ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2025»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2025»

PROCEEDINGS
of the XX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2025»

2025
Астана

УДК 001(06)
ББК 72я631
F96

«ǴYLYM JÁNE BILIM – 2025» студенттер мен жас ғалымдардың XX Халықаралық ғылыми конференциясы = XX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2025» = The XX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2025». – Астана: – 3813 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-08-5373-7

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.В сборник вошли доклады студентов, магистрантов, докторантов имолодыхученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001(06)
ББК 72я431
F96

ISBN 978-601-08-5373-7

Л.Н. Гумилев атындағы Еуразия ұлттық университеті, 2025

СЕКЦИЯ 2

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ И КОММ УНИКАЦИОННЫЕ ТЕХНОЛОГИИ

Подсекция 2.2

Интеллектуальные информационные системы

255.	Сафонова Софья Александровна «Современные аспекты информационной безопасности в облачных вычислениях: модели, угрозы и методы защиты»	1034
256.	Смаилова Назгүл Батырбекқызы «Терең оқыту арқылы кітап ұсыныстарын әзірлеу: collaborative filtering, content-based және nlp әдістерінің комбинациясы»	1041
257.	Тажібай Аружан Айдосқызы, Кудубаева Сауле Альжановна «Көру қабілеті әлсіз адамдарға арналған аі дауыстық көмекші: нақты уақытта объектілерді анықтау және қашықтықты бағалау»	1046
258.	Тайжанов Азамат Жанкелдіұлы «Python тілінде фильмдердің интеллектуалды ұсыныс жүйесін әзірлеу»	1051
259.	Умирзахов Сундетали Кабылбекович «Сұраныстарды интеллектуалды талдау негізінде ұйымның сайты үшін чат-бот құру»	1055
260.	Шайхстан Марғұлан «IOT Сенсорлары негізінде ауа ластану деңгейін болжау»	1060

Подсекция 2.3

Современные тенденции в программной инженерии и управлении в условиях цифровой индустрии

261.	Bekenova A.B. «Development of a registration panel for users and doctors with integration into the database»	1077
262.	Bolat A.Zh. «Data analysis methods and decision making using big data and machine learning tools»	1081
263.	Алтайұлы А. «Visual studio интегралды ортасында «қойма қызметкерлеріне арналған» мәліметтер қорын жобалау»	1086
264.	Арап А.Қ. «Ақылды сурет салушы роботты әзірлеу»	1088
265.	Артыкбекқызы А. «Ақылды үйлердегі заттар интернеті(iot) мен робототехниканың өзара әрекеттесуі»	1091
266.	Ахметова А.Д. «Тоңазытқыштағы өнімдерді бақылауға және тағам әзірлеу ұсынысын беруге арналған программалық қосымша»	1096
267.	Дәрібай Д.Д. «Робототехниканы қолдану арқылы қойма логистикасындағы қолданыстағы басқару жүйелерін талдау»	1100
268.	Жамбулов С.Ж. «Білім алушыларды информатика және программалау олимпиадаларына дайындауда жасанды интеллекттің қолданысы»	1102
269.	Каиржан Р.С. «Development of system for recognition of emotional states of employees based on computer vision methods on Raspberry Pi»	1108
270.	Кайрекенова Н.Р. «Өнеркәсіптік роботты көру үшін машиналық оқытудың заманауи тәсілдері: әдістер, деректер жиынтығы және оптимизациялау»	1111

