ИНФОРМАТИКА

COMPUTER SCIENCE

ҒТАХР 20.19.21

10.51889/2959-5894.2025.90.2.014

С.А. Адилжанова[1], А.Е. Рахыш[1*], Г.А. Абдулкаримова[2], Ф.Р. Гусманова[1]

[1]әл Фараби атындағы Қазақ ұлттық университеті, Алматы қ., Қазақстан
[2]Абай атындағы Қазақ ұлттық педагогикалық университеті, Алматы қ., Қазақстан
[*]*e-mail: rakhysh_aigerim3@live.kaznu.kz*

АСА МАҢЫЗДЫ МЕМЛЕКЕТТІК ИНФРАҚҰРЫЛЫМНЫҢ КИБЕРҚАУІПСІЗДІГІН БАҒАЛАУ ӘДІСТЕРІ

Аңдатпа

Цифрландыру мен технологияларды интеграциялауды арттыру жағдайында мемлекеттік маңызды инфрақұрылымды киберқауіптерден қорғау басты міндетке айналды. Мұндай нысандарға жасалған кибершабуылдар экономикаға, ұлттық қауіпсіздікке және азаматтардың әл-ауқатына елеулі зиян келтіруі мүмкін. Бұл мақалада мемлекеттік маңызды инфрақұрылымның киберқауіпсіздігін бағалаудың заманауи әдістері, соның ішінде тәуекелдерді талдауға, қауіптерді модельдеуге, Байес желілерін пайдалануға, сценарийлік талдауға және гибридтік әдістерге негізделген дәстүрлі және инновациялық тәсілдер қарастырылады. Осы тақырып бойынша соңғы бесжылдықтағы ғылыми зерттеулерге шолу жүргізіліп, негізгі тенденциялар мен қолданыстағы тәсілдердің шектеулері анықталды. Әртүрлі салалар үшін бағалау әдістерін бейімдеу және киберқауіпсіздікті қауіпсіздіктің дәстүрлі тәсілдерімен біріктіру мәселесіне ерекше назар аударылады. Мақала киберқауіпсіздікті бағалаудың жаңа әдістерін әзірлеумен, жетілдірумен айналысатын киберқауіпсіздік мамандары мен зерттеушілерге арналған.

Түйін сөздер: киберқауіпсіздікті бағалау әдістері, аса маңызды мемлекеттік инфрақұрылым, тәуекелдерді бағалау, киберқауіпсіздік, бағалау өлшемдері.

С.А.Адилжанова[1], А.Е.Рахыш[1], Г.А. Абдулкаримова[2], Ф.Р.Гусманова[1]
[1]Казахский Национальный университет имени аль Фараби, г.Алматы, Казахстан
[2]Казахский Национальный педагогический университет имени Абая, г.Алматы, Казахстан

МЕТОДЫ ОЦЕНКИ КИБЕРБЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ГОСУДАРСТВЕННОЙ ИНФРАСТРУКТУРЫ

Аннотация

В условиях растущей цифровизации и интеграции технологий защита критически критической государственной инфраструктуры от киберугроз становится ключевой задачей. Кибератаки на такие объекты могут нанести значительный ущерб экономике, национальной безопасности и благополучию граждан. В статье рассматриваются современные методы оценки кибербезопасности государственной критической инфраструктуры, включая традиционные и инновационные подходы, основанные на анализе рисков, моделировании угроз, использовании байесовских сетей, анализе сценариев и гибридных методах. Был проведен обзор научных исследований за последние пять лет по данной теме, выявивший основные тенденции и ограничения существующих подходов. Особое внимание уделено вопросу адаптации методов оценки для различных отраслей и интеграции кибербезопасности с традиционными подходами к обеспечению безопасности. Статья предназначена для специалистов по кибербезопасности и исследователей, занимающихся разработкой новых методов оценки кибербезопасности.

Ключевые слова: методы оценки кибербезопасности, критическая государственная инфраструктура, оценка рисков, кибербезопасность, критерии безопасности.

