ҚАЗІРГІ ЗАМАНҒЫ МАҢЫЗДЫ МӘСЕЛЕЛЕР

Халықаралық ғылыми журнал

АКТУАЛЬНЫЕ ПРОБЛЕМЫ СОВРЕМЕННОСТИ

Международный научный журнал

ACTUAL PROBLEMS OF PRESENT

The international scientific journal

№3 (49)

Қарағанды
Болашақ-Баспа
2025

ҚАЗІРГІ ЗАМАНҒЫ МАҢЫЗДЫ МӘСЕЛЕЛЕР: Халықаралық ғылыми журнал. № 3 (49) - 2025. - Қарағанды: «Болашақ - Баспа» РББ, 2025 - 94 б.

ISSN 2312 – 4784

Журналдың бөлімдері бойынша редакциялық алқасының құрамы:

«Қазіргі заманғы маңызды мәселелер» Халықаралық ғылыми журналы Қазақстан Республикасы Мәдениет және ақпарат Министрлігімен тіркелген (25.09.2015 ж. № 15583-Ж мерзімді баспасөз басылымын есепке қою туралы куәлік).

Басылымның мерзімділігі: тоқсанына 1 рет

Негізгі тақырыптық бағыттары: ғылымның әр түрлі салалары қамтылған. Журнал ғылыми мақалалар, зерттеу материалдарын, хабарламалар, рецензиялар және т. б. жариялайды.

Мақала қайта басылған жағдайда журналға сілтеме жасалу міндетті. Авторлар келтірілген фактілердің, дәйексөздердің, жеке атаулардың, соның ішінде географиялық атаулардың шынайылығына жауапты.

Қазақстан Республикасының аумағында 75319 индексі бойынша тіркелген.

Ресей Федерациясының бұқаралық коммуникациялар және мәдени мұраны қорғау саласындағы заңнаманың сақталуын қадағалау жөніндегі федералдық қызметі РФ аумағында «Қазіргі заманғы маңызды мәселелер» (Қазақстан Республикасы) халықаралық журналын таратуға рұқсат берілген. 2006 жылғы 6 шілдедегі № 78 РП шетелдік мерзімді баспасөз басылымдарының өнімдерін таратуға рұқсаттама РФ аумағында № 88044 индексі, "Пресса России" Біріккен каталогында № 000053 индексі бойынша тіркелген.

«Қазіргі заманғы маңызды мәселелер» Халықаралық ғылыми журналы «Ресейлік ғылыми дәйексөз индексі» Ұлттық ақпараттық-талдау жүйесіне (РИНЦ)

енгізілген. 18.02.2016 ж.№ 75-02 / 2016 шарт

АКТУАЛЬНЫЕ ПРОБЛЕМЫ СОВРЕМЕННОСТИ: Международный научный журнал. № 3 (49) - 2025. - Караганда: РИО « Болашак-Баспа », 2025. – 94 с.

ISSN 2312 – 4784

Международный научный журнал «Актуальные проблемы современности» зарегистрирован Министерством культуры и информации Республики Казахстан (Свидетельство о постановке на учёт периодического печатного издания и№ 15583-Ж от 25.09.2015г.).

Периодичность издания: 1 раз в квартал

Основная тематическая направленность ППИ: разные направления науки. Журнал публикует научные статьи, материалы исследований, сообщения, рецензии и др.

Подписка на территории Республики Казахстан по индексу **75319**

Федеральная служба по надзору за соблюдением законодательства в сфере массовых коммуникаций и охране культурного наследия Российской Федерации разрешает распространение международного журнала «Актуальные проблемы современности» (Республика Казахстан) на территории РФ. Разрешение на распространение продукции зарубежных периодических печатных изданий РП № 78 от 6 июля 2006 г. Подписка на территории РФ по индексу 88044 в объединенном каталоге «Пресса России» № 000053

Международный научный журнал «Актуальные проблемы современности» включен в национальную информационно-аналитическую систему «Российский индекс научного цитирования» (РИНЦ) – Договор № 75-02/2016 от 18 февраля 2016 г.

ACTUAL PROBLEMS OF Present: International scientific journal. № 3 (49) - 2025. - Karagandy: EPD «Bolashaq-Baspa», 2025. – 94 p.

ISSN 2312 – 4784

The international scientific journal «Actual problems of present» was registered by the Ministry of Culture and Information of the Republic of Kazakhstan (Certificate of registration of periodicals and № 15583-Ж dated September 25, 2015).

Frequency of publication: quarterely

The main thematic focus : different branches of science. The journal publishes scientific articles, materials of the research, reports, reviews, etc.
When reprinting, a link to the journal is required. The authors are responsible for the accuracy of the facts, quotes, proper names, including geographical names.
Subscription on the territory of the Republic of Kazakhstan on the index 75319

The Federal Service for the Supervision of Compliance with the Law in the Field of Mass Communications and the Protection of the Cultural Heritage of the Russian Federation allows the distribution of the international journal «Actual problems of modernity» (Republic of Kazakhstan) on the territory of the Russian Federation. Permission to distribute products of foreign periodicals of the RF № 78 dated July 6, 2006. Subscription on the territory of the Russian Federation by the index 88044 in the joint catalog "Press of Russia" № 000053

The international scientific journal «Actual problems of present» включен в национальную информационно-аналитическую систему «Российский индекс научного цитирования» (РИНЦ) – Договор No. 75-02 / 2016 dated February 18, 2016

МАЗМҰНЫ

ОГЛАВЛЕНИЕ

CONTENTS

DOI: 10.64863/2312-4784/2025-3-49/42-58

Совершенствование управления кибербезопасности на предприятиях Казахстана

Дарибекова Айгуль Сагатбековна[1], Дарибеков Серик Сагатбекович[2], Дарибекова Назгуль Сагатбековна[1]

[1]Кандидат экономических наук, ассоц. профессор, НАО «Карагандинский технический университет имени Абылкаса Сагинова», кафедра «Экономика и менеджмент предприятия», г. Караганда, 100027, Республика Казахстан, a.daribekova@ktu.edu.kz, ORCID 0000-0003-4923-4142

[2]Кандидат экономических наук, ассоц. профессор, «Карагандинский университет имени Е.А. Букетова», кафедра «Менеджмент», г. Караганда, 100024, Республика Казахстан Daribekov_Serik@buketov.edu.kz, ORCID 0000-0001-7838-6458

[1]Магистр экономических наук, старший преподаватель, НАО «Карагандинский технический университет имени Абылкаса Сагинова», кафедра «Экономика и менеджмент предприятия», г. Караганда, 100027, Республика Казахстан, n.daribekova@ktu.edu.kz, ORCID 0000-0002-5454-6629

Аннотация

В современном цифровом мире кибербезопасность стала важнейшим аспектом современных технологий. В связи с растущей зависимостью от Интернета и увеличением использования электронных устройств потребность в кибербезопасности как никогда высока. 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 настоящее время является одной из неотъемлемых частей в удовлетворении ежедневных потребностей граждан. Цифровая трансформация помогает компаниям адаптироваться под запросы изменяющегося рынка и внедрять прогрессивные модели ведения бизнеса. Отраслевые лидеры всерьез озабочены переводом своих процессов в digital и технологическим превосходством относительно конкурентов. Это возможность повысить эффективность процессов и, как следствие, улучшить качество своих продуктов или услуг, а также существенно увеличить прибыль для акционеров и владельцев бизнеса. Важным условием эффективной киберзащиты является интеграция современных технологий искусственного интеллекта, аналитики больших данных и облачных решений, позволяющих оперативно выявлять угрозы, минимизировать риски и предотвращать киберинциденты в реальном времени. Актуальность темы кибербезопасности в финансовом секторе обусловлена не только ростом количества и сложности атак, но и возрастающими требованиями со стороны регуляторов, клиентов и международных партнёров. В условиях цифровизации экономики обеспечение устойчивости ИТ-инфраструктуры становится важнейшим фактором доверия к финансовым институтам. Кроме того, на фоне глобальных трендов — таких как удалённая работа, цифровые валюты и open banking — расширяется спектр угроз, требующих адаптации существующих подходов к защите информации. Это исследование направлено на выявление ключевых аспектов обеспечения кибербезопасности в Республике Казахстан, с учётом лучших международных практик и нормативных стандартов.

