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

Бұл зерттеу аномалияларды анықтау әдістерін ақпараттық қауіпсіздік жүйелерін құру үшін қолдану мүмкіндіктерін талдауға бағытталған. Isolation Forest, Local Outlier Factor (LOF), One-Class SVM, K-Means және DBSCAN әдістерінің тиімділігі салыстырылды. Нәтижелер бойынша, ең тиімді аномалияларды анықтау құралдары ретінде Isolation Forest және LOF әдістері таңдалды. Бұл әдістер шынайы аномалияларды дәл және тұрақты түрде анықтап, ақпараттық қауіпсіздік жүйелерінің сенімділігін арттырады.

Ал K-Means әдісі аномалияларды анықтауда шамадан тыс сезімталдық танытып, жалған позитивтердің көптігіне әкелуі мүмкін, бұл оның ақпараттық қауіпсіздік жүйелерінде қолданылуын шектейді. DBSCAN және One-Class SVM әдістері де кейбір жағдайларда тиімді болуы мүмкін, бірақ олардың тұрақтылығы мен өнімділігі ақпараттық қауіпсіздік талаптарына толық сәйкес келе бермейді.

Зерттеу нәтижелері аномалияларды анықтау әдістерін ақпараттық қауіпсіздік жүйелерінде қолдану үшін маңызды нұсқаулықтар ұсынады. Isolation Forest және LOF әдістері жоғары дәлдік пен тұрақтылықпен аномалияларды анықтауға мүмкіндік береді, сондықтан олар ИБ жүйелерінде кеңінен қолдануға тиімді болып табылады. Болашақ зерттеулерде осы әдістерді жетілдіру мен әртүрлі жағдайларда сынақтан өткізу арқылы олардың тиімділігін одан әрі арттыруға болады.

Қолданылған әдебиеттер тізімі

1. Xu H. et al. Deep isolation forest for anomaly detection //IEEE Transactions on Knowledge and Data Engineering. – 2023. – Т. 35. – №. 12. – С. 12591-12604.

2. Попова И. А. Обнаружение аномалий в наборе данных с помощью алгоритмов машинного обучения без учителя Isolation Forest и Local Outlier Factor //StudNet. – 2020. – Т. 3. – №. 12. – С. 1460-1470.

3. Nuriddinovich K. S. Исследование обнаружения аномалий в сетевом трафике с использованием one-class svm //Journal of Modern Educational Achievements. – 2024. – Т. 1. – №. 1. – С. 214-222.

4. Ahmed M., Seraj R., Islam S. M. S. The k-means algorithm: A comprehensive survey and performance evaluation //Electronics. – 2020. – Т. 9. – №. 8. – С. 1295.

5. Deng D. DBSCAN clustering algorithm based on density //2020 7th international forum on electrical engineering and automation (IFEEA). – IEEE, 2020. – С. 949-953.

6. Котенко И. В. и др. Методика обнаружения аномалий и кибератак на основе интеграции методов фрактального анализа и машинного обучения //Информатика и автоматизация. – 2022. – Т. 21. – №. 6. – С. 1328-1358.

ӘӨЖ 004.056.5

КОРПОРАТИВТІК ЖЕЛІЛЕРДІ МОДЕЛЬДЕУ ЖӘНЕ ҚОРҒАУ

Бердибаев Коркем Сагындыкулы, Иманали Абылай Жандосұлы

b.korkem2004@gmail.com, imanali_05@mail.ru

Л. Н. Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультеті Ақпараттық қауіпсіздік жүйесі кафедрасының 3 курс студенттері, Астана, Қазақстан

Ғылыми жетекші – Казиева Назым Магидулловна

Бүгінгі цифрлық әлемде бизнес ақпараттық технологияларға толық тәуелді болғандықтан, корпоративтік желіні қорғау бірінші кезектегі маңызды міндетке айналады. Компаниялар күн сайын қарапайым вирустық шабуылдардан бастап, киберқылмыскерлердің

күрделі, үйлестірілген әрекеттеріне дейін көптеген қауіптерге тап болады. Мұндай жағдайда, деректердің ағып кетуі немесе желінің жұмысындағы іркіліс үлкен қаржылық шығындарға және беделге нұқсан келтіруге әкелуі мүмкін болғанда, корпоративтік желіні модельдеу және тиімді қорғау дағдылары ақпараттық қауіпсіздік саласындағы кез келген маман үшін өте маңызды.[3]