СЕКЦИЯ 3
ЕСТЕСТВЕННЫЕ НАУКИ

2. Петров П.П. Методы защиты данных в ИТ-системах. — СПб.: Наука, 2019. — 256 с.
3. Сидоров С.С. Машинное обучение и его безопасность. — Новосибирск: Сибирская академия, 2021. — 190 с.
4. Андреев А.А. Защита искусственного интеллекта от атак. — Екатеринбург: Уральский университет, 2020. — 210 с.
5. Федоров Ф.Ф. Проблемы анализа и защиты ИИ. — Казань: Прогресс, 2018. — 150 с.
6. Беляев Б.Б. Технологии защиты ИИ. — М.: ИнфоТех, 2022. — 275 с.
7. Маликов М.М. Дифференциальная приватность в анализе данных. — Ростов-на-Дону: ЮФУ, 2021. — 180 с.
8. Гусев А.А. Методы федеративного обучения. — Тюмень: ТюмГУ, 2020. — 160 с.
9. Николаев В.Н. Реверс-инжиниринг нейросетевых архитектур. — СПб.: Лань, 2022. — 195 с.
10. Шевченко И.И. Атаки на искусственный интеллект. — М.: Альфа, 2020. — 210 с.
11. Черников В.В. Обфускация и шифрование в защите ИИ. — М.: Научный мир, 2019. — 230 с.
12. Лазарев А.А. Атаки на данные в моделях ИИ. — Саратов: СГУ, 2021. — 265 с.
13. Козлов И.П. Проблемы защиты ИИ от атак на входные данные. — Екатеринбург: Уралмаш, 2021. — 150 с.

УДК 004.056

NEUVECTOR ЖӘНЕ KUBERNETES: КОНТЕЙНЕРЛІК ОРТАДАҒЫ ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ ТӘСІЛДЕРІ

Ерболатова Айдана Жасұланқызы
erbolatovaaidanaa@gmail.com
Л.Н. Гумилев атындағы ЕҰУ Ақпараттық қауіпсіздік мамандығының
2 курс магистранты, Астана, Қазақстан
Ғылыми жетекшісі – Оспанова А. Б.

Аннотация: Бұл мақалада **Kubernetes** контейнерлік ортасының қауіпсіздік архитектурасына теориялық талдау жүргізіліп, **NeuVector** шешімін желілік трафикті қорғау, шабуылдардың алдын алу және **Zero Trust** моделін жүзеге асыру үшін пайдалану мәселесіне баса назар аударылды. **Kubernetes** жүйесінің негізгі қауіпсіздік механизмдері, соның ішінде **RBAC, Admission Controllers** және желілік саясаттар қарастырылып, олардың шектеулері талданды. **NeuVector** шешімінің мүмкіндіктеріне, атап айтқанда **DPI** технологиясы, қауіптерді автоматты түрде анықтау және **CI/CD** процестерімен интеграциялау механизмдеріне жан-жақты шолу жасалды. Зерттеу барысында желілік сегментацияны жүзеге асыру, **DDoS** шабуылдарынан қорғау әдістері және қауіптерді модельдеу мәселелері зерттелді. **NeuVector** және **Kubernetes** жүйелерінің ықтимал осалдықтары белгілі **CVE** деректері негізінде талданып, контейнерлік орталардың автоматтандырылған қауіпсіздігін дамытуға қатысты болашақ бағыттар қарастырылды.

Кілт сөздер: NeuVector, Kubernetes, Kubernetes компоненттері, контейнер қауіпсіздігі.

Kubernetes-тің бұлттық және жергілікті инфрақұрылымдарда кеңінен таралуымен контейнерлік орталардың қауіпсіздігін қамтамасыз ету қажеттілігі артып келеді. Контейнерлеу қосымшаларды орналастыруды және басқаруды жеңілдетеді, бірақ сонымен қатар контейнерлердің бұзылуы, деректердің сыртқа шығуы және контейнерлер арасындағы өзара әрекеттесулердегі осалдықтарды пайдалануға қатысты жаңа шабуыл векторларын тудырады. Red Hat-тың **State of Kubernetes Security** есебіне сәйкес, ұйымдардың 93%-ы контейнерлік ортадағы қауіпсіздік инциденттерімен бетпе-бет келген, бұл кешенді шешімдердің қажеттілігін растайды [1].

Kubernetes контейнерлік орталардың икемділігі мен ауқымдылығын қамтамасыз етеді, алайда оның күрделі архитектурасы қосымша қауіпсіздік қатерлерін тудырады. Конфигурациядағы қателіктер, API-дің жеткіліксіз қорғалуы және аутентификация механизмдерінің әлсіздігі кластердің бұзылуына әкелуі мүмкін. **Red Hat State of Kubernetes Security** есебіне сәйкес, инциденттердің шамамен 55%-ы қате баптаулармен, ал 38%-ы осал контейнерлерге байланысты [2].

