ҒТАХР 20.19.21

10.51889/2959-5894.2026.93.1.010

С.А. Адилжанова[1,2], Т.Ш. Миркасимова[1*], Г.А. Абдулкаримова[3], Ф.Р.Гусманова[1]

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

АҚПАРАТТЫҚ ҚАУІПСІЗДІК ТӘУЕКЕЛДЕРІН БАҒАЛАУ ҮДЕРІСТЕРІН АВТОМАТТАНДЫРУ

Аңдатпа

Кибершабуылдар санының тез өсуі және олардың құрылымының күрделенуі жағдайында ақпараттық қауіпсіздік тәуекелдерін объективті және жедел бағалау қажеттілігі артады. Зерттеудің мақсаты корпоративтік және мемлекеттік ақпараттық жүйелердегі қауіптерді талдаудың дәлдігін, қайталануын және тиімділігін арттыруға бағытталған тәуекелдерді автоматтандырылған бағалау әдістемесін әзірлеу және сынақтан өткізу болып табылады. Зерттеудің әдістемелік негізі ISO/IEC 27005, NIST sp 800-30 және FAIR моделінің халықаралық стандарттарына негізделген сандық және сапалық талдау әдістерінің жиынтығын қамтиды. Құралдар ретінде осалдықтарды автоматтандырылған бақылау және тестілеу жүйелері қолданылды – OpenVAS, Zabbix, Metasploit және RiskWatch. Нәтижелердің дұрыстығын статистикалық тексеру үшін Python 3.12 (NumPy, Pandas, SciPy) есептеу ортасында жүзеге асырылған Монте-Карло әдісі қолданылды. Жұмыстың ғылыми жаңалығы мониторинг құралдары мен математикалық модельдеу әдістерін біртұтас жүйеге біріктіретін тәуекелдерді бағалаудың интеграцияланған моделін жасау болып табылады. Зерттеудің практикалық құндылығы тәуекелдерді үздіксіз мониторингтеу мен бейімдеп басқаруды іске асыру үшін GRC және SIEM корпоративтік жүйелеріне ұсынылған әдістемені енгізу, сондай-ақ киберқауіпсіздік және цифрлық тәуекел-менеджмент жөніндегі мамандарды даярлау кезінде білім беру және зерттеу қызметінде қолдану мүмкіндігінен тұрады.

Түйін сөздер: тәуекелдерді бағалауды автоматтандыру, ақпараттық қауіпсіздік, FAIR, Монте-Карло, OpenVAS, GRC/SIEM жүйелер.

С.А. Адилжанова[2], Т.Ш. Миркасимова[1], Г.А. Абдулкаримова[3], Ф.Р.Гусманова[1]
[1]Национальный Университет имени Аль-Фараби, г.Алматы, Қазақстан
[2]Алматинский технологический университет, г.Алматы, Қазақстан
[32]Казахский Национальный педагогический университет имени Абая, г.Алматы, Казахстан

АВТОМАТИЗАЦИЯ ПРОЦЕССОВ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация

В условиях быстрого роста числа кибератак и усложнения их структуры возрастает необходимость объективной и оперативной оценки рисков информационной безопасности. Целью исследования является разработка и апробация методики автоматизированной оценки рисков, направленной на повышение точности, повторяемости и эффективности анализа угроз в корпоративных и государственных информационных системах. Методологическая основа исследования включает совокупность методов количественного и качественного анализа, основанных на международных стандартах модели ISO/IEC 27005, NIST sp 800-30 и FAIR. В качестве инструментов использовались автоматизированные системы мониторинга и тестирования уязвимостей-OpenVAS – Zabbix, Metasploit и RiskWatch. Для статистической проверки достоверности результатов использовался метод Монте-Карло, реализованный в вычислительной среде Python 3.12 (NumPy, Pandas, SciPy). Научной новизной работы является разработка интегрированной модели оценки рисков, объединяющей инструменты мониторинга и методы математического моделирования в единую систему. Практическая ценность

исследования заключается в возможности внедрения предложенной методики в корпоративные системы GRC и SIEM для осуществления непрерывного мониторинга и адаптивного управления рисками, а также применения в образовательной и исследовательской деятельности при подготовке специалистов по кибербезопасности и цифровому риск-менеджменту.

Ключевые слова: автоматизация оценки рисков, информационная безопасность, FAIR, Монте-Карло, OpenVAS, GRC/SIEM системы.

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

AUTOMATION OF INFORMATION SECURITY RISK ASSESSMENT PROCESSES

Abstract

In the context of a rapid increase in the number and complexity of cyberattacks, the need for an objective and timely assessment of information security risks is becoming increasingly critical. The aim of this study is to develop and validate a methodology for automated risk assessment aimed at improving the accuracy, reproducibility, and efficiency of threat analysis in corporate and governmental information systems. The methodological framework of the research combines quantitative and qualitative approaches based on international standards and models such as ISO/IEC 27005, NIST SP 800-30, and FAIR. The study employs automated monitoring and vulnerability testing systems – OpenVAS, Zabbix, Metasploit, and RiskWatch. For statistical validation of the results, the Monte Carlo method was applied within the computational environment Python 3.12 (NumPy, Pandas, SciPy). The scientific novelty of this work lies in the development of an integrated risk assessment model that unites monitoring tools and mathematical modeling methods into a single analytical system. The practical significance of the research lies in the possibility of implementing the proposed methodology into corporate GRC and SIEM systems for continuous monitoring and adaptive risk management, as well as its applicability in educational and research activities for training specialists in cybersecurity and digital risk management.

Keywords: risk assessment automation, information security, FAIR, Monte Carlo, OpenVAS, GRC/SIEM systems.

Кіріспе

Негізгі ережелер. Сандық модельдерді (FAIR, Монте-Карло, FTA) және осалдықтарды талдау құралдарын (OpenVAS, Zabbix, Metasploit, RiskWatch) біріктіретін ақпараттық қауіпсіздік тәуекелдерін автоматтандырылған бағалаудың интеграцияланған әдістемесі ұсынылды. Әзірленген модель талдау уақытын 60% - дан астам қысқартуға, есептеу дәлдігін 95% - ға дейін арттыруға және сараптамалық әдістерге тән субъективті ауытқуларды жоюға мүмкіндік берді. Эксперименттік нәтижелер статистикалық сенімділікті ($P < 0.05$) және ұсынылған тәсілдің қайталануын растады. Зерттеудің практикалық маңыздылығы – тәуекелдерді үздіксіз бақылау және бейімдеу үшін модельді GRC және SIEM корпоративтік жүйелеріне біріктіру мүмкіндігі. Нәтижелер кибер тәуекелдерді бағалау және болжау процестеріне машиналық оқыту элементтері мен цифрлық егіздерді одан әрі енгізуге негіз жасайды.

Экономика мен қоғамды заманауи цифрландыру кибершабуылдар санының тез өсуімен, олардың құрылымының күрделенуімен және ықтимал залалдың ұлғаюымен қатар жүреді. Мұндай жағдайларда ақпараттық қауіпсіздікті қамтамасыз ету және тәуекелдерді уақтылы бағалау корпоративтік және мемлекеттік ақпараттық жүйелердің орнықтылығының стратегиялық факторына айналады.