S.A.Adilzhanova[1], A.E.Rakhysh[1] , G.A.Abdulkarimova[2], F.R.Gusmanova[1]
[1]al Farabi Kazakh National University, Almaty, Kazakhstan
[2]Abai Kazakh National Pedagogical University, Almaty, Kazakhstan

METHODS FOR ASSESSING THE CYBERSECURITY OF CRITICAL STATE INFRASTRUCTURE

Abstract

In the context of increasing digitization and integration of technologies, protecting critical infrastructure from cyber threats is becoming a priority. Cyberattacks on such facilities can cause significant damage to the economy, national security, and the well-being of citizens. This article reviews modern methods for assessing the cybersecurity of critical infrastructure, including traditional and innovative approaches based on risk analysis, threat modeling, the use of Bayesian networks, scenario analysis, and hybrid methods. A review of scientific studies on this topic over the last five years are conducted, and the main trends and limitations of existing approaches are identified. Special attention is paid to the issue of adapting assessment methods for various industries and integrating cybersecurity with traditional security approaches. The article is intended for cybersecurity specialists and researchers involved in the development of new methods for assessing cybersecurity.

Keywords: cybersecurity assessment methods, critical infrastructure, risk assessment, cybersecurity, assessment criteria.

Негізгі ережелер

Аса маңызды мемлекеттік инфрақұрылымды қорғау XXI ғасырдағы басты міндеттердің бірі болып табылады, себебі технологиялардың дамуы киберқауіптер мен кибершабуылдарды арттырды. Киберқауіпсіздіктің маңызы артқан сайын оны бағалайтын өлшемдер мен әдістерді анықтау қажеттілігі туындайды. Киберқауіпсіздікті бағалау әдістері тәуекелдерді талдау, қауіптерді модельдеу, Байес желілерін қолдану, сценарийлік талдау және гибридтік тәсілдер сияқты дәстүрлі және инновациялық әдістерді қамтиды. Зерттеулер негізінде бағалау әдістерінің тиімділігі мен шектеулері анықталды, олардың әртүрлі салаларға бейімделу қажеттілігі көрсетілді. Киберқауіпсіздікті жалпы қауіпсіздік саясаттарымен біріктіру маңызды болып саналады, өйткені бұл кешенді тәсілдер кибершабуылдарға қарсы тиімді қорғаныс жасауға мүмкіндік береді.

Кіріспе

Цифрландыру мен технологияларды интеграциялаудың өсіп келе жатқан заманауи жағдайында мемлекеттік маңызды инфрақұрылымды (ММИ) қорғау өзекті міндеттердің бірі болып қала береді. Мемлекеттік маңызды инфрақұрылымдарға жасалатын кибершабуылдар экономикаға, қауіпсіздікке және азаматтардың әл-ауқатына елеулі зиян келтіруі мүмкін. Қарқынды дамып келе жатқан қауіптер, соның ішінде кибершабуылдар мен осалдықтарды анықтап қана қоймай, киберқауіпсіздіктің тұрақтылығын арттыратын сенімді бағалау әдістерін талап етеді [1]. Соңғы жылдары қауіпсіздік саласында киберқауіпсіздік мәселелері мен дәстүрлі сенімділікті бағалаудың конвергенциясы байқалды, сондай ақ бұл зерттеулермен де расталуда. Бағалаудың заманауи әдістерінде нормативтік құжаттарға негізделген классикалық тәсілдерден жасанды интеллект пен үлкен деректерді пайдаланатын инновациялық әдістерге дейін бар. Дегенмен, бар әртүрлілікке қарамастан, нақты контекстте әдістерді таңдау, бейімдеу және қолданумен байланысты мәселелер ғылыми және қолданбалы ортада қалады. Мысалы, кейбір салалар үшін әзірленген бірқатар әдістер басқа салаларда қолдану үшін өзгертуді қажет етеді. Бұл жұмыстың мақсаты – мемлекеттік маңызды инфрақұрылымның киберқауіпсіздігін бағалау үшін қолданылатын заманауи әдістерді,

олардың мүмкіндіктерін, шектеулерін және болашақ даму бағыттарын зерттеу. Негізгі міндеттерге мыналар жатады:

- қолданыстағы киберқауіпсіздікті бағалау әдістерін жіктеу;
- киберқауіпсіздікті бағалау өлшемдерін анықтау;
- алдағы зерттеулерде жасанды интеллект мүмкіндігін қолдану.

Бұл шолу қолданыстағы тәсілдерді жүйелейді және қолданылатын әдістерді әзірлеуге мүдделі зерттеушілер мен ғалымдарға аналитикалық негіз ұсынады.

Зерттеу әдіснамасы

Дәстүрлі қауіпсіздікті бағалау тәсілдері киберқауіпсіздікке аса назар аудармаған. Оны жеке салаларға қалдырумен келген немесе іске асыру қиын болатын жалпы киберқауіпсіздік тәсілдері мен нұсқаулықтарға сілтеме келтірген.