Қазіргі заманғы контейнерлеу есептеу орталарын қорғау көпдеңгейлі тәсілді талап етеді, ол қауіпсіздіктің әртүрлі аспектілерін – операциялық жүйе ядросы деңгейінен бастап кластердегі қызметтер арасындағы желілік өзара әрекеттесуге дейін қамтуы тиіс. Контейнерлер оркестрациясының жетекші платформасы болып табылатын Kubernetes кіріктірілген қауіпсіздік механизмдерін ұсынады. Алайда, олардың функционалы қазіргі заманғы қауіп-қатерлерге қарсы тұруға жеткіліксіз, сондықтан қосымша қорғау тетіктерін енгізу қажеттігі туындайды. Kubernetes кластерлерінің негізгі қауіптері контейнерлік ортадағы осалдықтарды пайдалануды, есептеу тораптарының бұзылуын, контейнерлер арасындағы байланыстарға шабуылдарды, сондай-ақ API-серверге рұқсатсыз қол жеткізуді қамтиды. Kubernetes қауіпсіздігі бірнеше деңгейде іске асырылады [3]: **операциялық жүйе ядросы деңгейі**; к**онтейнер деңгейі**; о**ркестрация деңгейі** және ж**елілік деңгей**. Kubernetes-тің көпдеңгейлі қауіпсіздік моделі жүйенің сыртқы және ішкі қауіп-қатерлерге төзімділігін арттырып, ықтимал қауіптерді барынша азайтуға мүмкіндік береді. Kubernetes кластерлерінің қауіпсіздігін қамтамасыз ету үшін қолжетімділікті басқару және сұраныстарды тексеру механизмдерін қолдану қажет. Бұл процесте **Role-Based Access Control** және **Admission Controllers** маңызды рөл атқарады, себебі олар рұқсатсыз әрекеттердің алдын алып, жүйенің қауіпсіздігін күшейтеді. **Role-Based Access Control** – кластер шегінде қандай субъектілер белгілі бір операцияларды орындай алатынын анықтайтын рөлдік қолжетімділікті басқару механизмі [4]. **Admission Controllers** – API-серверге жасалатын сұраныстарды өңдеу сатысында реттейтін саясаттар жиынтығы [5]. Бұл механизмдер Kubernetes ортасының қауіпсіздігін арттырып, кластердегі деректер мен ресурстарды қорғауға көмектеседі.

Kubernetes кластеріндегі желілік қауіпсіздік контейнерлер арасындағы өзара әрекеттесуді реттеуде маңызды рөл атқарады. Желілік саясаттар трафикті басқаруға мүмкіндік бергенімен, олардың кейбір шектеулері бар, бұл қауіпсіздік деңгейін төмендетуі мүмкін. Сондықтан желілік саясаттардың мүмкіндіктерін, олардың шектеулерін талдап, қауіпсіздікті арттыру жолдарын қарастыру өзекті мәселе болып табылады. Қауіпсіздік деңгейін арттыру үшін **NeuVector** сияқты мамандандырылған шешімдерді қолдану ұсынылады. Бұл құралдар трафикті кеңейтілген сүзгілеу, аномалияларды анықтау және нақты уақыт режимінде қауіп-қатерлердің алдын алу механизмдерін қамтамасыз етеді. Kubernetes кіріктірілген қауіпсіздік механизмдеріне ие болғанымен, ол барлық ықтимал қауіп-қатерлерден кешенді қорғаныстыны қамтамасыз ете алмайды [6]. Kubernetes кластерінің қауіпсіздігін күшейту үшін қосымша шараларды енгізу қажет. Оларға трафикті мінез-құлықтық талдау жүйелерімен интеграциялау, қауіп-қатерлерді автоматтандырылған түрде анықтау және қолжетімділікті басқаруда **Zero Trust** концепциясын қолдану жатады.

