References:

1. Finansovaya otchetnost' AO «Otbasy banka» za 2022 god v sootvetstvii s Mezhdunarodnymi standartami finansovoj otchetnosti i otchet Nezavisimogo auditora – elektronnyj resurs. URL: https://hcsbk.kz/ru/about-the-bank/reporting/ (data obrashcheniya 25.03.2025 g.).

2. Sh.R. Bergenova, A.A. Abdukalikova \"Sostoyanie ipotechnogo kreditovaniya v Respublike Kazahstan i ego rol' v ekonomike strany\" – stat'ya, - 2020 g.

3. V kakih bankah luchshie usloviya ipoteki v 2023 godu v RK – elektronnyj resurs. URL: https://bizmedia.kz/2022/12/30/luchshe-usloviya-dlya- ipoteki-v-2023-v-rk/ (data obrashcheniya 01.04.2025 g.).

4. Oficial'nyj sajt AO «Otbasy bank»: Istoriya - elektronnyj resurs. URL: https://hcsbk.kz/ru/about-the-bank/history/ (data obrashcheniya 05.04.2025 g.).

5. Otbasy bank, Vikipediya – elektronnyj resurs. URL: https://ru.wikipedia.org/wiki/Otbasy_bank (data obrashcheniya 11.04.2025 g.).

6. Ipotechnoe kreditovanie: pravovye i ekonomicheskie aspekty\" – uchebnik, avtor O.G.Subbotina, - 2019 g, 264 str.

7. Problemy razvitiya ipotechnogo kreditovaniya v Kazahstane – elektronnyj resurs. URL: https://articlekz.com/article/12256 (data obrashcheniya 21.04.2025 g.);

8. NPA: Koncepciya razvitiya zhilishchno-kommunal'noj infrastruktury do 2026 goda – elektronnyj resurs. URL: https://legalacts.egov.kz/npa/view?id=14434573 (data obrashcheniya 05.03.2025 g.)

9. Vidy gosudarstvennyh ipotechnyh programm i programmy arendnogo zhil'ya – elektronnyj resurs. URL: https://anyk.kz/ru/introduction (data obrashcheniya 01.04.2025 g.);

10. «Sovremennoe sostoyanie ipotechnogo kreditovaniya v Kazahstane: tendencii i perspektivy» – stat'ya, avtory G.A. Kurmanova, R.K. Zhұmabekova, - 2021 g

МРНТИ 06.81.55 **10.51889/3078-8579.2025.84.2.003**

А.Ж. Асанова [1]
[1]Абай атындағы Қазақ Ұлттық Педагогикалық Университеті,
Алматы қ., Қазақстан

ӘЛЕУМЕТТІК ЖЕЛІЛЕРДІ ДАМЫТУДЫҢ ЖӘНЕ АҚПАРАТТЫҚ ҚАУІПСІЗДІККЕ ТӨНЕТІН ҚАУІПТЕРДІҢ ЭКОНОМИКАЛЫҚ САЛДАРЫ

Аңдатпа

Мақалада әлеуметтік желілердегі маркетингтің ел экономикасына ақпараттық қауіпсіздікке қатысты тәуекелдерді ескере отырып әсері талданады. Жедел цифрландыру жағдайында әлеуметтік желілер тек қарым-қатынас пен контент алмасу құралы ғана емес, сондай-ақ тауарлар, қызметтер мен идеяларды ілгерілетудің қуатты құралына айналуда. Компаниялар цифрлық маркетингті аудитория аясын кеңейту, сату көлемін арттыру және тұтынушылардың адалдығын қалыптастыру үшін белсенді қолдануда. Алайда цифрлық кеңістіктегі белсенділік артқан сайын ақпараттық қауіпсіздікке төнетін қауіптер де өсуде. Жеке деректердің таралуы, аккаунттардың бұзылуы, ақпаратты бұрмалау және кибершабуылдар компанияларға ғана емес, тұтас елге де елеулі беделдік және қаржылық шығын келтіруі мүмкін. Мұндай оқиғалар цифрлық платформаларға деген сенімді төмендетіп, электрондық коммерция мен жалпы цифрлық экономиканың дамуына кедергі келтіреді. Мақалада әлеуметтік желілердегі маркетингке байланысты негізгі қауіптер қарастырылып, олардың экономика мен ұлттық қауіпсіздікке әсері мысалдармен келтірілген. Сонымен қатар, Қазақстан Республикасындағы кибершабуылдар жөніндегі статистика ұсынылып, олардың ел экономикасына төндіретін қатерлері сипатталған.

