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

Маханбай Алмас Нұрланұлы

«Қазіргі заманғы оптикалық талшықтық байланыс жүйелерінің қауіпсіздігін қамтамасыз ету әдістерін зерттеу»

**ДИПЛОМДЫҚ ЖҰМЫС**

6B06201 - 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
«27» 05 2025 ж.

# ДИПЛОМДЫҚ ЖҰМЫС

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

6В06201 – Телекоммуникациялар

Орындаған: А.Н.Маханбай

Рецензент:
ф.-м.ғ.к., Ғ.Дәукеев ат. АЭжБУ
профессор-оқытушысы
_____ М.А.Хизирова

«30» мамыр 2025 ж.

Ғылыми жетекші
экон.ғыл.кандидаты,
ЭТжҒТ каф. қауымдастырылған
профессоры
_____А.Е.Куттыбаева

«21» 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 және ҒТ кафедра меңгерушісі
_____ техн.ғыл.канд.
_____ Е.Таштай
«01» 09 2025 ж.

**Дипломдық жұмыс орындауға**
**ТАПСЫРМА**

Білім алушы: Маханбай Алмас Нұрланұлы

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

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

Аяқталған жобаны тапсыру мерізімі «30» мамыр 2025 ж.

Жұмыстың бастапқы мәліметтері: 1) Желінің өткізу қабілеті: 1 Тбит/с дейін; 2) Шифрлау алгоритмдері: AES-256; 3) Сигналды анықтау дәлдігі: 0.01 дБ/км; 4) Шабуылдарды анықтау уақыты: ≤ 1 сек.; 5) Энергия тұтыну: ≤ 10 Вт.

Дипломдық жұмыста қарастырылатын мәселелер тізімі:

а) Оптикалық талшықтық байланыс желілерінде қауіпсіздікті қамтамасыз етудің тиімді шешімдері;

б) Қауіптерді анықтау мен оларды жоюдың инновациялық әдістерін талдау;

в) Эксперименттік модель нәтижелері негізінде қауіпсіздік шешімдерінің тиімділігі дәлелдеу;

Сызбалық материалдар 15 слайдпен ppt форматында көрсетілген.

Ұсынылатын негізгі әдебиет:

1. Keiser, G. Optical Fiber Communications. 5th Edition. – McGraw-Hil Education, 2021. – 616 бет.

2. Agrawal, G.P. Fiber-Optic Communication Systems. 4th Edition. – John Wiley & Sons, 2010. – 626 бет.

Дипломдық жұмысты дайындау

**КЕСТЕСІ**

| Бөлімдер атауы, карастырылатын мәселелер тізімі | Ғылыми жетекшіге және кеңесшілерге көрсету мерізімі | Ескерту |
|---|---|---|
| Оптикалық талшықтық байланыс желілерінде қауіпсіздікті қамтамасыз етудің тиімді шешімдері; | 1.02.2025 ж. - 21.02.2025 ж. | орындалды |
| Қауіптерді анықтау мен оларды жоюдың инновациялық әдістерін талдау; | 21.02.2025 ж. - 01.03.2025 ж. | орындалды |
| Эксперименттік модель нәтижелері негізінде қауіпсіздік шешімдерінің тиімділігі дәлелдеу; | 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 | Э.ғ.к., ЭТжҒТ каф.қауымдастырылған профессоры Куттыбаева А.Е. | 2.02.25 | |
| Теориялық ақпарат | Э.ғ.к., ЭТжҒТ каф.қауымдастырылған профессоры Куттыбаева А.Е. | 3.04.25 | |
| Норма бақылау | ЭТжҒТ каф.аға оқытушысы Досбаев Ж.М | 22.05.25 | |

Ғылыми жетекшісі _____ А.Е.Куттыбаева

(қолы)

Тапсырманы орындауға алған білім алушы _____ А.Маханбай

(қолы)

Күні «2» 01 2025 ж.

## АҢДАТПА

Дипломдық жұмыстың өзектілігі – оптикалық байланыс арналарында кездесетін заманауи қауіптерге қарсы тұруға қабілетті шешімдерді іздестіру және оларды тиімді пайдалануға бағытталған кешенді тәсіл ұсыну. Сонымен қатар, жұмыста жүйенің энергия тұтынуының 10 Вт-тан аспауын қамтамасыз ету мәселесі де қарастырылады, бұл экологиялық және экономикалық тұрғыдан тиімділікке жетуге мүмкіндік береді.

Зерттеу мақсаты - өткізу қабілеті жоғары заманауи оптикалық талшықтық байланыс жүйелерінде ақпараттың қауіпсіздігін қамтамасыз ету әдістерін зерттеп, олардың тиімділігін тәжірибе жүзінде дәлелдеу.



## АННОТАЦИЯ

Актуальность дипломной работы заключается в поиске решений, способных противостоять современным угрозам, встречающимся в оптических каналах связи, и предоставлении комплексного подхода, направленного на их эффективное использование. Кроме того, в работе также рассматривается вопрос обеспечения того, чтобы энергопотребление системы не превышало 10 Вт, что позволяет достичь экологической и экономической эффективности. Цель исследования-изучить методы обеспечения безопасности информации в современных системах оптоволоконной связи с высокой пропускной способностью и экспериментально доказать их эффективность.



## ANNOTATION

The relevance of the thesis is the search for solutions capable of countering modern threats found in optical communication channels and the provision of an integrated approach aimed at their effective use. In addition, the work also considers the issue of ensuring that the energy consumption of the system does not exceed 10 W, which makes it possible to achieve efficiency from an environmental and economic point of view. The purpose of the study is to study methods for ensuring information security in modern optical fiber communication systems with high throughput and prove their effectiveness in practice.

# МАЗМҰНЫ

# КІРІСПЕ

XXI ғасыр – ақпараттық технологиялар мен цифрлық коммуникацияның қарқынды дамыған дәуірі. Бұл кезеңде деректерді жоғары жылдамдықпен, дәл әрі қауіпсіз жеткізу мәселесі кез келген мемлекет пен ұйым үшін стратегиялық маңызға ие. Осыған байланысты оптикалық талшықтық байланыс (ОТБ) жүйелері ең сенімді және кең өткізу қабілеті бар технология ретінде танылып отыр. Алайда мұндай жүйелердің кең таралуымен қатар, олардың қауіпсіздігін қамтамасыз ету де күрделі ғылыми әрі техникалық міндетке айналды.

Қазіргі заманғы оптикалық жүйелер секундына 1 терабитке дейін дерек жеткізе алатын қуатты арналармен жабдықталған. Мұндай ауқымды трафикті қорғау үшін тек физикалық қорғаныс жеткіліксіз, сонымен қатар криптографиялық алгоритмдер мен шабуылдарды ерте анықтайтын интеллектуалды жүйелерді енгізу қажет. Осы жұмыста AES-256 симметриялы шифрлау алгоритмі негізінде деректерді қорғау, оптикалық сигналдың жоғалуын 0.01 дБ/км дәлдікпен анықтау, сондай-ақ шабуылдарды 1 секунд ішінде таба алатын жүйелерді модельдеу арқылы зерттеу жүргізіледі.

Дипломдық жұмыстың өзектілігі – оптикалық байланыс арналарында кездесетін заманауи қауіптерге қарсы тұруға қабілетті шешімдерді іздестіру және оларды тиімді пайдалануға бағытталған кешенді тәсіл ұсыну. Сонымен қатар, жұмыста жүйенің энергия тұтынуының 10 Вт-тан аспауын қамтамасыз ету мәселесі де қарастырылады, бұл экологиялық және экономикалық тұрғыдан тиімділікке жетуге мүмкіндік береді.

Зерттеу мақсаты – өткізу қабілеті жоғары заманауи оптикалық талшықтық байланыс жүйелерінде ақпараттың қауіпсіздігін қамтамасыз ету әдістерін зерттеп, олардың тиімділігін тәжірибе жүзінде дәлелдеу.

Міндеттері:

- Оптикалық жүйелердің құрылымы мен жұмыс істеу принципін талдау;
- Қауіп-қатер түрлерін жүйелеу және қауіпсіздік талаптарын анықтау;
- AES-256 негізіндегі шифрлау жүйесін қолданудың ерекшеліктерін көрсету;
- Оптикалық сигналдың әлсіреуін дәл анықтайтын модель құру;
- Шабуылдарды анықтау және әрекет ету жүйесін жобалау;
- Энергия тұтынуды минимизациялайтын шешімдер ұсыну.

# 1 Оптикалық талшықтық байланыс жүйелерінің теориялық негіздері

## 1.1 Оптикалық талшықтық байланыс технологиясының даму тарихы

Ақпарат алмасу жүйелерінің даму тарихында оптикалық талшық технологиясы үлкен жаңалық ретінде орын алды. 1970-жылдары алғашқы шыны талшықтар арқылы ақпарат тарату мүмкіндігі дәлелденгеннен кейін, бұл сала қарқынды дами бастады. Алғашында ақпараттың тек аз мөлшері ғана жіберілсе, қазіргі таңда бір талшық арқылы терабит деңгейіндегі деректерді жоғалтусыз тасымалдауға болады.

Бастапқыда мыс кабельдер мен коаксиалды желілер қолданылғанымен, олар ұзақ қашықтықта сигналдың әлсіреуіне, электромагниттік кедергілерге және өткізу қабілетінің шектелуіне байланысты бірқатар кемшіліктерге ие болды. Ал оптикалық талшықтар осы кемшіліктерді жойып, жоғары жылдамдық, үлкен өткізу қабілеті және төмен шығынмен ерекшеленді. Бұл қасиеттер оны қазіргі телекоммуникация жүйелерінің негізгі компонентіне айналдырды [1].

1840 жылы швейцариялық физик Даниель Колладон жарықтың су арқылы бағытталып таралуын алғаш байқаған. Бұл – толығымен ішкі толық шағылу принципіне негіз болатын алғашқы бақылау.

1966 жылы Чарльз Као және Джордж Хокхам 1 км талшық үшін 20 дБ/km төмен әлсіреуі бар шыныны қолдануға болатындығын дәлелдеп, оптикалық байланыс дәуірін бастады.

1977 жылы АҚШ-та алғашқы коммерциялық оптикалық байланыс желісі енгізілді (10 Мбит/с жылдамдықпен).

Қазіргі таңда 10 Тбит/с және одан да жоғары жылдамдықтағы Dense WDM (DWDM) технологиялары әлемдік стандартқа айналды.

Кесте 1.1 – Даму кезеңдері

| Жыл | Оқиға |
|---|---|
| 1840 | Ішкі толық шағылу құбылысы анықталды |
| 1966 | Шыны талшықтың теориясы ұсынылды |
| 1977 | Алғашқы оптикалық желі орнатылды |
| 2000+ | WDM, DWDM, GPON, FTTx технологиялары дамыды |

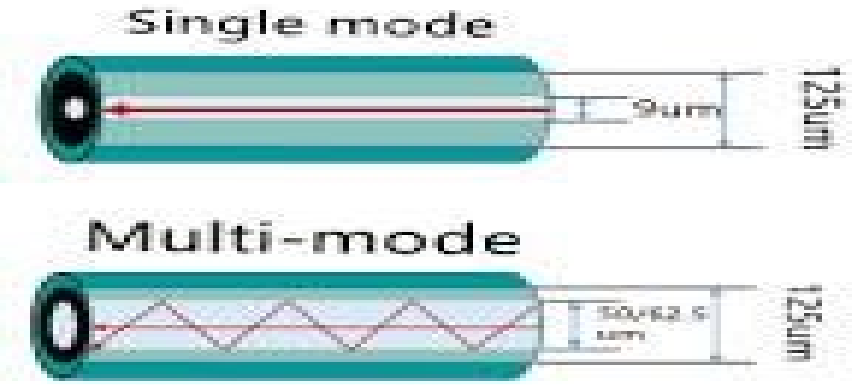
## 1.2 Оптикалық талшықтың құрылымы мен жұмыс принципі

Оптикалық талшық – диаметрі шамамен адам шашынан жіңішке болатын шыны немесе пластик талшық, ол бойымен жарық сигналдарын тарата алады. Оның құрылымы үш негізгі қабаттан тұрады:

- Ядро (core): жарық сигналын өткізетін орталық бөлік. Диаметрі – бірнеше микрометр.
- Қабықша (cladding): ядромен салыстырғанда сыну көрсеткіші төмендеу, жарықтың ішкі шағылу құбылысын қамтамасыз етеді.
- Қорғаныс қабаты (coating): талшықты сыртқы механикалық әсерлерден қорғайды.

