового взаимодействия. Эти нормы стали основой европейской концепции цифрового суверенитета и способствовали формированию правовой культуры в вопросах кибербезопасности.

Методологическая основа настоящего исследования базируется на трех взаимодополняющих подхода. Во-первых, используется сравнительный анализ, предполагающий сопоставление правовых основ, институциональных моделей, стратегий и стандартов, реализуемых в Европейском союзе и в Республике Казахстан. Во-вторых, применяется контент-анализ официальных документов, таких как национальные стратегии, законы, программы, а также аналитических материалов международных организаций, включая Международный союз электросвязи, Европейское агентство по кибербезопасности, Организацию экономического сотрудничества и развития и др. В-третьих, проводится SWOT-анализ, направленный на выявление сильных и слабых сторон, возможностей и угроз, присущих казахстанской системе кибербезопасности в контексте заимствования европейского опыта. Такой комплексный подход позволяет не только описать структуру кибербезопасности в ЕС, но и определить элементы, которые возможно применить и адаптировать к национальным реалиям и цифровым приоритетам Казахстана.

Система кибербезопасности в Европейском союзе. На фоне стремительного развития цифровых технологий и роста трансграничных киберугроз Европейский союз выстроил многоуровневую и институционально устойчивую систему кибербезопасности, включающую правовое регулирование, функционирование профильных институтов, защиту критической цифровой инфраструктуры и развитие международного сотрудничества. Такая модель не только отражает внутренние потребности ЕС, но и служит ориентиром для других государств.

Одним из центральных компонентов правового регулирования является Общий регламент по защите данных (General Data Protection Regulation, или GDPR), вступивший в силу в 2018 году. Этот нормативный акт определяет общие правила обработки персональных данных в странах ЕС и стал основой концепции «цифрового суверенитета». Согласно Европейской комиссии, GDPR способствует укреплению доверия пользователей к цифровой среде и создает стимулы для организаций к внедрению безопасных информационных систем [3]. На практике он предусматривает штрафы до 20 млн евро или 4% от годового оборота компании, что делает его одним из самых жёстких инструментов цифрового регулирования.

Дополняющим элементом является директива NIS2, принятая в декабре 2022 года, которая расширяет объём обязательств для организаций, обеспечивающих устойчивость сетей и информационных систем. Она распространяется на более широкий спектр секторов, включая энергетику, здравоохранение, транспорт, финансовые и почтовые услуги, а также публичное управление. В частности, государства-члены обязаны создать национальные стратегии кибербезопасности, определить органы по надзору и обеспечить обмен информацией между участниками [3, с. 12]. Ожидается, что полное внедрение директивы увеличит охват регулирования в ЕС до 160 000 компаний по сравнению с примерно 15 000, подпадавшими под первую директиву NIS [3, с. 13].

Институциональную основу системы кибербезопасности составляет Агентство Европейского союза по кибербезопасности (ENISA), обладающее мандатом на разработку методических рекомендаций, проведение учений и поддержку государств-членов в построении стратегий. В рамках Акта о кибербезопасности 2019 года ENISA получила полномочия координировать европейскую систему сертификации ИКТ-продуктов, обеспечивая технологическую устойчивость и доверие к цифровому рынку [3, с. 16]. В 2022 году ENISA провела более 20 учений и консультаций с участием представителей бизнеса и государств-членов, в том числе масштабную тренировку «Cyber Europe» [3, с. 19].

На национальном уровне активно действуют органы вроде Федерального ведомства по информационной безопасности Германии (BSI) и Национальной комиссии по информатике и свободам Франции (CNIL). Они реализуют положения европейского законодательства, проводят мониторинг и контроль за

исполнением норм, а также участвуют в реагировании на инциденты. Например, в 2023 году CNIL наложила административные штрафы на общую сумму более 100 млн евро за нарушение требований GDPR, включая громкие кейсы против Google и TikTok [3, с. 23].