Ключевые слова: кибербезопасность, банки, инновации, финансовый, киберстрахование.

Қазақстандық кәсіпорындарда киберқауіпсіздікті басқаруды жетілдіру

Дәрібекова Айгүл Сағатбекқызы[1], Дәрібеков Серік Сағатбекұлы[2], Дәрібекова Назгүл Сағатбекқызы[1]

[1]Экономика ғылымдарының кандидаты, қауымд. профессор, «Әбілқас Сағынов атындағы Қарағанды техникалық университеті», «Кәсіпорынның экономикасы және менеджменті» кафедрасы, Қарағанды қ., 100027, Қазақстан Республикасы, a.daribekova@ktu.edu.kz, ORCID 0000-0003-4923-4142

[2]Экономика ғылымдарының кандидаты, қауымд. профессор, «Е.А. Бөкетов атындағы Қарағанды университеті», «Менеджмент» кафедрасы, Қарағанды қ., 100024, Қазақстан Республикасы Daribekov_Serik@buketov.edu.kz, ORCID 0000-0001-7838-6458

[1]Экономика ғылымдарының магистрі, аға оқытушы, Әбілқас Сағынов атындағы Қарағанды техникалық университеті», «Кәсіпорынның экономикасы және менеджменті» кафедрасы, Қарағанды қ., 100027, Қазақстан Республикасы, n.daribekova@ktu.edu.kz, ORCID 0000-0002-5454-6629

Аннотация

Қазіргі цифрлық әлемде киберқауіпсіздік заманауи технологиялардың ең маңызды аспектілерінің бірі болып табылады. Интернетке тәуелділіктің артуы және электрондық құрылғыларды пайдалану көлемінің ұлғаюына байланысты киберқауіпсіздікке деген қажеттілік бұрынғыдан да жоғары. Киберқауіпсіздік мәселелері мемлекеттің ұлттық қауіпсіздігі мәселелерімен тікелей байланысты. Интернет пен әлеуметтік желілер қоғамдық сананы басқару, белгілі бір әлеуметтік топтарға ықпал ету үшін қолданылуы мүмкін. Қазіргі уақытта цифрлық технологияларды ауқымды қолдану азаматтардың күнделікті қажеттіліктерін қанағаттандырудың ажырамас бөлігіне айналды. Цифрлық трансформация компанияларға өзгеріп жатқан нарықтың сұраныстарына бейімделуге және бизнесті жүргізудің прогрессивті үлгілерін енгізуге көмектеседі. Салалық көшбасшылар өз процестерін digital-ға көшіру және бәсекелестеріне қатысты технологиялық басымдыққа қол жеткізу мәселесіне шындап көңіл бөлуде. Бұл процестердің тиімділігін арттыруға, соның салдарынан өнімдер мен қызметтердің сапасын жақсартуға, сондай-ақ акционерлер мен бизнес иелерінің табысын айтарлықтай көбейтуге мүмкіндік береді. Киберқорғаудың тиімді шарттарының бірі – жасанды интеллекттің заманауи технологияларын, үлкен деректерді талдау мен бұлттық шешімдерді интеграциялау, олар қауіп-қатерлерді жедел анықтауға, тәуекелдерді азайтуға және киберинциденттердің алдын алуға мүмкіндік береді. Қаржы секторында киберқауіпсіздік тақырыбының өзектілігі тек шабуылдардың саны мен күрделілігінің өсуімен ғана емес, сонымен бірге реттеушілердің, клиенттердің және халықаралық серіктестердің өсіп келе жатқан талаптарымен де байланысты. Экономиканы цифрландыру жағдайында IT-инфрақұрылымның тұрақтылығын қамтамасыз ету қаржы институттарына деген сенімнің басты факторы болып табылады. Сонымен қатар, қашықтан жұмыс істеу, цифрлық валюталар және open banking сияқты жаһандық үрдістер аясында ақпаратты қорғаудың қолданыстағы тәсілдерін бейімдеуді қажет ететін қатерлер спектрі кеңеюде. Бұл зерттеу Қазақстан Республикасындағы киберқауіпсіздікті қамтамасыз етудің негізгі аспектілерін, үздік халықаралық тәжірибелер мен нормативтік стандарттарды ескере отырып, анықтауға бағытталған.

Кілт сөздер: киберқауіпсіздік, банктер, инновациялар, қаржылық, киберсақтандыру.

Improving cybersecurity management in Kazakhstan enterprises

Daribekova Aigul Sagatbekovna[1], Daribekov Serik Sagatbekovich[2], Daribekova Nazgul Sagatbekovna[1]

[1]PhD in Economics, Associate Professor, "Abylkas Saginov Karaganda Technical University", Department of "Economics and Management of Enterprise", Karaganda, 100027, Republic of Kazakhstan, a.daribekova@ktu.edu.kz, ORCID 0000-0003-4923-4142

[2]PhD in Economics, Associate Professor, "Karaganda University named after E.A. Buketov", department of "Management", Karaganda, 100024, Republic of Kazakhstan, Daribekov_Serik@buketov.edu.kz, ORCID 0000-0001-7838-6458

[1]Master of economics, senior lecturer, NJSC "Karaganda Technical University named after Abylkas Saginov", department of "Economics and Enterprise Management", Karaganda, 100027, Republic of Kazakhstan, n.daribekova@ktu.edu.kz, ORCID 0000-0002-5454-6629

Abstract

In today's digital world, cybersecurity is one of the most important aspects of modern technologies. The need for cybersecurity is higher than ever due to increased internet addiction and increased use of electronic devices. Cybersecurity issues are directly related to the issues of national security of the state. The internet and social networks can be used to control public consciousness, to influence certain social groups. Currently, the large-scale use of digital technologies has become an integral part of meeting the daily needs of citizens. Digital transformation helps companies adapt to the demands of a changing market and implement progressive models for doing business. Industry leaders are seriously paying attention to the issue of transferring their processes to digital and achieving technological superiority over their competitors. This makes it possible to increase the efficiency of processes, and, as a result, improve the quality of products and services, as well as significantly increase the income of shareholders and business owners. One of the most effective conditions for cybersecurity is the integration of modern artificial intelligence technologies, big data analysis and cloud solutions, which will make it possible to promptly detect threats, minimize risks and prevent cybersecurity. The relevance of the topic of cybersecurity in the financial sector is due not only to the growing number and complexity of attacks, but also to the growing demands of regulators, customers and international partners. Ensuring the stability of the IT infrastructure in the context of digitalization of the economy is a key factor in trust in financial institutions. At the same time, against the background of such global trends as remote work, digital currencies and open banking, the spectrum of threats is expanding, which requires adapting existing approaches to Information Protection. This study is aimed at identifying the main aspects of ensuring cybersecurity in the Republic of Kazakhstan, taking into account the best international practices and regulatory standards.