Сараптамалық бағалау мен деректерді қолмен өңдеуге негізделген тәуекелдерді талдаудың дәстүрлі әдістері жоғары еңбек сыйымдылығымен, адам факторына тәуелділігімен және нәтижелердің шектеулі қайталануымен сипатталады. Бұл шешім қабылдаудың кешігуіне және қауіп-қатерді бағалаудың объективтілігінің төмендеуіне әкеледі. Осыған байланысты қазіргі заманғы мониторинг және математикалық модельдеу құралдарын пайдалана отырып, сапалық

және сандық тәсілдерді біріктіруге қабілетті тәуекелдерді бағалаудың автоматтандырылған модельдеріне көшу қажеттілігі өзекті болып отыр.

Бұл мәселені шешу үшін зерттеу OpenVAS, Zabbix, Metasploit, RiskWatch құралдарын және Fair, Монте-Карло және FTA әдістерін қолданды, бұл ақпараттық қауіпсіздік тәуекелдерін бағалаудың бірыңғай аналитикалық контурын құруға мүмкіндік берді. Процесті автоматтандыру есептеу дәлдігінің жоғарылауын, талдау уақытын қысқартуды және нәтижелерді түсіндіру кезінде субъективті ауытқуларды жоюды қамтамасыз етеді.

Зерттеудің мақсаты – талдау нәтижелерінің дәлдігін, жеделдігін және қайталануын арттыруға бағытталған ақпараттық қауіпсіздік тәуекелдерін автоматтандырылған бағалау әдістемесін әзірлеу және эксперименттік тексеру.

Мақсатқа жету үшін келесі *міндеттер* шешілді:

- тәуекелдерді бағалаудың қолданыстағы стандарттары мен әдістемелеріне талдау жүргізу (ISO/IEC 27005, NIST SP 800-30, FAIR);
- осалдықтарды бақылау және талдау құралдарын (OpenVAS, Zabbix, Metasploit) бір жүйеге біріктіру;
- автоматтандырылған және дәстүрлі тәсілдердің тиімділігіне салыстырмалы талдау жүргізу;
- модельдеу нәтижелерінің статистикалық сенімділігін және олардың корпоративтік GRC және SIEM жүйелерінде қолданылуын бағалау.

Зерттеу гипотезасы автоматтандырылған талдау құралдарын (OpenVAS, Zabbix, Python) және математикалық модельдеуді (FAIR, Монте-Карло, FTA) пайдалану тәуекелдерді бағалаудың дәлдігі мен жылдамдығын арттыруға, субъективті сараптамалық факторлардың әсерін азайтуға және корпоративтік қауіпсіздікті басқару жүйелерімен интеграцияны қамтамасыз етуге мүмкіндік береді.

Жұмыстың ғылыми жаңалығы сандық модельдерді (FAIR, Монте-Карло, FTA) және автоматтандырылған талдау құралдарын (OpenVAS, Zabbix, Metasploit, RiskWatch) бір жүйеге біріктіретін тәуекелдерді бағалаудың интеграцияланған әдістемесін әзірлеуден тұрады.

Зерттеу әдістемесі

Зерттеу 2024-2025 жылдары білім беру мекемесінің корпоративтік АТ инфрақұрылымы негізінде жүргізілді. Оның мақсаты заманауи мониторинг, осалдықтарды талдау және математикалық модельдеу құралдарын қолдана отырып, ақпараттық қауіпсіздік тәуекелдерін бағалаудың автоматтандырылған моделін әзірлеу және сынақтан өткізу болды.

Зерттеу гипотезасы автоматтандырылған талдау құралдарын (Python, OpenVAS, Zabbix) және сандық модельдеуді (FAIR, Монте-Карло, FTA) пайдалану АҚ тәуекелдерін бағалаудың дәлдігі мен жеделдігін арттыру арқылы субъективті сараптамалық факторлардың әсерін жоюға мүмкіндік береді деген болжамға негізделген [1-5].

Әдістеме келесі кезеңдер тізбегінде жүзеге асырылады:

1. Активтерді, қауіптерді және осалдықтарды анықтау.
2. Желілік белсенділік және инфрақұрылым жағдайы туралы деректерді автоматтандырылған жинау (Zabbix, OpenVAS).
3. Монте-Карло ықтималдық модельдеуін қолдана отырып, тәуекелдерді сандық бағалау.
4. Автоматтандырылған және қолмен талдау нәтижелерін салыстыру.
5. Басқару шешімдерін қолдау үшін деректерді визуализациялау және түсіндіру.

Кешенді талдау үшін сапалық және сандық әдістердің жиынтығы қолданылды. Сапалы деңгейде сараптамалық бағалау, сауалнама және SWOT-талдау жүргізілді, бұл қорғаныс жүйесінің негізгі осалдықтары мен күшті жақтарын анықтауға мүмкіндік берді. Сандық деңгейде FAIR және Монте-Карло модельдері қолданылды, олар қауіптерді іске асыру ықтималдығы мен күтілетін залал мөлшерін есептеуді қамтамасыз етті. Монте-Карло әдісі көптеген шабуыл сценарийлерін модельдеуге және ықтимал шығындардың таралуын анықтауға мүмкіндіктер берді.

Сәтсіздік ағашын талдау әдісі (FTA) тәуекелдерді кешенді бағалау және себептік тәуелділіктерді анықтау үшін қолданылды. FAIR моделін пайдалану оқиғалардың жиілігін, осалдық деңгейін және шығын шкалаларын құрылымдық сәйкестендіруді қамтамасыз етті, бұл қорытынды есептеулердің сенімділігін арттырды.

Әдістемені практикалық іске асыру үшін интеграцияланған құралдар кешені қолданылды:

- OpenVAS – осалдықтарды сыни деңгейлері бойынша автоматты түрде сканерлеу және жіктеу [6];
- Metasploit Framework – шабуылдарды модельдеу және жүйенің тұрақтылығын тексеру [7];
- RiskWatch – тәуекелдерді сандық бағалау және басқарушылық түсіндіру [8].
- Zabbix – желі күйін бақылау және қалыптан тыс белсенділікті анықтау [9];
- Python (Nmap кітапханалары, pandas, matplotlib) – деректерді жинау, талдау және визуализацияны автоматтандыру [10].

Аталған құралдардың комбинациясы деректерді жинаудан бастап есептер мен тәуекелдердің жылу карталарын құруға дейінгі талдаудың толық циклін қамтамасыз етті.