Түйін сөздер: әлеуметтік медиа, ақпараттық қауіпсіздік, кибершабуылдар, экономикалық тұрақтылық, деректердің бұзылуы, қауіптер.

Асанова А.Ж.[1]
[1] Казахский Национальный Педагогический Университет имени Абая
г.Алматы, Казахстан

ЭКОНОМИЧЕСКИЕ ПОСЛЕДСТВИЯ РАЗВИТИЯ СОЦИАЛЬНЫХ СЕТЕЙ И УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация

Статья посвящена анализу влияния маркетинга в социальных сетях на экономику страны с учётом рисков, связанных с информационной безопасностью. В условиях стремительной цифровизации социальные сети становятся не только каналом общения и обмена контентом, но и мощным инструментом продвижения товаров, услуг и идей. Компании активно используют цифровой маркетинг для увеличения охвата аудитории, повышения продаж и формирования лояльности потребителей. Однако вместе с ростом активности в цифровом пространстве увеличиваются и угрозы информационной безопасности. Утечки персональных данных, взлом аккаунтов, фальсификация информации и кибератаки могут привести к серьёзным репутационным и финансовым потерям как компании, так и страны в целом. Более того, такие инциденты подрывают доверие к цифровым платформам, препятствуют развитию электронной коммерции и цифровой экономики в целом. В статье рассматриваются ключевые угрозы, связанные с маркетингом в соцсетях, а также приводятся примеры их последствий для экономики и национальной безопасности. Также приведена статистика по кибератакам в Республике Казахстан, а также перечислены угрозы, которые они несут для экономики страны.

Ключевые слова: социальные сети, информационная безопасность, кибератаки, экономическая стабильность, утечка данных, угрозы.

Assanova A.Zh.[1]
[1]Kazakh National Pedagogical University named after Abai,
Almaty, Kazakhstan

ECONOMIC CONSEQUENCES OF THE DEVELOPMENT OF SOCIAL NETWORKS AND THREATS TO INFORMATION SECURITY

Abstract

The article is dedicated to analyzing the impact of social media marketing on the country’s economy, taking into account the risks related to information security. In the context of rapid digitalization, social media platforms have become not only channels for communication and content exchange but also powerful tools for promoting products, services, and ideas. Companies actively use digital marketing to expand their audience reach, increase sales, and build customer loyalty. However, as activity in the digital space grows, so do the threats to information security. Personal data leaks, account hacking, information falsification, and cyberattacks can cause significant reputational and financial losses both for companies and for the country as a whole. Moreover, such incidents undermine trust in digital platforms and hinder the development of e-commerce and the digital economy overall. The article examines the key threats associated with social media marketing and provides examples of their consequences for the economy and national security. It also presents statistics on cyberattacks in the Republic of Kazakhstan and outlines the risks they pose to the country’s economy.

Keywords: social media, information security, cyberattacks, economic stability, data leakage, threats

КІРІСПЕ

Цифрлық технологиялар дәуірінде әлеуметтік желілер брендтерді ілгерілету мен аудиториямен өзара әрекеттесу үшін негізгі каналға айналды. Олар маркетингті айтарлықтай өзгертті, оны қолжетімді әрі персоналдаған етті. Екінші жағынан, әлеуметтік желілерді белсенді пайдалану ақпараттық қауіпсіздікке жаңа тәуекелдер тудырады, бұл тек пайдаланушылардың брендке деген сеніміне ғана емес, сонымен қатар елдің экономикалық дамуына да әсер етуі мүмкін.

Әлеуметтік желілер брендтерге беделін қалыптастыру және жаңа клиенттер тарту үшін ерекше мүмкіндіктер береді. Олар компанияларға аудиториямен тікелей байланыс орнатуға, жедел кері байланыс алуға және клиенттердің тілектеріне сәйкес өнімдері мен қызметтерін бейімдеуге мүмкіндік береді. Сонымен қатар, әлеуметтік желілердегі маркетинг брендтің көрінуін арттырады, шағын және орта бизнеске клиенттік базаны кеңейтуге көмектеседі, сатылымды ынталандырады, бұл өз кезегінде экономикаға оң ықпалын тигізеді.

Әлеуметтік желілердің танымалдығы артқан сайын брендтер ақпараттық қауіпсіздікке байланысты жаңа қауіптерге тап болады. Қауіпсіздіктің бұзылуы, деректердің ағып кетуі және кибершабуылдар брендтің беделіне ауыр зиян келтіріп, пайдаланушылардың сенімін шайқалтады. Егер компанияның әлеуметтік желідегі аккаунты бұзылса, бұл жалған ақпараттың немесе жалған ұсыныстардың таралуына әкелуі мүмкін, ол тек клиенттерді алдаумен ғана шектелмей, компанияға қаржылық шығын әкеледі.

ЗЕРТТЕУ МАТЕРИАЛДАРЫ МЕН ӘДІСТЕРІ

Зерттеу жүргізу үшін әлеуметтік желілердегі маркетингтің ел экономикасына әсер ету үрдістерін зерттеуге арналған ашық дереккөздердегі жарияланымдарға талдау жүргізілді, сондай-ақ Қазақстан Республикасындағы киберқылмыстарға қатысты статистикалық мәліметтер сарапталды. Сонымен қатар халықаралық компаниялардың деректері зерттелді.

НӘТИЖЕЛЕР МЕН ТАЛҚЫЛАУЛАР

Ғаламдану мен цифрландыру жағдайында ақпараттық қауіпсіздік ұлттық қауіпсіздіктің ажырамас бөлігіне айналуда. Әлеуметтік желілерде жұмыс істейтін ірі компаниялардың деректерін бұзу ел экономикасының тұрақтылығына қауіп төндіруі мүмкін, себебі бұл ірі компаниялар мен олардың жеткізушілері мен серіктестерін қамтиды. Пайдаланушылардың қаржылық деректері зардап шексе, бұл цифрлық төлем жүйелеріне деген сенімсіздікті туғызып, цифрлық экономиканың дамуын тежейді және елдің ЖІӨ-не әсер етеді.

Қазіргі таңда Қазақстан NCSI рейтингісінде 78-орында тұр, Беларусь, Молдова, Әзірбайжан және Ресейден кейін қалып отыр. 2023 және 2024 жылдарға арналған мәліметтер бойынша Қазақстанда ең жиі кибершабуылдарға ұшырайтын салалар төмендегі (1-кесте) көрсетілген.

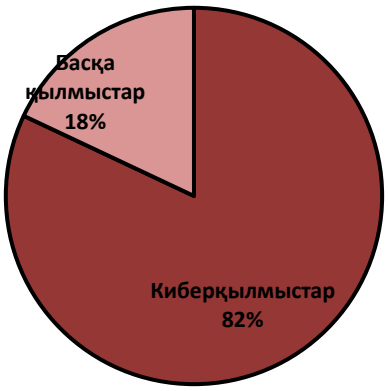
1-кесте – 2023 және 2024 жылдары
Қазақстанда кибершабуылдарға ұшыраған секторлар

Қазақстандағы 2023 және 2024 жылдардағы кибершабуылдар	
Секторлар:	Бағытталған кибершабуылдар:
БАҚ	DDoS шабуылдарының толқыны, тоғыз тәуелсіз басылымдар мен журналистердің аккаунттары әсер етті
Мемлекеттік мекемелер	Мемлекеттік деректерге қол жеткізу және мекемелердің жұмысын бұзу.
Қаржы ұйымдары	Клиенттердің қаржылық ақпараты мен дербес деректерін ұрлау.
Телекоммуникациялық компаниялар	Зиянды бағдарламаларды тарату және дербес деректерге қол жеткізу.
Ескерту: автор дереккөз негізінде құрастырған [1]	

БАҚ ең осал болып шықты және басқа секторлармен салыстырғанда шабуылдардың 19% нысанаға айналды (1-сурет).

1 – сурет-2023-2024 жылдары Қазақстанда кибершабуылдарға ұшыраған секторлар., %
Ескерту: сурет дереккөз негізінде құрастырылған [1]

2024 жылы Қазақстанда интернет-алаяқтықтың 3645 жағдайы тіркелген, бұл өткен жылдың сәйкес кезеңімен салыстырғанда 8,3%-ға өсімді көрсетеді (2-сурет).



2-сурет – Қазақстандағы киберқылмыс деңгейі, 2024 ж.
Ескерту: сурет [2] дерегінің негізінде құрастырылған

2025 жылғы қаңтар-наурыз айларының қорытындысы бойынша Қазақстанда ақпараттық қауіпсіздік саласында 30 мың оқиға тіркелді, бұл 2024 жылдың сәйкес кезеңімен салыстырғанда 2 есе көп. Кибершабуылдардың ең көп саны ботнет-активтілікке қатысты болды – 17,6 мың оқиға, ал бір жыл бұрын бұл көрсеткіш небәрі 1,7 мың жағдайды құраған. Компьютерлік вирустар, желілік құрттар мен трояндық бағдарламаларға байланысты инциденттер жиі тіркелді: олардың саны бір жылда 17,9%-ға азайып, 7,9 мың жағдайды құрады. Керісінше, интернеттегі фишингтік шабуылдар 37,2%-ға көбейіп, 2 мың жағдайға жетті. Интернет-ресурстарға қол жеткізу мүмкіндігінің болмауына байланысты инциденттер саны 48,1%-ға қысқарып, 112 жағдай болды. Сонымен қатар, 23 DDoS-шабуыл тіркелді, ал

бір жыл бұрын мұндай шабуылдардың саны 30 болған. Рұқсатсыз қол жеткізу және контентті өзгертуге байланысты 9 жағдай тіркелді, бұл 2024 жылғы қаңтар-наурыз аралығында болған 13 фактіден аз.

Соңғы 7 жылда Қазақстандағы киберқылмыс 10 еседен астам өсті, ал өткен жылдың қорытындысы бойынша киберқылмыстар барлық құқықбұзушылықтардың 18%-ын құрады. Киберқылмыстың кең таралуының негізгі себебі – компаниялар мен пайдаланушылардың цифрлық кеңістікте, соның ішінде әлеуметтік желілер мен цифрлық платформаларда белсенді болуы, ал бұл кеңістік «қауіпсіз емес маркетингке» бейім.

Әлеуметтік желілердегі қауіпсіз емес маркетинг – бұл деректердің құпиялығына, пайдаланушылардың қауіпсіздігіне қауіп төндіретін немесе брендтерге шығын келтіретін стратегиялар мен тәсілдерді қолдану. Кейбір компаниялар қолданушылардың жеке қызығушылықтары, денсаулық жағдайы немесе қаржылық ахуалы туралы мәліметтерге сүйене отырып, жоғары дәлдікпен бағытталған жарнама жүргізеді. Мұндай ақпарат тұтынушыларға пайдалы көрінуі мүмкін, бірақ егер бұл мәліметтер пайдаланушының келісімінсіз қолданылса немесе жеткілікті түрде қорғалмаса, олар киберқылмыскерлердің қолына түсуі мүмкін. Мысалы, Facebook қолданушыларының жеке деректері саяси мақсатта пайдаланылған Cambridge Analytica оқиғасы халықаралық жанжал туғызды [3].

Конкурстар мен ұтыс ойындары арқылы жүргізілетін маркетинг брендке назар аудартуы мүмкін, бірақ тиісті қауіпсіздік қамтамасыз етілмесе, бұл іс-шаралар пайдаланушылар үшін тұзаққа айналуы ықтимал. Алаяқтар көбіне брендтердің жалған парақшаларын жасап, конкурстарды көшіріп, қатысушылардың телефон нөмірі, мекенжайы және басқа да жеке деректерін жинайды. Бұл мәліметтер кейін спам немесе алаяқтық әрекеттер үшін пайдаланылады.

Әлеуметтік желілерде беделін арттыру үшін кейбір компаниялар жалған пікірлер жазып, лайктар мен пікірлердің санын қолдан көбейтеді. Бұл бренд туралы оң көзқарас қалыптастыруы мүмкін, бірақ қолданушылар жалғандықты байқаған сәтте сенім жойылады. Одан бөлек, жалған пікір жазатын аккаунттар бұзылып немесе қолды болуы мүмкін, бұл мұндай әдістерді аса қауіпті етеді.

Егер компания өз аккаунттарын тиісті деңгейде қорғамаса, олар бұзуға осал болады. Мұндай жағдайлардың ең белгілі мысалдарының бірі – 2020 жылы ірі компаниялар мен танымал тұлғалардың Twitter-аккаунттарының бұзылуы. Хакерлер верификацияланған аккаунттарға қол жеткізіп, пайдаланушыларды алаяқтық схемаға тарту мақсатында жалған биткойн үлестіру туралы хабарламалар жариялады. Бұл тек жазылушылар арасында дүрбелең тудырып қана қоймай, брендтердің беделіне де нұқсан келтірді [4].

Кейбір компаниялар пайдаланушылардың келісімінсіз деректерін жинау үшін жасырын трекерлер мен технологияларды қолданады. Мысалы, Facebook пайдаланушылар қолданбадан шыққаннан кейін де олардың басқа қосымшалар мен сайттардағы әрекеттерін қадағалау үшін арнайы технологияны пайдаланған. Бұл қоғамдық наразылық тудырып, дербес мәліметтердің құпиялығын сақтау мәселесін көтерді.

Чат-боттар пайдаланушылармен өзара әрекеттесу үшін қолданылады, бірақ егер олар тым көп жеке ақпарат сұраса немесе жеткілікті қорғалмаған болса, бұл деректердің таралуына әкелуі мүмкін. Пайдаланушылар мұндай арналар арқылы құпия ақпаратты өздері де байқамай беріп қояды, әрі бұл деректердің қалай қолданылатынын немесе қорғалатынын түсінбеуі мүмкін.

TikTok қосымшасы пайдаланушылар деректерінің Қытай үкіметіне берілуі мүмкін деген күдікпен сынға ұшырады. Бұл құпиялылықтың бұзылуына қатысты алаңдаушылық тудырды. Кейбір жағдайларда бренд жасөспірімдерге бағытталған агрессивті жарнама жүргізуге жол берген, бұл мұндай әдістердің этикалық сипаты жөнінде сұрақтар туындатты. Кейбір елдер бұл қосымшаны қауіпсіздікке қауіп төндіреді деп, оны бұғаттау мәселесін қарастырды [5].

Uber компаниясы агрессивті маркетинг және бақылау әдістерін қолданған. Бір жағдайда компания пайдаланушылар қосымшадан шыққаннан кейін де олардың орналасқан жерін бақылаған. Бұл әрекет жағымсыз реакция мен дербес деректердің құпиялығының бұзылуы жөнінде күдік тудырды. Uber кибершабуылдарға осал деректерді сақтағаны үшін сынға ұшыраған [6].

Amazon компаниясы бәсекелестері мен пайдаланушылары туралы деректерді жинау үшін жасырын технологияларды пайдаланған. Компания тұтынушылардың деректерін өз бизнес үдерістерін жетілдіру мақсатында қауіпсіз емес түрде қолданды деп айыпталды, бұл мұндай әрекеттердің этикалық сипатына күмән тудырды. Мысалы, Amazon платформасындағы үшінші тарап сатушыларының деректерін бәсекелес тауарлар шығару үшін пайдаланғаны үшін сынға ілікті [7].

Пандемияның басында Zoom қосымшасы тез танымал болды, бірақ ақпараттық қауіпсіздік мәселелерімен бетпе-бет келді. «Зумбомбинг» – бейнекездесулерге рұқсатсыз кіру – пайдаланушылар деректерінің жеткіліксіз қорғалуы салдарынан кең таралған мәселеге айналды. Қосымша пайдаланушыларды ескертпестен деректерді пайдалану және жеткіліксіз құпиялық шаралары үшін сынға ұшырады [8].

Қазіргі уақытта TEMU және онлайн-казино секілді бизнес түрлері агрессивті жарнама әдістерін қолдану арқылы көп пайдаланушыны тартуға бағытталған маркетингтік стратегияларды белсенді қолдануда. Бұл екі түрлі бизнес өзіне тән тәсілдерді пайдаланғанымен, көбінесе тітіркендіргіш немесе тіпті қауіпті деп қабылдануы мүмкін тактикаларды қолданады.

TEMU – бұл төмен бағалар мен тауарлардың кең ауқымы арқылы жылдам танымал болған онлайн сауда платформасы [9]. TEMU өзінің платформасын әлеуметтік желілер мен іздеу жүйелері арқылы белсенді түрде жарнамалап, кең аудиторияны нысанаға алады. Оның жарнамалары Instagram, Facebook және TikTok сияқты платформаларда жиі кездеседі, мұнда олар жеңілдіктер мен акциялар арқылы назар аударады.

TEMU-дің негізгі стратегияларының бірі – жеңілдіктер ұсыну мен рефераль ды бағдарламаларды қолдану. Пайдаланушылар достарын тартқаны үшін бонус алады, бұл платформаның аудиториясын жылдам кеңейтуге мүмкіндік береді. Сонымен қатар, компания жиі купондар мен уақытша жеңілдіктер ұсынады, бұл шұғылдық сезімін тудырып, пайдаланушыларды тезірек сатып алуға итермелейді.

Платформа пайдаланушылардың әрекеттері туралы мәліметтерді қолдана отырып, жекелендірілген ұсыныстарды көрсетеді. Пайдаланушыларға бұрын қараған немесе қызығушылық танытқан тауарлар көрсетіледі. Бұл сатып алу ықтималдығын арттырады, бірақ деректердің құпиялығы мен қауіпсіздігіне қатысты сұрақтар туындатады.

Онлайн-казино агрессивті маркетингке сүйенеді, әсіресе жаңа ойыншыларды тарту және бұрынғыларын ұстап қалу үшін түрлі психологиялық тәсілдерді қолданады. Ең кең таралған әдістердің бірі – тіркелу кезінде бонустар ұсыну. Жаңа пайдаланушыларға жиі «тегін» ақша немесе слоттарда «тегін» айналдыру мүмкіндігі беріледі, бұл оларды ойынды жалғастырып, нақты ставкалар жасауға ынталандырады.

Казино белсенді пайдаланушыларға тұрақты акциялар мен VIP бағдарламалар ұсынады, бұл оларды көбірек ақша жұмсауға ынталандырады. Мысалы, пайдаланушылар адалдық ұпайларын жинап, оларды ақшаға немесе қосымша бонустарға айырбастай алады. Бұл байланыс сезімін тудырып, платформадан тәуелділікке әкелуі мүмкін.

Казино таргетинг пен ремаркетингті белсенді қолданады – яғни сайтқа бұрын кірген немесе құмар ойындарға қызығушылық танытқан пайдаланушыларға жарнама көрсетіледі. Бұл әсіресе құмар ойындардан бас тартқысы келетін адамдар үшін тітіркендіргіш болуы мүмкін, өйткені олар жарнамадан тыс қалмайды.

Көбінесе бонустар мен акциялар күрделі шарттармен бірге беріледі, оларды жаңа пайдаланушыларға түсіну қиын. Мысалы, бонус ақшасын алу үшін белгілі бір талаптарды

орындау қажет – белгілі мөлшерде ставка жасау немесе қосымша ақша енгізу сияқты. Бұл ойыншыларды платформада ұзағырақ ұстауға және жеңісті оңай алуға болады деген жалған әсер қалдыруға бағытталған.

Платформалар (TEMU және онлайн-казино) көбінесе мәжбүрлі жарнама мен деректерді пайдалануы үшін сынға ұшырайды. TEMU жағдайында пайдаланушылардың жеке деректерінің көп мөлшерде жиналуы жекелендірілген маркетинг үшін маңызды болғанымен, бұл қауіпсіздікке байланысты мәселелерді туындатуы мүмкін. Ал онлайн-казино көбінесе тәуелділік тудыратын шарттар мен жасырын комиссиялар үшін сыналады, бұл пайдаланушылардың қаржылық қауіпсіздігіне қауіп төндіреді.

Бұл маркетингтік стратегиялар бизнес тұрғысынан тиімді болғанымен, олардың ашықтығы мен қауіпсіздігіне қатысты сұрақтар туындайды. Себебі мұндай сервистерді елемеу ел экономикасына әсер етеді. Екі платформа да нақты реттеуге жатпайды, бұл өз кезегінде пайдаланушылардың тәуелді болуына әкеледі.

Кибершабуылдар ел экономикасына күрделі әрі көпқырлы әсер етеді, бұл жеке кәсіпорындарды ғана емес, тұтас салаларды, мемлекеттік құрылымдарды және инвестициялық климатты қамтиды. Міне, негізгі әсер ету бағыттары:

1. Тікелей экономикалық шығын

Кибершабуылдар ақша ұрлау, IT-инфрақұрылымның бұзылуы, өндірістік процестердің тоқтауы мен деректердің жоғалуына әкеледі. Бұл бизнес пен мемлекетке тікелей қаржылық шығын әкеледі – шабуыл ауқымына қарай бұл шығындар миллиондаған, тіпті миллиардтаған долларды құрауы мүмкін. Мысал ретінде 2017 жылы жаһандық бизнеске 10 миллиард доллардан астам зиян келтірген NotPetya вирусын атауға болады.

2. Сенім жоғалту мен беделге нұқсан келуі

Шабуылға ұшыраған компаниялар тұтынушылар, серіктестер және инвесторлардың сенімінен айырылады. Бұл акция құнының төмендеуіне, клиенттердің кетуіне және сатылым көлемінің қысқаруына әкелуі мүмкін. Ал мемлекет үшін – халықаралық беделдің төмендеуіне және ұлттық киберқауіпсіздікке деген сенімнің әлсіреуіне себеп болады.

3. Киберқауіпсіздікке шығындардың өсуі

Шабуылдардан кейін компаниялар мен мемлекеттік құрылымдар ақпараттық қауіпсіздік жүйелеріне, персоналды оқытуға және аудитке қомақты қаражат салуға мәжбүр болады. Бұл бизнестің және мемлекеттің шығын құрылымына әсер етеді.

4. Сындарлы инфрақұрылым жұмысының бұзылуы

Көлік, энергетика, банк жүйесі мен мемлекеттік органдарға жасалған шабуылдар өмірлік маңызды қызметтердің тоқтап қалуына әкелуі мүмкін. Бұл ұлттық қауіпсіздік пен экономикалық тұрақтылық үшін өте қауіпті.

5. Инвестициялардың төмендеуі және іскерлік ахуалдың нашарлауы

Ақпараттық қауіпсіздік саласындағы тәуекелдердің артуы инвесторларды, әсіресе жоғары технологиялық салаларда, қорқытуы мүмкін. Бұл шетелдік капитал ағынының азаюына және экономиканың цифрлық трансформациясының баяулауына әкеледі.

Осылайша, кибершабуылдар – бұл тек технологиялық қауіп қана емес, сонымен қатар елеулі экономикалық сын-қатер. Бұл жүйелі мемлекеттік және корпоративтік жауапты, сондай-ақ киберқауіпсіздік саласында белсенді халықаралық ынтымақтастықты талап етеді.

Казахстан экономикасына әсері: Кибершабуылдар Қазақстан экономикасына да айтарлықтай әсер етуде – бұл жеке компаниялармен қатар мемлекеттік құрылымдарға да зиян келтіреді. 2022 жылы елдегі әр онынші компания киберинциденттің салдарынан 2,5 млн теңгеге дейін, ал әр жиырмасыншы – 8 млн теңгеден астам шығынға ұшыраған. Мұндай оқиғалардан жалпы қаржылық шығын 65% ұйымды қамтыған, оның ішінде өндірістің тоқтауы, табыстың жоғалуы және инфрақұрылымды қалпына келтіру шығындары бар.

Ерекше осал салалар – мұнай-газ және құрылыс секторлары, мұнда кибершабуылдар ірі қаржылық шығындар мен өндірістік процестердің бұзылуына әкеліп соғады. Кей

жағдайларда шығын көлемі 8 млн теңгеден асып, компаниялардың қаржылық тұрақтылығына айтарлықтай әсер етеді.

Банк секторы да кибершабуылдардың өсуімен бетпе-бет келуде. 2023 жылы банк секторында 130-дан астам шабуыл тіркелген, бұл қолма-қол ақшасыз төлемдер көлемінің артуы мен интернет- және мобильді банкингтің кең қолданылуымен байланысты. Шабуылдардың көбеюі интернет-алаяқтық жағдайларының өсуімен қатар жүріп, қаржы операцияларының қауіпсіздігі мен клиенттердің сеніміне қауіп төндіреді [10].

Осылайша, кибершабуылдар Қазақстан экономикасына көпқырлы әсер етеді – қаржылық шығындарға, бизнес-процестердің бұзылуына және цифрлық сервистерге деген сенімнің төмендеуіне әкеледі. Мұндай тәуекелдерді азайту үшін киберқауіпсіздік шараларын күшейту, кадрларды оқыту және заманауи қорғаныс технологияларын енгізу қажет.

ҚОРЫТЫНДЫ.

Әлеуметтік желілердегі ақпараттық қауіпсіздік тек жекелеген брендтерге ғана емес, бүкіл елдің экономикалық дамуына да әсер етеді. Әсіресе ірі компаниялардағы деректердің таралуы ұлттық цифрлық инфрақұрылымға деген сенімді әлсіретіп, айтарлықтай экономикалық шығындарға әкелуі мүмкін. Егер ел сенімді ақпараттық қауіпсіздік шараларын қамтамасыз етпесе, бұл шетелдік инвестицияларды тартуға кедергі келтіріп, цифрлық экономиканың дамуын баяулатуы ықтимал.

Кибершабуылдар еңбек нарығына әсер етіп, бизнес үшін қосымша шығындар туындатады – компаниялар деректерді қорғауға, қызметкерлерді оқытуға және технологияларды жетілдіруге қаражат жұмсауға мәжбүр болады. Ақпараттық қауіпсіздікті белсенді қолдайтын елдер неғұрлым тұрақты экономикалық орта қалыптастырып, инвесторларды тартып, цифрлық брендтердің тәуекелсіз дамуына жол аша алады.

Пайдаланылған әдебиеттер тізімі:

1. Актуальные киберугрозы в странах СНГ 2023-2024. [Электронный ресурс]. – 2024. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-v-stranah-sng-2023-2024/#id6 (дата обращения: 06.11.2024).

2. Количество киберпреступлений в Казахстане. [Электронный ресурс]. – 2024. – URL: https://inbusiness.kz/ru/last/kolichestvo-kiberprestuplenij-v-kazahstane-vyroslo-v-10-raz (дата обращения: 06.11.2024).