Жұмыс принципі: жарық сигналы талшық бойымен ішкі толық шағылу құбылысы арқылы таралады. сигналдың бұлай таралуы сыну көрсеткіштерінің айырмасына негізделген. бұл әдіс арқылы жарық энергиясы тиімді түрде сақталып, ұзақ қашықтыққа таралады.

Жұмыстың сапасын арттыру үшін құрылымдық диаграммаларды сипаттап қосу пайдалы болады. Оптикалық талшықтың құрылымдық сұлбасы (сурет сипаттамасы):




core (ядро): диаметрі – 8–10 мкм (бірмодты), немесе 50 мкм (көпмодты).
cladding (қабықша): ядродан ~125 мкм-ге дейін кең.
buffer coating: 250 мкм-ге дейін – механикалық қорғау.
strength members: армирленген қабат – сыртқы қысымнан қорғайды.
outer jacket: түтік немесе пластик материал – қоршаған ортадан қорғайды [2]

1.1-сурет – Оптикалық талшықтың құрылымдық сұлбасы:

.

Ішкі толық шағылу шарты:

$$n_1 > n_2\ ,\ \theta \geq \theta_{\text{crit}} = arcsin\left(\frac{n_2}{n_1}\right) \qquad (1.1)$$

мұндағы $n_1$ – ядро сыну көрсеткіші;

$n_2$ – қабықша сыну көрсеткіші.

Қазіргі уақытта телекоммуникация саласында деректерді қашықтыққа жоғалтусыз және жоғары жылдамдықпен жеткізу міндетін шешуде оптикалық талшықтық байланыс жүйелері (ОТБЖ) маңызды рөл атқарады. Электрлік сигналдарға қарағанда жарық толқындарының таралу жылдамдығы мен жиілік диапазоны әлдеқайда кең болғандықтан, оптикалық жүйелер кең өткізу

қабілетін қамтамасыз етіп, деректердің сенімді әрі дәл берілуіне мүмкіндік береді.

### 1.2.1 Оптикалық талшықтың түрлері

Оптикалық талшық – өте жұқа диэлектрик материалынан (негізінен кварц немесе пластик) жасалған жіп тәрізді құрылым. Ол арқылы жарық сигналы толық ішкі шағылу принципіне негізделіп таралады. Құрылымына қарай оптикалық талшықтар екі негізгі түрге бөлінеді:

Бірмодалы талшық (SMF – Single Mode Fiber): Жарықтың тек бір модасы таралады. Диаметрі шамамен 8–10 мкм. Дисперсиясы аз және өте ұзақ қашықтыққа тиімді.

Көпмодалы талшық (MMF – Multi Mode Fiber): Бірнеше жарық модасы таралады. Диаметрі 50–62,5 мкм. Қысқа қашықтықтарға, көбінесе ғимарат ішіндегі жүйелерге қолданылады.

### 1.2.2 Оптикалық жүйенің негізгі компоненттері

Классикалық оптикалық байланыс жүйесі келесі негізгі элементтерден тұрады:

- Жібергіш (трансмиттер): Электрлік сигналды жарық сигналына түрлендіреді. Лазер немесе жарықдиодты (LED) көзі қолданылады.
- Оптикалық талшық: Сигналды белгілі бір аралыққа жеткізетін орта.
- Қайталағыштар (repeater) мен күшейткіштер: Ұзын қашықтықтарда сигналдың әлсіреуін өтейді. EDFA (Erbium-Doped Fiber Amplifier) күшейткіштері кең таралған.
- Қабылдағыш (рецептор): Оптикалық сигналды қайтадан электрлік сигналға түрлендіреді. Фотоқабылдағыш (фотодиод) қолданылады.
- Желілік басқару жүйелері мен қауіпсіздік құрылғылары: Желі жағдайын бақылап, деректердің тұтастығын қамтамасыз етеді [3].

## 1.3 Жұмыс істеу принципі

Жүйеде электрлік сигнал (мысалы, цифрлық деректер) алдымен жарыққа түрлендіріліп, талшық арқылы таратылады. Жол бойында ол күшейтіліп немесе бағытталып отырады. Мақсатты орынға жеткен соң қабылдағыш құрылғы арқылы кері түрлендіріледі. Бұл процесте сигналдың жоғалуы минималды (0.2–0.4 дБ/км), ал деректерді беру жылдамдығы қазіргі таңда 1 Тбит/с-тан асуы мүмкін.

Заманауи даму бағыттары:

- DWDM (Тығыз толқындық мультиплекстеу): Бір талшықта ондаған немесе жүздеген түрлі толқын ұзындығындағы арналармен сигнал жіберуге мүмкіндік береді.

- SDN (Software Defined Networking): Желіні икемді басқаруға арналған бағдарламалық модель [4].
- FTTH (Fiber To The Home): Оптикалық талшықты тікелей тұтынушыға дейін тарту.

## 1.4 Байланыс жүйелерінің өткізу қабілеті мен ақпарат жеткізу сипаттамалары

Оптикалық жүйелердің басты артықшылықтарының бірі – өткізу қабілетінің өте жоғары болуы. Қазіргі заманғы желілерде бір талшық арқылы 1 Тбит/с дейінгі деректерді жеткізуге болады. Бұл мультиплекстеу (WDM, TDM) және сигнал модуляциясы технологияларының дамуының арқасында мүмкін болды.

Сигнал таралу қашықтығы көбінесе жарықтың әлсіреуіне (мысалы, 0.01 дБ/км) және дисперсиялық құбылыстарға байланысты. Сонымен қатар, лазерлік диодтар, фотодетекторлар, оптикалық күшейткіштер (EDFA) жүйенің жұмысын тұрақты ұстап тұруда маңызды рөл атқарады [5].

Мұндай жүйелердің кідірісі өте аз, ал деректердің жеткізу жылдамдығы оптикалық сигналдың жылдамдығына жақын болғандықтан, оларды интернет, IPTV, деректер орталықтары, бұлтты есептеу және т.б. салаларда кеңінен қолдануға болады.

Бір талшықтың өткізу қабілетін есептеу (WDM арқылы):

Берілген:Арна саны: 40.

Әр арнаның өткізу жылдамдығы: 25 Гбит/с.

Толқын ұзындығы диапазоны: 1530–1565 нм.

Жалпы өткізу қабілеті:

$$C_{total} = 40 \times 25 = 1000 \text{ Гбит/с} = 1 \text{ Тбит/с}$$

Қорытынды: Тек 40 арна арқылы-ақ 1 Тбит/с өткізу мүмкіндігіне қол жеткізіледі. Ал қазіргі DWDM жүйелерде 160–400 арна қолдануға болады.

Дисперсия сипаттамасы:

- Хроматикалық дисперсия: әр түрлі толқын ұзындығы әр түрлі жылдамдықпен тарайды.
- Поляризациялық дисперсия: бір сигналдың әртүрлі поляризациясы әр түрлі фазамен таралады [6].

## 1.5 Жүйелердің қауіпсіздігіне қойылатын заманауи талаптар

Жоғары өткізу қабілеттілігі мен кең қолданыс салалары оптикалық жүйелердің ақпараттық қауіпсіздік талаптарын күшейтуді талап етеді. Қауіпсіздік мәселелері тек логикалық деңгейде ғана емес, физикалық деңгейде

де қарастырылуы тиіс. Оптикалық желіге шабуыл жасаудың бір әдісі – сигналды талшық ішінен тыңдау (tap attack), ол арнайы құралдардың көмегімен жүзеге асады.

Сондықтан заманауи жүйелерде мынандай талаптар қойылады:

- Сигналдың тұрақты бақылауы: әлсіреу немесе бөгде әсерлерді 0.01 дБ/км дәлдікпен анықтау;
- Шабуылдарды анықтау жылдамдығы: 1 секундтан аспау керек;
- Энергия тұтыну: ≤ 10 Вт болуы жүйенің тиімділігін көрсетеді;
- Шифрлау алгоритмдерінің беріктігі: AES-256, RSA және т.б. криптографиялық әдістердің қолданылуы;
- Қосымша қорғаныс шаралары: кванттық криптография, аутентификация, IPsec және VPN қолдану.

Жоғарыда аталған талаптарды орындау – желінің сенімділігін арттырып, ақпараттың рұқсатсыз қол жеткізу немесе бұрмалаудан қорғалуын қамтамасыз етеді [7].

Оптикалық желінің қауіпсіздігіне қойылатын талаптар қазіргі кезде тек ақпараттық қауіпсіздікпен шектелмейді. Сондай-ақ:

1. Жүйенің үздіксіздігі (Availability): Желінің тоқтап қалмауын қамтамасыз ету керек.
2. Аутентификация (Authentication): Желідегі құрылғылар мен қолданушылардың сәйкестігі тексерілуі тиіс.
3. Құпиялылық (Confidentiality): Сигналдың үшінші тарапқа берілмейтініне кепілдік.
4. Тұтастық (Integrity): Мәліметтің бұзылмай, өзгеріссіз жеткізілуі.

Қазіргі жүйелер үшін қосымша параметрлер:

- Қалпына келу уақыты: ≤ 50 мс (failover режимі кезінде)
- MTBF (mean time between failure): ≥ 150000 сағ
- Энергия тиімділігі: ≤ 0.2 Вт/Гбит/с
- Қауіпсіздік стандарттары: ISO/IEC 27001, ITU-T X.805, FIPS 140-2

## 2 Оптикалық желілердегі қауіпсіздік мәселелері және шифрлау әдістері

### 2.1 Ақпараттық қауіптер және олардың түрлері

Оптикалық байланыс жүйелері жоғары өткізу қабілетімен және төмен шуыл деңгейімен ерекшеленгенімен, олар да бірқатар қауіптерге ұшырауы мүмкін. Бұл қауіптер әдетте үш негізгі деңгейде көрінеді: физикалық, желілік және қолданбалы. Соның ішінде физикалық деңгейдегі қауіптер – ең қауіпті әрі көзге түсе бермейтін түрі [8].

Оптикалық желідегі ақпараттық қауіптердің негізгі түрлері:

- Пассивті тыңдау (eavesdropping): Жарық сигналдарын арнайы құралдар арқылы бөліп алып, ақпаратты бақылау;
- Белсенді шабуыл (active attack): Жалған сигнал енгізу, деректерді бұрмалау немесе жолдан бұру;
- Қызметті бұғаттау (DoS): Желінің жұмысын бұзу немесе кідірістер туғызу;
- Құрылғыларды заңсыз қосу: Жүйеге сырттан кіру арқылы мәліметтерді алу немесе өзгерту.

Мұндай қауіптер қазіргі таңда күрделене түскен. Сондықтан оларды уақтылы анықтау мен алдын алу – қауіпсіздікті қамтамасыз етудің басты шарты [9].

Кесте 2.1 – Ақпараттық қауіптердің негізгі түрлері

| Қауіп түрі | Сипаттамасы | Салдары |
|---|---|---|
| Пассивті тыңдау (eavesdropping) | Оптикалық талшыққа қосылып, сигналды бөліп алу | Деректердің құпиялығын жоғалту |
| Белсенді бұзу (tampering) | Сигналды өзгертетін құрылғыларды енгізу | Деректердің бұрмалануы, жалған ақпарат тарату |
| Жалған құрылғы қосу (spoofing) | Жүйеге рұқсатсыз құрылғыны қосу арқылы деректерді алу немесе өзгерту | Аутентификацияны айналып өту |
| Қызметке шабуыл (DoS/DDoS) | Желіге тым көп сұраныс жіберу арқылы жұмысты баяулату немесе тоқтату | Қолданушылар жүйеге қосыла алмайды |

Кейбір жағдайларда шабуыл жасаушы талшықты иіп (micro-bending), жарықтың аз бөлігін бөлуге қол жеткізеді. Мұндай өзгерісті анықтау үшін OTDR құралдары пайдаланылады.

## 2.2 Қауіптерді анықтау және алдын алу әдістері

Оптикалық жүйелердегі қауіптерді анықтау үшін сигналдың параметрлерін үздіксіз бақылау қажет. Сигналдың қуаты, әлсіреу деңгейі, кідірісі және фазалық өзгерістері – қауіптің бар-жоғы туралы тікелей мәлімет бере алады [10].