Защита критической цифровой инфраструктуры осуществляется через национальные программы, включая немецкую концепцию KRITIS. Она охватывает объекты энергетики, водоснабжения, телекоммуникаций и транспорта, предписывая обязательные меры по внедрению систем информационной безопасности, тестированию устойчивости к атакам и оперативной отчётности о происшествиях. Согласно данным BSI, только в 2023 году было зарегистрировано более 1 100 инцидентов, касающихся критической инфраструктуры [3, с. 25].

Международное измерение представлено сотрудничеством с НАТО, которое включает обмен разведывательной информацией, согласование стратегий и участие в совместных киберучениях. ЕС и НАТО регулярно координируют действия по линии Hybrid CoE и осуществляют обмен аналитикой по угрозам. Дополнительно, Акт о кибербезопасности ЕС закрепил единый подход к сертификации цифровых продуктов, что содействует созданию единого киберпространства [3, с. 30].

Таким образом, модель ЕС опирается на сбалансированное сочетание жёсткого регулирования, институциональной координации и международного взаимодействия, обеспечивая высокий уровень цифровой устойчивости и управления киберрисками.

Система кибербезопасности Республики Казахстан. Казахстан последовательно выстраивает государственную политику в сфере кибербезопасности, опираясь на стратегические документы, правовое регулирование и институциональные инициативы. Основу этой политики составляет Концепция кибербезопасности «Киберщит Казахстана», утверждённая постановлением Правительства № 407 от 30 июня 2017 года. Документ определяет приоритетные направления защиты цифровой инфраструктуры и создания безопасной информационной среды [4].

Нормативно-правовая база включает в себя ряд ключевых законов и подзаконных актов. Закон Республики Казахстан «Об информатизации» устанавливает основы функционирования цифрового государства и положения об обеспечении информационной безопасности. В свою очередь, Закон «О персональных данных и их защите» от 2013 года регулирует правовые аспекты обработки и защиты персональных данных. В отличие от европейского законодательства, казахстанская правовая модель не содержит комплексных механизмов ответственности за утечки данных. Например, отсутствует чётко определённая обязанность субъектов уведомлять контролирующие органы о произошедших инцидентах в установленные сроки [4, с. 18].

Для технического регулирования в области информационной безопасности действуют национальные стандарты, основанные на международных, в частности ISO/IEC 27001. Однако фактический уровень их внедрения остаётся ограниченным: по данным Deloitte, в 2022 году только 34% финансовых организаций Казахстана полностью соответствовали стандартам ИБ, тогда как 42% продемонстрировали частичное соответствие, а 24% не имели формализованного подхода к управлению киберрисками [5, с. 9]. В мае 2024 года в Казахстане был принят стандарт СТ РК ISO/IEC 27002-2023 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Средства управления информационной безопасностью» [13]. Этот стандарт разработан для применения организациями всех типов и размеров в качестве справочного материала при определении и внедрении средств управления рисками информационной безопасности в системе менеджмента информационной безопасности на основе ISO/IEC 27001. Однако его практическое внедрение в организациях Казахстана находится на начальном этапе.

Институциональная структура организована децентрализованно. Формирование государственной политики осуществляет Министерство цифрового развития, инноваций и аэрокосмической промышленности. В его структуре действует Комитет по информационной безопасности. Реализацию мер по обеспечению безопасности автоматизированных систем госорганов и инфраструктурных объектов координирует Центр анализа и расследования кибератак (ЦАРКА). Вместе с тем отсутствие нормативной базы не позволяет признать его статус полностью официальным. Более того функции по защите национального киберпространства от внешних угроз возложены на Комитет национальной безопасности. На наш взгляд, отсутствие

единого центра компетенций, аналогичного ENISA, ограничивает координацию между ведомствами и затрудняет разработку единой политики.

Справедливости ради следует также отметить, что система реагирования на инциденты развита фрагментарно. В рамках реализации «Киберщит Казахстан» был создан национальный сегмент системы мониторинга, в который входят государственные и критически важные объекты. Однако, по мнению специалистов, в текущем виде эта система остаётся технически зависимой от внешних решений, а обмен информацией между государственными и частными субъектами не регламентирован [5, с. 15].