Бұл мақаланың мақсаты корпоративтік желілерді қорғаудың теориялық негіздеріне шолу жасау ғана емес, сонымен қатар желілерді модельдеуге арналған заманауи бағдарламалық құралдарды пайдалана отырып іске асырылуы мүмкін практикалық әдістерді көрсету болып табылады. Бұл құралдар шынайы желілердің модельдерін жасауға және бақыланатын ортада қорғаудың әртүрлі әдістерімен тәжірибе жасауға мүмкіндік береді, бұл оларды оқыту және дағдыларды жетілдіру үшін таптырмас құралға айналдырады.[4]

Біз желі инфрақұрылымын қалай дұрыс модельдеу керектігін, қандай негізгі қауіптер бар және оларды қалай болдырмауға болатынын қарастырамыз. Желілерді модельдеуге арналған танымал бағдарламалық құралдарды пайдалана отырып, межжелілік экрандарды баптаудың практикалық мысалдарына ерекше назар аударылады. Қадамдық нұсқаулар мен көрнекі мысалдар арқылы сіз теориялық концепциялардың нақты қауіпсіздік шараларына қалай айналатынын көре аласыз.

Бұл мақала студенттер мен ақпараттық қауіпсіздік саласындағы жаңадан бастаған мамандар үшін пайдалы нұсқаулық болуға бағытталған, оларға корпоративтік желілерді қорғаудың негіздерін түсінуге ғана емес, сонымен қатар осы қарқынды дамып келе жатқан салада жұмыс істеу үшін қажетті практикалық дағдыларды алуға көмектеседі.

Корпоративтік желіні модельдеу — нақты желілік инфрақұрылымның абстрактілі бейнесін жасау процесі. Ол желіні физикалық түрде орналастыруға дейін талдауға, жобалауға және оңтайландыруға мүмкіндік береді. Модельдеу желінің әртүрлі жағдайлардағы мінез-құлқын түсінуге, оның өнімділігін бағалауға және ықтимал осалдықтарды анықтауға көмектеседі.[5]

Негізгі принциптер:

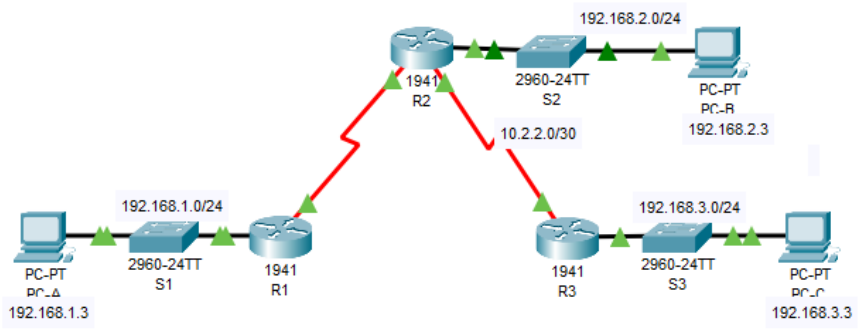
- Логикалық топология:
  - Деректердің желі арқылы қалай берілетінін сипаттайды.
  - IP-мекенжайын, VLAN, маршруттауды анықтайды.
  - Мысал: Бөлімдер мен серверлік аймақтарға бөлінген кәсіпорын желісінің құрылымы.

1 кесте. Логикалық топология.

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/0	192.168.1.1	255.255.255.0	N/A	S1 F0/1
	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	N/A	N/A
R2	G0/0	192.168.2.1	255.255.255.0	N/A	S2 F0/2
	S0/0/0	10.1.1.1	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.1	255.255.255.252	N/A	N/A
R3	G0/0	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	10.2.2.2	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/2
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S2 F0/1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

- Физикалық топология:
  - Құрылғылардың және қосылымдардың физикалық орналасуын сипаттайды.
  - Кабельдердің, коммутаторлардың, маршрутизаторлардың түрлерін қамтиды.

■ Мысал: Сервер бөлмесіндегі желілік жабдықтың орналасуы және оны қосу тәсілі.



1 сурет. Физикалық топология.

○ Желілерді модельдеуге арналған бағдарламадағы қарапайым топологияның мысалы:

■ Бұл суретте біз желідегі негізгі байланыстарды түсіну үшін бірнеше компьютер, бір коммутатор және маршрутизатор сияқты желінің негізгі құрылымын орналастырамыз.