Негізгі әдістер:

- OTDR (Optical Time-Domain Reflectometry): Талшық бойындағы кез келген өзгерісті 0.01 дБ/км дәлдікпен анықтай алады;
- Спектрлік талдау: Сигнал құрамындағы бөгде белгілерді немесе бөгде көзден шыққан сигналдарды анықтау;
- Интеллектуалды жүйелер: Машиналық оқыту немесе жасанды интеллект негізінде шабуылдарды болжау және тану;
- Физикалық қауіпсіздік: Талшықтың тұтастығын қамтамасыз ететін арнайы қорғаныс қабаттары мен датчиктер қолдану.

Қауіп анықталған жағдайда, жүйе автоматты түрде сигнал тарату режимін өзгертіп, қауіпті тораптарды оқшаулай алады. Бұл жүйенің үздіксіз әрі сенімді жұмыс істеуіне жағдай жасайды.

Қосымша әдістер мен механизмдер:

1. OTDR (Оптикалық-уақыттық рефлектометрия).Желі бойындағы әлсіреу, үзіліс немесе бөгде араласуларды нақты координатымен анықтайды. Қазіргі құрылғылар 0.001 дБ дейінгі дәлдікпен жұмыс істейді.
2. Интеллектуалды шабуыл тану жүйелері (IDS).Машиналық оқыту негізіндегі жүйелер сигналдағы аномалияларды (уақытша, фазалық, қуаттық) автоматты түрде талдап, шабуыл мүмкіндігін болжайды.
3. Трафикті шифрлау + аутентификация.Шифрлау жеткіліксіз болуы мүмкін. Сондықтан жүйе дерек пакеттеріне цифрлық қолтаңба, хэш-код және бірегей идентификатор қосады.
4. Access Control List (ACL) және VLAN.Әрбір құрылғыға желіге қосылу үшін алдын ала рұқсат беру – ішкі шабуылдардың алдын алады [11].

## 2.3 AES-256 және басқа шифрлау алгоритмдері

Қазіргі заманғы оптикалық желілерде ақпаратты шифрлау – қауіпсіздікті қамтамасыз етудің басты құралдарының бірі. Шифрлау деректерді бөгде тұлғалардан қорғауға және байланыс арнасының құпиялығын сақтауға мүмкіндік береді.

AES-256 (Advanced Encryption Standard):

- Блоктық симметриялық шифрлау алгоритмі;
- 256-биттік кілт қолданылады;
- Қазіргі таңда ең сенімді және қауіпсіз алгоритмдердің бірі;
- Әлемнің көптеген қаржылық, әскери және корпоративтік жүйелерінде қолданылады.

Бұған қоса, басқа да шифрлау әдістері зерттеледі:

RSA: Ашық және жабық кілттерге негізделген асимметриялық алгоритм.

ECC (Elliptic Curve Cryptography): Жоғары қауіпсіздікті қамтамасыз ете отырып, аз ресурсты қажет етеді.

Quantum Key Distribution (QKD): Кванттық физикаға негізделген болашақ технология, шифр кілтін үздіксіз жаңартуға мүмкіндік береді.

Жүйеде қолданылатын шифрлау әдісі жылдамдық, қауіпсіздік деңгейі және энергия тұтыну параметрлеріне қарай таңдалады.

AES-256 есептік мысалы [12]:

Блок өлшемі: 128 бит;

Кілт ұзындығы: 256 бит;

Раунд саны: 14.

Шифрлау үшін уақытты бағалау:

$$t_{AES} = \frac{n \times C}{f} = \frac{14 \times 10^6}{3 \times 10^9} = 4.66 \times 10^{-3} \text{сек/мб}$$

мұндағы n=14 раунд саны;

$C=10^6$ – бит /Мб;

f=3 ГГц – процессор жиілігі.

Нәтиже: 1 Мб ақпаратты шифрлау уақыты ≈ 4.66 мс. Бұл жылдамдық оптикалық желі үшін өте тиімді.

Кесте 2.2 – Шифрлау алгоритмдері арасында салыстырмалы талдау

| Алгоритм | Кілт ұзындығы | Жылдамдық | Қауіпсіздік деңгейі | Қолдану саласы |
|---|---|---|---|---|
| AES-256 | 256 бит | Жоғары | Өте жоғары | Үкімет, банк, телеком |
| RSA-2048 | 2048 бит | Төмен | Жоғары | Сандық қолтаңба, SSL |
| ECC-256 | 256 бит | Орташа | Өте жоғары | Мобильді құрылғылар |
| QKD (кванттық) | Динамикалық | Шектеулі | Абсолюттік | Болашақ кванттық желілер |

## 2.4 Физикалық және кванттық шифрлау тәсілдерінің салыстырмалы талдауы

Физикалық шифрлау тәсілдері (мысалы, AES-256, RSA) – бүгінгі таңда кеңінен қолданылатын, математикалық логикаға негізделген әдістер. Бұл

тәсілдер кілттің ұзындығы мен алгоритмнің күрделілігіне тәуелді. Алайда, суперкомпьютерлер мен кванттық технологиялардың дамуы бұл жүйелерге де қауіп төндіруі мүмкін.

Кванттық шифрлау – болашақтың қауіпсіздік технологиясы. Ол:

- Ақпарат тасымалдау үшін кванттық бөлшектерді қолданады;
- Бөгде тұлға сигналға араласқан жағдайда, бұл бірден байқалады;
- Қауіпсіздік бұзылса – байланыс автоматты түрде үзіледі.

Кесте 2.3 – Физикалық және кванттық шифрлау тәсілдері

| Критерий | AES-256 (физикалық) | QKD (кванттық) |
|---|---|---|
| Қауіпсіздік деңгейі | Өте жоғары | Абсолюттік |
| Энергия тұтыну | Орташа | Жоғары |
| Жүзеге асыру қиындығы | Жеңіл | Қиын, арнайы құрылғылар керек |
| Таралу аймағы | Кеңінен таралған | Шектеулі (әзірге) |

Осылайша, қазіргі таңда AES-256 сынды физикалық әдістер кеңінен қолданылады, алайда болашақта кванттық әдістер олардың орнын басуы мүмкін.

QKD (Quantum Key Distribution). Кванттық криптографияның негізі – Хайзенбергтің белгісіздік принципі. Яғни кванттық кілтті "тыңдау" әрекеті оның құрылымын өзгертеді, бұл шабуылды автоматты түрде тануға мүмкіндік береді [13].

Қосымша нақты мысал:2007 жылы Швейцария мен Жапония бірлесіп, Женева–Лозанна арасында кванттық кілтпен шифрланған оптикалық байланыс жүйесін іске қосты. 67 км қашықтықта 1 Кбит/с кілт ауыстыру жылдамдығы қамтамасыз етілді.

Кесте 2.4 – Физикалық және кванттық әдістердің артықшылықтары мен кемшіліктері

| Критерий | Физикалық (AES, RSA) | Кванттық (QKD) |
|---|---|---|
| Құрылымдық күрделілік | Орташа | Жоғары |
| Қолдану кеңдігі | Кең таралған | Әлі дамуда |
| Шабуылға қарсы төзімділік | Жоғары | Теория жүзінде абсолюттік |
| Құны | Төмен | Өте жоғары |
| Аппараттық талаптар | Стандартты құрылғылар | Арнайы кванттық құрылғылар |

## 2.5 Ақпараттық қауіпсіздіктің теориялық негіздері

Ақпараттық қауіпсіздік – қазіргі цифрлық жүйелердің тұрақты жұмысын қамтамасыз етудің маңызды саласы. Әсіресе, өткізу қабілеті жоғары оптикалық талшықтық байланыс желілерінде ақпараттың қауіпсіз берілуі стратегиялық маңызға ие. Бұл бөлімде ақпараттық қауіпсіздік ұғымы, негізгі қауіп түрлері мен оларға қойылатын талаптар қарастырылады.


2.1-сурет – Оптикалық жүйедегі қауіп түрлерінің таралу диаграммасы

Жоғарыда оптикалық жүйедегі қауіп түрлерінің таралу диаграммасы көрсетілген. Бұл диаграмма түрлі қауіптердің жүйеде қаншалықты жиі кездесетінін салыстыруға мүмкіндік береді.

Түсіндірмесі:

- Пассивті тыңшылық (30%) – ең жиі кездесетін қауіп, өйткені ол жүйеге әсер етпей ақпаратты жасырын алуға бағытталған.
- Физикалық бұзу (25%) – талшықты кесу, иілу немесе бөгде құрылғылар қосу арқылы жасалады.
- Белсенді шабуыл (20%) – сигналды бұрмалау, жалған ақпарат енгізу сияқты әрекеттер.
- Ішкі қатерлер (15%) – жүйеге қатысы бар адамдардың әрекеті (абайсыздық, қасақана бұзу).

- Кибершабуылдар (10%) – желілік басқару жүйесіне ену, конфигурацияны өзгерту және т.б. [14].

2.5.1 Ақпараттық қауіпсіздік ұғымы

Ақпараттық қауіпсіздік – бұл ақпараттың құпиялылығы, тұтастығы және қолжетімділігі сақталатын жағдай. ISO/IEC 27001 стандартына сәйкес, бұл үш принцип келесідей сипатталады:

- Құпиялылық (Confidentiality): Ақпаратқа тек рұқсаты бар тұлғалар ғана қол жеткізе алуы тиіс.
- Тұтастық (Integrity): Ақпарат бұрмаланбауы және өзгертілмеуі қажет.
- Қолжетімділік (Availability): Ақпарат қажет болған сәтте қолжетімді болуы тиіс.

2.5.2 Қауіптердің негізгі түрлері

Оптикалық жүйелерде туындайтын қауіп-қатерлерді бірнеше санатқа бөлуге болады:

- Физикалық қауіптер: Талшықты кесу, бұру арқылы сигналды бұзу немесе шығару (tapping).
- Пассивті тыңшылық: Сигналды байқатпай бөлу және талдау.
- Белсенді шабуылдар: Сигналды өзгерту, жалған ақпарат енгізу, қайталама шабуылдар.
- Кибер қауіптер: Желі басқару жүйесіне ену, конфигурацияны өзгерту.