В последние годы Казахстан демонстрирует положительную динамику по международным оценкам. Согласно отчёту Международного союза электросвязи (ITU) за 2024 год, страна вошла во вторую группу стран (Tier 2 — Advancing), набрав 94,04 балла из 100 возможных [6]. Это позволило Казахстану войти в одну категорию с такими государствами, как Австрия, Канада и Китай. Для сравнения: в рейтинге 2021 года Казахстан занимал 31-е место из 194 стран и второе в регионе СНГ, уступая только России.

В современных реалиях можно выделить ключевые сильные и слабые стороны, а также возможности и угрозы, характеризующие текущее состояние национальной системы кибербезопасности. Среди сильных сторон – наличие государственной стратегии, формирование нормативной базы и повышение цифровой устойчивости на международном уровне. К числу слабых сторон относятся институциональная фрагментация, отсутствие единого национального центра компетенций и ограниченное внедрение международных стандартов. Для решения вышеназванных проблем представляется возможным применение и адаптация передового европейского опыта, развитие международного сотрудничества и цифровой трансформации экономики. Вместе с тем сохраняются угрозы, связанные с зависимостью от зарубежных технологий, низкой правоприменительной практикой и уязвимостью критической инфраструктуры. Несмотря на наличие базовой правовой и институциональной структуры, Казахстану предстоит решить целый комплекс системных задач, чтобы выйти на уровень зрелых государств ЕС в сфере кибербезопасности. Эти аспекты формируют основу для последующего сопоставления с европейским опытом и адаптации наиболее эффективных механизмов.

Результаты и обсуждение. Сравнительный анализ систем кибербезопасности ЕС и Республики Казахстан. При сопоставлении систем кибербезопасности Европейского союза и Республики Казахстан выделяются несколько структурных различий, формирующих принципиально разные подходы к регулированию цифровой среды. Ниже представлены ключевые направления, в которых прослеживается расхождение (см. Таблица 1).

Таблица 1. Ключевые различия систем кибербезопасности ЕС и Казахстаном

Категория	Европейский союз	Казахстан
Правовая строгость	Высокая степень формализации. Директивы NIS2 и регламент GDPR устанавливают обязательные требования. За нарушения предусмотрены штрафы до 4% от годового оборота.	Средняя. Законы «Об информатизации» и «О персональных данных» содержат базовые положения, однако санкционная практика развита слабо, конкретные меры не раскрыты.
Институциональная модель	Централизованная. ENISA выступает как координирующий орган, взаимодействует с национальными структурами и разрабатывает рекомендации.	Распределённая. Полномочия разделены между МЦРИАП, КНБ и ЦАРКА. Отсутствует единый орган координации и нормативное закрепление функционала ЦАРКА.

Обязательные стандарты	Применение международных стандартов (включая ISO/IEC 27001 и 27002) и собственных механизмов сертификации (в рамках NIS2 и Cybersecurity Act).	ISO/IEC 27001 используется ограниченно. В 2024 году утверждён нацстандарт СТ РК ISO/IEC 27002-2023, но внедрение на практике остаётся на ранней стадии.
Уведомления об инцидентах	Уведомления обязательны. Установлены сроки, механизмы контроля, ответственность за неинформирование.	Отсутствует обязательность уведомления. Практика обмена данными нерегламентирована. Координация между субъектами фрагментарна.
Международная интеграция	ЕС активно участвует в глобальной цифровой дипломатии, реализует Cyber Diplomacy Toolbox, сотрудничает с НАТО и ENISA.	Казахстан участвует в мероприятиях ITU, ОБСЕ и ШОС, однако международное взаимодействие носит декларативный характер и не подкреплено обязательствами.
Индекс кибербезопасности (ITU)	Ведущие позиции: Литва — 1-е место, Франция — 7-е. ЕС страны в целом занимают топ-10 рейтинга	Tier 2 (группа Advancing) — 94.04 балла из 100 возможных, 2024 год. Казахстан на одном уровне с Канадой и Китаем [ITU, 2024].
Примечание – составлено автором на основе источников [3], [6], [7], [9], [10], [11].		