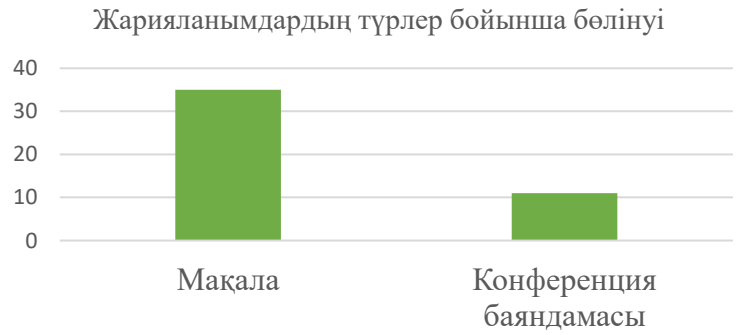
Жоғарыда аталған мәселелерді шешу үшін дәстүрлі қауіпсіздікті бағалау тәсілдері әртүрлі тәсілдермен алмастырылды, бұл киберқауіпсіздікке қатысты қауіптерді ескеруге және бағалауды неғұрлым жан-жақты етуге мүмкіндік берді. Мұндай өзгерістерге келесілерді жатқызамыз:

– бағалау әдістері жүйе қауіпсіздігіне киберқауіптер мен осалдықтардың әсерін анықтайды, мұндай әдіске мысал ретінде киберқауіпті талдау және тәуекелдерді бағалау (Hazard Analysis and Risk Assessment (HARA)) әдісін жатқызсақ болады.

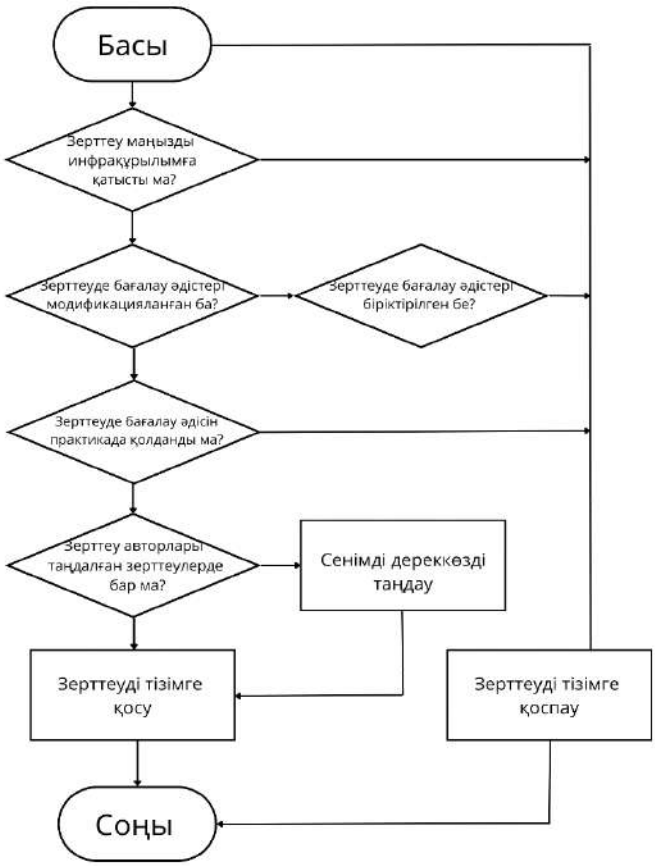
– қауіпсіздікті бағалау әдістерін киберқауіпсіздік саласына бейімдеу; мұндай тәсілдің мысалы ретінде ену режимдерін, олардың салдарын және сыни маңыздылығын талдау (Intrusion Modes, Effects, and Criticality Analysis (IMECA)), сондай-ақ дәстүрлі тәсіл (Failure Modes, Effects, and Criticality Analysis (FMECA)) басып кірулерді талдау үшін қолданылады;

– қауіпсіздік пен киберқауіпсіздікті бағалаудың бірнеше әдістерін комбинациялау [2].

2019-2024 жылға дейін «аса маңызды инфрақұрылымның киберқауіпсіздігін бағалау» тақырыбында өте көп ғылыми мақалалар мен конференция баяндамалары жарияланған, атап айтсақ, 389 мақала табылды. Оның ішінде ағылшыннан басқа тілдегі мақалалар, қайталанғандары, қолжетімді еместерін санамағанда 126 мақала қалды. Соның ішінен тақырыпты жақсы ашып тұрған 46 мақала талданып, ең көп қолданылатын бағалау әдістері анықталды. Мақалалардың ішінде конференцияда оқылған баяндамалар да болды, олардың саны диаграммада көрсетілді (сурет 1). Мақалаларды қандай критерийлерге сай алғанымызды (сурет 2 схемада көрсеттік).