Негізгі қауіптер:

○ Сыртқы қауіптер:

■ Хакерлік шабуылдар: Желіге рұқсатсыз кіру.

■ Вирустар мен зиянды бағдарламалық қамтамасыз ету: Жүйеге зиян келтіретін бағдарламалар.

○ Ішкі қауіптер:

■ Конфигурация қателері: Желілік жабдықты дұрыс баптамау.

■ Теріс пайдалану: Қызметкерлердің заңсыз әрекеттері.

○ Шабуылдардың негізгі түрлері:

■ DoS/DDoS шабуылдары: Желіні трафикпен шамадан тыс жүктеу.

■ Фишинг: Алдау арқылы деректерді ұрлау.

Қорғаудың негізгі құралдарына кіріспе:

○ Желіаралық экрандар (firewalls):

■ Кіріс және шығыс трафигін бақылайды.

■ Ережелер негізінде трафикті сүзгілейді.

○ Шабуылдарды анықтау жүйелері (IDS):

■ Күдікті әрекеттердің бар-жоғын трафикті талдайды.

■ Ықтимал шабуылдар туралы ескертеді.

○ Қол жеткізуді бақылау (ACL):

■ Қол жеткізуді бақылау тізімдері маршрутизатор немесе коммутатор интерфейсі арқылы қандай трафиктің өтуі мүмкін екенін анықтайды.

■ IP-мекенжайлары, порттар және хаттамалар негізінде трафикті сүзу үшін пайдаланылады.

Біз модельдеуге арналған бағдарламалық қамтамасыз ету мүмкіндіктерін пайдалана отырып, корпоративтік желілерді қорғаудың теориялық білімдерін практикалық қолдануға тереңірек кіреміз. Негізгі назар межжелілік экрандар, шабуылдарды анықтау жүйелері және виртуалды жеке желілер сияқты қауіпсіздіктің негізгі құралдарын баптау мен жұмысын көрсетуге аударылады.

Желілік қауіпсіздікте іргелі рөл атқаратын межжелілік экрандардан бастайық, олар трафикті бақылайды және берілген ережелер негізінде сүзеді. Олардың түрлері әртүрлі болуы

мүмкін: қарапайым пакеттік сүзгілерден бастап күрделі күйді қадағалайтын межжелілік экрандарға және веб-қосымшаларды қорғауға арналған мамандандырылған WAF-тарға дейін.

Біз трафикті басқару үшін кеңейтілген ACL-ді қалай баптау керектігін, қандай пакеттерге рұқсат етіліп, қандай пакеттерге тыйым салынғанын анықтайтынын көрсетеміз.[1]

```
enable
configure terminal

access-list 1 deny 192.168.1.0 0.0.0.255
access-list 1 permit any

interface FastEthernet0/0
ip access-group 1 out

access-list 101 deny tcp 192.168.1.0 0.0.0.255 any eq 80
access-list 101 permit ip any any

interface FastEthernet0/1
ip access-group 101 in

show access-lists

no access-list 1
no access-list 101
```

3 сурет. ACL-мен желілік трафикті фильтрлеу.

Содан кейін біз желідегі аномалиялар мен күдікті әрекеттерді анықтай отырып, қауіптерді бақылауға қызмет ететін шабуылдарды анықтау жүйелеріне көшеміз. IDS-нің желілік және хосттық жүйелерді қоса алғанда, әртүрлі түрлері бар. Біз порттарды сканерлеу немесе DoS шабуылдары сияқты нақты шабуыл түрлерін анықтау үшін негізгі IDS-ді қалай баптау керектігін көрсетеміз және оқиғалардың үрдістері мен оқиғаларын анықтау үшін IDS журналдарын қалай талдау керектігін көрсетеміз.[2]

Желінің үздіксіз жұмыс істеуін қамтамасыз ету үшін резервтік арналардың болуы және циклдардың алдын алу үшін STP сияқты хаттамаларды қолдану маңызды. Біз STP бар сақиналық топологияны қалай құруға болатынын және желі қауіпсіздігін күшейту үшін Cisco IOS командаларын қалай пайдалануға болатынын көрсетеміз.