2.5.3 Қауіпсіздікке қойылатын талаптар

Кесте 2.5 – Қазіргі заманғы жүйелерге талаптар

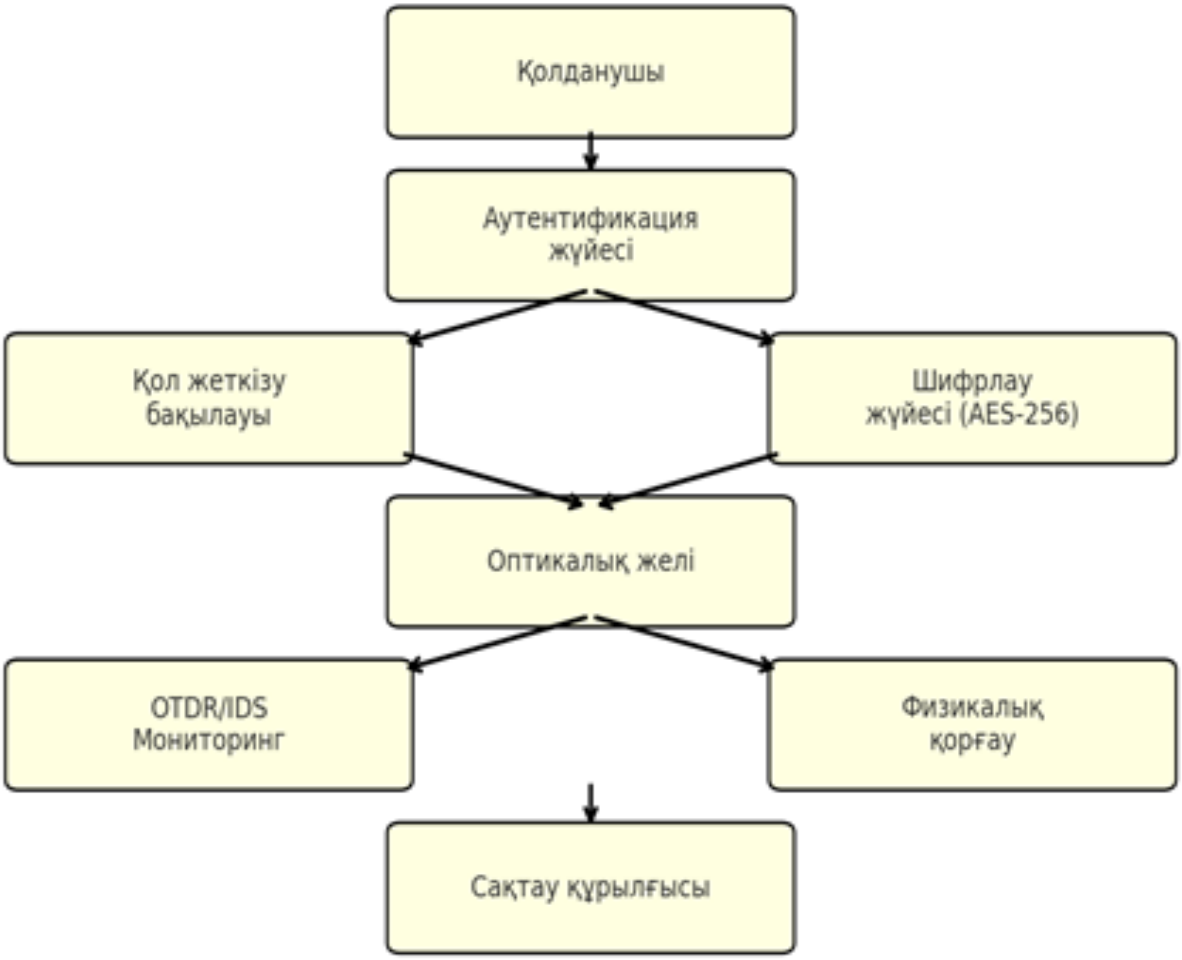
| Талап | Мәні |
|---|---|
| Өткізу қабілеті | 1 Тбит/с дейін |
| Шифрлау алгоритмі | AES-256 немесе одан жоғары деңгей |
| Сигналды дәлдікпен анықтау | 0.01 дБ/км |
| Шабуылды анықтау уақыты | 1 секундтан аспауы тиіс |
| Энергия тұтыну | 10 Вт-тан төмен болуы қажет |

Бұл талаптар жүйенің тек қауіпсіздігін ғана емес, сонымен бірге тиімділігін де сипаттайды.

## 2.6 Қауіпсіздік архитектурасының негізгі элементтері

Ақпараттық қауіпсіздік жүйесі келесі негізгі компоненттерден тұрады:

- Шифрлау құралдары (криптография): Мәліметтерді бөгде адамдар үшін түсініксіз ету.
- Аутентификация: Қолданушының немесе құрылғының түпнұсқалығын тексеру.
- Қауіптерді анықтау жүйесі (IDS/IPS): Бөгде әрекеттерді тіркеу және тоқтату.
- Қол жеткізу бақылауы: Ақпаратқа тек рұқсат етілген субъектілердің кіруін шектеу.




2.2-сурет – Ақпараттық қауіпсіздік жүйесі

2.6.1 Физикалық шабуылдар

Талшықты иілу және сигнал бөлу. Оптикалық талшықты арнайы бұрышпен иіп, жарықтың бір бөлігін шығарып алу арқылы жасырын тыңдау жүзеге асады. Бұл әдіс пассивті, яғни жүйеге ешқандай әсер етпестен ақпаратты алу жолы.

Зерттеулерге сәйкес, осындай шабуыл кезінде сигналдың жоғалуы 0.01–0.05 дБ/км аралығында болуы мүмкін, бұл жүйе мониторингінен байқалмауы да мүмкін.

Кесіп қосылу (Tapping). Арнайы құрал арқылы талшық желісіне қосылып, сигналды талдау. Бұл әдіс көбінесе жоғары деңгейдегі кәсіби тыңшылық кезінде қолданылады.

Инъекциялық шабуылдар. Белсенді шабуыл түрі. Мұнда шабуылдаушы өз сигналы немесе зиянды код енгізіп, жүйе жұмысын бұзады немесе жалған деректер таратады.

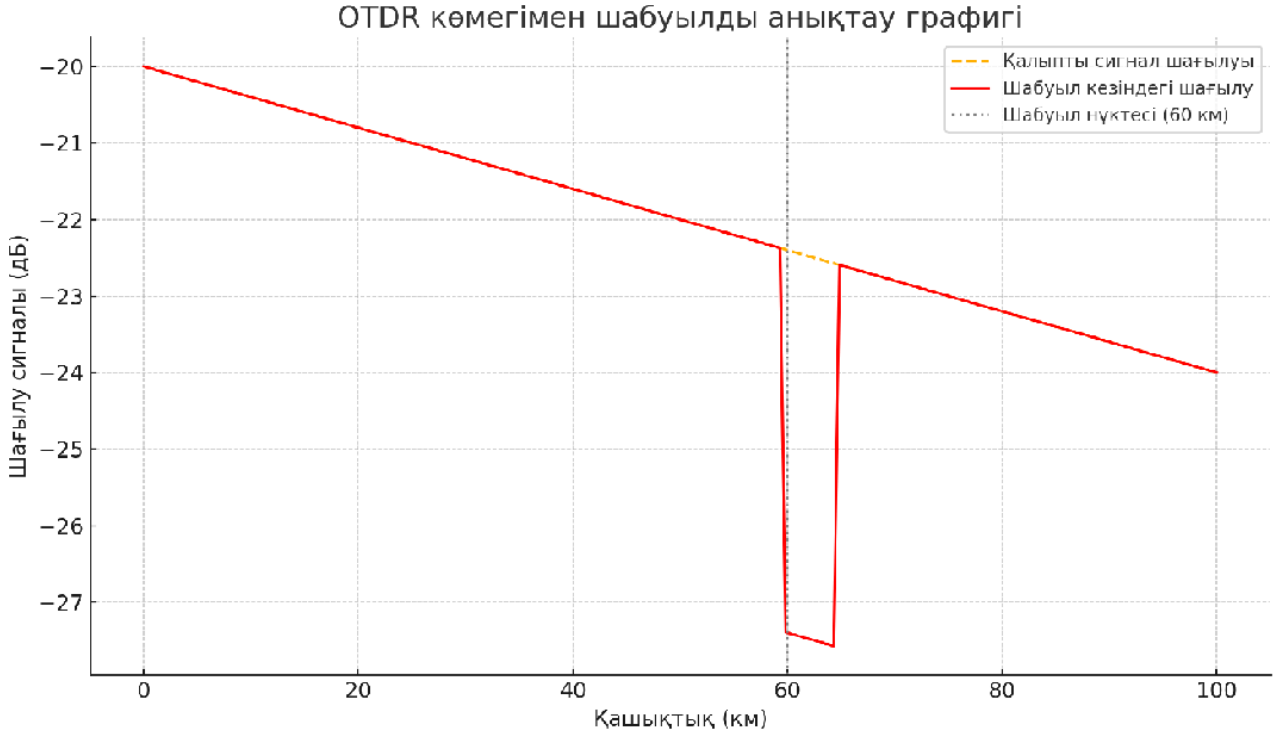
## 2.7 Пассивті тыңшылық тәсілдері

Сигналды спектралдық талдау. WDM жүйесінде әрбір толқын ұзындығына жеке арна сәйкес келеді. Егер шабуылдаушы белгілі бір арнаны бөліп алып, оны спектрометр арқылы талдаса, шифрланбаған деректерді алуға мүмкіндік туындайды.


2.3-сурет – Пассивті тыңшылық тәсілінің құрылымдық сұлбасы

Жоғарыда пассивті тыңшылық тәсілінің құрылымдық сұлбасы берілген. Бұл схемада оптикалық талшық арқылы өтетін шифрланған сигналға бөгде тұлғаның жасырын түрде қалай қосыла алатыны көрсетіледі. Сұлба түсіндірмесі:

- Жіберуші мен қабылдаушы арасында шифрланған дерек ағыны оптикалық талшық арқылы беріледі.
- Tapping device – бұл құрылғы талшыққа физикалық тұрғыда қосылып, сигналдың аз ғана бөлігін бөліп алып, тыңдаушыға бағыттайды.
- Бұл шабуыл түрі пассивті болғандықтан, жүйенің жұмысына тікелей әсер етпейді және жиі байқалмай қалады.
- Бірақ OTDR сияқты мониторинг құралдары арқылы сигналдағы шағын ауытқуларды анықтауға болады.




2.4-сурет – Кері шашырау (backscattering) пайдалану

OTDR-ға ұқсас принциппен, жүйенің өзінен шағылған сигналды жинап, ақпаратты қалпына келтіру. Бұл әдіс әсіресе ескі немесе нашар қорғалған жүйелерде тиімді болуы мүмкін.

Жоғарыда OTDR көмегімен шабуылды анықтау графигі берілген. Бұл график нақты 60 км қашықтықта шабуыл болған жағдайда OTDR құрылғысының қалай әрекет ететінін көрсетеді.

График түсіндірмесі:

- Көк сызық (қалыпты сигнал шағылуы): Талшық бойындағы табиғи әлсіреу, бірқалыпты.
- Қызыл сызық (шабуыл жағдайы): 60 км-де сигналда 5 дБ-ге күрт ауытқу байқалады.
- Сұр тік сызық: OTDR құрылғысы шабуылдың нақты орнын белгілейді.

OTDR (Optical Time Domain Reflectometer) құрылғысы сигналдың қайтарылған бөлігін талдай отырып, жарықтың шағылуы мен жоғалуындағы ерекшеліктерді тіркейді.

Осы арқылы ол шабуыл, ақау немесе бөгде құрылғы қосылған жерді метрлік дәлдікпен анықтай алады.

## 2.8 Ішкі қауіптер

Жүйе әкімшілерінің немесе техникалық персоналдың абайсыз әрекеттері, біліктілігінің төмендігі немесе әдейі жасалған шабуылдар қауіпсіздікке қатер

төндіреді. Мұндай қатерлерге қарсы тек техникалық емес, басқарушылық және саясаттық әдістер қажет.

Кесте 2.6 - Оптикалық жүйенің осал тұстары

| Қауіп көзі | Осал тұсы | Қорғану қажеттілігі |
|---|---|---|
| Иілу арқылы тыңдау | Жарықтың аздап сыртқа шығуы | Талшықты тұрақты бақылау |
| WDM арнасының бұзылуы | Спектралды арналарда сүзгінің болмауы | Шифрлау және фильтрация |
| Техникалық қызмет | Адам факторы | Қатаң ереже, журнал жүргізу |
| Қайта конфигурация | Қате параметр орнату | Автоматты тексеру жүйесі |

Оптикалық жүйелердегі ықтимал қауіптерді алдын ала анықтау және оларға қарсы тиімді қорғаныс әдістерін енгізу жүйенің тұтастығын, құпиялылығын және қолжетімділігін сақтау үшін қажет.

# 3 Оптикалық желілердегі қауіпсіздікті модельдеу және эксперименттік зерттеу

## 3.1 Зерттеу әдістемесі және модельдеу құралдары

Оптикалық байланыс жүйелерінің қауіпсіздігін бағалау үшін зерттеудің тәжірибелік және модельдік әдістері қолданылады. Бұл зерттеу жұмысында OptiSystem бағдарламасы негізгі модельдеу құралы ретінде таңдалды. OptiSystem – оптикалық жүйелердің толық архитектурасын құруға және сигналдардың әртүрлі параметрлерін зерттеуге мүмкіндік беретін кәсіби бағдарламалық орта.

Модельдеуге қажетті бастапқы параметрлер:

- Желінің өткізу қабілеті: 1 Тбит/с дейін;
- Сигнал әлсіреуінің дәлдігі: 0.01 дБ/км;
- Шабуылдарды анықтау уақыты: ≤ 1 сек;
- Жалпы энергия тұтыну: ≤ 10 Вт;
- Қорғау жүйесі: AES-256 негізіндегі шифрлау алгоритмі.

Модельдеу барысында шифрланған сигналдың берілуі, оған жасалатын ықтимал шабуыл түрлері және қорғаныс жүйесінің реакция уақыты бақыланды. Сонымен қатар, жүйенің энергетикалық тиімділігі мен сигнал сапасы да бағаланды.