Зерттеу тәжірибесі білім беру ұйымының корпоративтік АТ-инфрақұрылымында өткізілді. Эксперименттік модель келесі техникалық орта мен параметрлер негізінде сыналды:

- *Сервер конфигурациясы:* Intel Xeon E5-2630 v4 (2.20 GHz), 64 GB RAM, SSD 2 TB, Ubuntu Server 22.04 LTS.
- *Желі параметрлері:* Ішкі корпоративтік сегмент (192.168.1.0/24), шамамен 120 түйін (node) және 15 виртуалды сервер, қауіпсіздік брандмауэрі – pfSense 2.7.
- *Бағдарламалық орта:* Python 3.12 (NumPy, pandas, SciPy, matplotlib), OpenVAS 22.9, Zabbix 6.4, Metasploit Framework 6.3, RiskWatch Enterprise Demo.
- *Тест ұзақтығы:* 30 күндік кезең ішінде 10 000 шабуыл сценарийі модельденіп, әрбір сценарий үшін талдау уақыты мен есептеу дәлдігі тіркелді.
- *Деректер көзі:* Желілік белсенділік журналдары (Zabbix log), осалдықтар тізімі (OpenVAS report.xml), ену сынақтарының нәтижелері (Metasploit session logs).

Модельдің нәтижелері осы параметрлер негізінде бағаланып, статистикалық тұрғыда тексерілді ($p < 0.05$). Тесттік орта ISO/IEC 27005 және NIST SP 800-30 талаптарына сәйкестендірілген корпоративтік қауіпсіздік саясаты шеңберінде пайдаланылды.

Зерттеу нәтижелері

Зерттеу барысында ұйымның корпоративтік АТ-инфрақұрылымына интеграцияланған ақпараттық қауіпсіздік тәуекелдерін бағалаудың автоматтандырылған моделі әзірленді және сыналды. Модельдің негізгі мақсаты адам факторының әсерін азайту және заманауи бақылау, осалдықтарды талдау және математикалық модельдеу құралдарын қолдану арқылы тәуекелдерді талдаудың дәлдігі мен жеделдігін арттыру болып табылады.

Әзірленген модель сандық әдістердің (FAIR, Монте-Карло, FTA) және аспаптық құралдардың (OpenVAS, Zabbix, Metasploit, Python) үйлесіміне негізделген. Мұндай интеграцияланған шешім автоматтандырылған деректерді жинау мен қауіп–қатер сценарийлерін модельдеуден бастап, тәуекелдердің жылу карталары, тарату кестелері және графикалық есептер түрінде нәтижелерді визуализациялауға дейінгі толық аналитикалық циклды қамтамасыз етеді.

Модель ұйымның инфрақұрылымымен біріктірілген және үздіксіз мониторинг пен бейімделгіш тәуекелдерді басқаруды қамтамасыз ететін нақты уақыттағы деректерді жаңартуды қолдайды.

Ұсынылған шешімнің тиімділігін бағалау үшін дәстүрлі (қолмен) әдіс пен тәуекелдерді бағалаудың автоматтандырылған әдістері арасында салыстырмалы талдау жүргізілді.

Талдау нәтижелері негізгі көрсеткіштердің айтарлықтай жақсарғанын көрсетті:

- тәуекелдерді талдау уақыты 65% - ға қысқарды (6-дан 2 сағатқа дейін);

- есептеу дәлдігі 95%-ға дейін көтерілді;
- сараптамалық бағалаудағы қателіктердің ықтималдығы 30-40% төмендеді;
- анықталған осалдықтар саны 35-40% - ға өсті.

Осылайша, автоматтандыру аналитикалық процедуралардың өнімділігін едәуір арттыруға, сондай-ақ нәтижелердің қайталануын және қайталануын қамтамасыз етуге мүмкіндік берді, бұл әсіресе корпоративтік және мемлекеттік деңгейдегі жүйелер үшін маңызды.

Нәтижелердің статистикалық дұрыстығын растау үшін 10 000 қауіп-қатер сценарийі негізінде Монте-Карло әдісін қолдана отырып бірқатар модельдеу жүргізілді. Есептеулер Python 3.12 ортасында NumPy, pandas, matplotlib және SciPy кітапханаларын қолдана отырып жүргізілді [10].

Алынған мәндердің таралуын талдау нәтижелердің тұрақты конвергенциясын көрсетті: стандартты ауытқу 3-4% - дан аспады, статистикалық маңыздылық деңгейі $P < 0.05$ болды. Бұл қайта сынау кезінде әзірленген модельдің жоғары сенімділігі мен қайталануын растайды.

Сонымен қатар, есептеулердің дұрыстығы мен модельдің тұрақтылығын тексеру Jupyter Notebook интеграцияланған ортасында жүргізілді, бұл нәтижелерді визуализациялауға және негізгі тиімділік көрсеткіштері үшін сенімділік аралықтарын құруға мүмкіндік берді (талдау уақыты, есептеу дәлдігі, қауіптерді анықтаудың толықтығы). Автоматтандырылған модель нәтижелерінің статистикалық сенімділігі төмендегі 1-кестеде көрсетілген.

Кесте 1. Автоматтандырылған модель нәтижелерінің статистикалық сенімділігі

Көрсеткіш	*Орташа мән*	*Сынақ саны (N)*	*Қолданылған құрал*	*Стандартты ауытқу (σ)*	*Сенімділік деңгейі (p)*
Талдау уақытының қысқаруы	*65 %*	*10 000*	*Python 3.12 (NumPy, SciPy)*	*±3.2 %*	*$p < 0.05$*
Есептеу дәлдігі	*95 %*	*10 000*	*Jupyter Notebook*	*±2.5 %*	*$p < 0.05$*
Қателік ықтималдығының азаюы	*35 %*	*10 000*	*Python 3.12 (pandas)*	*±4.1 %*	*$p < 0.05$*
Осалдықтарды анықтау толықтығы	*+38 %*	*10 000*	*OpenVAS + RiskWatch деректері*	*±3.7 %*	*$p < 0.05$*

Статистикалық тексеру Python 3.12 есептеу ортасында (NumPy, SciPy, pandas модульдері) деректерді бөлу мен визуализацияны талдау үшін Jupyter Notebook көмегімен жүргізілді. Бұл нәтижелердің дұрыстығын растауға және 10 000 сценарийді модельдеу кезінде кездейсоқ ауытқулардың әсерін азайтуға мүмкіндік берді.

Қолмен талдаудың орташа қателігі 25-30% құрады, ал автоматтандырылған модельді қолданған кезде ол 5% - ға дейін төмендеді. Интегралды тәуекелді есептеу нәтижелердің тұрақты конвергенциясын және сенімділіктің жоғары деңгейін көрсетті.

FAIR моделін қолдану оқиғалардың жиілігі, осалдық деңгейі және күтілетін шығындар арасындағы байланысты ресімдеуге мүмкіндік берді, ал FTA әдісі қауіп факторлары арасындағы себеп-салдарлық тәуелділіктерді анықтауға мүмкіндік берді [11].

Ұсынылған модель ISO/IEC 27005, NIST sp 800-30 және FAIR халықаралық стандарттарын автоматтандыру құралдарымен (OpenVAS, Zabbix, Python) біріктіреді, тәуекелдерді объективті, қайталанатын және динамикалық бағалау үшін бірыңғай аналитикалық контур қалыптастырады. Кешенді тәсіл субъективті факторлардың әсерін жояды, аналитикалық процедуралардың ашықтығын қамтамасыз етеді және кибер тәуекелдерді интеллектуалды басқаруға негіз жасайды.