Корпоративтік желіні модельдеу желіні нақты орналастыруға дейін талдауға, жобалауға және оңтайландыруға мүмкіндік беретін маңызды кезең болып табылады. Бұл тек ықтимал осалдықтарды анықтауға ғана емес, сонымен қатар желі жұмысының тиімділігін айтарлықтай арттыруға мүмкіндік береді. Межжелілік экрандар алдыңғы қатарлы қорғаныс болып табылады, трафикті бақылайды және рұқсатсыз кіруге жол бермейді, ал шабуылдарды анықтау жүйелері желіні үнемі бақылап, күдікті әрекеттерді анықтап, ескертеді. Резервтік арналар көмегімен ақауларға төзімді желілерді құру жұмыстың үздіксіздігін және қауіпсіз қашықтағы қол жеткізуді қамтамасыз етеді.

Корпоративтік желіні қорғау үздіксіз процесс екенін атап өту қажет. Бағдарламалық жасақтама мен дерекқорларды үнемі жаңарту, сондай-ақ желілік трафикті тұрақты бақылау талап етіледі. Бұлтты есептеу және заттар интернеті сияқты технологиялардың қарқынды дамуын ескере отырып, ақпараттық қауіпсіздік саласындағы соңғы үрдістерден хабардар болу маңызды.

Желілерді модельдеу арқылы білімді практикалық қолдану ақпараттық қауіпсіздік бойынша білікті мамандарды даярлаудың ажырамас бөлігі болып табылады. Желілерді модельдеуге арналған бағдарламалармен жұмыс істеу барысында алынған дағдылар қауіпсіз желі ортасын құру және қолдау арқылы теориялық білімді практикада тиімді қолдануға мүмкіндік береді.

Қолданылған әдебиеттер тізімі

1. Configure Commonly Used IP ACLs - Cisco Documentation
2. Современные проблемы безопасности корпоративных сетей - Н. Андреев
3. "Безопасность корпоративных сетей / Учебно-методическое пособие" - Биячуев Т.А., Осовецкого Л.Г.
4. "Построение защищенных корпоративных сетей" - Рашид Ачилов
5. "Практическая безопасность сетей" - NetSkills

УДК 004.056.5

АНАЛИЗ ВРЕДОНОСНЫХ ПРОГРАММ С ПОМОЩЬЮ ИИ И КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА

Ерболатов Али
alierbolatov9@gmail.com
Магистрант кафедры Информационной безопасности, Астана, Казахстан
Научный руководитель – Сантеева Сая Әділбайқызы, PhD, старший преподаватель

Аннотация: Статья посвящена анализу использования искусственного интеллекта (ИИ) для выявления и анализа вредоносных программ, а также рассмотрению криптографических методов защиты от таких угроз. С развитием технологий ИИ возрастает угроза их использования для создания вредоносных программ, что делает необходимым разработку эффективных механизмов защиты. В статье рассматриваются основные методы защиты ИИ, включая шифрование, обфускацию и дифференциальную приватность, а также способы их применения в контексте защиты от реверс-инжиниринга и атак. Особое внимание уделено интеграции ИИ и криптографических технологий для создания более безопасных и устойчивых к угрозам систем. Исследуются примеры реальных атак на модели ИИ и способы их предотвращения с использованием современных технологий защиты. Предложены рекомендации по усилению безопасности ИИ-моделей и перспективы развития в этой области.

Ключевые слова: искусственный интеллект, криптография, защита данных, вредоносные программы, реверс-инжиниринг, шифрование, обфускация, дифференциальная приватность, киберугрозы, атаки на данные, машинное обучение, безопасность ИИ.

Введение

С развитием технологий искусственного интеллекта (ИИ) в последние десятилетия они начинают играть ключевую роль в различных областях, таких как медицина, финансы, кибербезопасность и многие другие. Однако с увеличением применения ИИ возрастает и угроза его использования в злонамеренных целях, таких как создание вредоносных программ. Вредоносные программы, использующие ИИ, могут эффективно обходить традиционные методы защиты, что требует разработки более инновационных и гибких защитных систем [1, с. 18].

Одной из основных проблем, с которой сталкиваются специалисты по безопасности, является реверс-инжиниринг моделей ИИ. Этот процесс позволяет злоумышленникам извлекать информацию о внутренней структуре и параметрах модели, что открывает возможности для атак на данные или кражи интеллектуальной собственности. Для защиты ИИ от таких угроз активно разрабатываются различные методы, включая шифрование, обфускацию нейросетевых весов и использование дифференциальной приватности [2, с. 45].

Целью данной работы является анализ применения искусственного интеллекта для