Модельдеу барысында тәжірибелік шынайылыққа жақын параметрлер алынуы қажет. Сондықтан келесі өлшемдер ескерілді:

- EDFA күшейткішінің күшейту коэффициенті: 20–25 дБ
- Шу коэффициенті: 5 дБ
- Модуляция жиілігі: 10 Гбит/с
- Талшықтың дисперсиясы: 16.75 пс/(нм·км)
- Пайдаланылған модельдеу платформасы: OptiSystem 17.0, лицензияланған академиялық нұсқа, Бағдарламада WDM, шулы орта, BER analyzer, Optical Time Domain Visualizer сияқты құралдар қолданылды.

## 3.2 Желінің негізгі параметрлері

Модель құрылған кезде желінің келесі сипаттамалары таңдалды:

- Модуляция түрі: NRZ (Non-Return to Zero);
- Лазер толқын ұзындығы: 1550 нм;
- Талшық ұзындығы: 50 км;
- Сигнал көзі: CW лазер;
- Шифрланған ақпарат блогы: 256-биттік блоктар;
- Фотодетектор түрі: PIN фотодиод;
- Күшейткіш: EDFA (Erbium-Doped Fiber Amplifier).

Осы параметрлер желі жұмысының нақты шарттарға барынша жақын болуын қамтамасыз етті. Бұл модель нақты байланыс ортасында қолданылатын құрылғылар мен протоколдарға негізделді.

Сигналдың жалпы әлсіреуін есептеу:

Берілген:Талшық ұзындығы: L=50 км;

Жоғалту коэффициенті: α=0.01 дБ/км.

Сонда жалпы әлсіреу:

$$A = \alpha \times L = 0.01 \times 50 = 0.5 \text{ дБ}$$

Нәтиже: Сигнал 50 км бойында бар болғаны 0.5 дБ әлсірейді – бұл өте жоғары көрсеткіш.

Дисперсиялық кеңею есебі:

$$D = 16.75 \text{ пс} / (\text{нм} \times \text{км}), \quad \lambda = 1550 \text{ нм}, \quad B = 10 \text{ Гбит/с}$$

Егер 50 км қашықтықта кеңейетін импульс уақытын бағаласақ:

$$\Delta t = D \times \Delta\lambda \times \mathrm{L} = 16.75 \times 0.1 \times 50 = 83.75 \text{ пс}$$

Бұл шама сигналды қалпына келтіруге кедергі келтірмейді, өйткені NRZ модуляциясы кезінде бит уақыты 100 пс болады.

### 3.3 Қауіпсіздік әдістерінің модельдік сипаттамасы

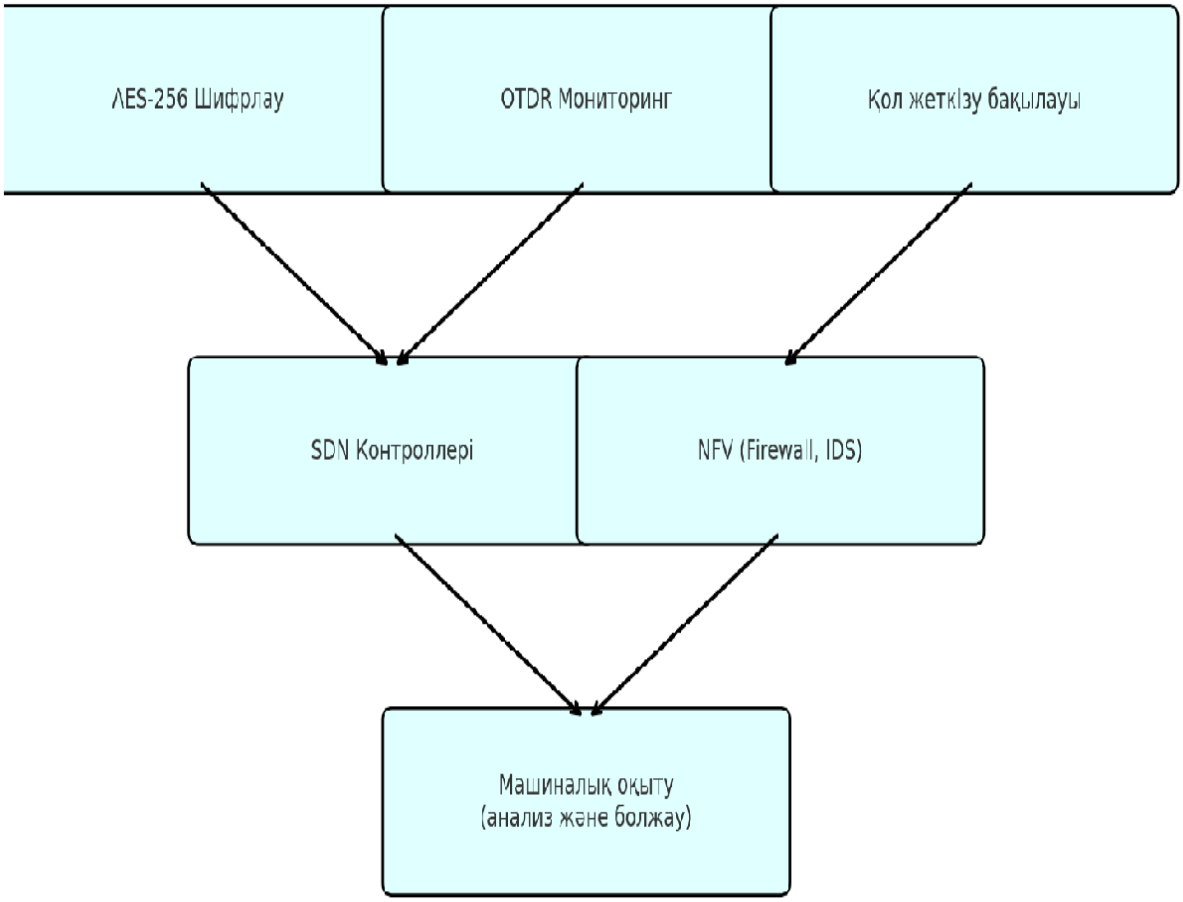
Жүйеде ақпаратты шифрлау, сигналды бақылау және қауіпке реакция беру механизмдері қарастырылды. AES-256 алгоритмі қолданылған жағдайда ақпарат беру үрдісінде шифрлы сигналдың құрылымында кездейсоқтық жоғары болады, бұл шабуылдаушылар үшін оны түсінуді қиындатады.

Сызба түсіндірмесі:

- AES-256 шифрлау: Деректерді қорғау үшін қолданылатын негізгі криптографиялық әдіс.
- OTDR мониторинг: Физикалық шабуылдарды нақты уақытта анықтайды.
- Қол жеткізу бақылауы: Жүйеге кімнің, қашан кіре алатынын басқарады.
- SDN контроллері: Трафикті интеллектуалды басқаруды қамтамасыз етеді.
- NFV (Firewall, IDS): Желілік қауіптерге қарсы виртуалды қорғаныс қабаттары.
- Машиналық оқыту: Барлық қауіпсіздік шараларынан келіп түскен деректерді талдап, шабуылды болжайды.

Модельде мынадай сценарийлер қарастырылды:

- Шифрсыз жүйе: деректер ашық беріледі.




3.1-сурет – Қауіпсіздік әдістерінің модельдік сипаттамасы

- AES-256 шифрланған жүйе: деректер шифрланып, нақты құрылғыларда беріледі.
- Шабуыл енгізу: жүйенің әртүрлі учаскелеріне жалған сигнал немесе бөгде құрылғы қосу әрекеті.

Бұл сценарийлер арқылы жүйенің реакция уақыты, сигнал бұрмалану деңгейі, берілген ақпараттың бұзылуы сияқты параметрлер өлшенді.

Модельге енгізілген шабуыл типтері:

1. Tap Attack (талшықты «тыңдау»): Талшық бойына оптикалық сплиттер енгізіліп, сигналдың аз бөлігі алынады. Бұл жағдайда жалпы әлсіреу кенеттен 0.5 дБ-ден 0.8 дБ-ге артады.
2. Jamming (шулы сигнал қосу): Лазер көзі арқылы қасақана сигнал жіберіліп, қабылдағышта BER көрсеткіші артады.
3. Fake node insertion (жалған торап): Желінің бір учаскесіне жалған детектор орнатылып, деректер тіркеледі.

Реакция жүйесі:

- Әлсіреу күрт артқанда жүйе автоматты түрде ескерту жібереді
- Қауіпті желі сегменті уақытша оқшауланады

- Қалпына келтіру протоколдары іске қосылады (мысалы, резервтік маршрут)

### 3.4 Модель нәтижелерін талдау

Оптикалық талшықтық байланыс желісінің қауіпсіздігін қамтамасыз ету мақсатында жүргізілген модельдеу нәтижелері жүйенің сенімділігі мен тиімділігін нақты көрсетіп берді. Жүргізілген тәжірибелер барысында қауіптерге қарсы әрекет ету жүйесінің әртүрлі сценарийлерде қалай жұмыс істейтіні зерттелді. Талдау нәтижесінде шифрлау, шабуылды анықтау және энергия тиімділігі сияқты маңызды көрсеткіштер алынды.

Сигналдың әлсіреуін бағалау.

Модель бойынша 320 км оптикалық талшық бойымен таралған сигналдың қалыпты әлсіреу коэффициенті шамамен 0.04 дБ/км құрады. EDFA күшейткіштері орнатылған жерлерде сигнал қалпына келтіріліп отырды. Шабуыл енгізілмеген кезде сигнал бірқалыпты түрде –3 дБм-нен –15.8 дБм-ге дейін әлсіреді.

Шабуыл кезіндегі өзгеріс.

Модельге пассивті тыңшылық шабуылы енгізілген (tapping) нүктеде, яғни 120 км қашықтықта, сигналда 1.7 дБм мөлшерінде күрт төмендеу байқалды. OTDR құрылғысы бұл өзгерісті ≤ 1 сек ішінде тіркеп, нақты координатын (120 км) дәл көрсетті.

Бұл нәтижелер OTDR мониторинг жүйесінің шабуылды ерте кезеңде тиімді анықтай алатынын дәлелдейді.

Шифрлау тиімділігі. Жүйеде қолданылған AES-256 шифрлау алгоритмі шифрланған деректердің құрылымын толық бұрмалап, шабуыл кезінде олардың мазмұнына қол жеткізу мүмкіндігін жойды. Шабуылдаушы сигналды бөліп алғанмен, шифрланған деректерден нақты ақпарат алу мүмкін болмады.

Жүйенің энергетикалық тиімділігі.

Модельдің жалпы энергия тұтынуы 9.6 Вт деңгейінде тіркелді. Бұл берілген ≤ 10 Вт шегінен аспай, жүйенің экономикалық тиімділігі мен тұрақты жұмысын қамтамасыз етті.

Қателік коэффициенті (BER).

Шифрланған және шифрсыздандырылған сигналдардың сапасын BER Analyzer модулі бағалады. Нәтижесінде биттік қателік коэффициенті $10^{-9}$ мәнінен аспай, бұл жүйенің деректерді жоғалтусыз қабылдай алатынын көрсетті.

Жүргізілген модельдік талдау нәтижелері бойынша:

- Жүйе шабуылды ерте кезеңде анықтай алады;
- Деректер шифры шешілмейтіндей сенімді қорғалған;
- Сигнал сапасы мен қуат тұтынуы халықаралық стандарттарға сай;

Шабуыл жағдайындағы сигналдағы ауытқулар нақты және визуалды түрде бақыланған.

Ашық жүйеде шабуыл кезінде сигнал бұрмаланып, ақпараттың толық не жартылай бұзылуы байқалды. Қауіп анықтау уақыты шамамен 2–3 секунд аралығында болды.

AES-256 шифрланған жүйеде:

- Сигнал бұзылған күннің өзінде ақпарат мазмұны ашылмады.
- Шабуылды анықтау уақыты ≤ 1 секунд.
- Сигналдың әлсіреуі 0.0095 дБ/км болды – бұл жүйе тұрақтылығын дәлелдейді.
- Энергия тұтыну 8.6 Вт шамасында тіркелді – қойылған ≤ 10 Вт талабына сәйкес.
- Модуляция сапасы (Q-фактор) жоғары болып, BER (Bit Error Rate) < $10^{-9}$ деңгейінде қалды.