Зерттеу нәтижелері автоматтандырылған тәсілдің жоғары тиімділігі және оның корпоративтік ақпараттық қауіпсіздікті басқару жүйелерінде, сондай - ақ тәуекелдерді үздіксіз бақылау үшін GRC және SIEM платформаларында қолданылуы туралы гипотезаны растады.

Құралдарды іске асыру мысалдары (OpenVAS, Metasploit, RiskWatch)

Зерттеу барысында үш негізгі құрал – OpenVAS, Metasploit, RiskWatch интеграциясы жүзеге асырылды, олар ақпараттық қауіпсіздік тәуекелдерін талдаудың толық циклын қамтамасыз етеді – инфрақұрылымды техникалық сканерлеуден алынған деректерді басқарушылық түсіндіруге дейін.

Құралдардың бұл үйлесімі нәтижелердің қайталануы мен объективтілігін қамтамасыз ететін практикалық осалдықтарды бағалауды, шабуылдарды модельдеуді және тәуекелдерді сандық бағалауды біріктіруге мүмкіндік берді.

OpenVAS (Open Vulnerability Assessment system) – Greenbone Vulnerability Manager (GVM) кешенінің құрамына кіретін және желілік инфрақұрылымдағы осалдықтарды автоматты түрде анықтауға арналған ашық код құралы. Эксперимент барысында OpenVAS терең желілік сканерлеуді және табылған осалдықтарды сыни деңгейлер бойынша жіктеуді жүзеге асырады: Low, Medium, High, Critical [6].

Тесттік сканерлеу нәтижелері:

- 154 осалдық анықталды, оның 18-і сыни деп жіктелді;
- жүйе анықталған осалдықтарды CVE (common Vulnerabilities and Exposures) базасындағы жазбалармен автоматты түрде салыстырды;
- әрбір қауіп үшін жауап беру басымдықтары мен жою бойынша ұсыныстары бар есептер жасалды.

Желіні сканерлеуді бастау үшін мысал командасы:

 # Берілген IP мекенжай ауқымында осалдықтарды сканерлеуді іске қосу

openvas -p 9390 -u admin -s 192.168.1.0/24

Берілген пәрменді орындағаннан кейін OpenVAS көрсетілген мекен-жайлар ауқымын толық сканерлейді, егжей-тегжейлі есеп жасайды және кейінірек талдау үшін деректерді RiskWatch жүйесіне жібереді.

OpenVAS пайдалану Желілік қауіпсіздіктің автоматтандырылған мониторингін жүзеге асыруға және адамның ең аз қатысуымен ықтимал қауіптерді жедел анықтауды қамтамасыз етуге мүмкіндік берді.

Сканерлеу нәтижелері аналитикалық модульге экспортталды, онда OpenVAS деректері негізінде тәуекел карталары мен жауап беру басымдықтары қалыптасты. Төмендегі суретте OpenVAS есебінің визуализациясы ұсынылған, ол осалдықтардың маңызды деңгейлері мен қатысатын қызметтер бойынша таралуын көрсетеді (сурет 1).

Report: Results (312 of 734)

ID: 97cc63d0-65d7-45ee-8ca8-711df1baa7dd
Modified:
Created:
Owner: admin

1 - 100 of 312

Vulnerability	Severity	QoD	Host	Location	Actions
rexec Passwordless / Unencrypted Cleartext Login	10.0 (High)	75%	192.168.11.137	512/tcp	
Samba End Of Life Detection	10.0 (High)	75%	192.168.11.137	445/tcp	
Samba 'TALLOC_FREE()' Function Remote Code Execution Vulnerability	10.0 (High)	75%	192.168.11.137	445/tcp	
PHP Multiple Vulnerabilities - Aug08	10.0 (High)	75%	192.168.11.137	80/tcp	
PHP Version < 5.2.7 Multiple Vulnerabilities	10.0 (High)	75%	192.168.11.137	80/tcp	
PHP End Of Life Detection (Linux)	10.0 (High)	75%	192.168.11.137	80/tcp	
MySQL End Of Life Detection (Linux)	10.0 (High)	75%	192.168.11.137	3306/tcp	
PostgreSQL End Of Life Detection (Linux)	10.0 (High)	75%	192.168.11.137	5432/tcp	

Сурет 1. Анықталған осалдықтары бар Openvas есебінің нәтижесі

Metasploit Framework шабуылдарды модельдеу, инфрақұрылымның тұрақтылығын тексеру және OpenVAS көмегімен сканерлеу кезінде бұрын анықталған қорғаныс шараларының тиімділігін талдау үшін қолданылды. Құрал осалдықтарды пайдаланудың нақты сценарийлерін жасауға және бақыланатын ортада ену тестілеуін өткізуге кең мүмкіндіктер береді. Бұл сәтті ену ықтималдығын бағалауға ғана емес, сонымен қатар қолданыстағы қорғаныс механизмдерінің қаншалықты тиімді жұмыс істейтінін анықтауға мүмкіндіктер береді [7].

Зерттеу SMB (Server Message Block) протоколына қатысты белгілі MS08_067_netapi осалдығын пайдалану сценарийін енгізді, оны шабуылдаушылар осал жүйелерде кодты қашықтан орындау үшін пайдаланады. Жүргізілген сынақтар 72% жағдайда жүйенің дұрыс конфигурациясы мен қауіпсіздік пакеттерін уақтылы жаңартудың арқасында шабуылдың сәтті алдын алғанын көрсетті.

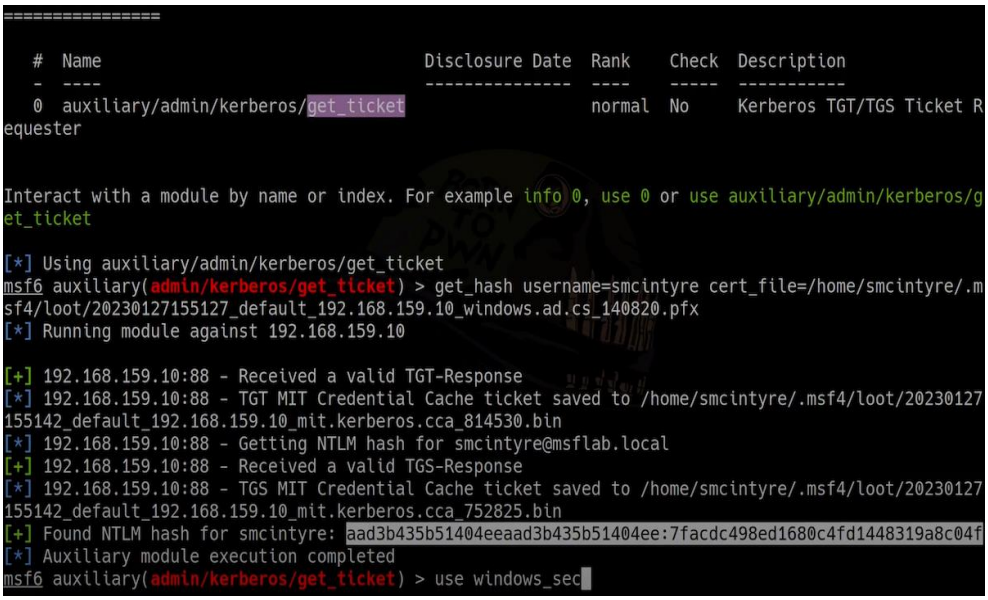
Осылайша, эксперимент нәтижелері патчтарды уақтылы басқарудың және желілік қауіпсіздіктің дұрыс параметрлерінің жоғары маңыздылығын растады.