Заключение

Оценка национальной модели кибербезопасности Казахстана в контексте европейского опыта позволяет выделить несколько направлений институционального и нормативного совершенствования.

Во-первых, необходим переход от фрагментированной модели управления к централизованной. Учреждение независимого национального агентства по кибербезопасности обеспечит более устойчивую координацию между государственными структурами, частным сектором и международными партнёрами. Это особенно важно на фоне растущего количества инцидентов, затрагивающих критическую инфраструктуру [9].

Во-вторых, расширение внешнего сотрудничества, особенно в рамках диалога с Европейским союзом и НАТО, позволит Казахстану использовать наработанные механизмы информационного обмена, совместных учений и оценки рисков. Европейская инициатива «Cyber Diplomacy Toolbox» может служить основой для такого взаимодействия [10].

Третьим приоритетом является поэтапное внедрение международных стандартов управления информационной безопасностью, в первую очередь ISO/IEC 27001. Внедрение данного стандарта в структурах государственного сектора должно быть закреплено нормативно, с одновременным выделением ресурсов на его реализацию и аудит [11]. Наконец, устойчивость национальной системы невозможна без квалифицированных специалистов. Поддержка образовательных треков в вузах, а также внедрение национальной системы сертификации на базе международных требований (например, CompTIA, CISSP) может способствовать созданию экспертного кадрового пула, способного реагировать на угрозы и разрабатывать комплексные решения [12].

Таким образом, европейская модель демонстрирует, что кибербезопасность – это не совокупность технических мер, а результат институционального дизайна и долгосрочной политической воли. Для

Казахстана переход к системному подходу возможен лишь при условии синхронного реформирования нормативных, организационных и образовательных оснований. Перспективы дальнейших исследований следует направить на мониторинг эффективности отдельных механизмов адаптации – в частности, пилотных внедрений стандартов и институтов оценки зрелости систем информационной безопасности.

Вклад авторов:

Сегизбаева Б.С. – работа с использованием материалов исследования и методов, работа с литературой, сбор и анализ материалов, оформление научной статьи в соответствии с требованиями;

Таштемханова Р.М. – работа с использованием материалов исследования и методов, определение целей и задач научной статьи, критический анализ содержания текста.

Список литературы

1. Данные становятся новым «золотом»: Токаев поручил готовить специалистов по кибербезопасности. Доступно по ссылке: https://informburo.kz/novosti/dannye-stanovyatsya-novym-zolotom-tokaev-porucil-gotovit-specialistov-po-kiberbezopasnosti (Дата обращения: 10.05.2025).

2. European Commission. (2023) Cybersecurity in the European Union: Legal and Strategic Foundations. Brussels: Publications Office of the EU, p. 84. Available via the link: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies (Accessed: 10.05.2025).

3. ENISA. (2023) ENISA Threat Landscape. Brussels: European Union Agency for Cybersecurity, p. 93. Available via the link: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (Accessed: 10.05.2025).

4. О кибербезопасности: Концепция кибербезопасности «Киберщит Казахстана»: постановление Правительства РК от 30 июня 2017 г. № 407. Доступно по ссылке: https://online.zakon.kz/document/?doc_id=35136946 (Дата обращения: 10.05.2025).

5. Deloitte. (2022) Cybersecurity Readiness of Financial Institutions in Central Asia. Almaty: Deloitte Kazakhstan, p. 23 Available via the link: https://www2.deloitte.com/content/dam/Deloitte/kz/Documents/about-deloitte-kz/Deloitte%20RA_KZ_banks_cyber%20review_combined%20with%20all%20UZ%20AZ%20results_20221010.df (Accessed: 10.05.2025).