Сурет 1. Зерттеулер саны



Сурет 2. Зерттеулерді жинау критерийлері

Зерттеу нәтижелері

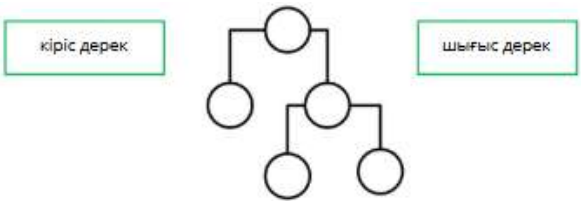
Таңдалған мақалаларды талдау барысында, 4 түрлі киберқауіпсіздікті бағалау әдістерін анықтадық. Толығырақ 3-суретте көрсетілді.

Сурет 3. Киберқауіпсіздікті бағалау әдістері

Электрондық кестелерге негізделген үдерістің типтік мысалы – істен шығу режимдерін, олардың салдарын және диагностикалық мүмкіндіктерін талдау (failure mode, effect, and diagnostic analysis (FMEDA)), бұл өнім немесе қосалқы жүйе деңгейіндегі істен шығу жиілігі, істен шығу режимдері және диагностикалық мүмкіндіктер туралы мәліметтерді алу үшін жүйелі талдау әдісі. FMEDA-ның негізгі мақсаты – құрылғылардың архитектуралық көрсеткіштерін және кездейсоқ істен шығуларға байланысты қауіпсіздік мақсаттарының бұзылуын бағалау, сондай-ақ қажетті қауіпсіздік деңгейіне жетпеген жағдайда қауіпсіздік олқылықтарын жою үшін жеткілікті ақпарат беру [3].

Электрондық кестелерге негізделген тағы бір мысал – тәуекелге бағытталған тексеріс , ол мұнай-газ және химия өнеркәсібінде кеңінен қолданылады және өзін жақсы жағынан көрсетті. Бұл тәсіл бастапқыда мұнай өңдеу өнеркәсібіне арналған. Бұл стандарт техникалық қызмет көрсету іс-шаралары мен салалардағы негізгі оқиғалар арасындағы байланысты анықтайды (4-сурет). Ол басқа салаларда және инспекциялық қызмет түрлерінде де бейімделіп, қолданылады, бұл құрылғының/жүйенің істен шығу механизмдері мен жиілігін анықтауға мүмкіндік береді. Ағаш негізіндегі әдістер 5-суреттегідей ағаш түріндегі графикалық көріністен бейнеленеді. Ағаш негізіндегі әдістің классикалық мысалы – жүйенің сенімділігін бағалау үшін қолданылатын істен шығу ағашын талдау (fault tree analysis (FTA)).

Сурет 4. Кестеге негізделген әдіс



Сурет 5. Граф ағаштарына негізделген әдіс

Модельге негізделген әдістер деп (6-сурет) әртүрлі үлгілерді – графиктерді, теңдеулерді және т.б. пайдалана отырып, бағалауды жүзеге асыратын тәсілдерді түсінеміз.

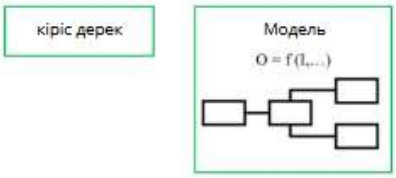
Байестік желі (БЖ), ол шартты тәуелділіктер негізінде айнымалылардың ұжымдық үлестірімінің факторизациясын орындай алатындықтан, белгісіз дәлелдерден белгісіз тұжырымдарға дейін рационализациялау гипотезасын білдіреді [4]. БЖ белгісіздік пен толық емес проблемаларды шешуге көмектеседі; осылайша, ол бірнеше домендерде кеңінен қолданылады. БЖ әдетте желілердің қауіптері мен осалдықтарын зерттеу үшін пайдаланылады, олар тәуекелдердің сандық және сапалық бағасын беретін циклді емес графиктер болып табылады. Модельге негізделген сенімділік дәлелдерін басқару – растау дәлелдерін басқаруға арналған әртүрлі әрекеттерді қарастыратын басқа үлгіге негізделген әдіс, атап айтқанда ұсынылатын дәлелдерді анықтау, дәлелдемелерді қайта пайдалану мүмкіндігі, дәлелдеме ақпаратын жинау, іздеу, бағалау және сенімділік дәлелдемелерін өзгерту әсерін талдау және дәлелдемелерді пайдалану, мысалы, сәйкестікті басқару және дәлелдеу.