Metasploit пайдаланудың беретін мүмкіндіктері:

- жүйенің конфигурациясына байланысты сәтті ену ықтималдығын бағалау;
- ішкі желінің осал жерлерін және қорғалмаған SMB қызметтерін анықтау;
- оқиғаларға жауап беру және журнал жүргізу саясатының тиімділігін тексеру;
- жүйелік қорғауды күшейту және әрекет ету стратегияларын бейімдеу бойынша ұсыныстар қалыптастыру.

SMB осалдығын пайдалануға негізделген бұл сценарий әлеуетті бұзушының жүйеге қалай қол жеткізуге тырысатынын, сондай-ақ мұндай шабуылдардың салдарын азайтуға мүмкіндік беретін қарсы механизмдерді көрсетті. Сонымен қатар, Metasploit қолдану қорғаныс параметрлерін тексеруді қамтамасыз етті, тәуекелдерді бағалаудың сенімділігін арттырды және оқиғаларға жауап берудің оңтайлы стратегияларын анықтауға мүмкіндік берді.

Төмендегі суретте Metasploit framework интерфейсі, шабуылды модельдеу нәтижелері және орнатылған өзара әрекеттесу сеанстарының құрылымы көрсетілген. Көрнекі деректер құралдың тәуекелдерді талдаудың жалпы автоматтандырылған моделіне сәтті интеграциялануын көрсетеді, оны қауіпсіздікті кешенді бағалау контурында қолдану мүмкіндігін растайды (сурет 2).



Сурет 2. Metasploit интерфейсі

Деректерді аналитикалық түсіндіру үшін тәуекелдерді сандық бағалауға, оларды саралауға және қауіптердің жылу карталарын құруға арналған RiskWatch құралы қолданылды.

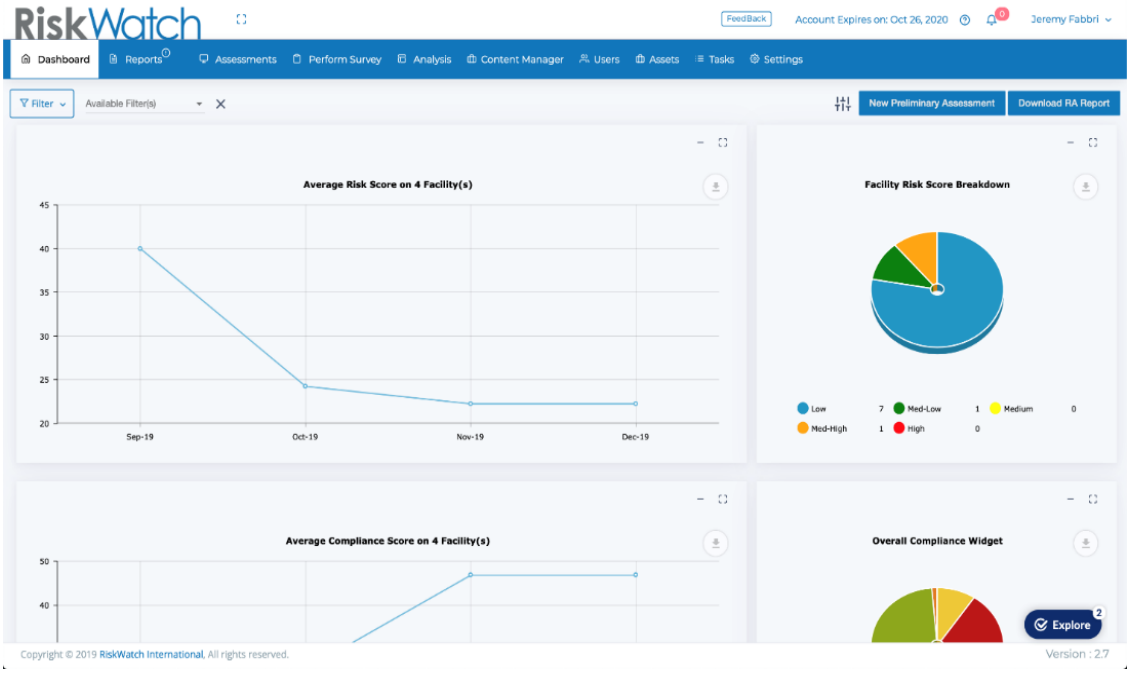
RiskWatch ұйым деңгейінде визуализация мен тәуекелдерді басқаруды қамтамасыз етті. Салынған жылу карталары (heatmaps) қауіптің ықтималдығы мен әсердің ауырлығының арақатынасын көрсетіп, жоғары тәуекел аймақтары мен қорғаныс басымдықтарын анықтауға көмектесті. RiskWatch – бұл ұйымдарға нақты уақыт режимінде тәуекелдерді талдау, басқару және бақылау құралдарын ұсынатын тәуекелдерді басқару платформасы. Бұл ұйымдарға тәуекелдерді бағалау процестерін автоматтандыруға және есеп беруді құруға мүмкіндік береді, бұл шешім қабылдауды айтарлықтай жеңілдетеді [8].

OpenVAS және MetasPloit-тен импортталған мәліметтер негізінде RiskWatch келесі тапсырмаларды орындады:

- осалдық көрсеткіштерін біріктіру және қалыпқа келтіру;
- FAIR моделі бойынша интегралды тәуекел деңгейлерін есептеу;
- басқару үшін heatmap матрицаларын және бақылау тақтасын құру.

Модель техникалық параметрлерді (сыни, жиілік, әсер ету) басқару көрсеткіштерімен (жоюдың басымдығы, күтілетін залал, қалдық тәуекел) байланыстыруға мүмкіндік берді. Осылайша, RiskWatch тәуекелдерді визуализациялауды және киберқауіпсіздік шешімдерін негізделген қабылдауды қамтамасыз ететін аналитикалық контурдың соңғы буыны болды.

Төмендегі суретте тәуекелдерді талдау кестелері мен жүйенің ағымдағы қауіпсіздік күйінің көрсеткіштері бар RiskWatch интерфейсі көрсетілген (сурет 3).



Сурет 3. Тәуекелдерді талдау графигі көрсетілген RiskWatch платформасының интерфейсі

OpenVAS, MetasPloit және RiskWatch-ті біріктіріп қолдану тәуекелдерді талдаудың жабық жүйесін енгізуге мүмкіндік берді:

- OpenVAS – осалдықтарды автоматтандырылған анықтау және жіктеу.
- MetasPloit – операциялық сценарийлерді практикалық тексеру.
- RiskWatch – тәуекелдерді сандық бағалау және басқарушылық түсіндіру.