6. Министерство цифрового развития, инноваций и аэрокосмической промышленности РК. Казахстан вошёл в группу Advancing по кибербезопасности в рейтинге ITU. Доступно по ссылке: https://www.gov.kz/memleket/entities/mdai/press/news/details/845520?lang=ru (Дата обращения: 10.05.2025).

7. ENISA. (2023) ENISA Threat Landscape 2023: Analysis of Cybersecurity Threats. Brussels: European Union Agency for Cybersecurity, p. 89. Available via the link: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (Accessed: 10.05.2025).

8. Центр анализа и расследования кибератак (ЦАРКА). (2022) Обзор законодательства РК в сфере кибербезопасности. Алматы: ЦАРКА. Доступно по ссылке: https://zarca.kz/analytics (Дата обращения: 10.05.2025).

9. Zhumabekov, D. (2023) Cybersecurity Governance in Kazakhstan: Institutional Gaps and Strategic Priorities. Almaty: KISI Press, p. 64.

10. Council of the European Union. (2021) Cyber Diplomacy Toolbox: Strengthening EU's External Cyber Capacity. Brussels. Available via the link: https://www.consilium.europa.eu/media/52812/cyber-toolbox.pdf (Accessed: 10.05.2025).

11. О внедрении ISO/IEC 27001 в госсекторе РК. Доступно по ссылке: https://www.standard.kz/ru/post/isoiec-270012013 (Дата обращения: 10.05.2025).

12. OECD. (2022) Center for Cybersecurity Education. Training and Certification in Cybersecurity: Regional Gaps and Solutions. Paris: OECD Publishing. Available via the link: https://www.oecd.org/cybersecurity (Accessed: 10.05.2025).

13. СТ РК ISO/IEC 27002–2023. (2024) Информационная безопасность, кибербезопасность и защита конфиденциальности. Средства управления информационной безопасностью. Введ. в действ. с 01.05.2024. Астана: КГП «Казахстанский институт стандартизации и метрологии», с. 71.

Б.С. Сегизбаева, Р.М. Таштемханова
Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан
(E-mail: bbizhanova8@gmail.com, tashtemkhanova@mail.ru)

Еуропалық одақтың киберқауіпсіздікті қамтамасыз ету тәжірибесі: салыстырмалы тәсіл және Қазақстан үшін қолдану мүмкіндіктері

Аңдатпа. Жаһандану мен жедел цифрландыру жағдайында киберқауіпсіздік ұлттық қауіпсіздіктің, экономикалық дамудың және мемлекеттердің әлеуметтік тұрақтылығының ажырамас стратегиялық басымдығына айналуда. Киберқатерлер барған сайын күрделі әрі трансұлттық сипат алып, мемлекеттік органдарға, қаржы жүйесіне, сыни инфрақұрылымға, әлеуметтік және ақпараттық желілерге жасалатын шабуылдар көлемінің артуына әкелуде. Бұл жағдай ақпаратты қорғау мен сыни инфрақұрылымды қорғауды қамтитын кешенді әрі орнықты киберқауіпсіздік жүйесін құру қажеттігін туындатады.

Еуропалық одақ киберқауіпсіздік саласында кешенді тәсілді қалыптастырды. Ол ЕО-ның киберқауіпсіздік жөніндегі жалпы стратегиясына, NIS директивасына және GDPR нормативтік актісіне сүйенеді. Еуропалық модель алдын алу шараларын, институционалдық жауапкершілікті, дербес деректерді қорғауды, азаматтардың цифрлық құқықтарын сақтауды, сондай-ақ мамандандырылған агенттіктер мен ғылыми-зерттеу орталықтарының әлеуетін дамытуды үйлестіреді. Сонымен қатар, ЕО НАТО және БҰҰ сияқты халықаралық құрылымдармен өзара іс-қимылды нығайта отырып, киберқауіпсіздікті жаһандық мәселе ретінде қарастырады.

Мақаланың мақсаты – Еуропалық одақтың тәжірибесін салыстырмалы тұрғыда талдап, оны Қазақстан жағдайында бейімдеу мүмкіндіктерін айқындау. Зерттеу барысында стратегиялық құжаттарға контент-талдау, институционалдық үлгілерге салыстырмалы талдау және Қазақстандағы киберқауіпсіздік жүйесіне SWOT-талдау жүргізілді.