Keywords: cybersecurity, banks, innovations, financial, cyber insurance.

1. Введение

В современном мире информационно-коммуникационные технологии применяются в различных областях профессиональной деятельности, научной и практической работе, для самообразовательных и других целей. Информационные науки связаны со сбором, хранением и анализом данных. Развитие технологий привело к созданию огромных объемов данных, и информационные науки стали играть важную роль в управлении и анализе этих данных.

Год за годом в мире становится все больше угроз и происходит все больше утечек данных. Чаще всего утечке данных подвергаются медицинские и государственные учреждения или

организации из сферы розничной торговли. В большинстве случаев причина – действия преступников. Некоторые организации привлекают злоумышленников по понятной причине – у них можно украсть финансовые и медицинские данные.

Однако мишенью может стать любая компания, ведь преступники могут охотиться за данными клиентов, шпионить или готовить атаку на одного из клиентов. Очевидно, что масштаб киберугроз будет расширяться, следовательно, глобальные расходы на решения по кибербезопасности будут увеличиваться. По прогнозам Gartner, в целом расходы на кибербезопасность в мире достигнут $188,3 млрд в 2023 году, а к 2026 году превысят $260 млрд. Правительства разных стран борются с преступниками, помогая организациям внедрять эффективные методы кибербезопасности (Кузьмичева Т.Г., Голованова 2025).

В современном цифровом мире кибербезопасность стала важнейшим аспектом современных технологий. В связи с растущей зависимостью от Интернета и увеличением использования электронных устройств потребность в кибербезопасности как никогда высока.

В современном мире важнейшим конкурентным фактором в банковском секторе является внедрение инноваций и развитие информационных технологий. Однако данный процесс сопровождается также появлением новых видов мошенничества. Наибольший интерес для киберпреступников представляет финансовый сектор. Проблема развития киберпреступности является крайне актуальной и злободневной вследствие масштабов потерь, которые ежегодно несут кредитные организации по всему миру. Однако, на текущем этапе снижение кибер-рисков, в том числе в банковском секторе, развито слабо ввиду новизны проблемы, отсутствия исторической практики борьбы с киберпреступностью на уровне отдельных организаций, а также сложности в анализе и оценке данного вида рисков. В связи с этим тема исследования является актуальной как с теоретической, так и с практической точки зрения.

Целью исследования является рассмотрение и разработка рекомендаций по обеспечению кибербезопасности компаний в современных условиях.

Задачами исследования являются: рассмотрение теоретических основ кибербезопасности в современных условиях; анализ обеспечения кибербезопасности в Казахстане; совершенствование системы управления кибербезопасностью в республике.

2. Материалы и методы

Использованы методы исследования:

- анализ и обзор литературы и нормативно- правовых актов. Проанализированы международные и казахстанские определения термина «кибербезопасность». Использованы определения из законов, стратегий, концепций, а также научных публикаций, обзор источников, нормативные и аналитические документы.

- сравнительный анализ: сравниваются определения кибербезопасности в различных странах и организациях (Казахстан, Великобритания, Сингапур, ISO, авторы западных руководств), проведен сравнительный анализ угроз (фишинг, DDoS, вредоносное ПО и т.п.) и показана их динамики за 2022–2024 годы.

- статистический анализ: анализируются количественные данные по кибератакам; используются данные социологических опросов по осведомленности населения, применена динамическая оценка.:

- контент-анализ цифровых угроз: проведена оценка развития и применения технологий DeepFake, вредоносных программ, инсайдерских угроз, атак на цепочки поставок, анализируются современные тренды в сфере ИИ, цифровизации и синтетических данных.

- дана оценка стратегического уровня (policy analysis): исследованы государственные инициативы в области кибербезопасности (Концепция «Киберщит», стратегия цифровой экосистемы, планы создания киберполигона, BugBounty и др.)., рассмотрен вклад Казахстана в международные рейтинги, включая Глобальный индекс кибербезопасности (GCI).

- представлен графический и визуальный анализ: использованы рисунки отражающие: взаимосвязь кибербезопасности с другими областями (по ISO), ключевые угрозы, рейтинги и

показатели осведомленности населения, направления государственной политики.

3. Результаты и их обсуждение

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». 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 технологическими научным достижениям, укрепляя преимущественно технический взгляд на кибербезопасность. Крейген Д., Диакун-Тибо Н., и Персе Р., поддерживают данный подход (Исабаева С.Б. 2019).

Определения кибербезопасности, которые наиболее чётко описывают её сущностные элементы:

“Кибербезопасность в основном состоит из защитных методов, используемых для обнаружения и пресечения потенциальных злоумышленников” (Kemmerer, R. A. 2003).

“Кибербезопасность подразумевает защиту компьютерных сетей и содержащейся в них информации от проникновения, а также от злонамеренного повреждения или сбоя в работе” (Lewis, J. A. 2006).

“Кибербезопасность предполагает снижение риска вредоносных атак на программное обеспечение, компьютеры и сети. Сюда входят инструменты, используемые для обнаружения взломов, предотвращения проникновения вирусов, блокирования вредоносного доступа, принудительной аутентификации, обеспечения шифрованной связи и так далее” (Amoroso, 2006).

“Искусство обеспечивать существование и непрерывность информационного общества нации, гарантируя и защищая в киберпространстве ее информацию, активы и критически важную инфраструктуру” (Canongia & Mandarino, 2014).

“Деятельность или процесс, возможности, или состояние, посредством которых информационно-коммуникационные системы и содержащаяся в них информация защищены от повреждения, несанкционированного использования, модификации или эксплуатации” (DHS, 2014).

“Кибербезопасность - это совокупность инструментов, политик, концепций безопасности, гарантий безопасности, руководящих принципов, подходов к управлению рисками, действий, обучения, передовой практики, гарантий и технологий, которые могут использоваться для защиты киберпространства, организации и активов пользователей” (ITU, 2009).

Ранее данный аспект в Республике Казахстан исследовала Татаринова Л., которая предлагала внести на законодательной основе понятие «Кибербезопасность» (Татаринова Л., 2014). Она также отметила об отсутствии четкого определения термина «защита информации». Международный обзор термина «Кибербезопасность», представлена в таблице 1.