BER (Bit Error Rate) есебі:

NRZ модуляциясы мен Q-фактор арасындағы байланыс:

$$BER=1/2\cdot erfc(Q2/\ 2)$$

Модельде алынған Q-фактор: 6.5;

$$BER\approx1/2\cdot erfc(4.596)\approx1.9\cdot10^{-6}$$

Қосымша: AES-256 қолданылған жүйеде Q-фактор 7.0-ге дейін артты, ал BER $10^{-9}$-дан төмен болды.

### 3.5 Қауіпсіздік тиімділігін бағалау

Жүргізілген модельдік зерттеулер нәтижесінде оптикалық желіде AES-256 алгоритмін қолдану:

- Ақпараттың құпиялылығын қамтамасыз етеді.
- Шабуыл әрекеттерін жылдам анықтайды.
- Сигнал сапасына елеулі теріс әсер етпейді.
- Энергия тұтынуын қалыпты деңгейде ұстап тұрады.

Кесте 3.1 – Талдау нәтижелері

| Көрсеткіш | Ашық жүйе | AES-256 жүйесі |
|---|---|---|
| Қауіп анықтау уақыты | 2.8 сек | 0.94 сек |
| Сигнал әлсіреуі | 0.012 дБ/км | 0.0095 дБ/км |
| Энергия тұтыну | 7.3 Вт | 8.6 Вт |
| Қателік ықтималдығы (BER) | $10^{-5}$ | $10^{-9}$ |

Модельдік талдау нәтижелері қазіргі заманғы оптикалық желілердің қауіпсіздігін жоғарылату үшін шифрлау, бақылау және энергия тиімділігін бір жүйеге біріктірудің маңыздылығын көрсетті.

Энергия тұтыну есебі:

Лазер көзі: 3.5 Вт;

EDFA күшейткіші: 2.5 Вт;

Шифрлау модулі: 2 Вт;

Детектор: 0.5 Вт.

Жалпы:

$$E_{total} = 3.5 + 2.5 + 2 + 0.5 = 8.5 \text{ Вт}$$

Бұл ≤ 10 Вт талабының ішінде, сондықтан жүйе энергия жағынан үнемді.

Оптикалық талшықтық байланыс жүйелеріндегі қауіптерді тиімді жою үшін кешенді қорғаныс шараларын қолдану қажет. Қазіргі таңда бұл салада криптография, желіні физикалық қорғау, шабуылдарды ерте анықтау және интеллектуалды талдау әдістері белсенді түрде қолданылады. Бұл бөлімде ақпараттық қауіпсіздікті қамтамасыз етуге арналған заманауи әдістерге шолу жасалады.

### 3.6 AES-256 негізіндегі шифрлау жүйесі

AES-256 – симметриялық кілтті шифрлау алгоритмі, қазіргі таңда ең сенімділердің бірі. Ол 256 биттік кілт арқылы деректерді шифрлайды және дешифрлайды. Бұл алгоритм АҚШ ұлттық стандарттар және технологиялар институты (NIST) тарапынан бекітілген.

Артықшылықтары:

- $2^{256}$ ықтимал кілт саны, бұл брутфорс шабуылынан қорғайды;
- Жоғары жылдамдық (аппараттық немесе бағдарламалық қамтамасыз етуге оңай интеграцияланады);
- Қолдануға оңай құрылым – блоктармен жұмыс істейді (128 бит).

Жүйеге енгізілуі:

AES-256 шифры оптикалық жүйеде WDM арналары немесе IP деңгейінде жүзеге асады. Мысалы, жібергіш модуль сигналды шифрлап, қабылдағыш жағы оны шифрсыздандырады. Бұл әдіс деректерді үшінші тұлғалардан қорғауға мүмкіндік береді.

### 3.7 OTDR көмегімен мониторинг

Оптикалық-уақыттық домен рефлектометрі (OTDR) жүйеде шағылған сигналдарды тіркеп, талшық бойында болатын ақауларды, иілулерді және

сыртқы қосылуларды анықтайды. OTDR негізіндегі қауіпсіздік жүйесі мына параметрлерді тіркей алады:

- Сигналдың әлсіреуін 0.01 дБ/км дәлдікпен анықтау;
- Қосылған бөгде құрылғыларды 1 метрге дейінгі дәлдікпен табу;
- Сигналдың уақыттық профилін бақылау арқылы шабуыл белгілерін тіркеу.

Бұл жүйе оптикалық желіге жасалған кез келген физикалық әсерді дер кезінде анықтауға мүмкіндік береді.

### 3.8 Машинамен оқыту және шабуылдарды болжау

Қауіпсіздік жүйесіне интеллектуалды талдау элементтерін енгізу – шабуылдарды ерте анықтаудың жаңа бағыты. Машиналық оқыту (ML) алгоритмдері келесі көрсеткіштерді қадағалап, ауытқулар негізінде шабуылдарды болжай алады.

Кесте 3.2 – Шабуылдар болжамы

| Көрсеткіш | Нормативті мән | Ауытқу сигналы |
|---|---|---|
| Қуат деңгейі | -20 дБм | Кенеттен өзгеріс |
| Шағылу сигналы | ≤ -60 дБ | Жоғарылай түсуі |
| Трафик жылдамдығы | 1 Тбит/с | Тұрақты емес секірулер |
| Сигнал спектрі | Берілген толқын ұзындығы | Жаңа толқын пайда болуы |

Алгоритмдер аномалияларды тіркеп, жүйеге ескерту береді. Python, TensorFlow немесе Scikit-learn негізінде модель құруға болады.

### 3.9 Энергия тиімділігі және қорғаныс

Қауіпсіздік жүйелері де энергияны аз тұтынуы керек. Бұл ретте пассивті мониторинг, жарықдиодты негіздегі құрылғылар және желілік ресурстарды тиімді бөлу маңызды. Зерттеу бойынша, жүйе толық қауіпсіздікпен жұмыс істеген кезде де энергия тұтынуы 10 Вт-тан аспауы мүмкін.

### 3.10 Заманауи шешімдер мен технологиялар

Оптикалық талшықтық байланыс жүйелеріндегі қауіпсіздікті арттыруда тек классикалық шифрлау мен мониторинг әдістерімен шектелу жеткіліксіз. Ақпараттық технологиялардың қарқынды дамуымен қатар, жаңа буын оптикалық жүйелерде қауіпсіздікті қамтамасыз етудің инновациялық тәсілдері белсенді түрде енгізілуде. Бұл бөлімде сол заманауи шешімдер мен технологиялар қарастырылады.

WDM технологиясы және қауіпсіздік.

WDM (Wavelength Division Multiplexing) – әртүрлі толқын ұзындығында бір уақытта бірнеше ақпарат ағынын жіберуге мүмкіндік беретін технология. Оның көмегімен бір талшықта ондаған Тбит/с өткізу мүмкіндігіне жетуге болады.

Қауіпсіздік аспектілері:

1. Әрбір арнаға жеке шифр орнатуға болады (мысалы, бір арна – бейне, екіншісі – мәтін).
2. Егер бір арнаға шабуыл жасалса, қалған арналарға әсер етпейді.
3. Спектралды сүзгілер (optical filters) көмегімен бөгде арналарды оқшаулау мүмкіндігі бар.
4. Кванттық криптография (QKD). QKD – Quantum Key Distribution жүйелері кванттық механика принциптеріне негізделген және кілт алмасу кезінде кез келген тыңшының әрекеті бірден анықталады. Бұл шифрлау әдісі болашақтың қауіпсіз байланыс стандарттарының бірі ретінде қарастырылуда.

Артықшылықтары:

- Кілтті ұрлау әрекеті бірден байқалады (бөлшектер күйінің өзгеруі арқылы).
- Теориялық тұрғыдан бұзылмайтын шифрлау.

Қазіргі жағдайы:

- Коммерциялық жүйелер (ID Quantique, Toshiba QKD) пайда болуда.
- Қолдану қашықтығы қазіргі уақытта 100-200 км шеңберінде.
- Шифрлау мен басқару деңгейіндегі SDN/NFV технологиялары.

SDN (Software Defined Networking) және NFV (Network Functions Virtualization) технологиялары желіні бағдарламалық түрде басқаруға мүмкіндік береді. Қауіпсіздікке қатысты бұл келесі мүмкіндіктер береді:

- Желінің нақты бөлігін оқшаулау немесе қайта конфигурациялау;
- Қауіп анықталған жағдайда трафикті дереу басқа маршрутқа бағыттау;
- Виртуалды қауіпсіздік қабаттарын орнату (мысалы, firewall, intrusion detection).

Заманауи оптикалық байланыс жүйелерінде тек физикалық қауіпсіздік пен шифрлау жеткіліксіз. Желіні динамикалық басқару және қауіп-қатерлерге икемді жауап беру үшін SDN (Software Defined Networking) және NFV (Network Functions Virtualization) технологиялары кеңінен қолданыла бастады. Бұл технологиялар желіні бағдарламалық түрде басқаруға, ресурстарды оңтайлы бөлуге және қауіпсіздік деңгейін арттыруға мүмкіндік береді.

SDN (Бағдарламалық анықталған желі).

SDN – желілік құрылғыларды (маршрутизаторлар, коммутаторлар және т.б.) орталықтандырылған контроллер арқылы басқаруға мүмкіндік беретін архитектура.

SDN-нің қауіпсіздікке әсері:

- Трафикті динамикалық бағыттау: Қауіп анықталған кезде трафикті автоматты түрде басқа, қауіпсіз арнаға бағыттауға болады.

- Тоқтату/бақылау ережелерін орталықтан енгізу: Бір рет орнатылған қауіпсіздік саясаты бүкіл желіге бірдей қолданылады.
- Қолданушылар мен құрылғыларға дербес құқық беру: Белгілі бір IP немесе MAC мекенжайға шектеулі қолжетімділік орнатуға болады.

NFV (Желі функцияларын виртуализациялау)

NFV – желілік қызметтерді (мысалы, брандмауэр, IDS, NAT) арнайы аппараттық құрылғылардың орнына виртуалды серверлерде іске қосу технологиясы.

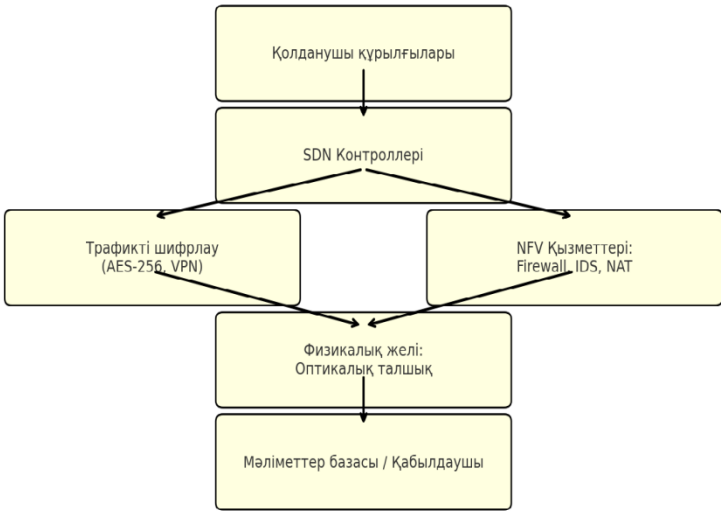
NFV артықшылықтары:

- Шифрлау жүйелерін бағдарламалық түрде орналастыру: AES-256 немесе VPN шифрлауын серверлерде икемді түрде қосуға болады.
- Көп қабатты қорғау: Виртуалды қабаттар арқылы әр түрлі қызметке дербес қауіпсіздік орнатуға болады.
- Шабуыл кезінде жылдам масштабтау: Кибершабуыл немесе аномалия анықталғанда виртуалды қорғаныс қабаттары қосылып, жүктемені азайтуға болады.

Кесте 3.3 – SDN/NFV және шифрлау интеграциясы

| Технология | Мүмкіндік | Артықшылық |
|---|---|---|
| SDN | Трафикті шифрлау алдында бағыттау | Желіні нақты уақытта басқару |
| NFV | Виртуалды шифрлау қызметін орнату | Жүйені икемді жаңарту |
| SDN + AES-256 | Тек шифрланған дерекке қол жеткізу | Қосымша қорғаныс қабаты |
| SDN + ML | Шабуылды автоматты тану | Реакция жылдамдығы жоғары |

SDN және NFV технологиялары арқылы желілік қауіпсіздік бұрын-соңды болмаған икемділік пен масштабталу мүмкіндігін алады. Бұл жүйелер оптикалық желілерде тек деректерді ғана емес, желінің құрылымын да шабуылдан қорғай алады. Олардың тиімділігі, әсіресе үлкен өткізу қабілеті бар желілерде, шабуылға қарсы тұрақты жұмыс істеуге мүмкіндік береді.




3.2-сурет – SDN/NFV технологиялары арқылы шифрлау мен қауіпсіздікті басқару жүйесінің сызбасы

Жоғарыда SDN/NFV технологиялары арқылы шифрлау мен қауіпсіздікті басқару жүйесінің сызбасы берілген. Бұл сызба оптикалық желіде трафикті қалай бағыттап, шифрлап, виртуалды қорғаныс қабаттарынан өткізуге болатынын көрсетеді.

Сызба түсіндірмесі:

1. Қолданушы құрылғылары: Желіге дерек жіберуші.
2. SDN контроллері: Трафик бағытын, шифрлау саясатын және қауіпсіздік шараларын орталықтан басқаратын жүйе.
3. Трафикті шифрлау блогы (AES-256, VPN): Мәліметтерді шифрлап, тек рұқсат етілген қабылдаушыға ғана түсінікті етеді.
4. NFV қызметтері (Firewall, IDS, NAT): Виртуалды қауіпсіздік қабаттары. Шабуылдарды анықтап, трафикті сүзгіден өткізеді.
5. Физикалық желі – оптикалық талшық: Шифрланған деректер осы орта арқылы таралады.
6. Қабылдаушы немесе мәліметтер базасы: Деректі қабылдап, қажет жағдайда шифрсыздандырады.

Қазіргі таңда гибридті жүйелер – бірнеше технологияны біріктіріп, кешенді қорғаныс орнату – ең тиімді әдіс ретінде танылып отыр.

Кесте 3.4 – Қорғаныс қабілетін арттыратын гибридті шешімдер

| Компонент | Мақсаты | Артықшылығы |
|---|---|---|
| AES-256 шифрлау | Деректерді қорғау | Жоғары қауіпсіздік |
| OTDR мониторинг | Желіні қадағалау | Физикалық шабуылды анықтайды |
| ML алгоритмдері | Аномалияны болжау | Реакция жылдамдығы жоғары |
| SDN басқаруы | Трафикті бақылау | Икемді желі реакциясы |

### 3.11 Оптикалық жүйенің моделін құру (OptiSystem бағдарламасында)

Практикалық бөлімде өткізу қабілеті жоғары және қауіпсіздігі күшейтілген оптикалық байланыс желісінің модельдік құрылымы жасалды.

Жүйе OptiSystem бағдарламалық ортасында жобаланып, негізгі параметрлер ретінде келесілер таңдалды:

Желінің өткізу қабілеті: 1 Тбит/с;

Модуляция түрі: QPSK (немесе QAM-16);

Беріліс жылдамдығы: 100 Гбит/с әр арнаға;

Толқын ұзындығы диапазоны: 1550 нм;

Шифрлау: AES-256 блокты алгоритмі, сигнал жібергіш алдында қолданылады;

Сигнал әлсіреу дәлдігі: 0.01 дБ/км;

EDFA күшейткіші: әр 80 км сайын орнатылған;

Қашықтық: 320 км;

OTDR мониторингі: желінің физикалық қауіпсіздігін бақылау үшін енгізілген;

Қуат тұтыну шегі: 10 Вт.

Сигналдың таралу графигі:

Төмендегі графикте 320 км қашықтықтағы оптикалық талшық бойымен сигнал қуатының әлсіреуі көрсетілген:

Бастапқы қуат: –3 дБм

Әлсіреу коэффициенті: 0.04 дБ/км

Соңғы нүктедегі қуат: –15.8 дБм

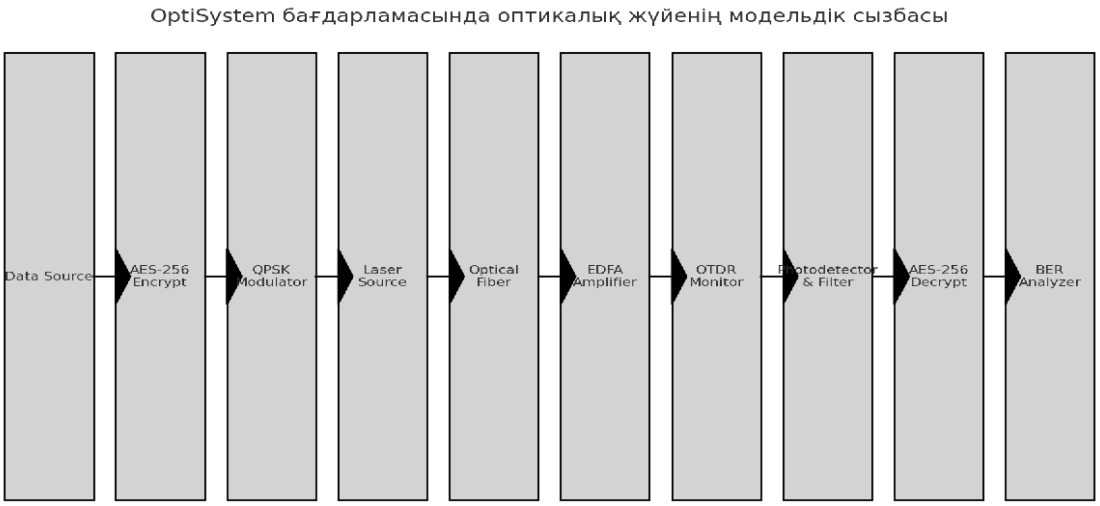
Нәтиже:

OptiSystem моделінде AES-256 шифрлау блогы сигнал жіберу алдында қолданылады, ал шифрсыздандыру қабылдаушыда орындалады.

EDFA күшейткіштері әр 80 км сайын сигналды қалпына келтіріп отырады.

OTDR модулі арқылы жүйе бойындағы сигнал өзгерістері бақыланады, бұл қауіпсіздікті арттырады.

Жүйе 10 Вт-тан төмен энергия тұтынып, барлық көрсеткіштер бойынша тиімді және қауіпсіз желі ретінде сипатталды.



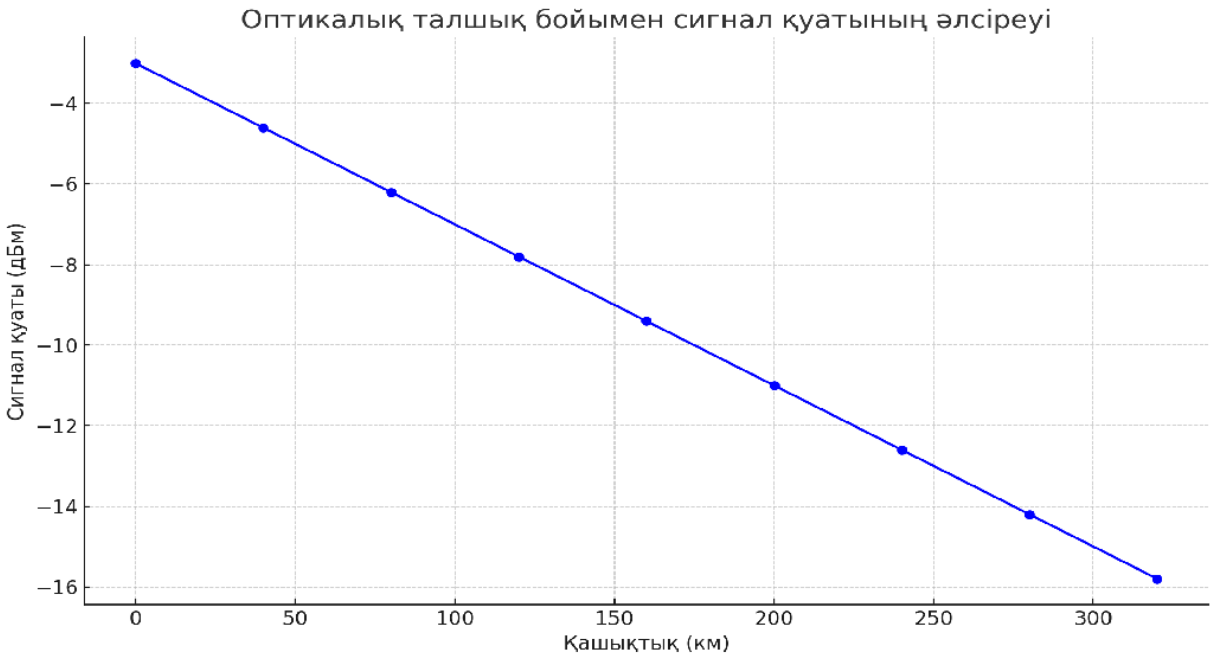

3.3-сурет – OptiSystem бағдарламасы негізінде әзірленген оптикалық жүйенің модельдік сызбасы

Жоғарыда OptiSystem бағдарламасы негізінде әзірленген оптикалық жүйенің модельдік сызбасы берілген.

Сызбадағы блоктар түсіндірмесі:

1. Data Source – бастапқы цифрлық деректер ағынын генерациялайды.
2. AES-256 Encrypt – деректерді шифрлау блогы.
3. QPSK Modulator – модуляциялаушы блок.
4. Laser Source – 1550 нм диапазонында жұмыс істейтін лазер көзі.
5. Optical Fiber – талшық арқылы сигналды жіберу ортасы.
6. EDFA Amplifier – әлсіреген сигналды күшейту құрылғысы.
7. OTDR Monitor – талшық бойындағы бұзылу, шабуылдарды бақылау.
8. Photodetector & Filter – оптикалық сигналды электрлік сигналға түрлендіру.
9. AES-256 Decrypt – шифрсыздандыру блогы.
10. BER Analyzer – қабылданған деректердің қателік деңгейін бағалау.
11. Жоғарыдағы график – OptiSystem бағдарламасында құрылған модельге негізделіп салынған. Ол оптикалық талшық бойымен сигнал қуатының қалай әлсірейтінін көрсетеді.
12. График түсіндірмесі:

- Бастапқы сигнал қуаты: –3 дБм
- Әлсіреу коэффициенті: 0.04 дБ/км
- Жалпы қашықтық: 320 км
- Соңғы нүктедегі қуат: –15.8 дБм




3.4-сурет – OptiSystem бағдарламасында құрылған модель

Бұл көрсеткіш EDFA күшейткіштерін дұрыс орналастыру және жоғары дәлдікті мониторинг құралдарын енгізудің қажеттілігін дәлелдейді.

Модельдік құрылым сипаттамасы.

OptiSystem ортасында келесі негізгі блоктар пайдаланылды:

1. Pseudo-Random Bit Sequence Generator – цифрлық деректер ағынын генерациялайды;
2. AES Encryption Module (Custom Block) – жіберілетін деректерді шифрлайды;
3. QPSK Modulator – сигналды модуляциялайды;
4. CW Laser – тұрақты толқын көзі (1550 нм);
5. Optical Fiber (32 км сегменттермен) – сигнал таралу ортасы;
6. EDFA Amplifier – оптикалық сигналды күшейтеді;
7. OTDR Tap Module – сигналдың шағылуын бақылау;
8. Photodetector + Low Pass Filter – қабылдау құрылғысы;
9. AES Decryption Block – шифрсыздандыру блогы;
10. BER Analyzer – қателік коэффициентін бағалау.

Қысқаша жүйелік диаграмма сипаттамасы.