Зерттеу нәтижелері Қазақстан үшін институционалдық жаңғырту, ведомствоаралық үйлестіруді күшейту, ақпараттық қауіпсіздік саласындағы мамандарды даярлау деңгейін арттыру және халықаралық стандарттарды енгізу қажеттігін көрсетеді. Сондай-ақ ұлттық киберқауіпсіздік мәдениетін қалыптастыру, халықтың цифрлық сауаттылығын арттыру, жеке сектор мен ғылыми қауымдастықты тарту маңызды болып табылады.

Осылайша, Еуропалық одақтың тәжірибесі Қазақстанда орнықты әрі тиімді киберсаясат қалыптастыру үшін үлгі ретінде пайдаланылуы мүмкін. Бұл жаһандық киберқауіптерге қарсы ұлттық төзімділікті күшейтуге және цифрлық трансформация жағдайында үйлесімді дамуды қамтамасыз етуге мүмкіндік береді.

Түйін сөздер: киберқауіпсіздік, цифрлық тұрақтылық, сыни инфрақұрылым, цифрландыру, ақпараттық жүйелер, мемлекеттік реттеу, халықаралық стандарттар, дербес деректерді қорғау, киберқатерлер, киберсаясат.

B.S. Segizbayeva, R.M. Tashtemkhanova
L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
(E-mail: bbizhanova8@gmail.com, tashtemkhanova@mail.ru)

The European Union's Experience in Ensuring Cybersecurity: A Comparative Approach and Opportunities for Kazakhstan

Abstract. In the context of globalization and accelerated digitalization, cybersecurity has become a strategic priority directly affecting national security, economic development, and the social stability of states. Cyber threats are increasingly complex and transnational in nature, with growing attacks on government institutions, financial systems, critical infrastructure, as well as social and information networks. These challenges highlight the necessity of building a comprehensive and sustainable cybersecurity system that integrates legal regulation, institutional mechanisms, human capacity building, and international cooperation.

The European Union has developed a comprehensive approach to cybersecurity based on key strategic and regulatory documents such as the EU Cybersecurity Strategy, the NIS Directive, and the GDPR. The European model combines preventive measures, institutional responsibility, data protection, respect for citizens' digital rights, and the development of specialized agencies and research centers. Particular emphasis is placed on international cooperation, including collaboration with NATO and the United Nations, viewing cyber threats as a global issue.

The aim of this article is to conduct a comparative analysis of the EU's experience and identify opportunities for its adaptation within the context of Kazakhstan. The study applies methods of content analysis of strategic documents, comparative analysis of institutional models, and a SWOT analysis of Kazakhstan's national cybersecurity system.

The findings demonstrate that Kazakhstan should prioritize institutional modernization, enhance interagency coordination, improve the training of specialists in information security, and adopt international standards. An equally important task is fostering a national culture of cybersecurity, which involves improving digital literacy, engaging the private sector, and involving the academic community.

Thus, the EU's experience can serve as a model for shaping a sustainable and effective cyber policy in Kazakhstan, strengthening national resilience to global cyber threats and ensuring balanced development in the era of digital transformation.

Keywords: cybersecurity, digital resilience, critical infrastructure, digitalization, information systems, state regulation, international standards, personal data protection, cyber threats, cyber policy.

References

1. Dannye stanovjatsja novym «zolotom»: Tokaev poruchil gotovit' specialistov po kiberbezopasnosti. Dostupno po ssylke: https://informburo.kz/novosti/dannye-stanovyatsya-novym-zolotom-tokaev-porucil-gotovit-specialistov-po-kiberbezopasnosti (Data obrashhenija: 10.05.2025). [in Russian]

2. European Commission. (2023) Cybersecurity in the European Union: Legal and Strategic Foundations. Brussels: Publications Office of the EU, p. 84. Available via the link: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies (Accessed: 10.05.2025).