Таблица 1. Международный обзор термина «Кибербезопасность»

Автор / ресурс	Определение
Schatz, Bashroush & Wall (2017)	Кибербезопасность рассматривается как совокупность мер и практик по защите «киберсреды» и информационных систем от несанкционированного вмешательства, потери целостности или доступности
Joanna Kulesza (2022)	Кибербезопасность - это широкий термин, обозначающий меры, принимаемые государственными и частными организациями, направленные на обеспечение безопасности онлайн-коммуникаций и ресурсов. Кибербезопасность - это использование аппаратного и программного обеспечения, а также индивидуальных навыков для снижения рисков, связанных с онлайн-передачей и хранением данных, таких как технологии шифрования, антивирусное программное обеспечение и обучение сотрудников.
Grispos, Shapiro, Maras, (2021)	«Кибербезопасность предполагает применение методов и управление ими с целью защиты конфиденциальности, целостности и доступности информации и информационных активов в киберпространстве.»
Francesco Schiliro (2023)	«Кибербезопасность - это сбор и согласование ресурсов, включая персонал и инфраструктуру, структуры и процессы, для защиты сетей и компьютерных систем с поддержкой кибербезопасности от событий, которые нарушают целостность и нарушают права собственности, что приводит к определенным потерям».
Мосчовитс С. (2018)	«Кибербезопасность - это постоянное применение передового опыта, предназначенного для обеспечения и сохранения конфиденциальности, целостности и доступности цифровой информации, а также безопасности людей и окружающей среды»

С учетом расширения и усиления процессов цифровизации число и серьезность киберпреступлений в будущем будет возрастать. Это создаст новые и трансформирует существующие угрозы экономической безопасности предприятий МСБ. В связи с этим, задачей менеджмента становится создание и развитие на предприятиях специализированных подразделений по противодействию угрозам информационной безопасности, исходящим как от собственного персонала, так и из внешней среды. Это требует значительных расходов. Так, по данным исследовательской компании Astute Analytica, затраты на информационную безопасность в мире в ближайшие годы будут увеличиваться в среднем на 13,4% ежегодно.

Кибербезопасность – это деятельность, нацеленная на обеспечение защиты пользователей, их информационных систем, сетей, и программ от цифровых атак. Основной целью таких кибератак может являться как получение конфиденциальной информации пользователя для дальнейшего злоупотребления этой информации в собственных целях хакера, так и нарушение работы целого бизнес-процесса.

В стандарте ISO/IEC 27032:2012 также охарактеризована взаимосвязь терминов «кибербезопасность», «сетевая безопасность», «безопасность приложений, «безопасность в Интернете» и «безопасность ключевых систем информационной инфраструктуры», которая отражена на рисунке 1 (United Nations Office on Drugs and Crime, 2019).

.

Рисунок 1. Взаимосвязь кибербезопасности с другими видами безопасности в соответствии со стандартом ISO/IEC 27032:2012

Наличие надежного плана реагирования на инциденты, регулярное резервное копирование и использование решений для восстановления после сбоев гарантируют, что банки смогут быстро восстановиться после атаки и продолжить бесперебойное обслуживание клиентов.

Банковская отрасль сталкивается с постоянными и сложными киберугрозами, поскольку хакеры постоянно совершенствуют свои тактики для использования уязвимостей (рисунок 2) (Vitlyakova S. S., 2019).

Рисунок 2. Угрозы кибербезопасности, с которыми сталкиваются банки

Поскольку на карту поставлены огромные объемы конфиденциальных финансовых данных и информации о клиентах, банки являются основными целями для киберпреступников.

- Фишинговые атаки. Фишинг остается одной из самых распространенных угроз в банковской отрасли. Киберпреступники используют мошеннические электронные письма, текстовые сообщения или веб-сайты, которые выглядят как настоящие, чтобы обманом заставить клиентов или сотрудников раскрыть конфиденциальную информацию, такую как номера счетов, пароли или личные данные. Получив доступ, хакеры могут украсть деньги, совершить кражу личных данных или проникнуть во внутренние системы банка.

- Вредоносное ПО и программы-вымогатели. Вредоносное ПО, включая программы-вымогатели, является еще одной серьезной угрозой для банковского сектора. Вредоносное ПО — это вредоносное программное обеспечение, которое может заражать банковские системы, красть данные или даже останавливать операции. Программы-вымогатели, в частности,

блокируют пользователей от их собственных систем или данных, в то время как злоумышленники требуют выкуп за восстановление доступа.

Не все угрозы исходят извне стен банка. Внутренние угрозы — будь то от недовольных сотрудников, подрядчиков или даже сторонних поставщиков — представляют значительный риск для кибербезопасности банка. Инсайдеры, имеющие доступ к конфиденциальным данным, могут намеренно или непреднамеренно сливать информацию или предоставлять точку входа для хакеров.

Эти атаки особенно опасны, поскольку их трудно обнаружить, и они могут оставаться незамеченными в течение месяцев, что позволяет хакерам извлекать ценную информацию еще до того, как банк поймет, что его данные были взломаны.

- Атаки на третьих лиц и цепочки поставок. Банки полагаются на сторонних поставщиков и поставщиков для предоставления различных услуг, от облачного хранения до обработки платежей. К сожалению, эти сторонние поставщики также могут быть слабым звеном в цепочке кибербезопасности банка. Кибератака на стороннего поставщика может создать бэкдор для хакеров, чтобы получить доступ к конфиденциальным данным банка. В последние годы атаки на цепочки поставок участились: киберпреступники выбирают в качестве своей мишени мелких и менее защищенных поставщиков, чтобы получить доступ к более крупным финансовым учреждениям.

Угроза кибербезопасности из потенциальной возможности превращается в реальную кибератаку в случае, когда соответствующими уязвимостями воспользуется некоторый источник – субъект, которым может быть физическое лицо, материальный объект или физическое явление (Price water house Coopers 2019).

В случае реализации потенциальная угроза становится кибератакой, т.е. попыткой проникновения в информационную инфраструктуру, которая может неблагоприятно отразиться на кибербезопасности.

Одним из важнейших трендов развития финансового сектора экономики является цифровая трансформация, включающая, прежде всего, ориентацию на потребителя, мобильность и скорость, данные. Цифровая трансформация (цифровизация) бизнеса – это процесс превращения традиционной организации в цифровую компанию, в которой присутствуют как материальные, так и цифровые объекты. В последние годы активно развивается индустрия финансовых технологий.

Процесс цифровизации экономики, ставший ее критическим фактором в последние годы, проявился и в банковских операциях за счет активного распространения электронных платежей, электронной коммерции, внедрения инновационных цифровых сервисов, расширяющих спектр банковских продуктов, содействия привлечения клиентов и тем самым формирование конкурентной политики и получение конкурентных преимуществ. Кроме того, глобальное распространение COVID-19 в 2020 году потребовало перехода на бизнес-модель дистанционного банковского обслуживания, а именно на платформу онлайн-банкинга.

Внедрение современных информационных технологий и инноваций, которое направлено на улучшение жизни человечества, а также процессы глобализации и интеграции параллельно с собой несут активное развитие новых методов мошенничества. Киберпреступность, как один из ключевых современных видов мошенничества, уже превратилась в глобальную международную проблему. Развитие киберпреступности происходит очень динамично, и постоянно возникают новые проблемы.

Важно обеспечить, чтобы банковские системы и операции были структурированы так, чтобы обнаруживать киберугрозы и реагировать на инциденты кибербезопасности, тем самым ограничивая дестабилизацию или финансовые потери. А в сфере финансовых услуг проблема принимает другое измерение, потому что ожидаемые выгоды кажутся чрезвычайно привлекательными.

ИИ в данном контексте действует как катализатор для принятия обоснованных, датацентричных решений.

Использование интеллектуальных систем обработки документов за счет классификации информации значительно ускоряет обработку больших объемов документов, уменьшая вероятность ошибок и повышая эффективность работы сотрудников.

По данным Autonomous Next, использование искусственного интеллекта в банковской сфере позволит к 2030 году сэкономить более одного триллиона долларов (Weinrauch V., 2024).