Модельге негізделген бағалау әдісінің ішінде ең танымалы Монте-Карло симуляциялау әдісі болып табылады. Көп жағдайда күрделі жүйелердің мінез-құлқын статистикалық модельдеу және кездейсоқ таңдау әдісі арқылы болжауға болады. Бұл сарапшыларға жүйедегі ақаулардың ықтималдығын бағалауға және жақсартуды қажет ететін негізгі бағыттарды анықтауға көмектеседі, сондықтан ол тәуекелді бағалау әдістерінің бірі болып саналады. Сенімділікті талдау жүйе жұмысының белгісіздігін және құрамдас бөліктерінің сенімділігін ықтималдық үлестірімдері арқылы көрсетеді, осылайша әртүрлі сценарийлерде жүйенің әрекетін модельдейді. Әрбір құрамдас бөлік өзінің істен шығу үлестіріміне сәйкес істен шығуы мүмкін болатын жағдайларды бірнеше рет модельдеу арқылы жүйенің бұл ақауларға қалай жауап беретінін бақылап, оның сенімділігі анықталады [5].

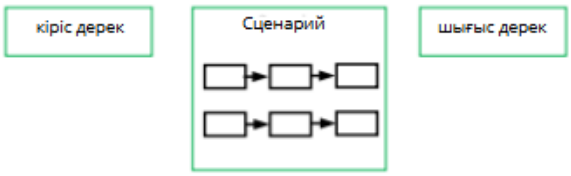
Ақырында, ықтималдық қауіпсіздікті бағалау атом электр станциясының тәуекелін бағалаудың ең кең таралған әдісі болып табылады. Ол оқиғалар мен қателер ағашының әдістеріне негізделген графикалық тәсілді қолданады. Сценарий негізіндегі процестерге келетін болсақ (7-сурет), олар әдетте қауіпсіздікке және/немесе киберқауіпсіздікке қатысты сценарийлерге назар аудару арқылы әртүрлі дереккөздерден (қақтығыстар, зерттеулер, сарапшылық деректер және т.б.) алынған сценарийлер жинағын профильдеуге негізделген.

Сценарий негізіндегі процестің типтік мысалы HARA болып табылады, мұнда ақаулар және/немесе функционалдық жеткіліксіздіктер қауіпсіздікке қатысты сценарийлерді (белгілі-қауіпсіз және белгілі-қауіпті), сондай-ақ белгісіз-қауіпсіз сценарийлерді анықтау тұрғысынан

талданады, сондай-ақ қажетті қарсы шараларға қосымша назар аудара отырып, қауіпті сценарийлерді талдайды [6].



Сурет 6. Модельге негізделген әдіс



Сурет 7. Сценарийге негізделген әдіс

Киберқауіпсіздікті бағалау әдістері қарастырылды, оларды қандай көрсеткіштер арқылы бағалайтынымыз 8-суретте көрсетілді.

Сурет 8. Бағалау өлшемдері

– Қауіпсіз істен шығу үлесі – диагностика анықтай алмайтын қауіпті істен шығу ықтималдығын өлшеу үшін қолданылатын өлшем.

– Қауіпсіздік тұтастығы – барлық қауіпсіздікке арналған аспаптық функциялардың белгіленген уақыт аралығында және барлық белгіленген шарттарда қанағаттанарлық деңгейде жұмыс істейтінін растау үшін қолданылады.

– Сағат сайынғы істен шығу ықтималдығы – жүйенің қажет болған жағдайда өз қауіпсіздік функциясын орындауына кедергі келтіретін қауіпті істен шығу ықтималдығы.

– Бұзу уақытының орташа мәні – біркелкі жұмсалған күш-жігерді ескере отырып, нақты шабуылды жүзеге асыруға қажет уақыттың есептік көрсеткіші.

– Негізгі зақымдану жиілігі – жүйенің істен шығу ықтималдығы мен адам өлімі (немесе қоршаған ортаға әсері) негізінде бастапқы оқиғалар жиілігін ескере отырып, жиілікті және салдарын өлшеуге арналған өлшем.