NeuVector – контейнерленген орталарды қорғауға арналған кешенді шешім, ол желіні егжей-тегжейлі бақылау, шабуылдардың алдын алу және қауіп-қатерлерге автоматтандырылған жауап беру мүмкіндіктерін ұсынады. Бұл құрал **Kubernetes** кластерлерінің қауіпсіздігіне бағытталған және нақты уақыт режимінде желіні сегментациялау, трафиктің мінез-құлықтық талдауын жүргізу, сондай-ақ аномалиялық белсенділікті бұғаттау механизмдерін жүзеге асырады. **NeuVector** архитектурасының үш негізгі компоненті 1-ші кестеде көрсетілген [7].

Компонент	Сипаттама
Enforcer	Кластер түйіндерінде орналастырылатын агент, ол желілік трафикті талдайды, қауіпсіздік саясаттарын қолданады және күдікті қосылымдарды бұғаттайды.
Scanner	Контейнерлік образдарды орналастыру алдында олардың осалдықтары мен ықтимал қауіптерін талдауға арналған компонент
Controller	Қауіпсіздік саясаттарын өңдеуге, оқиғаларды басқаруға және жүйенің жұмысын үйлестіруге жауапты орталық басқарушы түйін.

Кесте – 1. NeuVector компоненттері

NeuVector-дің негізгі механизмдерінің бірі – Stateful Deep Packet Inspection (DPI), яғни күйге тәуелді терең пакет инспекциясы. Бұл әдіс желілік трафиктегі аномалияларды анықтауға, контейнерлер арасындағы өзара әрекеттесуді талдауға және осалдықтарды пайдалануға бағытталған шабуылдар мен деректердің сыртқа таралуын болдырмауға мүмкіндік береді. Сонымен қатар, NeuVector трафиктің мінез-құлықтық талдауын қолданады [8]. Бұл әдіс қолданбалардың қалыпты жұмысынан ауытқуларды анықтауға, белсенділікті алдын ала белгіленген үлгілер бойынша жіктеуге және күдікті әрекеттерге автоматтандырылған түрде әрекет етуге мүмкіндік береді. Қолданбаның өмірлік циклінің барлық кезеңдерінде қауіпсіздікті қамтамасыз ету үшін **NeuVector** үздіксіз интеграция және орналастыру **(CI/CD)** процестерімен, сондай-ақ **DevSecOps** әдіснамасымен интеграцияланады.

Kubernetes ортасындағы желілік қауіп-қатерлерді азайту үшін **Zero Trust** және **Microsegmentation** сияқты тиімді сегментация модельдерін қолдану қажет. **Zero Trust** концепциясы қатаң қолжетімділік бақылауына және түйіндер арасындағы сенімділікті барынша шектеуге негізделген. Бұл тәсіл кез келген желілік белсенділік оның шығу тегіне қарамастан тексеріліп, рұқсат етілуі тиіс деген қағиданы ұстанады. **Microsegmentation** жұмыс жүктемелерін желілік өзара әрекеттесу деңгейінде оқшаулауға мүмкіндік береді, осылайша ықтимал шабуыл векторларын шектейді. Бұл модельдерді **Kubernetes** кластерлеріне енгізу қауіпсіздік деңгейін айтарлықтай арттырады, рұқсатсыз қолжетімділік қаупін азайтады, шабуылдардың таралуын болдырмайды және деректердің сыртқа таралуының алдын алады. **NeuVector** желілік трафикті егжей-тегжейлі бақылауды және шабуылдардың алдын алуды қамтамасыз ететін динамикалық желілік сегментацияны іске асырады. **NeuVector**-дің желілік сегментация саласындағы негізгі мүмкіндіктері мыналарды қамтиды:

- **L7 деңгейіндегі желілік өзара әрекеттесулерді бақылау**.
- **Нақты уақыт режимінде бейімделетін қауіпсіздік саясаттарын қолдану**.
- **Күдікті қосылымдарды автоматтандырылған түрде анықтау және бұғаттау**.