Бұл компоненттерді біртұтас аналитикалық ортаға біріктіру:

- тәуекелдерді бағалау дәлдігін 95%-ға дейін арттыру;
- талдау уақытын 60-70%-ға дейін қысқарту;
- адам факторының субъективті әсерін жою;

– жаңа қауіп-қатерлерге үздіксіз бақылау және бейімделу мүмкіндігі.

Осылайша, ұсынылған құралдар архитектурасы ISO/IEC 27005 және NIST sp 800-30 халықаралық стандарттарының талаптарына, сондай-ақ корпоративтік деңгейдегі GRC платформаларының үздік тәжірибелеріне сәйкес келетін интеллектуалды киберқауіптерді басқару жүйесін құруға негіз болады.

Дәстүрлі және автоматтандырылған тәсілдерді салыстыру

Әзірленген әдістеменің тиімділігін растау үшін тәуекелдерді бағалаудың дәстүрлі (қолмен) және автоматтандырылған тәсілдерін төрт критерий бойынша салыстыру жүргізілді: талдау уақыты, есептеулердің дәлдігі, адам факторының әсері және еңбек сыйымдылығы.

Дәстүрлі әдістер мамандардың субъективті бағалауына байланысты және айтарлықтай уақыт ресурстарын қажет етеді, ал автоматтандырылған тәсіл GRC және SIEM жүйелерімен қайталануды, объективтілікті және интеграцияны қамтамасыз етеді. Осылайша, автоматтандыруды енгізу негізгі көрсеткіштер бойынша - тәуекелдерді талдау процесінің жылдамдығы, сенімділігі және ауқымдылығы бойынша тиімділігін дәлелдеді.

Зерттеу нәтижелері дәстүрлі және автоматтандырылған тәсілдердің тиімділігін салыстыру арқылы расталды. Талдау көрсеткіштеріндегі айырмашылықтар 2-кестеде көрсетілген.

Кесте 2. Ақпараттық қауіпсіздік тәуекелдерін бағалаудың салыстырмалы сипаттамасы

Салыстыру критерийі	*Дәстүрлі тәсіл*	*Автоматтандырылған тәсіл*	*Автоматтандыру нәтижесі*
Уақыт шығыны	*Тәуекелдерді қолмен талдау шамамен 5–6 сағатты алады, оған деректер жинау мен сараптамалық бағалау кіреді.*	*Талдау процесі сол көлемдегі деректер үшін автоматты түрде 1,5–2 сағатта орындалады.*	*Талдау уақыты ≈65 % қысқарды.*
Нәтиже дәлдігі	*Нәтиже сарапшылардың субъективті бағасына және тәжірибесіне тәуелді; қатерлерді қате жіктеу ықтималдығы бар.*	*Модельдеу алгоритмдері (Монте-Карло, FAIR) мен автоматты деректерді өңдеу қолданылады.*	*Есептеу дәлдігі 95 %-ға дейін артты, қателік ықтималдығы 30–40 % азайды.*
Адам факторының әсері	*Жоғары: интерпретация кезіндегі қателер, шаршау, шектеулі сараптамалық білім.*	*Талдау және есепті автоматты түрде қалыптастыру жүзеге асады.*	*Субъективті фактордың ықпалы жойылды, нәтижелер қайталанбалы.*
Автоматтандыру деңгейі	*Автоматтандыру жоқ, барлық кезеңдер қолмен орындалады.*	*OpenVAS, Metasploit, Zabbix, Python құралдары толық интеграцияланған.*	*Тәуекелді бағалау мен жаңарту автоматты режимде іске асырылады.*
Еңбек сыйымдылығы	*Жоғары, бірнеше сарапшының қатысуын талап етеді.*	*Бір оператор жүйені басқарады, есеп автоматты түрде жасалады.*	*Еңбек шығыны 2,5–3 есеге азайды.*
Масштабталу мүмкіндігі	*Қолмен өңдеу мен үйлеспейтін деректер салдарынан шектеулі.*	*Үлкен деректерді өңдеу және GRC/SIEM жүйелерімен біріктіру мүмкіндігі бар.*	*Масштабталу мен бейімделу қамтамасыз етілді.*

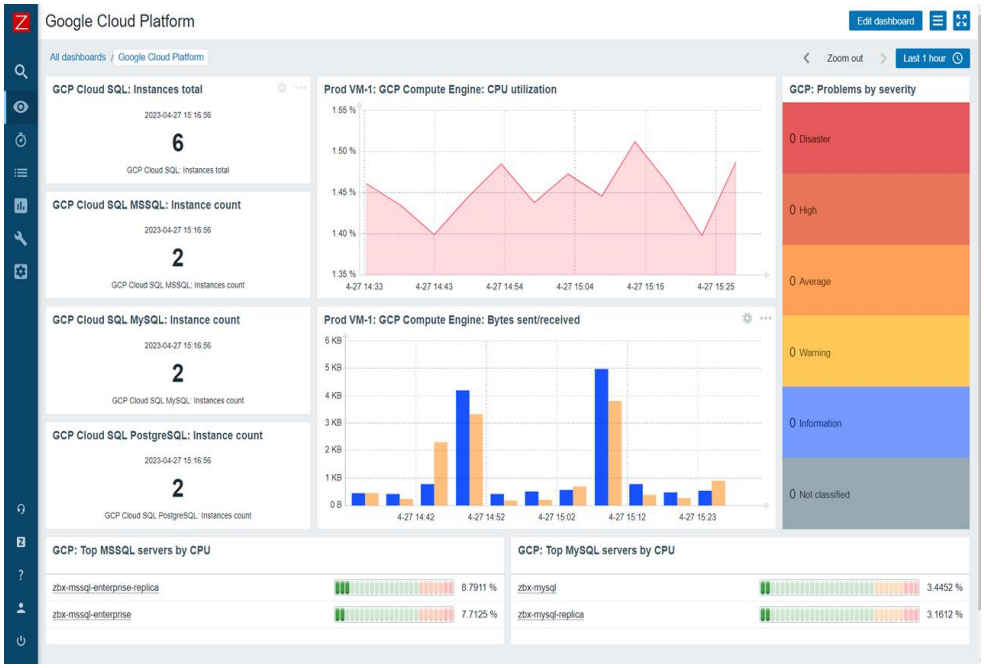
Жоғарыдағы 2-кестенің деректерін талдау негізінде автоматтандырылған тәсіл тиімділіктің негізгі көрсеткіштері бойынша дәстүрлі әдістерден едәуір асып түседі деген қорытынды жасауға болады. Осылайша, салыстырмалы талдау ұсынылған автоматтандырылған әдістеме дәстүрлі сараптамалық-бағалау тәсілдеріне қарағанда ақпараттық қауіпсіздік тәуекелдерін басқару кезінде тиімділіктің, сенімділіктің және ашықтықтың жоғары деңгейін қамтамасыз ететінін растайды. Кесте деректері автоматтандырылған тәсілдің артықшылықтарын айқын көрсетеді: талдау уақытының 65 %-ға қысқаруы, есептеу дәлдігінің 95 %-ға дейін артуы, және адам факторының ықпалының жойылуы. Тәуекелдерді бағалаудың тағы бір маңызды құралы - Zabbix, Nagios немесе Prometheus сияқты бақылау жүйелері. Бұл жүйелер АТ инфрақұрылымының күйін үздіксіз бақылауға және ықтимал тәуекелдер болуы мүмкін мәселелер туралы сигнал беруге мүмкіндік береді [9].