Киберқауіпсіздік пен жүйенің сенімділігін бағалау әдістерінің ішінде ең көп қолданылытаны - Марков тізбектері. Ол өзара күрделі байланысқан және күйлер арасында өтпелі стохастикалық жүйелердің сенімділігін модельдеу мен бағалауға арналған математикалық негізді қамтамасыз етеді. Марков тізбектерін қолдану арқылы сенімділік пен киберқауіпсіздікті бағалау әдісі уақыт өте келе жүйенің күйлерінің ықтималдығын өлшейді, жұмыс істеу, істен шығу және жөндеу үдерістерінің барлық мүмкін күйлерін ескереді. Бұл әдіс жүйенің өнімділігін бағалауға және пайдалану мен техникалық қызмет көрсету жоспарларына қажетті сенімділік көрсеткіштерін анықтауға мүмкіндік береді. Марков тізбегі негізінде жүйенің киберқауіпсіздігін талдау бірнеше қадамдар арқылы жүзеге асырылады:

– Жүйенің барлық ықтимал күйлерін, соның ішінде қалыпты жұмыс істеу және істен шығу күйлерін анықтап, толық күй кеңістігін құру;

– Белгілі бір уақытта күйдің өзгеру ықтималдығын көрсететін өтпелі ықтималдық матрицасын жасау. Бұл матрица Марков тізбегін талдаудың негізгі элементі болып табылады және ол күйлер арасындағы өтпелі жылдамдықтарды, оның ішінде істен шығу және жөндеу жылдамдықтарын көрсетеді;

– Өтпелі ықтималдық матрицасынан алынған тұрақтылық теңдеулерін шешу арқылы жүйенің ұзақ мерзімді тұрақты күйін анықтау;

– Тұрақты күйлердің ықтималдығын пайдалану арқылы жөндеуге кететін орташа уақыт, жүйенің қолжетімділігі және істен шығуға дейінгі орташа уақыт сияқты негізгі сенімділік көрсеткіштерін есептеу.

Талданған мақалалардағы бағалау өлшемдері мен әдістерді сәйкестендірейік, ол 1-кестеде көрсетілді.

Кесте1. Мақалаларда жиі кездескен бағалау өлшемдері мен әдістері

Бағалау өлшемі	*Бағалау әдісі*	*Мақала атауы*
Қауіпсіз істен шығу үлесі	*Динамикалық осалдықты бағалау графигі*	*Attack Graph-based Solution for Vulnerabilities Impact Assessment in Dynamic Environment[7]*
Тәуекелді жіктеу	*Шабуыл ағашын талдау*	*Model-based assurance evidence management for safety–critical systems[8]*
Тәуекелді жіктеу	*Қауіптерді талдау және тәуекелдерді бағалау*	*Safety and security co-engineering for highly automated vehicles[9]*
Бұзу уақытының орташа мәні	*Ену тәсілдері, әсері және маңыздылығын талдау*	*Combining IMECA analysis and penetration testing to assess the cybersecurity of industrial robotic systems[10]*
Жүйенің істен шығу ықтималдығы	*Киберқауіпсіздік тәуекелдерін бағалау*	*Cybersecurity Risk Assessment of Industrial Control Systems Based on Order-α Divergence Measures Under an Interval-Valued Intuitionistic Fuzzy Environment[11]*

Сондай-ақ, киберқауіпсіздікті бағалау үшін жасанды интеллект мүмкіндіктерін де қолдансақ болады. Маңызды инфрақұрылымды қорғауға арналған үлкен тілдік модельдердің қолданбаларының тиімділігін арттыру үшін оның өмірлік циклін құпиялылық және тұрақтылық үштігімен сәйкестендіру маңызды. Ол үшін келесі нұсқаулықты пайдалана аламыз.

1) Жобалау: киберқауіпсіздікті бағалау бағытын орнату;

Мақсатты нақтылау: Жобаның негізгі мақсатын анықтау. Мысалы, модель қауіп туралы ақпаратты талдай ма, осалдықтарды бағалауға көмектесе ме немесе төтенше жағдайға жауап бере ме? Қолдану аясы: қай инфрақұрылымдық аймақтарға назар аударылатынын анықтау

2) Модельді таңдау: киберқауіпсіздік талаптарына сәйкестендіру;

Қауіпсіздік және сенімділік: қауіпсіздік пен деректер құпиялылығына басымдық беретін қолданбалар үшін үлгіні таңдау;

3) Модельдің өнімділігі және бейімделуі: киберқауіпсіздікті бағалау тиімділігін қамтамасыз ету. Өнімділікті бағалау: модельдің инфрақұрылымға қауіптерді анықтау, жіктеу және болжау қабілетін бағалау;