Осы мүмкіндіктер **NeuVector**-ді **Kubernetes** кластерлерін қорғаудың жетекші құралдарының бірі етеді, сервистердің сенімді оқшауланuын және желілік деңгейдегі шабуылдардың алдын алуды қамтамасыз етеді.

Контейнерлік ортада қауіпсіздікті қамтамасыз ету үшін ықтимал шабуыл түрлерін жан-жақты зерттеу маңызды. Kubernetes ортасы динамикалық және масштабталатын болғандықтан, ол күрделі желілік шабуылдарға, соның ішінде DDoS шабуылдарына ұшырауы мүмкін. **DDoS шабуылдары Kubernetes** кластерлері үшін елеулі қауіп төндіреді, себебі олар қызмет көрсетуден бас тартуға, есептеу ресурстарының сарқылуына және контейнерлік қосымшалардың істен шығуына әкелуі мүмкін. **Kubernetes** үшін өзекті **DDoS** шабуылдарының негізгі түрлері 2-ші кестеде көрсетілген [9].

Шабуыл түрі	Сипаттама
Kubernetes API-серверіне бағытталған шабуылдар	Шабуылдаушылар **Kubernetes API** серверіне үлкен көлемде сұраныстар жіберіп, оны шамадан тыс жүктейді және қызмет көрсетуді тоқтатуға мәжбүрлейді.
Жалған контейнерлік образдарды жүктеу арқылы ресурстарды азайту	Шабуыл барысында үлкен көлемдегі контейнерлік образдар жаппай жүктеліп, түйіндерді шамадан тыс жүктейді, нәтижесінде диск кеңістігі мен желілік ресурстар таусылады.
Pod-тар арасындағы өзара әрекеттесуді пайдалану	Желілік өзара әрекеттесудің осал тұстарын пайдалану арқылы шабуылдаушылар кластер ішінде бақылаусыз өсетін трафик ағынын туындатып, жүйені тұрақсыздандырады.
Kube-proxy осалдықтарын пайдалану	Шабуылдаушылар k**ube-proxy**-дің әлсіз прокси ережелерін пайдаланып, рекурсивті сұраныстарды тудырады және жүйені істен шығарады.

Кесте – 2. Kubernetes үшін өзекті **DDoS** шабуылдарының негізгі түрлері

Kubernetes жүйесіндегі ықтимал осалдықтарды анықтау және оларды тиімді түрде бейтараптандыру маңызды міндет болып табылады. NeuVector қауіпсіздік платформасы бұл қауіптерді анықтау және жою үшін жетілдірілген механизмдерді ұсынады. 3-ші кестеде Kubernetes жүйесінде 2024 жылы жиі кездескен осалдықтар, сондай-ақ олардан қорғану үшін NeuVector ұсынатын шешімдер көрсетілген [10-11].

Осалдық	Осалдық сипаттамасы	NeuVector шешімі
CVE-2024-9042 (Лог жүктемесінің артуы)	Windows негізіндегі Kubernetes түйіндерінде лог жүргізу жүйесінің осалдығы, ол шабуылдаушыға қашықтан код орындауға және жүйені лог файлдарымен шамадан тыс жүктеуге мүмкіндік береді.	Процестердің мінез-құлқын бақылау және аномалияларды анықтау. Күдікті әрекеттерді автоматты түрде бұғаттау.
CVE-2024-9486 (Образдардың осалдығы)	Kubernetes Image Builder құралындағы тіркелгі деректерінің әдепкі параметрлері арқылы шабуылдаушының түйіндерге root деңгейінде қол жеткізуіне мүмкіндік береді.	Контейнерлік образдарды орналастырмас бұрын осалдықтарын тексеру. Zero Trust желілік саясаты арқылы рұқсат етілмеген қосылымдарды шектеу.
DoS-шабуыл (Образдарды шамадан тыс жүктеу)	Ірі көлемдегі контейнерлік образдарды жаппай жүктеу арқылы жүйенің жұмысын баяулату.	Параллельді жүктеулер санын шектеу Rate-limiting орнату.

		Желідегі аномалды белсенділікті бақылау және бұғаттау.