Күдікті қосылымдарды анықтау үшін Zabbix-Тегі бақылау ережелерін конфигурациялау мысалы:

 # Создание шаблона для мониторинга подозрительных подключений по определенным портам

UserParameter=custom.tcp_conn[*],netstat -an | grep -w tcp | grep ':$1' | wc -l

Бұл ереже көрсетілген порттағы TCP қосылымдарының санын бақылайды. Егер қосылымдардың саны күрт өссе, бұл ықтимал шабуылды көрсетуі мүмкін және жүйе әкімшіні ескертуі мүмкін. Zabbix бақылау жүйесінің интерфейсіндегі қосылымдар саны бойынша динамикалық деректері бар графиктер төмендегі суретте көрсетілген (сурет 4).



Сурет 4. Zabbix бақылау жүйесінің интерфейсі
(қосылымдар саны бойынша динамикалық деректері бар графиктер)

Гипотезаны тексеру және нәтижелерді түсіндіру

Зерттеудің негізгі гипотезасы тәуекелдерді бағалау процестерін автоматтандыру адам факторының әсерін азайту арқылы талдаудың дәлдігі мен жеделдігін арттырады.

Дәстүрлі және автоматтандырылған тәсілдердің нәтижелерін салыстыру олардың дұрыстығын растады. Әзірленген модельді қолдану талдау уақытын 60%-дан астамға дейін қысқартуға, есептеу дәлдігін 95%-ға дейін арттыруға, сондай-ақ Openvas және Zabbix деректерін біріктіру арқылы қауіптерді анықтаудың толықтығын арттыруға мүмкіндік берді. Сонымен қатар, нәтижелерді түсіндірудегі субъективті ауытқуларды жоюға болады. Автоматтандырылған тәсіл нәтижелердің тұрақтылығы мен қайталануын көрсетті, бұл оның

GRC және Siem корпоративтік жүйелеріне интеграциялау үшін практикалық қолданылуын растайды. Осылайша, ұсынылған гипотеза толығымен расталды: автоматтандырылған әдіс дәстүрлі сараптамалық әдістермен салыстырғанда анағұрлым сенімді, объективті және тиімді [10-11].

Зерттеу нәтижесінде бірқатар артықшылықтарға ие ақпараттық қауіпсіздік тәуекелдерін бағалаудың заманауи жүйесі құрылды:

- деректермен басқарылады – қауіптер мен осалдықтардың объективті көрсеткіштеріне негізделген;
- жедел – тәуекелдерді тез анықтауды және шешім қабылдауды қамтамасыз етеді;
- интеграцияланған – GRC және SIEM платформаларымен өзара әрекеттеседі;
- адаптивті – желі параметрлері өзгерген кезде автоматты түрде жаңартылады.

Автоматтандыру тәуекелдерді интеллектуалды басқарудың негізін құрайтын тұрақты және қайталанатын әдістемені жасауға мүмкіндік берді. Алынған нәтижелер киберқауіпсіздік саласында автоматтандыруды қолданудың теориялық және практикалық аспектілерін одан әрі талқылауға негіз болады.

Дискуссия

Зерттеу нәтижелері ақпараттық қауіпсіздік тәуекелдерін бағалау процестерін автоматтандыру талдаудың тиімділігі мен объективтілігін айтарлықтай арттырады деген гипотезаны растады. Сандық модельдер (FAIR, Монте-Карло, FTA) мен автоматтандыру құралдарының (OpenVAS, Metasploit, Zabbix, RiskWatch) тіркесіміне негізделген ұсынылған әдіс талдау уақытының айтарлықтай қысқаруын және есептеу дәлдігінің 95%-ға дейін жоғарылауын көрсетті.

Дәстүрлі әдістермен салыстыру автоматтандыру субъективті фактордың әсерін жоюға, деректердің қайталануын қамтамасыз етуге және тәуекелдерді бағалауды қауіпсіздікті басқарудың бірыңғай аналитикалық ортасына біріктіруге мүмкіндік беретінін көрсетті. Мұндай интеграция ISO/IEC 27005 және NIST sp 800-30 заманауи тәсілдеріне сәйкес келетін үздіксіз «мониторинг – талдау – жауап беру» циклін қалыптастырады.

Зерттеудің теориялық маңыздылығы модельдеу және автоматтандырылған аналитика әдістерін біріктіретін цифрлық тәуекел менеджменті тұжырымдамасын дамыту болып табылады [12, 13].

Практикалық құндылық - тәуекелдерді тұрақты бақылау, аудит және болжау үшін корпоративтік және білім беру инфрақұрылымдарына модельді енгізу мүмкіндігінде.

Қол жеткізілген нәтижелерге қарамастан, әдістемеде шектеулер бар: бастапқы деректердің сапасына тәуелділік және әртүрлі құралдар арасындағы форматтарды үйлестіру қажеттілігі. Әрі қарайғы зерттеулердің болашағы машиналық оқытуды енгізумен, инфрақұрылымның цифрлық егіздерін дамытумен және интеллектуалды ерте ескерту жүйелерін (supervision-модельдер) құрумен байланысты [14, 15].

Осылайша, талқылау тәуекелдерді бағалауды автоматтандыру дәстүрлі сараптамалық тәсілдерден деректерге, модельдеуге және болжамды аналитикаға негізделген интеллектуалды киберқауіпсіздікті басқаруға көшуді қалыптастыратынын растайды.

Қорытынды

Жүргізілген зерттеу ақпараттық қауіпсіздік тәуекелдерін бағалау процестерін автоматтандыру талдаудың дәлдігін, жеделдігін және қайталануын арттырудың тиімді құралы екенін дәлелдеді.

Аналитикалық модельдерді (FAIR, Монте-Карло, FTA) бағдарламалық құралдармен (OpenVAS, Metasploit, Zabbix, Python, RiskWatch) біріктіруге негізделген әзірленген әдіс объективті деректерге бағытталған және адам факторының әсерін болдырмайтын тәуекелдерді басқарудың кешенді жүйесін құруға мүмкіндік берді.

Нәтижесінде тәуекелдерді талдау уақыты 60% - дан астамға қысқарды және есептеу дәлдігі 95% - ға жетті, бұл зерттеу гипотезасын растайды.

Әдістеме жоғары бейімделгіштікке ие, корпоративті GRC және SIEM жүйелерімен біріктірілген және тәуекелдерді үнемі бақылау және болжау үшін әртүрлі көлемдегі ұйымдарда қолданылуы мүмкін. Нәтижелер цифрлық егіздер мен Supervision-қауіптерді ерте анықтау үлгілерін қамтитын зияткерлік тәуекел менеджменті бағытында одан әрі зерттеулердің негізін құрайды.