4) Бағалау және қайталау: аса маңызды инфрақұрылымды қорғаудың дәлдігін жақсарту; Модельдің қауіпті анықтау дәлдігі, жауап беру жылдамдығы және салалық деректерді өңдеу мүмкіндігі сияқты көрсеткіштерді пайдалану;

5) Үлкен тілдік модельдерді қолдану: модельді іске қосу;

Орнатқаннан кейін модельдің өнімділігін бақылау және қауіптерді көрсету үшін оны жаңарту үшін тұрақты механизмдерді құру қажет. Барлық аталған қадамдарды 9-суретте келтірілген сұлба бойынша көрсетуге болады. Генеративті жасанды интеллект және үлкен тілдік модельдер маңызды инфрақұрылымды қорғауды жақсарта алатыны сөзсіз [12].

Сурет 9. Киберқауіпсіздікті бағалау моделі

Дискуссия

Қауіпсіздікті бағалау үшін танымал сенімділікті бағалау әдістерінің өзгертілген нұсқалары кеңінен қолданылады, мысалы, FMEA/FMECA, FTA және Байес желілері, Марков тізбектері.

Киберқауіпсіздікке келетін болсақ , не арнайы өзгерістер енгізіледі (мысалы, IMECA сияқты), не көп жағдайда киберқауіпсіздікті бағалау жалпы қауіпсіздікті бағалау процесіне біріктіріледі[13]. Көп жағдайда бағалау процесі тәуекелге негізделген тәсілге сүйенеді, оған тәуекелдерді анықтау, талдау, бағалау кіреді.

Негізгі шектеулерге мыналарды жатқызамыз:

– өлшемдік мәселелер (талдануы тиіс компоненттердің өте көп санына байланысты әдісті қолдану мүмкін емес);

– тым қатаң болжамдар (мысалы, істен шығулар немесе шабуылдар бір-бірінен тәуелсіз деп қарастырылады).

Мұндай шектеулерді еңсеру үшін қолданылатын әдістерге өзгерістер енгізілуде, мысалы, тек қауіпсіздік функциясының бөлігі болып табылатын элементтерге назар аудару, күрделі қауіпсіздік жүйелері үшін арнайы адаптивтелген тәсілдерді қолдану және т.б.

Зерттеулердің көпшілігінде қолданылатын әдістер қателерді, тек осалдықтарды немесе екеуін де қамтитын тәуекелдерді бағалауға бейімделген (тәуекелге негізделген тәсіл).

Нақты I&C жүйелерінде қолданылатын кейбір киберқауіптерді бағалау әдістері ұлттық стандарттарға негізделген. Мысалы, Қытай ұлттық стандарты GB/T 36466-2018: «Ақпараттық қауіпсіздік технологияларын енгізу бойынша нұсқаулық». Осы құжатқа сәйкес, алдымен тәуекелдің төрт элементі анықталуы және бағалануы қажет: сапалық (сараптамалық бағалау) және сандық комбинациясын пайдалана отырып, активтер, қауіптер, осалдықтар және қорғаныс мүмкіндіктері, сандық есептеу әдістері[14-15].

Осы төрт элементтің негізінде ақпараттық қауіпсіздік инциденттерінің туындау және зақымдану ықтималдығы есептеледі, содан кейін соңғы "тәуекел балы" анықталады.

Ақпараттық жүйелер мен физикалық жүйелерді біріктіру кезінде ақпараттық жүйелердің киберқауіпсіздігі және физикалық жүйелердің функционалдық қауіпсіздігі өзара әрекеттесе бастайды, бұл жаңа күрделі мәселенің пайда болуына әкеледі және ауыр тәуекелдерді тудырады. Бұл мәселені шешу үшін генеративті жасанды интеллект, үлкен тілдік модельдер сияқты жаңа, заманауи тәсілдер қажет.

Қорытынды

Бұл зерттеуде киберқауіпсіздік пен қауіпсіздікті бағалау мәселелеріне арналған соңғы бесжылдықтағы өзекті ғылыми мақалалар талданды.