Кесте – 3. Kubernetes жүйесіндегі осалдықтар және NeuVector қорғау механизмдері

Kubernetes жүйесінің жұмыс жүктемелерін басқару мүмкіндіктері кең болғанымен, оның күрделі архитектурасы ықтимал шабуыл векторларының пайда болуына жол ашады. Негізгі қауіптерге кластерлік түйіндердің осалдануы, контейнерлік образдардың осалдықтарын пайдалану, желілік инфрақұрылымға жасалатын шабуылдар және деректердің сыртқа шығуы жатады. Дегенмен, кез келген қауіпсіздік жүйесі сияқты, NeuVector да осалдықтар мен конфигурация қателіктеріне ұшырауы мүмкін. Ықтимал қатерлерге: **NeuVector программасындағы қателіктер**; қауіпсіздік саясаттарының дұрыс емес конфигурациясы; **сенімді компоненттерге бағытталған шабуылдар және қауіпсіздік саясаттарын айналып өтетін шабуылдар жатады.** Кез келген басқа жүйе сияқты, NeuVector өзі де шабуыл нысанына айналуы мүмкін. NeuVector-ге бағытталған нақты шабуылдарға тоқталып өтетін болсақ, **аутентификация токендерінің бұзылуы CVE-2023-32188 осалдығы [12]**. Бұл осалдықта шабуылдаушы кері инженерия әдісін қолданып, NeuVector-дің аутентификация үшін қолданатын JWT-токенін иемденіп, оны қолдан жасап шығара алды. Бұл оған NeuVector API арқылы рұқсатсыз әрекеттерді орындауға, оның ішінде ерікті кодты орындауға мүмкіндік берді. Осалдықты жою үшін келесі әрекеттер жасалды:

– JWT токеніне қол қою үшін пайдаланылатын сертификат жүйені орнату және жаңарту кезінде автоматты түрде генерацияланады.

– Контроллер JWT қол қою сертификатын автоматты түрде жасайды, оның жарамдылық мерзімі **90 күн**.

– **Пайдаланушы анықтайтын сәйкестік скрипттерін қолдануға шектеу енгізілді.** Әдепкі жағдайда, мұндай скрипттерді қосуға тыйым салынады. Оларды іске қосу үшін **Enforcer** үшін **CUSTOM_CHECK_CONTROL** орта айнымалысын орнату қажет.

– LDAP инъекциясының алдын алу үшін пайдаланушы логині енгізілетін жерде арнайы символдарды өңдеу механизмі енгізілді.

CVE-2024-24791 осалдығы **5.3.3-r7** нұсқасына дейінгі **NeuVector** жүйелеріне әсер етіп, енгізілген деректерді дұрыс өңдемеу мәселесімен байланысты болды [13]. Бұл осалдық шабуылдаушыға **еркін кодты орындау**ға мүмкіндік берді. Аталған осалдықтың негізгі себебі **Go программалау тілінде** `net/http` стандартты кітапханасындағы қауіпсіздік кемшіліктеріне байланысты болды. Бұл кемшілік желілік қосылыстардың үзілуіне және **қызмет көрсетуден бас тарту** шабуылдарының орын алуына әкелуі мүмкін еді. Нәтижесінде, қауіпсіздік механизмдерін айналып өту, контейнерлерді бұзу және желілік сегментацияның тұтастығын бұзу қаупі туындады. Осалдықты жою мақсатында **NeuVector** келесі шараларды жүзеге асырды: тәуелділіктерді жаңарту және осал кодты түзету; API қауіпсіздік тексерістерін күшейту; журнал жүргізу және мониторинг механизмдерін кеңейту және қол жеткізуді басқару жүйесін жетілдіру. Қауіпсіздік қатерлерінің алдын алу үшін **Go** нұсқасын **1.21.12** немесе **1.22.5** деңгейіне дейін жаңарту ұсынылды. Бұл болашақта осындай шабуылдардың орын алу ықтималдығын барынша азайтуға мүмкіндік береді.