Технология DeepFake, применяемая для мошеннических операций, представляет собой подделку изображений, видео или аудиофайлов с использованием ИИ и глубокого обучения. Эта технология может имитировать голоса, выражения лица и движения, создавая реалистичный, но фальшивый контент. Использование технологии DeepFake для мошенничества представляет собой серьезную угрозу. Соответственно целый ряд лабораторий и институтов занимаются исследованиями и разработкой методов обнаружения подобного мошенничества.

В Казахстане одним из подобных примеров является процесс тестирования биометрических решений поставщиков, осуществляемый в рамках их присоединения к Центру обмена идентификационными данными Национальной платежной корпорации. Частью этого процесса является оценка биометрических решений различных поставщиков на способность обнаружения фактов использования DeepFake технологий для фальсификации личности при получении финансовых услуг.

Глобальное развитие концепции Open Banking является значимым драйвером развития использования ИИ на финансовом рынке. Это направление, связанное с оперативным сбором данных и их последующей обработкой с применением ИИ, обеспечивает более открытый и унифицированный доступ к финансовым данным.

В сочетании с RegTech развитие систем Open Banking обеспечивает более эффективные механизмы регулирования и надзора в финансовой сфере. В контексте RegTech это означает, что регуляторы могут получать актуальную и точную информацию от финансовых учреждений в реальном времени. Это повышает эффективность регуляторов в микропруденциальном регулировании, выявлении финансовых преступлений, предотвращении мошенничества и обеспечении соблюдения законодательства. В целом, развитие Open Banking в рамках RegTech обеспечивает более интегрированный, прозрачный и эффективный подход к регулированию финансовой сферы, способствуя улучшению безопасности, снижению рисков и обеспечивая более высокий уровень соответствия нормативам.

В то же время, развитие Open Banking необходимо для развития технологий и подходов генерации синтетических данных, которые могут быть сформированы только на основе реальных данных, собранных со всего рынка, а их безопасный сбор в свою очередь невозможен без развитой системы Open Banking. Уже сейчас наблюдаемое развитие компаний в индустрии финансовых технологий Европейского союза, Великобритании и Австралии связывается с постоянными и последовательными усилиями по развитию Open Banking для свободного и безопасного обмена банковскими данными клиентов. Тем не менее, существует ряд ограничений для подключения к данным системам и их использованию. Между тем синтетические данные могут стать следующим драйвером роста финансовых технологий, связанных с развитием ИИ. В случае синтетических данных снижается порог входа и облегчается доступ к необходимым данным для использования более широким кругом компаний, в том числе стартапами.

В последние несколько лет значение финансовых технологий в деятельности коммерческих банков значительно расширилось. Основанием для этого является повышение качества обслуживания клиентов, гибкости, новаторского мышления и развитие цифровой инфраструктуры. Несмотря на противоречие, этот альянс повышает уязвимость коммерческих банков к рискам кибербезопасности из-за развития таких угроз, как атаки вредоносного ПО,

утечка и проблемы с целостностью данных. Банковский сектор наиболее уязвим к рискам кибербезопасности, чем любой другой финансовый институт.

Согласно новой методике, Казахстан занял место во второй группе (Tier 2 – Advancing), набрав 94,04 балла из 100 возможных., показанный на рисунке 3.

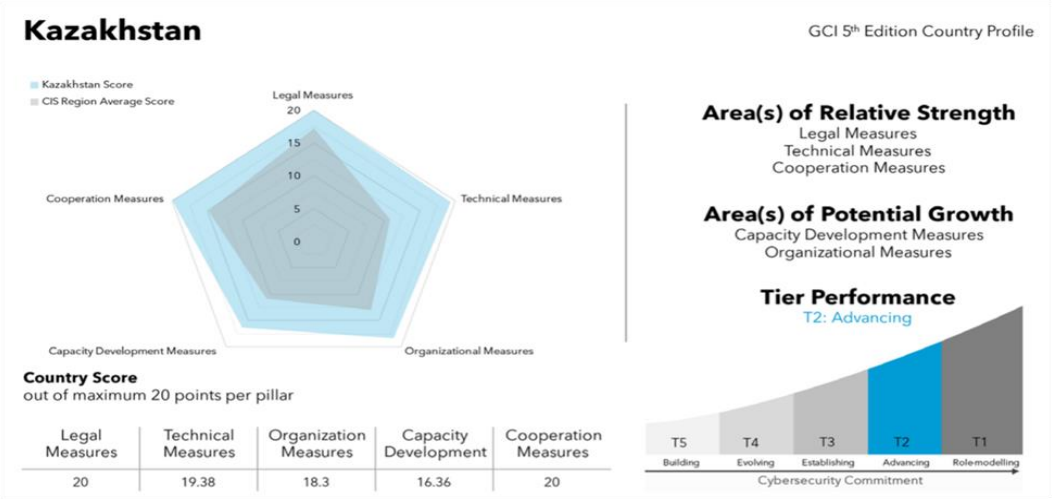

Рисунок 3. Место Казахстана в Глобальном индексе кибербезопасности в 2024 г.

Новая методика оценивает работу за 2023 год. Обновляется индекс 1 раз в два года. В отчете 2024 года используется обновленный пятиуровневый анализ, позволяющий более точно оценить достижения стран в области кибербезопасности. Уровни включают Tier 1 — Role-modelling, Tier 2 — Advancing, Tier 3 — Establishing, Tier 4 — Evolving и Tier 5 — Building (Puchkova A., 2024). Рейтинг GCI формируется на основе 83 параметров, охватывающих пять ключевых направлений кибербезопасности: юридический, технический, организационный аспекты, развитие потенциала и международное сотрудничество. Казахстан в рамках новой методики выполнил все требования в направлениях «юридический» и «сотрудничество», а также продемонстрировал достаточный технический уровень. Данный рейтинг оценивает готовность 194 стран к кибератакам.

В 2024 году в первой группе рейтинга МСЭ доминируют европейские страны и США. В этот список также входят Гана, Кения, Маврикий, Марокко, Руанда и другие страны. Второй уровень, известный как «передовые» страны, включает Казахстан, Китай, Россию, а также Швейцарию и Канаду.

В целях определения уровня осведомленности населения об угрозах информационной безопасности (кибербезопасности с октября по ноябрь 2024 года было проведено социологическое исследование среди населения) (Information Security Committee of the Ministry of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan., 2024).

В процессе исследования было охвачено:

- 3 города республиканского значения;
- 17 областей, райцентры, 11371 респондент.

Показатели осведомленности населения об угрозах информационной безопасности (кибербезопасности) и защиты персональных данных, представлен на рисунке 4.

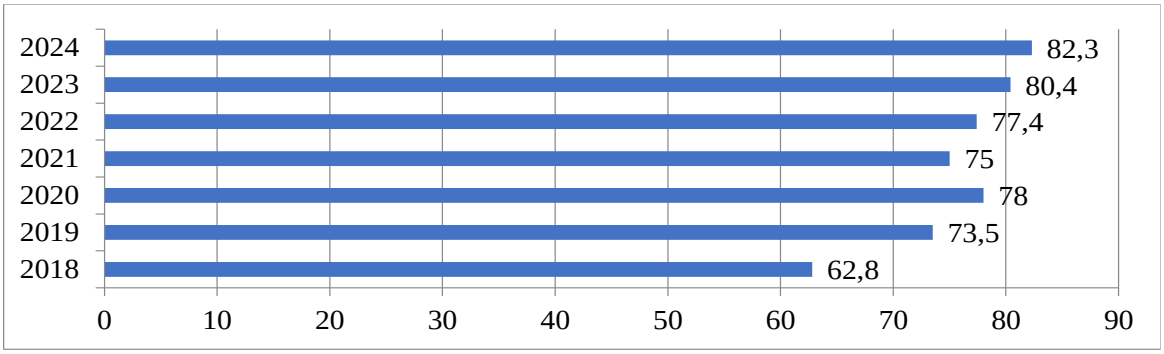

Рисунок 4. Динамика показателей осведомленности населения об угрозах информационной безопасности (кибербезопасности) и защиты персональных данных (на основе социологического опроса) за 2018-2024 гг.%

Из рисунка 4 видно, что государство проводит работу по осведомлению населения об угрозах кибербезопасности. В 2022 году процент осведомленности населения составил 77,4%, то в 2024 году на 4,9% больше, что составило 82,3%.