3. ENISA. (2023) ENISA Threat Landscape. Brussels: European Union Agency for Cybersecurity, p. 93. Available via the link: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (Accessed: 10.05.2025).

4. O kiberbezopasnosti: Koncepcija kiberbezopasnosti «Kibershhit Kazahstana»: postanovlenie Pravitel'stva RK ot 30 ijunja 2017 g. № 407. Dostupno po ssylke: https://online.zakon.kz/document/?doc_id=35136946 (Data obrashhenija: 10.05.2025). [in Russian]

5. Deloitte. (2022) Cybersecurity Readiness of Financial Institutions in Central Asia. Almaty: Deloitte Kazakhstan, p. 23 Available via the link: https://www2.deloitte.com/content/dam/Deloitte/kz/Documents/about-deloitte-kz/Deloitte%20RA_KZ_banks_cyber%20review_combined%20with%20all%20UZ%20AZ%20results_20221010.df (Accessed: 10.05.2025).

6. Ministerstvo cifrovogo razvitija, innovacij i ajerokosmicheskoj promyshlennosti RK. Kazahstan voshjol v gruppu Advancing po kiberbezopasnosti v rejtinge ITU. Dostupno po ssylke: https://www.gov.kz/memleket/entities/mdai/press/news/details/845520?lang=ru (Data obrashhenija: 10.05.2025). [in Russian]

7. ENISA. (2023) ENISA Threat Landscape 2023: Analysis of Cybersecurity Threats. Brussels: European Union Agency for Cybersecurity, p. 89. Available via the link: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (Accessed: 10.05.2025).

8. Centr analiza i rassledovanija kiberatak (CARKA). (2022) Obzor zakonodatel'stva RK v sfere kiberbezopasnosti. Almaty: CARKA. Dostupno po ssylke: https://zarca.kz/analytics (Data obrashhenija: 10.05.2025). [in Russian]

9. Zhumabekov, D. (2023) Cybersecurity Governance in Kazakhstan: Institutional Gaps and Strategic Priorities. Almaty: KISI Press, p. 64.

10. Council of the European Union. (2021) Cyber Diplomacy Toolbox: Strengthening EU's External Cyber Capacity. Brussels. Available via the link: https://www.consilium.europa.eu/media/52812/cyber-toolbox.pdf (Accessed: 10.05.2025).

11. O vnedrenii ISO/IEC 27001 v gossektore RK. Dostupno po ssylke: https://www.standard.kz/ru/post/isoiec-270012013 (Data obrashhenija: 10.05.2025). [in Russian]

12. OECD. (2022) Center for Cybersecurity Education. Training and Certification in Cybersecurity: Regional Gaps and Solutions. Paris: OECD Publishing. Available via the link: https://www.oecd.org/cybersecurity (Accessed: 10.05.2025).

13. ST RK ISO/IEC 27002-2023. (2024) Informacionnaja bezopasnost', kiberbezopasnost' i zashhita konfidencial'nosti. Sredstva upravlenija informacionnoj bezopasnost'ju. Vved. v dejstv. s 01.05.2024. Astana: KGP «Kazahstanskij institut standartizacii i metrologii», s. 71. [in Russian]

Сведения об авторах:

Сегизбаева Б.С. – саясаттану кафедрасының магистранты, Халықаралық қатынастар факультеті, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан.

Таштемханова Р.М. – тарих ғылымдарының докторы, саясаттану кафедрасының профессоры, Халықаралық қатынастар факультеті, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан.

Сегизбаева Б.С. – магистрант кафедры политологии, Факультет международных отношений, Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан.

Таштемханова Р.М. – доктор исторических наук, профессор кафедры политологии, Факультет международных отношений, Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан.

Segizbayeva B.S. – Master's student, Department of Political Science, Faculty of International Relations, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan.

Tashtemkhanova R.M. – Doctor of Historical Sciences, Professor, Department of Political Science, Faculty of International Relations, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan.