ИНФОРМАТИКА

COMPUTER SCIENCE

ҒТАХР 33.29.00 12.31.00

10.51889/2959-5894.2025.89.1.012

С.А. Адилжанова[1], Г.А.Абдулкаримова[2], Ф.Р. Гусманова[1*], Г.Т. Жубанышева[1]

[1]Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы қ,, Қазақстан.
[2] Абай атындағы Қазақ ұлттық педагогикалық университеті, Алматы қ,, Қазақстан
[*]*e-mail: grfarida77@gmail.com*

АҚПАРАТТЫҚ ҚАУІПСІЗДІК САЛАСЫНДАҒЫ ТӘУЕКЕЛДЕРДІ ТАЛДАУ ЖӘНЕ БАСҚАРУ ҮШІН ПЛАТФОРМА ҚҰРУ

Аңдатпа

Бұл мақала цифрлық егіздер технологиясын қолдану кезінде туындайтын ақпараттық қауіпсіздік тәуекелдерін талдау және басқаруға арналған платформа әзірлеуге бағытталған. Зерттеу цифрлық егіздердің 4.0 Индустриясы шеңберіндегі рөлі мен маңызын, әсіресе өндіріс, энергетика, ақылды қалалар және киберфизикалық жүйелер салаларында қарастырады. Ақпараттық қауіпсіздікке қатысты тәуекелдер мен олардың себептері анықталып, оларды азайту жолдары ұсынылады. Прогностикалық талдау, жасанды интеллект, адаптивті қауіпсіздік жүйелері, криптографиялық технологиялар және блокчейн сияқты жаңашыл әдістер талқыланып, олар цифрлық егіздер платформаларының қауіпсіздігін арттыруға және ақпараттық қауіпсіздікті қамтамасыз етуге мүмкіндік береді. Бұл әдістер цифрлық егіздер жүйелерінің сенімділігін арттыру үшін маңызды құралдар, ал оларды интеграциялау платформалардың жұмысын тиімді әрі қауіпсіз етуге ықпал етеді. Осының нәтижесінде, цифрлық егіздер жүйелерінің қауіпсіздігін қамтамасыз ету арқылы оларды басқарудың тиімділігін арттыру, бизнес процестерді оңтайландыру және жаңа мүмкіндіктер ашу мақсатында қолданылады. Сонымен қатар, осы әдістер ақпараттық қауіпсіздік талаптарына сай болуын және цифрлық егіздер платформаларының ұзақ мерзімді тұрақтылығын қамтамасыз етеді.

Түйін сөздер: Индустрия 4.0; тәуекелдерді басқару; машина оқыту; прогностикалық талдау; криптографиялық технологиялар.

С. А. Адилжанова[1], Г. А.Абдулкаримова[2], Ф.Р. Гусманова[1], Г. Т. Жубанышева[1]
[1]Казахский национальный университет им. аль-Фараби, г.Алматы, Казахстан
[2]Казахский национальный педагогический университет имени Абая, г.Алматы, Казахстаны

СОЗДАНИЕ ПЛАТФОРМЫ ДЛЯ АНАЛИЗА И УПРАВЛЕНИЯ РИСКАМИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация

Статья посвящена разработке платформы для анализа и управления рисками информационной безопасности, возникающими при использовании технологии цифровых близнецов. В исследовании рассматривается роль и значение цифровых близнецов в Индустрии 4.0, особенно в таких областях, как производство, энергетика, умные города и киберфизические системы. Будут выявлены риски, связанные с информационной безопасностью, и их причины, а также предложены способы их снижения. Обсуждаются новаторские методы, такие как прогностический анализ, искусственный интеллект, адаптивные системы безопасности, криптографические технологии и блокчейн, которые позволят повысить безопасность платформ цифровых близнецов и обеспечить информационную безопасность. Эти методы являются важными инструментами для повышения надежности цифровых систем близнецов, а их интеграция способствует повышению эффективности и безопасности работы

платформ. В результате этого цифровые близнецы используются с целью повышения эффективности управления системами за счет обеспечения их безопасности, оптимизации бизнес-процессов и открытия новых возможностей. Кроме того, эти методы обеспечивают соответствие требованиям информационной безопасности и долгосрочную стабильность платформ цифровых двойников.

Ключевые слова: Индустрия 4.0; управление рисками; машина обучение; прогностический анализ; криптографические технологии.

S.A. Adilzhanova[1], G.A. Abdulkarimova[2], F.R. Gusmanova[1], G.T. Zhubanysheva[1]
[1]Al-Farabi Kazakh National University, Almaty, Kazakhstan
[2]Abai Kazakh National Pedagogical University, Almaty, Kazakhstan

CREATION OF A PLATFORM FOR INFORMATION SECURITY RISK ANALYSIS AND MANAGEMENT

Abstract

This article is devoted to the development of a platform for the analysis and management of information security risks arising from the use of digital twin technology. The study examines the role and importance of digital twins in Industry 4.0, especially in areas such as manufacturing, energy, smart cities, and cyber-physical systems. The risks associated with information security and their causes will be identified, as well as ways to reduce them. Innovative methods such as predictive analysis, artificial intelligence, adaptive security systems, cryptographic technologies and blockchain are being discussed, which will enhance the security of digital twin platforms and ensure information security. These methods are important tools for improving the reliability of Gemini digital systems, and their integration contributes to improving the efficiency and security of the platforms. As a result, digital twins are used to improve the efficiency of system management by ensuring their security, optimizing business processes and opening up new opportunities. In addition, these methods ensure compliance with information security requirements and long-term stability of digital twin platforms.

Keywords: Industry 4.0; risk management; machine learning; predictive analysis; cryptographic technologies.

Негізгі ережелер

Зерттеу 4.0 индустриясының негізгі рөлін ескере отырып, цифрлық егіздердің ақпараттық қауіпсіздігі саласындағы тәуекелдерді талдау және басқару платформасын әзірлеудің маңыздылығын көрсетеді. Цифрлық егіздер деректерге шабуыл, желілік инфрақұрылымның осалдығы және құпия ақпараттың ағуы сияқты киберқауіптерге бейім. Құрылатын платформа нақты уақыт режимінде деректер мен жүйелерді қорғауды қамтамасыз ететін тәуекелдерді анықтау, талдау және азайту құралдарын ұсыну үшін қандай әдістерді қолдану керектігі қарастырылған. Зерттеудің негізгі қорытындысы-цифрлық егіздерді қолданудағы сенімділікті арттыру және өндіріс процестеріндегі ақауларды болдырмау үшін жасанды интеллект технологиялары мен үлкен деректерді біріктіру қажеттілігі.

Кіріспе

Ақпараттық қауіпсіздік қазіргі қоғамда және экономикада маңызды рөл атқарады. Жаһандану мен цифрландыру процесі ақпараттың құндылығын арттырып қана қоймай, оған қатысты қауіптер мен тәуекелдерді де күшейтеді. Ақпараттық жүйелер мен деректердің қорғалуы ұйымдар мен мемлекеттер үшін стратегиялық маңызға ие бола отырып, оларды түрлі кибершабуылдар мен қауіптерден қорғау қажеттілігі туындайды. Бұл тұрғыда ақпараттық қауіпсіздіктің тәуекелдерін талдау және басқару жүйелерінің тиімділігі артқан сайын, жаңа платформалар мен технологияларды қолдану маңыздылығы да арта түсуде.

Бұл жұмыста «Индустрия 4.0» шеңберіне аса назар аударып, цифрлық егіздер платформаларындағы ақпараттық қауіпсіздік тәуекелдерінің негізгі түрлері, олардың туындау себептері мен ықтимал шешімдері қарастырылады. Сонымен қатар, тәуекелдерді азайту үшін жаңа технологиялық шешімдер, оның ішінде жасанды интеллект, криптография және блокчейн технологияларын қолдану тәсілдері ұсынылады. *Цифрлық егіздер: тәуекелдер мен қауіпсіздік.* Цифрлық егіздер технологиясы «Индустрия 4.0» шеңберінде өндіріс процесін

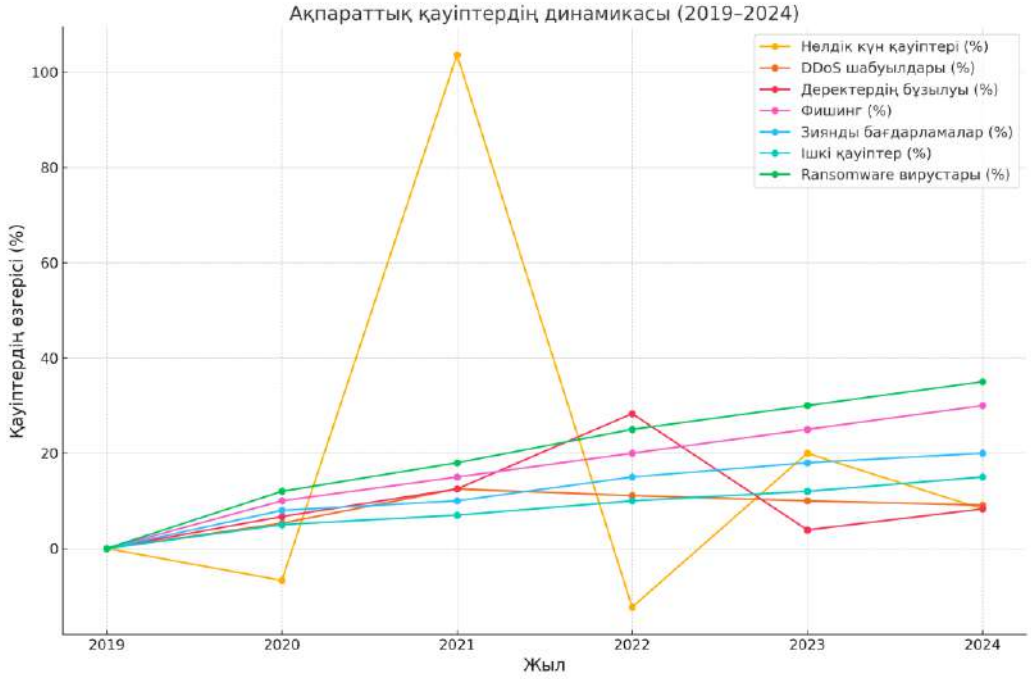
автоматтандыру және тиімділікті арттыруда маңызды рөл атқарады. Бірақ бұл технологияны қолдану ақпараттық қауіпсіздікке байланысты жаңа тәуекелдерді тудырады. Қауіптер цифрлық егіздер жүйесінің күрделілігіне, киберфизикалық жүйелер арасындағы өзара байланыстың артуына және ақпарат алмасу процестеріне негізделеді [1]. Деректер қауіпсіздігі мәселелерін қарастыруымызға болады. Цифрлық егіздер платформаларының мәлімет алмасу функциялары олардың қауіпсіздігіне тәуелді. Индустрия 4.0 цифрлық және физикалық әлемдер арасындағы алшақтыққа көпір салу үшін цифрлық егіздер технологиясына сүйенеді [2]. Рұқсатсыз қолжетімділік, деректердің ұрлануы немесе бұрмалануы сияқты қауіптер өндіріс процесінің бұзылуына алып келеді. Мысалы, өндірістік жабдықтың жағдайы туралы жалған мәліметтер енгізу жүйенің сенімділігін төмендетіп, дұрыс емес шешімдер қабылдануына ықпал етуі мүмкін. Мұндай жағдайлар өнімділіктің төмендеуіне және қаржылық шығындарға алып келеді [3]. Сонымен қатар цифрлық егіздер серверлерге бағытталған кибершабуылдар олардың тұрақтылығын төмендетіп, өндірістік процестердің үзілуіне әкелуі мүмкін. Мысалы, DDoS шабуылдары сервердің жұмысын шектесе, ал ransomware шабуылдары мәліметтерге қолжетімділікті толығымен шектеуі мүмкін [4] Мұндай жағдайлар компанияның өндірістік процестерін тоқтатып, айтарлықтай шығындар әкеледі. Ал бағдарламалық қамтамасыз ету осалдықтарына келетін болсақ, цифрлық егіздер күрделі бағдарламалық қамтамасыз ету жүйелеріне негізделгендіктен, жүйедегі осалдықтар зиянды бағдарламаларды енгізу немесе платформаның жұмысына кедергі келтіру қаупін арттырады. Бұл осалдықтар ақпараттық қауіпсіздік саясатына да кері әсерін тигізеді. Қателерді жою және қауіпсіздікті арттыру мақсатында тұрақты жаңартулар мен жүйелі тексерістер қажет болады [5].

Желілік инфрақұрылым тәуекелдерінде қарастырып өткеніміз жөн, себебі цифрлық егіздер желілік инфрақұрылымдарға тәуелді болғандықтан, желідегі осалдықтар жалпы жүйеге теріс әсер етуі мүмкін. IoT құрылғыларының қорғалмағандығы, әсіресе, бұл құрылғыларды кибершабуылдарға осал етеді [6].

Адам факторына байланысты қауіптер де кеңінен таралған. Цифрлық егіздерді басқару кезінде адам тарапынан жіберілетін қателіктер тәуекелдерді арттырады. Қате конфигурациялау, қауіпсіздік хаттамаларын сақтамау немесе құпия ақпараттың жариялануы жүйенің бұзылуына алып келуі мүмкін. Мұндай мәселелер жүйені пайдаланушылардың ақпараттық қауіпсіздік мәдениетінің жеткіліксіздігінен туындайды [7]. Сондықтан да қызметкерлерді оқыту басты міндет.

Осылайша цифрлық егіздер технологиясының қауіпсіздігі мен тиімділігі олардың ақпараттық қауіпсіздік тәуекелдеріне төтеп беру қабілетіне байланысты. Қауіптерді азайту үшін деректерді шифрлау, көпфакторлы аутентификацияны енгізу, қауіпсіздік хаттамаларын жүйелі түрде жаңарту және тұрақты мониторинг жүйелерін қолдану қажет [8]. Бұл шаралар цифрлық егіздер жүйесінің сенімділігін арттырып, «Индустрия 4.0» шеңберіндегі инновациялардың қарқынды дамуына ықпал етеді. Төмендегі деректер әлемдік киберқауіпсіздік талдауларына негізделген, оның ішінде Kaspersky lab және Cybersecurity Ventures секілді зерттеулеріннен алынған (1-сурет).

2021 жылы Нөлдік күн қауіптері өте көп таралуының себептері кейбір компаниялар мен ұйымдар бағдарламалық жасақтамаларды және жүйелерді жаңартуды кешіктіріп немесе елемей, осалдықтарды түзетпей қалдыруы, ақпараттық жүйелер мен желілердің күрделенуі, әсіресе қашықтан жұмыс істеу және бұлтты қызметтерге тәуелділік жоғарылағандықтан, осалдықтар мен қауіптердің көбейюіне ықпал етті [9]. Сонымен қатар осы жылдары бұл қауіп түрін шабуылдаушылар көбірек пайдаланып, нарыққа шығаруды және оны басқа қылмыскерлерге сатуды үйренді. DDoS шабуылдары, фишинг, деректердің бұзылуы кеңінен таралған, олар серверлерді немесе желілерді шамадан тыс жүктеу арқылы олардың жұмысының тоқтауына себеп болу арқылы, қолданушыларды алдау арқылы құпия ақпаратты (парольдер, банктік деректер) алу әрекеті, құпия деректердің рұқсатсыз жария етілуі немесе ұрлануы арқылы болатын шабуылдар [10].



Сурет 1. Ақпараттық қауіпсіздік саласындағы қауіптердің тенденциялары

Қазіргі таңда бұл қауіптер туралы ақпараттарды толыққанды біліп, әрдайым біліміміздіжаңартуымыз керек. Цифрлық егіздер мен физикалық жүйелер арасындағы өзара байланыс олардың қауіпсіздігін күрделендіреді. Мысалы, цифрлық егіздердің көмегімен басқарылатын өндірістік процеске бағытталған шабуыл тек ақпараттық қауіпсіздікті бұзып қана қоймай, физикалық өндіріс процесін де тоқтата алады. Бұл индустриалды инфрақұрылымға, энергия жүйелеріне немесе көлік саласына да қауіп тудыруы мүмкін. Цифрлық егіздер мен олардың ақпараттық қауіпсіздігі арасында маңызды байланыс бар. Бұл жүйелердің қауіпсіздігі тек виртуалды әлемде ғана емес, физикалық объектілер мен процестерге де әсер етеді[11]. Осыған байланысты, сыртқы және ішкі шабуылдар, қызметкерлердің қателіктері және жеткізушілермен байланыстардағы осалдықтар цифрлық егіздер жүйесін бұзу немесе тоқтату мақсатында қолданылуы мүмкін[12]. Осы қауіптерді басқару үшін ақпараттық қауіпсіздік шараларын қатаң сақтап, жүйелерді үздіксіз қадағалап отыру қажет.

Цифрлық егіздер негізінде платформа құру әдістері. Ақпараттық қауіпсіздік тәуекелдерін басқару платформасын дамыту «Индустрия 4.0» талаптарына жауап беруі және цифрлық егіздер технологиясының күрделілігін ескеруі тиіс [13]. Менің зерттеуімнің нәтижесінде бірнеше талдау тәсілдерін қарастырсақ болады. Төмендегі мен ұсынған тәсілдер платформаның қауіпсіздігін күшейтіп, оны заманауи сын-қатерлерге бейімдейді.

1. Болжаулық талдау және жасанды интеллект негізіндегі мониторинг. Кәдімгі мониторинг жүйелері нақты уақыттағы аномалияларды анықтауға бағытталған болса, прогностикалық талдау жүйесі болашақта туындауы мүмкін қауіптерді алдын ала болжауға мүмкіндік береді. Жасанды интеллект алгоритмдерін пайдалану арқылы платформаның қауіпсіздік деңгейін арттыруға болады. Мысалы, Machine Learning технологиясы пайдаланушылардың әрекет үлгілерін үйреніп, күдікті әрекеттерді ерте кезеңде анықтайды [14]. Бұл тәсілдер тәуекелдерді басқаруда проактивті әдістерді қолдануға жол ашады.

2. Киберқатерлерді автоматты түрде нейтрализациялау. Цифрлық егіздер платформалары үшін кибершабуылдарды автоматты түрде анықтап, блоктайтын жүйелерді дамыту қажет. Бұл жүйелер шабуылдың типін жылдам анықтап, оны дер кезінде тоқтата алады. Мысалы, арнайы алгоритмдер honeypot технологияларын пайдаланып, кибершабуылдаушыларды жалған

жүйеге бағыттайды және олардың әрекеттерін зерттейді [15]. Бұл ақпарат болашақ шабуылдарға дайындалуға көмектеседі.

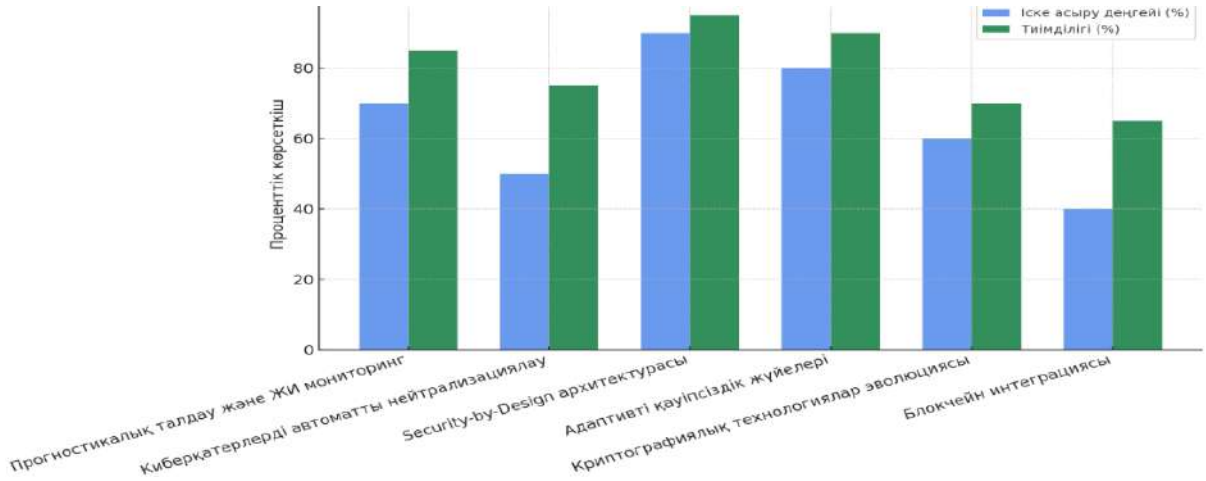
3. Қауіпсіздікке негізделген архитектуралық дизайн. Цифрлық егіздер платформаларының дизайны ақпараттық қауіпсіздік талаптарына толықтай сәйкес болуы керек. Бұл ретте Security by Design қағидасын қолдану ұсынылады. Бұл тәсіл платформаны жобалау кезеңінен бастап барлық қауіпсіздік аспектілерін ескере отырып жасалуды көздейді[16]. Платформаның әрбір модулі деректер шифрлау, аутентификация және желі қауіпсіздігі тұрғысынан тәуелсіз қорғаныс деңгейіне ие болуы тиіс.

4. Бейімделгіш қауіпсіздік жүйесі. Қауіпсіздік қатерлерінің өзгеруіне икемделе алатын адаптивті жүйелер цифрлық егіздер платформалары үшін ерекше маңызды. Бұл жүйелер динамикалық конфигурациялау арқылы нақты уақытта жаңа қауіптерге бейімделіп, өз жұмысын тиімді жалғастырады. Мысалы, бұлттық есептеулер негізінде жұмыс істейтін адаптивті жүйелер әртүрлі деңгейдегі шабуылдарға қарсы қосымша ресурстарды жылдам іске қосады [17].

5. Криптографиялық технологиялардың эволюциясы. Қазіргі шифрлау әдістері жеткілікті деңгейде тиімді болғанымен, кванттық есептеу технологияларының дамуымен олардың әлсіреуі ықтимал. Осыған байланысты, цифрлық егіздер платформаларын қорғау үшін квантқа төзімді криптография әдістерін енгізу маңызды. Бұл әдістер деректерді болашақта мүмкін болатын кванттық шабуылдардан қорғауды қамтамасыз етеді [18].

6. Блокчейн технологиясын интеграциялау. Деректердің тұтастығын сақтау және оның заңсыз өзгертілуіне жол бермеу үшін цифрлық егіздер платформаларында блокчейн технологиясын қолдану ұсынылады. Блокчейн әрбір мәліметтің өзгерісін қадағалап, деректердің қайталанбас және сенімді сақталуын қамтамасыз етеді [19]. Бұл тәсіл әсіресе желілік инфрақұрылым тәуекелдерін азайтуға көмектеседі. Осы келтірілген әдістерімнің деңгейін төменгі сызбадан көре аласыздар (Сурет 2).

Цифрлық қауіпсіздік шараларының тиімділік диаграммасы



Сурет 2. Әдістеріге талдау

Көріп отырғанымыздай:

- Прогностикалық талдау және ЖИ мониторингі жоғары тиімділігі (85%) және едәуір кең қолданылуы (70%) арқылы қауіпсіздікті болжауда маңызды рөл атқарады.

- Киберқатерлерді автоматты нейтрализациялаудың тиімділігі 75%, бірақ іске асыру деңгейі 50%, себебі оның жүзеге асырылуы үшін күрделі технологиялар қажет.

- Security-by-Design архитектурасының тиімділігі 95%, бұл оны ең сенімді әдістердің бірі етеді.

- Адаптивті қауіпсіздік жүйелері 90% тиімділік және 80% іске асыру көрсеткіші бұл тәсілдің

кеңінен қолданылатынын көрсетеді.

- Криптографиялық технологиялар эволюциясының тиімділігі 70%, ол деректердің қауіпсіздігін жақсарту үшін қажет.

- Блокчейн интеграциясы 65% тиімділік және 40% іске асыру деңгейі оның әлі де дамуды қажет ететінін көрсетеді.

Жаңа технологиялық тәсілдерді енгізу цифрлық егіздер платформаларының қауіпсіздігін арттырып, тәуекелдерді басқару тиімділігін күшейтеді. Жоғарыда ұсынылған әдістер «Индустрия 4.0» талаптарына сәйкес келетін сенімді жүйелерді дамытуға бағытталған. Цифрлық егіздер экожүйесінің күрделілігін ескере отырып, әрбір компоненттің қауіпсіздігіне ерекше көңіл бөлу маңызды. Ғылыми зерттеулер мен тәжірибелік сынақтарды жалғастыру бұл бағытта үздік шешімдерді табуға ықпал етеді.

Зерттеу әдіснамасы

4.0 индустриясындағы цифрлық егіздердің ақпараттық қауіпсіздігі саласындағы тәуекелдерді талдау және басқару платформасын әзірлеуді зерттеу әдістемесі қолданыстағы шешімдерді талдауды, негізгі қауіптер мен осалдықтарды анықтауды және машиналық оқытуды қолдана отырып тәуекелдерді бағалау моделін құруды қамтиды. Зерттеу кезеңдері талаптарды жинауды, алгоритмдерді әзірлеуді, бар жүйелермен интеграциялауды және нақты деректерді тексеруді қамтиды. Қауіпсіздіктің жоғары деңгейін қамтамасыз ететін цифрлық егіздер жағдайында тәуекелдерді бақылау мен басқарудың тиімді жүйесін құру күтілуде.

Зерттеу нәтижелері

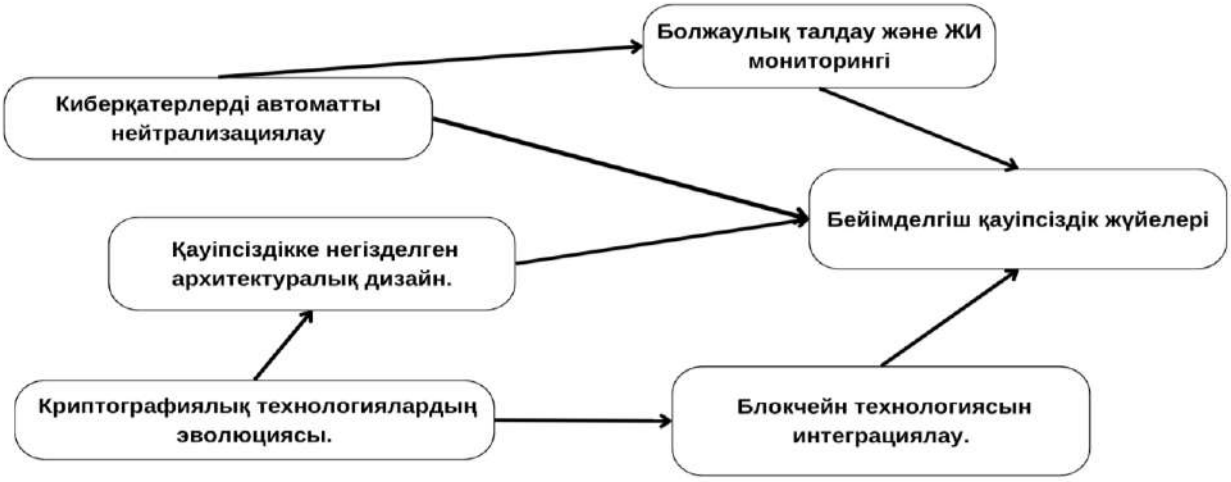
Цифрлық егіздерге тікелей қатысты киберқауіптерді автоматты нейтрализациялау әдісі толықтыруларды қажет етеді, себебі оған қосымша шараларды қоса енгізу керек. Мысалы, қауіптерді автоматты түрде нейтрализациялау үшін ЖИ мен машиналық оқытуды қолдана отырып, шабуылдарды алдын ала болжауға және әрекет етуге арналған алгоритмдерді дамыту арқылы, жиі кездесетін шабуыл түрлерін анықтау үшін нейрондық желілер мен шешімдер ағаштарын қолдануға болады, яғни бұл әдісті іске асыру үшін шабуылдарды алдын ала болжау аса маңызды. Дәл солай, қауіптерді ерте кезеңде анықтау үшін жүйенің барлық әрекеттерін бақылау және деректерді талдау үшін нақты уақыттағы мониторинг жүйесін құру жүйе шабуылдардың ерекше белгілерін анықтап, оларды автоматты түрде белгілей алады. Қауіпсіздік бейімделгіш және инфрақұрылымды қорғаудыңбасқа әдістерің қамтуы керек [20]. Қауіптерді нейтрализациялау үшін инциденттерді басқару жүйесі де маңызды рөл атқарады. Ал қауіптер анықталғаннан кейін олардың ауқымын бағалау және оларды басқару үшін инциденттерді тіркеу мен олардың деректерін сақтау керек, осылайша бұл шаралар шабуылдың таралуын болдырмауға көмектеседі. Жасанды интеллект, мониторинг, автоматты қорғаныс, жүйенің бейімделуі және қауіпсіздік шараларын жаңарту осы әдістердің тиімділігін арттыруға және қауіптерге жедел жауап беруге мүмкіндік береді. Бұл ұсынылған әдістер өзара байланысты және киберқауіпсіздік жүйесінде әртүрлі аспектілерді қамтып, жүйенің үздіксіз дұрыс жұмыс істеуіне көмектеседі сурет 3. Егер әдістердің бәрін бір тұтас математикалық модель ретінде қарастыратын болсақ, жасанды интеллект және болжаулық талдау әдістері арқылы жүйе болашақтағы қауіп-қатерлерді анықтауға көмектеседі.

Мұнда қауіп-қатердің ықтималдығын P функциясы арқылы есептеу жүргізіледі:

$$P(C) = \int(M, AI) \tag{1}$$

Мұндағы:

- C – қауіп-қатердің түрі,
- M – мониторинг жүйесі,
- AI – жасанды интеллект, деректерді өңдеу және болжау.



Сурет 3. Әдістердің өзара байланысы

Ықтималдылықты анықтауда қолданылатын шарттар:

- AI жүйесі тарихи зерттелген деректерге қарап болжау жасауы керек;
- M мониторинг жүйесі нақты уақыттағы деректерді жинап, жаңа шабуылдарды анықтауы тиіс;
- Қауіп-қатердің ықтималдылығы жүйе параметрлерінің статистикалық талдауына негізделеді.

Қауіп-қатер анықталған соң, автоматты түрде нейтрализациялау шаралары іске асады. Бұл нейтрализациялау шаралары:

$$N(C) = g(P, A, K) \tag{2}$$

Мұндағы:

- P – болжау нәтижелері, қауіп-қатердің табылған ықтималдылығы,
- N – автоматты нейтрализациялау,
- A – бейімделгіш қауіпсіздік жүйесі, табылған қауіп-қатерге жауап беріп, әрекеттерді бірден түзетеді,
- K – криптографиялық қорғау әдістері, деректердің құпиялылығын сақтайды.

Жүйе сыртқы немесе ішкі өзгерістерге бейімделеді(A), жаңа қауіп-қатерлерге қарсы тұру үшін параметрлерін өзгертіп отырады:

$$A = h(C, P, N) \tag{3}$$

Мұндағы:

- C – нақты қауіп-қатерлер,
- P – болжау нәтижелері,
- N – нейтрализациялау әрекеттері.

Қауіпсіздік негізінде жүйе құрылымын жобалау(D). Қауіпсіздік деңгейін анықтайтын әрбір жүйе компоненті үшін жалпы архитектуралық модель келесідей болады:

$$D = \sum_{i=1}^{n} s_i \tag{4}$$

Мұндағы:

- si – әрбір жүйе компонентінің қауіпсіздік деңгейі,
- n – жүйе компоненттерінің саны.

Қауіпсіздік деңгейін анықтаған уақыттағы қаралатын шарттар:

- Жүйелік талаптар мен стандарттар (ISO/IEC 27001, NIST, COBIT, CIS Controls және т.б.);

- Тәуекелдерді сканерлеу, осалдылықтарды табу (Nessus, OpenVAS, Qualys)
- Тәуекелдер матрицасын, ықтималдылық пен әсер деңгейін баға (төмен, орташа, ауыр).

Қауіпсіздік аудиттері мен тестілеу нәтижелерін саралау.

Құпия деректерді қорғау(K) және қауіпсіздікті қамтамасыз ету үшін криптографиялық әдістерді қолдану:

$$K = \sum_{i=1}^{m} k_i \quad (5)$$

Мұндағы:

- ki – криптографиялық әдістердің әрбір элементі,
- m – криптографиялық әдістер саны.

Криптографиялық әдістер үшін жүйенің қауіпсіздігін арттыру мақсатында параметрлерін таңдау керек, олар:

- Шифрлау алгоритмінің түрлерін қолдану(симметриялық, асимметриялық шифрлау);
- Мәліметтердің тұтастығы үшін хэш-функциялары(SHA-256, SHA-3, BLAKE2);
- Қауіпсіздік кілттерін басқару және сақтау;
- Аутентификация және шифрлау интеграциясы;
- Протоколдарды таңдау және т.б.

Барлық әдістердің өзара байланысын және жүйенің жұмысын сипаттайтын жалпы формула:

$$S = P(C) + N(C) + A + D + K \quad (6)$$

Бұл жерде:

- S – жалпы қауіпсіздік деңгейі,
- P(C) – қауіп-қатерлерді болжау,
- N(C) – нейтрализациялау шаралары,
- AA – бейімделгіш қауіпсіздік жүйесі,
- DD – архитектуралық дизайн,
- KK – криптографиялық қорғау әдістері.

Бұдан түсінетініміз әр әдістің өзіндік міндеттері бар. Қауіп-қатерлердің ықтималдығын болжау арқылы, қауіптің алдын алу үшін тиісті шаралар қолдануға мүмкіндік берсе, жүйенің алдын ала анықталған қауіп-қатерлеріне жауап беруін автоматтандыруды қамтамасыз етеді. Ал бейімделгіш қауіпсіздік жүйесі қауіп-қатерлерге қарсы жүйенің динамикалық түрде жауап беріп, архитектуралық дизайн қауіпсіздік деңгейін әрбір жүйе компонентінің қауіпсіздігіне қарай анықтайды. Кейін криптографиялық әдістердің көмегімен деректердің қауіпсіздігін қамтамасыз етеді. Платформа құру кезінде әдістердің өзара үйлесімді, әрі көп болғаны қауіпсіздік деңгейін арттырады.

Дискуссия

4.0 индустриясындағы цифрлық егіздердің ақпараттық қауіпсіздігін талдау және басқару платформасын дамыту өте маңызды, себебі ол өнеркәсіптік экожүйеде өзара байланысатын маңызды деректер мен жүйелерді бақылау және қорғаудың тиімді құралы. Бұл даму нәтижелері тәуекелдерді болжау және алдын алу үшін заманауи әдістерді, мысалы, машиналық оқыту және үлкен деректерді өңдеу технологияларын біріктірудің маңыздылығын көрсетеді. Сонымен қатар, 4.0 индустриясы жағдайында қауіпсіздікті қамтамасыз ету үшін бейімделген және интеллектуалды тәуекелдерді басқару жүйелерін енгізу қажеттілігін білдіретін басқа зерттеулермен үйлеседі. Мысалы, IoT жүйелері мен цифрлық егіздердің қауіпсіздігін зерттеу нақты уақыттағы қауіптерге икемді жауап беру қажеттілігіне баса назар аударады. Тәуекелдерді болжау модельдерінің дәлдігін арттыруға, қауіптерді басқарудың адаптивті әдістерін әзірлеуге және жаңа қауіптерді зерттеуге бағытталған зерттеулерге жол ашылады, себебі технология дамып, цифрлық егіздердің қолданылу ауқымы кеңейеді. Бұл сондай-ақ платформаның пайдаланушыларымен тиімдірек байланыс орнату үшін интерфейстерді жетілдіру мен әртүрлі өнеркәсіптік жүйелермен интеграция мүмкіндіктерін жақсартуды қамтуы мүмкін.

Қорытынды

Ақпараттық қауіпсіздік саласындағы тәуекелдерді талдау және басқару үшін платформалар құру мәселесі қазіргі заманғы цифрлық трансформацияның маңызды құрамдас бөлігіне айналып отыр. Киберфизикалық жүйелердің күрделілігі мен өзара байланысының артуы, ақпараттық алмасудың тәуелділігінен туындайтын жаңа қауіптер, өндірістік процестердің үздіксіздігі мен ұйымдардың тұрақтылығына қауіп төндіреді.

Қауіпсіздікті басқару және тәуекелдерді азайту үшін цифрлық егіздер платформаларына тиімді қорғаныс механизмдерін енгізу қажеттілігі туындайды. Қазіргі таңда болжаулық талдау, жасанды интеллект, кибершабуылдарды автоматты түрде нейтрализациялау, қауіпсіздікке негізделген архитектуралық дизайн және бейімделгіш қауіпсіздік жүйелерін қолдану платформаның қауіпсіздігін арттыруға мүмкіндік береді. Сонымен қатар, криптографиялық технологиялар мен блокчейн секілді әдістер деректердің тұтастығын сақтауда маңызды рөл атқарады.

Зерттеу нәтижелері көрсеткендей, осы әдістердің үйлесімді біріктірілуі қауіпсіздік деңгейін жоғары деңгейде қамтамасыз етіп, цифрлық егіздер экожүйесінің сенімділігін арттырады. Әрбір компоненттің қауіпсіздігіне мұқият көңіл бөлу, жүйелі мониторинг жүргізу және жаңа қауіптерге икемді жауап беру жүйелерін дамыту арқылы ақпараттық қауіпсіздік басқару тиімділігін арттыруға болады. «Индустрия 4.0» талаптарына сәйкес цифрлық егіздер платформаларын құру кезінде осы әдістердің толық жүзеге асырылуы өндірістік процестердің тұрақтылығын сақтауға және болашақтағы киберқатерлерге қарсы тұруға мүмкіндік береді.

Қорытындылай келе, цифрлық егіздер платформаларының қауіпсіздігі мен тәуекелдерді басқару мәселелерінің тиімді шешімі индустрияның инновациялық дамуына маңызды үлес қосады. Бұл технологиялар индустрияның тиімділігін арттыруға бағытталған маңызды қадам. Алайда, жаңа ғылыми зерттеулер мен технологиялық әзірлемелердің жалғасы қажет, себебі цифрлық егіздер экожүйесі күрделі әрі үздіксіз дамып келе жатқан сала.