По результатам социологического опроса, большинство респондетов были осведомлены об киберугрозах:

- получают знания о защите личной информации при использовании социальных сетей – 90,52%;
- осведомлены при использовании цифровой подписи – 85,06%;
- знают о потенциальных рисках детей при использовании интернета – 76,65%.

Вопросам развития сферы информационной безопасности в Казахстане уделяется значительное внимание. И результат работы, проводимой совместно органами, неправительственными организациями и бизнесом — это тенденция последних лет, когда наша страна стремительно улучшает свои позиции в глобальном индексе кибербезопасности.

Управление ООН по наркотикам и преступности определяет кибератаку следующим образом: «Под понятием «кибератака» обычно понимают преднамеренную эксплуатацию компьютерных сетей с целью предпринять атаку. Такие атаки, как правило, предпринимаются для нарушения надлежащего функционирования целей, таких как компьютерные системы, серверы или лежащая в их основе инфраструктура, при помощи хакинга, технологий APT (развитая устойчивая угроза), компьютерных вирусов, вредоносного программного обеспечения, заливки и иных средств несанкционированного или злонамеренного доступа». Согласно опросу, за последние годы население страны подвергались, следующим видам кибератак, показанные в таблице 2 (КИБЕРКОД, 2024).

Таблица 2. Анализ кибератак за 2022-2024 гг.

Угрозы	Годы			
	2022	2023	2024	2024 / 2023, %
Фишинговая атака	1200	2160	3 720	172
DoS/DDoS-атака	53	152	117	76,9
Эксплуатация уязвимости	1800	2726	3877	142,2

Из таблицы 2 видно, что за анализируемый период, произошел рост фишинговых атак. В 2024 году рост составил 72% по сравнению с 2023 годом, что составило 3720 единиц. Большинство фишинговых ресурсов использует такие типы имитации фишинга, как клоны интернет-ресурсов, розыгрыши и лотереи, формы авторизации.

Кроме этого, 2024 году количество фишинговых интернет-ресурсов, эмулирующих деятельность банков второго уровня РК, составил 95 преступлений, то есть 3% от всех преступлений. Эти данные указывают на усложнение методов фишинга, включая

использование ИИ для автоматизации атак, что требует от организаций усиленного контроля и постоянного повышения осведомленности сотрудников.

DoS-атака (Denial of Service) — буквально «отказ в обслуживании». Это тип атаки, в котором мошенники нападают с целью вызвать перегрузку подсистемы сервиса. В этом случае компьютер (или компьютеры) используется для заполнения сервера пакетами TCP и UDP.

В 2024 году количества этих атак снизилась на 35 единиц, что составила 117. При этом 35 % зафиксированных DoS/DdoS-атак были направлены на банки второго уровня РК и 22 % на государственный сектор. DdoS – это действия, направленные на перегрузку трафиком, когда на атакуемый ресурс отправляется большое количество злонамеренных запросов, из-за чего полностью «забиваются» все каналы сервера или вся полоса пропускания. При этом передача легитимного трафика на сервер затрудняется или становится невозможной.

Анализ угроз информационной безопасности за 2024 год демонстрирует, что Казахстан продолжает сталкиваться с растущей сложностью угроз. Особенно заметным становится активный рост атак на информационные системы, которые не успели адаптироваться к современным вызовам, что подчёркивает необходимость своевременного обновления программного обеспечения и внедрения более надёжных защитных мер.

Казахстан имеет отдельные законодательные акты в части кибербезопасности, а именно, Концепция Кибербезопасности РК ("Киберщит Казахстана") от 30 июня 2017 г., Стратегия кибербезопасности финансового сектора Республики Казахстан на 2020-2022 годы, Концепция развития цифровой экосистемы на 2022-2027 года («Киберщит-2»).

Кроме того, в планах разработать единую техническую политику в сфере ИКТ, в рамках которой предприятия и организации можно будет определять по уровням безопасности. И появится новая методика экономической системы информационной безопасности. Также рассмотрят возможность создания резервного Национального координационного центра информационной безопасности, "Киберполигона" по подготовке специалистов.

Отмечается, что в вопросе кибербезопасности уже был реализован ряд важных проектов. Например, в законе появилось понятие "киберстрахование", которое позволяет возмещать имущественный вред организации, причиненный в результате компьютерных инцидентов, а также моральный вред физическому лицу, причиненный в результате утечки данных.

Также был создан Комитет по ИБ, появились профстандарты в IT и запущен "пилот" частной платформы выявления уязвимостей BugBounty. Там уже зарегистрировано более 1,1 тыс. независимых экспертов, от которых получено более 1,2 тыс. отчетов с сообщениями об уязвимостях. (Zhumabekov, R., & Akhmetov, K., 2021).

На основе проекта Концепции "Киберщит-2" государство предлагает следующие основные направления по обеспечению кибербезопасности в Казахстане до 2027 года, которые показаны на рисунке 5 (Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан, 2023).

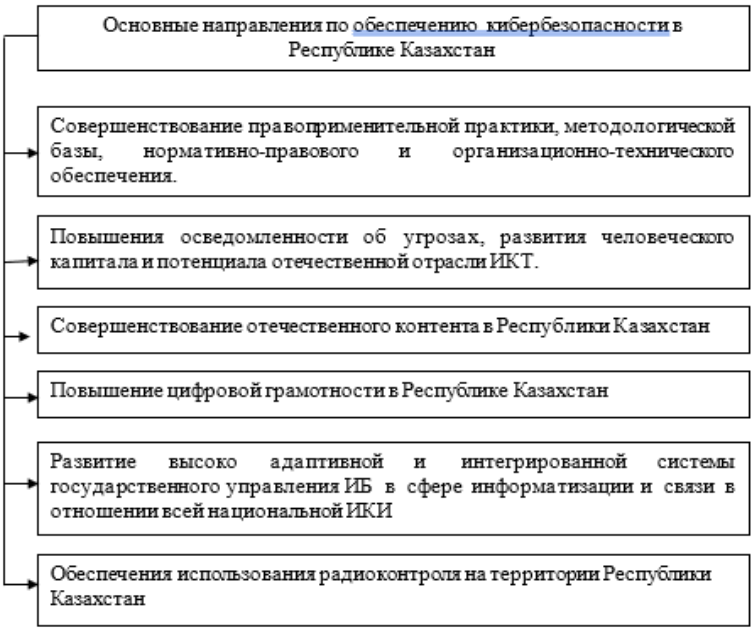

Рисунок 5. Основные направления по обеспечению кибербезопасности в Республике Казахстан

Для реализации указанной задачи в первую очередь необходимо развивать открытость информационного пространства Республики Казахстан. Его глубокая интегрированность с глобальным медиа пространством сопряжена с рисками деструктивного характера. С каждым годом отмечается наплыв противоправной информации, которая носит агрессивный характер, что находит прямое отражение в общественных настроениях.

С 2022 года выявлено свыше 249 739 интернет-ресурсов и ссылок на страницы в социальных медиа, содержащих противоправные материалы, в отношении которых направлено более 2 770 реагирующих документов (проектов предупредительных писем и проектов предписаний уполномоченного органа).

Среди других вызовов, связанных с распространением информации через глобальные медиа-платформы, необходимо отметить, неконтролируемое усиление зависимости от социальных сетей у определённых социальных групп населения, формирование в обществе социально-психологических фобий, навязывание чуждых национальному менталитету ценностей, этических норм, моральных устоев (культурная вестернизация) и так далее.

В Казахстане ранее предпринимались попытки системно подойти к решению вопроса развития отечественного сегмента сети Интернет и насыщению казахстанского рынка собственными аналогами популярных зарубежных IT-решений - социальной сети, службы электронной почты, видеопортала, браузера, поисковой системы и другие (в рамках «Дорожной карты по развитию безопасного казахстанского сегмента сети Интернет и цифрового информационного пространства Республики Казахстан»).

Тем не менее, до настоящего времени разработанные программные продукты не смогли преодолеть высокую конкурентность среди пользующихся мировой популярностью решений и не получили широкого распространения в стране.

Таким образом, из развивающихся в Казахстане в данное время видеосервисов необходимо отметить видеохостинги «Kaztube» (Международное информационное агентство «Казинформ») и «Aitube» (компания «Aitu Dala»), которые нацелены на поддержку и дистрибуцию отечественного контента.

Вместе с тем, в долгосрочной перспективе для снижения зависимости от глобальных медиа-платформ и степени их влияния целесообразным видится создание и постепенное развитие единой цифровой платформы («цифровой экосистемы»).

Для успеха реализации подобного проекта (с учетом предыдущего опыта создания отечественных продуктов, по сути, повторявших функционал зарубежных аналогов) необходимо интегрировать на создаваемой платформе уже существующие полезные и привлекательные для пользователей сервисы, чтобы данный продукт стал на самом деле незаменимым ежедневным средством как общения (мессенджер), так и получения всевозможных услуг и развлечений (банковские операции, государственные услуги, продажа авиа и железнодорожных билетов, заказ такси, купоны и скидки, видеохостинг, онлайн кинотеатр, интернет-телевидение, справочные службы, call-центры, новости и развлечения и так далее).

4. Заключение

Финансовая отрасль является одним из наиболее динамичных секторов экономики в контексте адаптации и внедрения ИИ. Финансовые организации способны получить значительные преимущества от внедрения ИИ (Longbing Cao (2021).

В настоящее время крупные игроки финансового рынка применяют потенциал ИИ в различных сферах своей деятельности:

- улучшении клиентского опыта;

Использование ИИ помогает финансовым организациям не только улучшать опыт использовании финансовых услуг, но и повышать их качество.

. ИИ в данном контексте действует как катализатор для принятия обоснованных, датацентричных решений. (Kumarkhanova et al., 2022).

Использование интеллектуальных систем обработки документов за счет классификации информации значительно ускоряет обработку больших объемов документов, уменьшая вероятность ошибок и повышая эффективность работы сотрудников.

Данные Insider Intelligence указывают, что три четверти банков с активами, превышающими 100 млрд долларов США, уже интегрировали технологии ИИ в свою деятельность и, согласно аналитическому центру IDC, прогнозируется, что к 2024 году финансовая сфера будет занимать ведущие позиции по размеру инвестиций в ИИ

Технология DeepFake, применяемая для мошеннических операций, представляет собой подделку изображений, видео или аудиофайлов с использованием ИИ и глубокого обучения. Эта технология может имитировать голоса, выражения лица и движения, создавая реалистичный, но фальшивый контент (Arxiv, 2025). Использование технологии DeepFake для мошенничества представляет собой серьезную угрозу. Соответственно целый ряд лабораторий и институтов занимаются исследованиями и разработкой методов обнаружения подобного мошенничества (Tkachenko et al., 2023).

В Казахстане одним из подобных примеров является процесс тестирования биометрических решений поставщиков, осуществляемый в рамках их присоединения к Центру обмена идентификационными данными Национальной платежной корпорации. (Жумадилова и др., 2021). Частью этого процесса является оценка биометрических решений различных поставщиков на способность обнаружения фактов использования DeepFake технологий для фальсификации личности при получении финансовых услуг.

Глобальное развитие концепции Open Banking является значимым драйвером развития использования ИИ на финансовом рынке. Это направление, связанное с оперативным сбором данных и их последующей обработкой с применением ИИ, обеспечивает более открытый и унифицированный доступ к финансовым данным. (Aubakirova & Yerdesh, 2021).

В сочетании с RegTech развитие систем Open Banking обеспечивает более эффективные механизмы регулирования и надзора в финансовой сфере (Alibekova et al., 2020). В контексте RegTech это означает, что регуляторы могут получать актуальную и точную информацию от финансовых учреждений в реальном времени. Это повышает эффективность регуляторов в микропруденциальном регулировании, выявлении финансовых преступлений, предотвращении мошенничества и обеспечении соблюдения законодательства. В целом,

развитие Open Banking в рамках RegTech обеспечивает более интегрированный, прозрачный и эффективный подход к регулированию финансовой сферы, способствуя улучшению безопасности, снижению рисков и обеспечивая более высокий уровень соответствия нормативам.

В то же время, развитие Open Banking необходимо для развития технологий и подходов генерации синтетических данных, которые могут быть сформированы только на основе реальных данных, собранных со всего рынка, а их безопасный сбор в свою очередь невозможен без развитой системы Open Banking. Уже сейчас наблюдаемое развитие компаний в индустрии финансовых технологий Европейского союза, Великобритании и Австралии связывается с постоянными и последовательными усилиями по развитию Open Banking для свободного и безопасного обмена банковскими данными клиентов. Тем не менее, существует ряд ограничений для подключения к данным системам и их использованию. Между тем синтетические данные могут стать следующим драйвером роста финансовых технологий, связанных с развитием ИИ. В случае синтетических данных снижается порог входа и облегчается доступ к необходимым данным для использования более широким кругом компаний, в том числе стартапами.

Цифровая трансформация помогает компаниям адаптироваться под запросы изменяющегося рынка и внедрять прогрессивные модели ведения бизнеса. Отраслевые лидеры всерьез озабочены переводом своих процессов в digital и технологическим превосходством относительно конкурентов. Это возможность повысить эффективность процессов и, как следствие, улучшить качество своих продуктов или услуг, а также существенно увеличить прибыль для акционеров и владельцев бизнеса.

Постоянное совершенствование технических и организационных механизмов защиты информации и выполнение всех нормативных, законодательных и договорных обязательств в области информационной безопасности, а также обновление правил внутреннего распорядка и политики информационной безопасности.

Предложение новых профессий, курсов по повышению квалификации, специальных курсов с возможностью дальнейшего трудоустройства для заинтересованных слоёв населения с целью повышения рабочих мест и подключения населения в работе с роботами и искусственным интеллектом. Механизмы адаптации к роботизации предполагают активную подготовку специалистов по дисциплинам STEAM: наука, технологии, инжиниринг, искусство, математика. На этих направлениях основываются сферы деятельности, в которых роботы пока не могут заменить человека.