Зерттеулерде қолданылатын әдістердің көпшілігі не симуляциялық модельдеуге, не теориялық тұжырымдамаларға негізделгенін ерекше атап өткен жөн. Зерттеулердің көпшілігі (46-дың 33-і) қауіпсіздік пен киберқауіпсіздікті бірлескен талдау үшін немесе тиісті қолдану салаларындағы жаңа қажеттіліктерді есепке алу үшін классикалық бағалау әдістерін өзгертуді немесе кеңейтуді ұсынады. Бұл тенденция ұзақ мерзімді тәжірибеде дәлелденген бағалаудың

классикалық әдістері әлі де кең сұранысқа ие екенін және аналитикалық күрделі қажеттіліктерді қанағаттандыру үшін одан әрі жетілдіруге негіз болатынын көрсетеді. Қарқынды дамып келе жатқан генеративті жасанды интеллект, цифрлық егіз, машиналық оқыту салаларын да киберқауіпсіздікті бағалауға қолдануға болады. Болашақта жасанды интеллектке негізделген бағалау моделін жасайтын боламыз. Алдағы зерттеулердің бәрі ЖИ-мен байланысты болмақ.

Пайдаланылған дереккөздердің тізімі

[1] Leszczyna R. Review of cybersecurity assessment methods: Applicability perspective //Computers & Security. – 2021. – T. 108. – C. 102376.

[2] Babeshko I., Di Giandomenico F. Safety and Cybersecurity Assessment Techniques for Critical Industries: A Mapping Study //IEEE Access. – 2023.

[3] Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES), Standard IEC 61508, 2010.

[4] A. Carrera-Rivera, W. Ochoa, F. Larrinaga, and G. Lasa, ''How-to conduct a systematic literature review: A quick guide for computer science research,'' MethodsX, vol. 9, Jan. 2022, Art. no. 101895, doi: 10.1016/j.mex.2022.101895

[5] Application of monte carlo simulations to system reliability analysis. https://www.911metallurgist.com/blog/wp-content/uploads/2016/01/ Application-of-Monte-Carlo-Simulations-to-System-Reliability-Analysis. pdf. Accessed: 2025-02-11.

[6] R. Gupta, S. Tanwar, N. Kumar, and S. Tyagi, ''Blockchain-based security attack resilience schemes for autonomous vehicles in industry 4.0: A systematic review,'' Comput. Electr. Eng., vol. 86, Sep. 2020, Art. no. 106717.

[7] A. Boudermine, R. Khatoun, and J.-H. Choyer, ''Attack graph-based solution for vulnerabilities impact assessment in dynamic environment,'' in Proc. 5th Conf. Cloud Internet Things (CIoT), Marrakesh, Morocco, Mar. 2022, pp. 24–31, doi: 10.1109/CIoT53061.2022.9766588.

[8] J. L. de la Vara, A. S. García, J. Valero, and C. Ayora, ''Model-based assurance evidence management for safety–critical systems,'' Softw. Syst. Model., vol. 21, no. 6, pp. 2329–2365, Dec. 2022, doi: 10.1007/s10270- 021-00957-z.

[9] C. Schwarzl, N. Marko, H. Martin, V. E. Jiménez, J. C. Triginer, B. Winkler, and R. Bramberger, ''Safety and security co-engineering for highly automated vehicles,'' Elektrotechnik Informationstechnik, vol. 138, no. 7, pp. 469–479, Nov. 2021, doi: 10.1007/s00502-021-00934-w.

[10] A. Abakumov and V. Kharchenko, ''Combining IMECA analysis and penetration testing to assess the cybersecurity of industrial robotic systems,'' in Proc. 12th Int. Conf. Dependable Syst., Services Technol. (DESSERT), Athens, Greece, Dec. 2022, pp. 1–7, doi: 10.1109/DESSERT58054.2022.10018823

[11] H. Guo, L. Ding, and W. Xu, ''Cybersecurity risk assessment of industrial control systems based on order—A divergence measures under an interval-valued intuitionistic fuzzy environment,'' IEEE Access, vol. 10, pp. 43751–43765, 2022, doi: 10.1109/ACCESS.2022.3169133.

[12] Yigit Y. et al. Critical infrastructure protection: Generative ai, challenges, and opportunities //arXiv preprint arXiv:2405.04874. – 2024.

[13] J. Alanen, J. Linnosmaa, T. Malm, N. Papakonstantinou, T. Ahonen, E. Heikkilä, and R. Tiusanen, ''Hybrid ontology for safety, security, and dependability risk assessments and security threat analysis (STA) method for industrial control systems,'' Rel. Eng. Syst. Saf., vo

[14] Risk-Based Inspection Methodology, Standard API RP 581, 3rd ed., Oct. 2020.

[15] A. Carrera-Rivera, W. Ochoa, F. Larrinaga, and G. Lasa, ''How-to conduct a systematic literature review: A quick guide for computer science research,'' MethodsX, vol. 9, Jan. 2022, Art. no. 101895, doi: 10.1016/j.mex.2022.101895