Пайдаланылған дереккөздердің тізімі

[1] Carol Lo, Thu Yein Win, Zeinab Rezaeifar, Zaheer Khan, Phil Legg. "Digital Twins in Industry 4.0 Cyber Security." 2023 IEEE Smart World Congress (SWC)|979-8-3503-1980-4/23/ DOI: 10.1109/SWC57546.2023.10449147

[2] Harshpreet Kaur, Munish Bhatia. "Scientometric Analysis Of Digital Twin in Industry 4.0.": DOI 10.1109/JIOT.2024.3459965.

[3] Banglie Yang, Linyu Zhu, Cheng Dai, Sahil Garg, Georges Kaddoum. "An Improved Reconstruction Based Multi-Attribute Contrastive Learning for Digital Twin-Enabled Industrial System." DOI 10.1109/JIOT.2024.3483038.*

[4] Katrina Groth, Dongfeng Zhu, Ali Mosleh. "Hybrid Methodology and Software Platform for Probabilistic Risk Assessment." 1-4244-1461-X/08/$25.00 ©2008 IEEE

[5] Ioannis Semertzis, Vetrivel Subramaniam Rajkumar, Alexandru Ştefanov, Frank Fransen, Peter Palensky. "Quantitative Risk Assessment of Cyber Attacks on Cyber-Physical Systems using Attack Graphs." 2022 10th Workshop on Modelling and Simulation of Cyber-Physical Energy Systems (MSCPES). DOI: 10.1109/MSCPES55116.2022.9770140

[6] Yuan Peng, Kaixing Huang, Weixun Tu, Chunjie Zhou. "A Model-Data Integrated Cyber Security Risk Assessment Method for Industrial Control Systems." 2018 IEEE 7th Data Driven Control and Learning Systems Conference May 25-27, 2018, Enshi, Hubei Province, China

[7] Cheng Zeng, Shaosheng Fan, Dongqi Liu. "Modeling and Risk Assessment of Cyber Attacks in Distribution Grid Cyber-Physical Systems." 2023 5th International Conference on Electrical Engineering and Control Technologies (CEECT)|979-8-3503-4225-3/23/$31.00 ©2023 IEEE | DOI: 10.1109/CEECT59667.2023.10420626

[8] Yangxin Teng, Mingxuan Li, Ling He,Feng Li ,Tao Chen,Jia Chen,Xu Wang. "Algorithm for Quickly Improving Quantitative Analysis of Risk Assessment of Large-Scale Enterprise Information Systems." 2020 IEEE 4th Information Technology, Networking,Electronic and Automation Control Conference (ITNEC 2020). 978-1-7281-4390-3/20

[9] Igli TASHI, Solange GHERNOUTI-HÉLIE. "Information Security Management is Not Only Risk Management." 2009 Fourth International Conference on Internet Monitoring and Protection. DOI 10.1109/ICIMP.2009.31

[10] Craig Rieger, Constantinos Kolias, Robert C. Ivans. "Trade-off Analysis of Operational Technologies to Advance Cyber Resilience through Automated and Autonomous Response to Threats." 2022 Resilience Week (RWS) | 978-1-6654-8819-8/22/$31.00 ©2022 IEEE | DOI: 10.1109/RWS55399.2022.9984031

[11] Sani M. Abdullahi, Sanja Lazarova-Molnar. "Toward a Unified Security Framework for Digital Twin Architectures." 2024 IEEE International Conference on Cyber Security and Resilience (CSR)| DOI: 10.1109/CSR61664.2024.10679442

[12] Cheng Qian , Xing Liu , Colin Ripley , Mian Qian , Fan Liang and Wei Yu, "Digital Twin—Cyber Replica of Physical Things: Architecture, Applications and Future Research Directions." Future Internet 2022, 14, 64. https://doi.org/10.3390/fi14020064

[13] A.S.Ahmed, S.KURNAZ. "Internet of Things: Security Threats and Proposed Solutions." 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications. DOI: 10.1109/HORA55278.2022.9800048

[14] J.J. FUERTES, M.Á. PRADA, J.R. RODRÍGUEZ-OSSORIO, R. GONZÁLEZ-HERBÓN, D. PÉREZ, AND M. DOMÍNGUEZ, "Environment for Education on Industry 4.0." Received September 15, 2021, accepted October 1, 2021, date of publication October 15, 2021, date of current version October 28, 2021. DOI 10.1109/ACCESS.2021.3120517

[15] F.Akbarian, E.Fitzgerald, M.Kihl. "Intrusion Detection in Digital Twins for Industrial Control Systems."

[16] D.Holmes, M. Papathanasaki, L.Maglaras, M.A.Ferrag, "Digital Twins and Cyber Security – Solution or Challenge?." 2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM. DOI: 10.1109/SEEDA-CECNSM53056.2021.9566277

[17] A.Alqudhaibi, M.Albarrak, S.Jagtapa, N.Williams, K.Salonitis. "Securing Industry 4.0: Assessing Cybersecurity Challenges and Proposing Strategies for Manufacturing Management." https://doi.org/10.1016/j.csa.2024.100067

[18] A.Palma, A.Sorrentino, S.Bonomi. "How to Assess Measurement Capabilities of a Security Monitoring Infrastructure and Plan Investment Through a Graph-Based Approach." https://doi.org/10.1016/j.eswa.2024.125623

[19] S.Toliupa, I.Parkhomenko, H.Shvedova "Security and Regulatory Aspects of the Critical Infrastructure Objects Functioning and Cyberpower Level Assessment."978-1-7281-2399-8/19/$31.00 ©2019 IEEE

[20] W.Hurst, M.Merabti, P.Fergus «Operational Support for Critical Infrastructure Security.» DOI 10.1109/HPCC.2012.215