Бұл зерттеуде **Kubernetes** негізіндегі контейнерлік орталарда қауіпсіздікті қамтамасыз етудің архитектуралық қағидалары және **NeuVector** шешімінің осалдықтарды пайдалану, рұқсатсыз қол жеткізу және **DDoS** шабуылдарына байланысты қатерлерді азайтудағы рөлі қарастырылды.

Зерттеу барысында **NeuVector** жүйесіне бағытталған ықтимал шабуыл векторлары да анықталды. Атап айтқанда, оның сүзу және қорғау механизмдерін айналып өтуге бағытталған шабуылдар талданды. **Kubernetes** пен контейнерлік орталарға қатысты белгілі **CVE** осалдықтарын зерттеу кешенді қауіпсіздік тәсілін қолданудың маңыздылығын растады. Бұл тәсіл желілік трафикті мінез-құлықтық талдауды және қауіптерге проактивті ден қоюды қамтуы тиіс.

Осылайша, **NeuVector Kubernetes** кластерлерінің қауіпсіздігін күшейтуге арналған маңызды құрал болып табылады. Дегенмен, оны басқа қауіпсіздік әдістерімен үйлестіре отырып қолдану қажет. Болашақ зерттеулердің бағыттары ретінде машиналық оқытуға негізделген автоматтандырылған шабуылдарды анықтау жүйелерін әзірлеу және контейнерлік орталарға арналған **Threat Intelligence** модельдерін жетілдіру қарастырылады.

Қолданылған әдебиеттер тізімі

1. **Red Hat.** State of Kubernetes Security Report, 2024. Сілтеме: https://www.redhat.com/en/engage/state-kubernetes-security-report-2024.

2. **State of Kubernetes Security Report, 2024.** Сілтеме: https://static.carahsoft.com/concrete/files/3616/8252/7918/3-4_State_of_Kubernetes_Security_Report.pdf

3. **Дарвеш Г., Хаммуд Д., Воробьева А. А.** Security in Kubernetes: best practices and security analysis // Вестник УрФО. Безопасность в информационной сфере. – 2022. – № 2 (44). – С. 63-69.

4. **Rostami G.** Role-based access control (RBAC) authorization in Kubernetes // Journal of ICT Standardization. – 2023. – Т. 11. – № 3. – С. 237-260.

5. **Muslim A., Recker S.** Controller-Based Admission Control for Containers // 2024 IEEE International Conference on Cloud Engineering (IC2E). – IEEE, 2024. – С. 34-43.

6. **German K., Ponomareva O.** An overview of container security in a Kubernetes cluster // 2023 IEEE Ural-Siberian Conference on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT). – IEEE, 2023. – С. 283-285.

7. Cabianca D. Managing Security Operations //Google Cloud Platform (GCP) Professional Cloud Security Engineer Certification Companion: Learn and Apply Security Design Concepts to Ace the Exam. – Berkeley, CA : Apress, 2024. – С. 433-566.

8. **NeuVector Documentation.** Сілтеме: https://open-docs.neuvector.com/.

9. **Sadiq A. et al.** Detection of denial of service attack in cloud-based Kubernetes using eBPF // Applied Sciences. – 2023. – Т. 13. – № 8. – С. 4700.

10. **Red Hat Security Advisory.** CVE-2024-9042. Сілтеме: https://access.redhat.com/security/cve/cve-2024-9042.

11. **Red Hat Security Advisory.** CVE-2024-9486. Сілтеме: https://access.redhat.com/security/cve/cve-2024-9486.

12. **NeuVector Release Notes 5.x.** Сілтеме: https://open-docs.neuvector.com/5.2/releasenotes/5x.

13. **SUSE Security Advisory.** CVE-2024-24791. Сілтеме: https://www.suse.com/security/cve/CVE-2024-24791.html.

УДК 004.056.55

СТЕГАНОГРАФИЯ НА ОСНОВЕ LSB: РЕАЛИЗАЦИЯ СОКРЫТИЯ ДАННЫХ В МЕДИАФАЙЛАХ

Жанатаев Мирас Куанышевич