Информация о финансировании

Это исследование было выполнено без какой-либо финансовой поддержки.

Конфликт интересов

Авторы заявляет об отсутствии конфликта интересов.

Авторские вклады

Дарибекова АС.- основное содержание; Дарибеков СС- перевод, редактирование, исправления; Дарибекова НС- дополнения и поиск информации.

Доступность источников

Данные, используемые в этой статье, доступны по запросу авторов.

Список литературы/ References

1. Alibekova, G., Medeni, T., Panzabekova, A., & Mussayeva, D. (2020). Digital transformation enablers and barriers in the economy of Kazakhstan. *Journal of Asian Finance, Economics and Business, 7*(7), 565–575. DOI: https://doi.org/10.13106/jafeb.2020.vol7.no7.565

2. Amoroso, E. (2006). *Cyber Security*. New Jersey: Silicon Press.

3. Arxiv. (2025). Detection of AI deepfake and fraud in online payments using GAN-based models. *ArXiv*. URL: https://arxiv.org/abs/2501.07033

4. Aubakirova, Z., & Yerdesh, E. (2021). Digital transformation: Banks shift to digitization and innovation. *Bulletin of Kazakh National University. Economic Series, 137*(3), 70–77. URL: https://be.kaznu.kz/index.php/math/article/view/2054

5. Canongia, C., & Mandarino, R. (2014). Cybersecurity: The new challenge of the information society. In *Crisis management: Concepts, methodologies, tools and applications* (pp. 60–80). Hershey, PA: IGI Global. DOI: http://dx.doi.org/10.4018/978-1-4666-4707-7.ch003

6. Cao, L. (2021). AI in finance: Challenges, techniques and opportunities. *ArXiv*. URL: https://arxiv.org/pdf/2107.09051

7. DHS. (2014). *A glossary of common cybersecurity terminology*. National Initiative for Cybersecurity Careers and Studies: Department of Homeland Security. URL: http://niccs.us-cert.gov/glossary#letter_c

8. Information Security Committee of the Ministry of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan. (2024). Sociological survey data among the population. URL: https://www.gov.kz/memleket/entities/infsecurity/press/article/details/109499?lang=ru

9. Issabayeva, S. B. (2019). Cybersecurity policy development in Kazakhstan: Analysis of m-commerce user acceptance. *Gosudarstvennoye upravleniye i gosudarstvennaya sluzhba, 1*(68), 34–49.

10. ITU. (2009). *Overview of cybersecurity. Recommendation ITU-T X.1205*. Geneva: International Telecommunication Union (ITU). URL: http://www.itu.int/rec/T-REC-X.1205-200804-I/en

11. Kemmerer, R. A. (2003). Cybersecurity. In *Proceedings of the 25th IEEE International Conference on Software Engineering* (pp. 705–715). DOI: http://dx.doi.org/10.1109/ICSE.2003.1201257

12. КИБЕРКОД. (2024). *Вызовы цифровой эпохи*. URL: https://sts.kz/storage/media/%C3%90%C2%BA%C3%90%C2%B8%C3%90%C2%B1%C3%90%C2%B5%C3%91%C3%90%C2%B4%C3%90%C2%B0%C3%90%C2%B9%C3%90%C2%B4%C3%90%C2%B6%C3%90%C2%B5%C3%91%C3%91%20%C3%91%C3%90%C2%B8%C3%90%C2%BD%C3%90%C2%B0%C3%90%C2%BB%201402%20%C3%90%C2%B2%C3%90%C2%B5%C3%90%C2%B1_compressed_MgA8leK.pdf

13. Kuzmicheva, T. G., & Golovanova, E. V. (2025). Sfery primeneniya kiberbezopasnosti [Areas of application of cybersecurity]. *Teoriya i praktika sovremennoy nauki, 1*(115), 96–99. URL: https://cyberleninka.ru/article/n/sfery-primeneniya-kiberbezopasnosti/viewer

14. Kumarkhanova, N., Maulina, N., & Zholdasbaeva, K. (2022). The impact of digital technologies on improving the efficiency of the financial market in Kazakhstan. *Bulletin of L.N. Gumilyov Eurasian National University. Economic Series, 139*(4), 95–104.

15. Lewis, J. A. (2006). *Cybersecurity and critical infrastructure protection*. Washington, DC: Center for Strategic and International Studies. URL: http://csis.org/publication/cybersecurity-and-critical-infrastructure-pr

16. Ministry of Digital Development, Innovations and Aerospace Industry of the Republic of Kazakhstan. (2023). *Concept of digital transformation and development of ICT and cybersecurity for 2023–2029*. Astana.

17. Moschovitis, C. (2018). *Cybersecurity program development for business: The essential planning guide*. John Wiley & Sons.

18. PricewaterhouseCoopers. (2019). *Risk management and cybersecurity*. PwC. URL: https://www.pwc.com/kz/ru/services/risk-assurance-services/cybersecurity.html

19. Prestupleniya v sfere komp'yuternykh tekhnologiy: monografiya [Crimes in the field of computer technology: Monograph]. (2014). L. F. Tatarinova. Almaty: Kazakh National University.

20. Puchkova, A. (2024). Kazakhstan ukrepil pozicii v Globalnom indekse kiberbezopasnosti [Kazakhstan has strengthened its position in the Global Cybersecurity Index]. URL: https://rus.baq.kz/kazahstan-ukrepil-pozitsii-v-globalnom-indekse-kiberbezopasnosti_183978

21. Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *The Journal of Digital Forensics, Security and Law*, *12*(2), 53–74. DOI: https://doi.org/10.15394/jdfsl.2017.1476

22. Tkachenko, N., et al. (2023). Opportunities for synthetic data in nature and climate finance. *Frontiers in Artificial Intelligence, 6*, 1168749. DOI: https://doi.org/10.3389/frai.2023.1168749

23. United Nations Office on Drugs and Crime. (2019). *Module 2: General types of cybercrime*. URL: https://www.unodc.org/documents/e4j/Cybercrime/Cybercrime_Module_2_General_Types_of_Cybercrime_RU.pdf

24. Vitlyakova, S. S. (2019). *Kiberbezopasnost, kak ugroza natsional'noy bezopasnosti (natsional'nym interesam) [Cybersecurity as a threat to national security (national interests)]*. Moscow: Infra.

25. Weinrauch, V. (2024). Schastlivyi sluchai: 5 preimushchestv ispolzovaniya iskusstvennogo intellekta v bankovskoy sfere [Happy occasion: 5 advantages of using artificial intelligence in the banking sector]. URL: https://www.internationalwealth.info/foreign-bank-accounts/preimushhestva-ispolzovanija-iskusstvennogo-intellekta-v-bankovskom-sektore

26. Zhumabekov, R., & Akhmetov, K. (2021). Development of cybersecurity in Kazakhstan: Current state and prospects. *Bulletin of L.N. Gumilyov Eurasian National University. Law Series, 136*(3), 45–54.

27. Zhumadilova, T., Kasenova, G., & Supugalieva, G. (2021). Digitalization of financial services of banks in Kazakhstan: Trends and prospects of development. *Bulletin of L.N. Gumilyov Eurasian National University. Economic Series, 136*(2), 188–198. URL: https://bulecon.enu.kz/index.php/main/article/view/647