3. Утечка данных компании Cambridge Analytica. [Электронный ресурс]. – 2020. – URL: https://www.interfax.ru/business/670301 (дата обращения: 06.11.2024).

4. Взлом Twitter-аккаунтов. [Электронный ресурс]. – 2020. – URL: https://www.bbc.com/russian/features-53453097 (дата обращения: 06.11.2024).

5. Передача данных пользователей TikTok. [Электронный ресурс]. – 2023. – URL: https://www.bbc.com/russian/news-64811551 (дата обращения: 06.11.2024).

6. Uber и уязвимость к кибератакам. [Электронный ресурс]. – 2021. – URL: https://www.pitsasinsurances.com/ru/article/a-decade-of-cyber-attacks/ (дата обращения: 06.11.2024).

7. Amazon использует секретные операции против конкурирующих компаний. [Электронный ресурс]. – 2024. – URL: http://surl.li/jxatia (дата обращения: 06.11.2024).

8. Zoom и его проблемы информационной безопасности. [Электронный ресурс]. – 2020. – URL: https://www.forbes.ru/tehnologii/413573-konec-epohi-zoom-kak-glavnyy-servis-pandemii-perezhivaet-obvineniya-v-utechke (дата обращения: 06.11.2024).

9. Расследование против Temu. [Электронный ресурс]. – 2024. – URL: https://informburo.kz/novosti/xotim-ctoby-tovary-ne-vredili-pokupatelyam-es-nacal-rassledovanie-protiv-temu (дата обращения: 06.11.2024).

10. Казахстан занял седьмое место в мире по количеству кибератак [Электронный ресурс]. – 2023. – URL: https://forbes.kz/articles/kaspersky_kazahstan_zanyal_sedmoe_mesto_v_mire_po_kolichestvu_kiberatak?utm_source=chatgpt.com (дата обращения: 06.05.2025).

References:

1. Aktual'nye kiberugrozy v stranakh SNG 2023-2024. [Elektronnyy resurs]. – 2024. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-v-stranah-sng-2023-2024/#id6 (data obrashcheniya: 06.11.2024).

2. Kolichestvo kiberprestupleniy v Kazakhstane. [Elektronnyy resurs]. – 2024. – URL: https://inbusiness.kz/ru/last/kolichestvo-kiberprestuplenij-v-kazahstane-vyroslo-v-10-raz (data obrashcheniya: 06.11.2024).

3. Utechka dannykh kompanii Cambridge Analytica. [Elektronnyy resurs]. – 2020. – URL: https://www.interfax.ru/business/670301 (data obrashcheniya: 06.11.2024).

4. Vzlom Twitter-akkauntov. [Elektronnyy resurs]. – 2020. – URL: https://www.bbc.com/russian/features-53453097 (data obrashcheniya: 06.11.2024).

5. Peredacha dannykh pol'zovateley TikTok. [Elektronnyy resurs]. – 2023. – URL: https://www.bbc.com/russian/news-64811551 (data obrashcheniya: 06.11.2024).

6. Uber i uiazvimost' k kiberatakam. [Elektronnyy resurs]. – 2021. – URL: https://www.pitsasinsurances.com/ru/article/a-decade-of-cyber-attacks/ (data obrashcheniya: 06.11.2024).

7. Amazon ispol'zuet sekretnye operatsii protiv konkuriruyushchikh kompaniy. [Elektronnyy resurs]. – 2024. – URL: http://surl.li/jxatia (data obrashcheniya: 06.11.2024).

8. Zoom i ego problemy informatsionnoy bezopasnosti. [Elektronnyy resurs]. – 2020. – URL: https://www.forbes.ru/tehnologii/413573-konec-epohi-zoom-kak-glavnyy-servis-pandemii-perezhivaet-obvineniya-v-utechke (data obrashcheniya: 06.11.2024).

9. Rassledovanie protiv Temu. [Elektronnyy resurs]. – 2024. – URL: https://informburo.kz/novosti/xotim-ctoby-tovary-ne-vredili-pokupatelyam-es-nacal-rassledovanie-protiv-temu (data obrashcheniya: 06.11.2024).

10. Kazakhstan zanyal sed'moe mesto v mire po kolichestvu kiberatak. [Elektronnyy resurs]. – 2023. – URL: https://forbes.kz/articles/kaspersky_kazahstan_zanyal_sedmoe_mesto_v_mire_po_kolichestvu_kiberatak?utm_source=chatgpt.com (data obrashcheniya: 06.05.2025).