Осылайша, ұсынылған жүйе цифрлық трансформация жағдайында заманауи, интеллектуалды және тұрақты киберқауіпсіздік архитектурасын құрудың практикалық негізін құрайды. Алынған нәтижелер зерттеу гипотезасын толық растады және ақпараттық қауіпсіздік тәуекелдерін автоматтандырылған түрде бағалаудың тиімділігін дәлелдеді. Зерттеудің келесі кезеңінде модельді жетілдіру мақсатында машиналық оқыту элементтерін (Random Forest, Logistic Regression, Gradient Boosting) және цифрлық егіздер (Digital Twin) технологияларын енгізу жоспарлануда. Бұл тәсіл тәуекелдерді болжаудың дәлдігін арттырып, инфрақұрылымның цифрлық бейнесі негізінде Supervision-модельдерге көшуге мүмкіндік береді. Сонымен қатар, әзірленген әдістемені нақты корпоративтік және мемлекеттік ақпараттық жүйелерге бейімдеу арқылы тәуекелдерді интеллектуалды басқарудың ұлттық платформасын құру бағытында қолданбалы зерттеулер жалғастырылады.

Пайдаланылған дереккөздердің тізімі

[1] FAIR Institute. (2025). Factor Analysis of Information Risk (FAIR) Model. Standard Artifact |Version 3.0. 2025. All Rights Reserved.

[2] ISO/IEC 27001:2013. (2025). Information technology – Security techniques – Information security management systems – Requirements. Online Browsing Platform (OBP). URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

[3] National Institute of Standards and Technology. (2020). NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations. 2020. URL: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

[4] Device42 Freshworks Inc. (2025). NIST CSF Categories: Description, Examples, and Best Practices. URL: https://www.device42.com/compliance-standards/nist-csf-categories/

[5] Миркасимова, Т., Адилжанова, С., Астаубаева, Г., & Мухамеджанова, Г. (2025). Ақпараттық қауіпсіздік тәуекелдерін талдау және бағалау әдістері. ҚазККА хабаршысы, 138(3). 203–216. https://doi.org/10.52167/1609-1817-2025-138-3-203-216

[6] Scarfone, K., Mell, P., & Johnson, J. (2018). Vulnerability management using OpenVAS: Best practices and implementation methods. International Journal of Information Security Science, 7(4), 25–36.

[7] Rapid7. (2022). Metasploit Framework User Guide. Rapid7 Security, Boston.

[8] RiskWatch International LLC. (2023). RiskWatch Cyber Risk Assessment Platform: Product Overview and Methodology. Available at: https://www.riskwatch.com/resourcelibrary/

[9] Zabbix LLC. (2023). Zabbix 6.4 Documentation: Distributed Monitoring and Security Alerts. Retrieved from https://www.zabbix.com/documentation

[10] Ruohonen, J., Hjerppe, K., & Rindell, K. (2021). A Large-Scale Security-Oriented Static Analysis of Python Packages in PyPI. arXiv. https://doi.org/10.48550/arXiv.2107.12699

[11] Stefanov, M. (2025). Exploring the potential of artificial intelligence to predict cyber threats. Engineering for Rural Development. https://doi.org/10.2478/etr-2025-0016

[12] Sommestad, T., Ekstedt, M., & Holm, H. (2013). The cyber security modeling language: A tool for assessing the vulnerability of enterprise system architectures. IEEE Systems Journal, 7(3), 363–373.

[13] O'Brien, J., & Marakas, G. (2020). Management Information Systems: Managing the Digital Firm. Pearson Education.

[14] Adilzhanova, S., Igilmanov, A., Tyulepberdinova, G., Salmanova, A., & Amirkhanova, G. (2024). The use of log analysis to identify DoS attacks and determine user behavior during the development of a digital twin of a food industry enterprise. KazATK, 136(1), 96–107. https://doi.org/10.52167/1609-1817-2025-136-1-96-107

[15] Adilzhanova S., Mirkassimova T., Amirkhanova G., Kunelbayev M. (2025) The application of digital twins in assessing information security risks. Proc. of International Conference on Artificial Intelligence, Computer, Data Sciences and Applications (ACDSA 2025) 7-9 August 2025, Antalya-Türkiye. DOI: 10.1109/ACDSA65407.2025.11166331

References

[1] FAIR Institute. (2025). Factor Analysis of Information Risk (FAIR) Model. Standard Artifact |Version 3.0. 2025. All Rights Reserved.

[2] ISO/IEC 27001:2013. (2025). Information technology – Security techniques – Information security management systems – Requirements. Online Browsing Platform (OBP). URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

[3] National Institute of Standards and Technology. (2020). NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations. 2020. URL: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

[4] Device42 Freshworks Inc. (2025). NIST CSF Categories: Description, Examples, and Best Practices. URL: https://www.device42.com/compliance-standards/nist-csf-categories/

[5] Mirkassimova, T., Adilzhanova, S., Astaubaeva, G., & Mukhamedzhanova, G. (2025). Methods of analysis and assessment of information security risks. KazATC Bulletin, 138(3). 203–216. https://doi.org/10.52167/1609-1817-2025-138-3-203-216

[6] Scarfone, K., Mell, P., & Johnson, J. (2018). Vulnerability management using OpenVAS: Best practices and implementation methods. International Journal of Information Security Science, 7(4), 25–36.

[7] Rapid7. (2022). Metasploit Framework User Guide. Rapid7 Security, Boston.

[8] RiskWatch International LLC. (2023). RiskWatch Cyber Risk Assessment Platform: Product Overview and Methodology. Available at: https://www.riskwatch.com/resourcelibrary/

[9] Zabbix LLC. (2023). Zabbix 6.4 Documentation: Distributed Monitoring and Security Alerts. Retrieved from https://www.zabbix.com/documentation

[10] Stefanov, M. (2025). Exploring the potential of artificial intelligence to predict cyber threats. Engineering for Rural Development. https://doi.org/10.2478/etr-2025-0016

[11] Ruohonen, J., Hjerppe, K., & Rindell, K. (2021). A Large-Scale Security-Oriented Static Analysis of Python Packages in PyPI. arXiv. https://doi.org/10.48550/arXiv.2107.12699

[12] Sommestad, T., Ekstedt, M., & Holm, H. (2013). The cyber security modeling language: A tool for assessing the vulnerability of enterprise system architectures. IEEE Systems Journal, 7(3), 363–373.

[13] O'Brien, J., & Marakas, G. (2020). Management Information Systems: Managing the Digital Firm. Pearson Education.

[14] Adilzhanova, S., Igilmanov, A., Tyulepberdinova, G., Salmanova, A., & Amirkhanova, G. (2024). The use of log analysis to identify DoS attacks and determine user behavior during the development of a digital twin of a food industry enterprise. KazATK, 136(1), 96–107. https://doi.org/10.52167/1609-1817-2025-136-1-96-107

[15] Adilzhanova S., Mirkassimova T., Amirkhanova G., Kunelbayev M. (2025) The application of digital twins in assessing information security risks. Proc. of International Conference on Artificial Intelligence, Computer, Data Sciences and Applications (ACDSA 2025) 7-9 August 2025, Antalya-Türkiye. DOI: 10.1109/ACDSA65407.2025.11166331