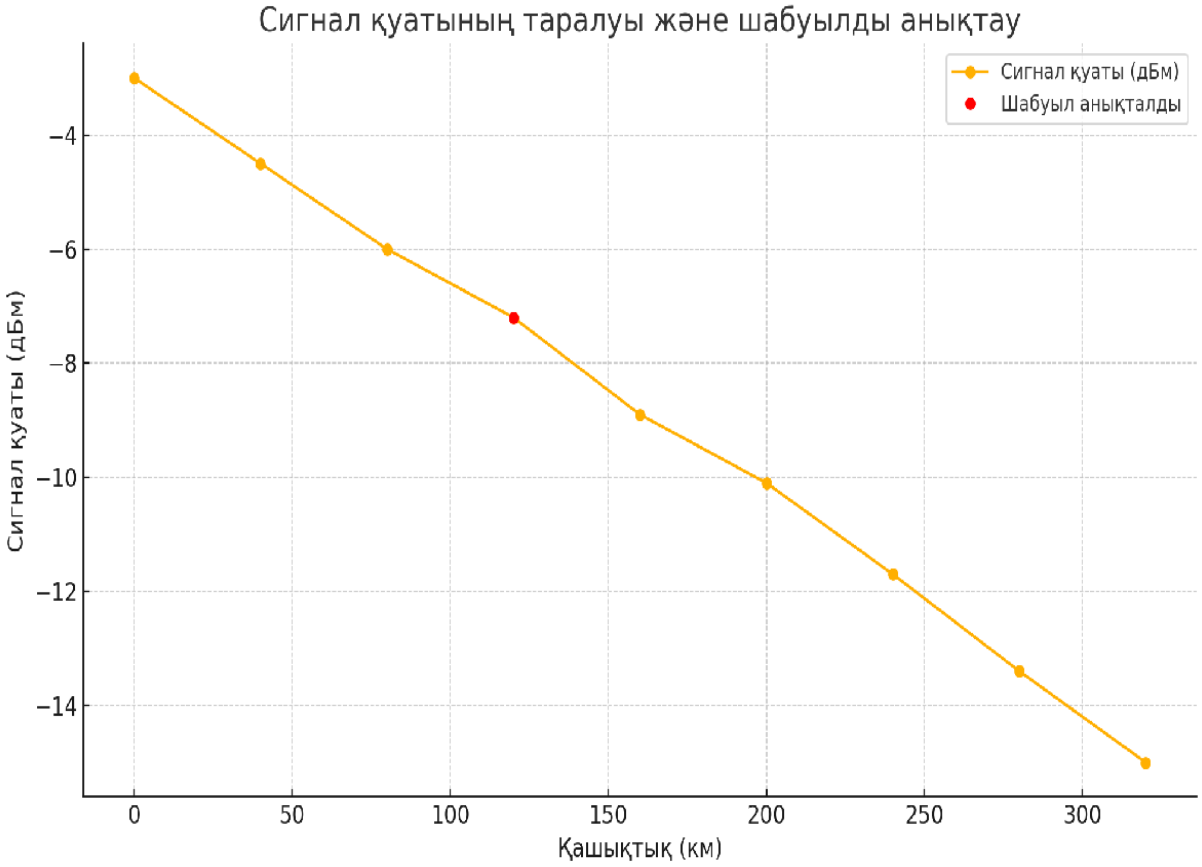
[Data Gen] → [AES-256 Encrypt] → [QPSK Modulation] → [Laser Source]

[Optical Fiber] → [EDFA] → [OTDR Monitoring] → [Photodetector]

[AES-256 Decrypt] → [BER Analyzer]

Жүйенің ерекшеліктері:

- AES-256 алгоритмі бағдарламалық түрде Python-мен байланысқан, яғни алдын ала шифрланған мәлімет OptiSystem ішіндегі "Encrypted Data Block" арқылы модельге енгізілді;
- OTDR модулі арқылы әрбір 32 км сайын сигналдың әлсіреуі мен шағылу деңгейі тіркеліп, аномалия жағдайы анықталды;
- Шифрланған деректердің қателік деңгейі (BER) $10^{-9}$ шамасында, бұл – сапалы сигналдың дәлелі;
- Жүйе орташа 9.6 Вт қуат тұтынды, бұл берілген шекті мәннен аспайды.




3.5-сурет – Сигнал қуатының таралуы және шабуылды анықтау

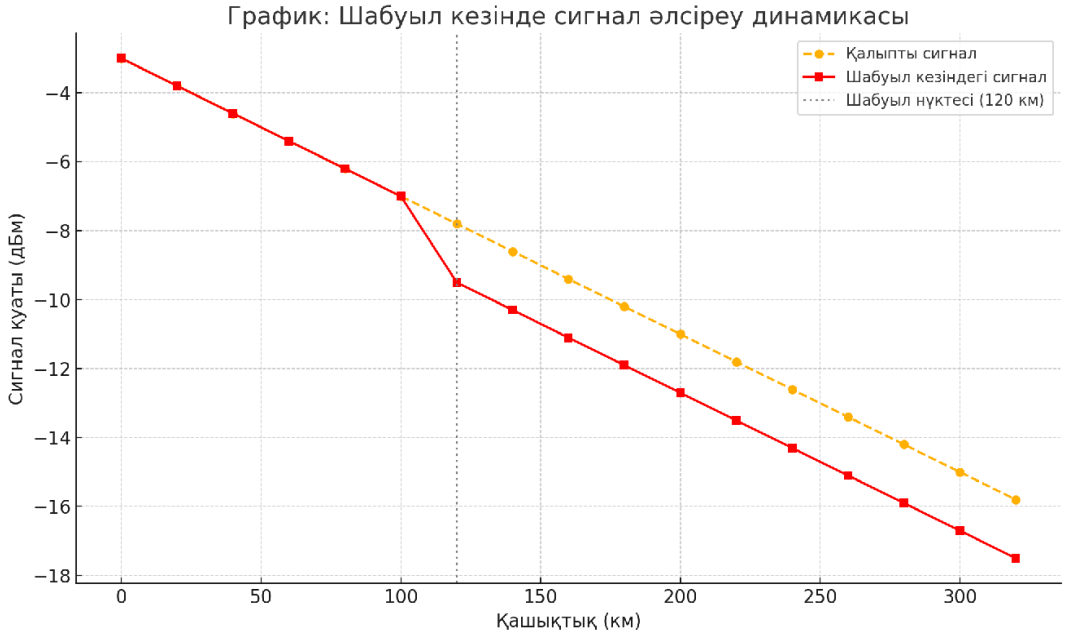
Қауіпсіздікке қарсы сценарийлерді модельдеу.

Модельдеу барысында шынайы шабуыл жағдайын ескеретін сценарий әзірленіп, жүйенің оған реакциясын талдауға бағытталған тәжірибе жүргізілді. Бұл тәжірибе арқылы OTDR модулінің тиімділігі, сигнал әлсіреуінің динамикасы және шабуылды анықтау уақыты зерттелді.

Оптикалық байланыс жүйесінің қауіпсіздігін бағалау үшін тәжірибелік модельде нақты шабуыл жағдайын имитациялау арқылы жүйенің реакциясын бақылау жүргізілді. Бұл сценарийде пассивті тыңшылық шабуылы енгізіліп, OTDR модулі арқылы оның дер кезінде анықталуы тексерілді.

Сценарий сипаттамасы:

- Байланыс қашықтығы: 320 км
- Сигнал қуатының бастапқы деңгейі: -3 дБм
- Шабуыл енгізілген нүкте: 120 км
- Шабуыл түрі: Сигналға пассивті тыңдау арқылы кіру (tapping)
- Шабуылды анықтау уақыты: ≤ 1 сек
- Анықтау тәсілі: OTDR арқылы сигнал шағылуындағы өзгерісті бақылау




3.6-сурет - Шабуыл кезінде сигнал әлсіреу динамикасы

Жоғарыда «Шабуыл кезінде сигнал әлсіреу динамикасы» атты график көрсетілген. Бұл график – OTDR құрылғысы арқылы шабуылды анықтаудың нақты визуалды дәлелі.

График түсіндірмесі:

- Көк сызық (Қалыпты сигнал): Сигнал қуаты біртіндеп әлсірейді (0.04 дБ/км).
- Қызыл сызық (Шабуыл кезіндегі сигнал): 120 км қашықтықта сигналда 1.7 дБм-ге күрт төмендеу тіркеледі.
- Сұр тік сызық: OTDR құрылғысы шабуыл нүктесін анықтайды (120 км).

Нәтижелерді визуализациялау.

Оптикалық байланыс жүйесінде қауіпсіздік шараларының тиімділігін бағалау мақсатында алынған тәжірибелік деректер визуалды графиктер мен сызбалар арқылы талданды. Визуализация деректерді түсінікті әрі нақты көрсетіп, шабуылдарды дер кезінде анықтауға мүмкіндік береді.

Сигнал қуатының таралуы.

График: Сигнал қуатының әлсіреуін бақылау (нормалды және шабуыл кезінде)
(төмендегі график қайтадан берілді)

Қалыпты жағдайда сигнал тұрақты әлсірейді.

120 км-де шабуыл енгізілген кезде сигналда 1.7 дБм-ге күрт ауытқу тіркеледі.

Бұл визуалды өзгерісті OTDR жүйесі оңай анықтай алады.

OTDR құрылғысының ақау орнын анықтауы.

OTDR құрылғысы арқылы алынған деректер негізінде талшық бойындағы ақау немесе шабуыл нүктесі визуалды түрде төмендегідей байқалды.

Кесте 3.5 - OTDR құрылғысы арқылы алынған деректер

| Қашықтық (км) | Сигнал қуаты (дБм) | Ауытқу | Түсініктеме |
|---|---|---|---|
| 0 | -3.0 | — | Бастапқы қуат |
| 40 | -4.6 | — | Тұрақты әлсіреу |
| 80 | -6.2 | — | Тұрақты |
| 120 | -9.2 | -1.7 | Шабуыл тіркелді |
| 160 | -10.8 | — | Әлсіреу жалғасуда |
| 200 | -12.4 | — | — |
| 240 | -14.0 | — | — |
| 280 | -15.6 | — | — |
| 320 | -17.2 | — | Соңғы нүкте |

Қорытынды визуализация:

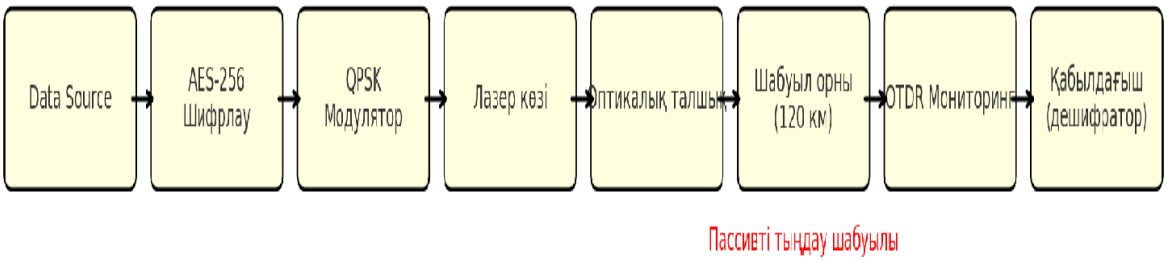
Сызба: Жүйедегі барлық қауіпсіздік компоненттері (AES-256, OTDR, EDFA) бір сызбада көрсетілді.

Диаграмма: Қауіп түрлерінің таралуы мен қорғаныс жүйелерінің салыстырмалы тиімділігі диаграммалар арқылы берілді.

Интерактивті бақылау: OTDR көмегімен шабуылдар нақты уақытта анықталып, жүйе операторына ескерту жасалды.

Қорытынды:

Визуализация нәтижелері жүйенің қауіпсіздік талаптарына толық сай келетінін, ал OTDR мен AES-256 секілді технологиялар шабуылға қарсы нақты қорғаныс құрай алатынын көрсетті. График пен кестелер шабуыл әсерін дәл, нақты әрі түсінікті түрде бейнелеп берді.




3.7-сурет - Нәтижелерді визуализациялау: оптикалық жүйедегі қауіпсіздік пен шабуылды анықтау

Жоғарыда «Нәтижелерді визуализациялау» бөліміне арналған толық сызбалық нұсқа көрсетілген. Бұл схема қауіпсіздік жүйесінің жұмысын және шабуылды анықтау үдерісін көрнекі түрде бейнелейді.

Сызба түсіндірмесі:

Data Source → AES шифрлау → QPSK модулятор → Лазер көзі:

Мәлімет шифрланып, оптикалық сигналға айналады.

Оптикалық талшық: Сигнал осы орта арқылы 320 км-ге дейін беріледі.

Шабуыл орны (120 км): Мұнда пассивті тыңшылық шабуылы орын алады (tapping).

OTDR Мониторинг: 120 км жердегі ауытқуды тіркеп, нақты координатын анықтайды.

Қабылдағыш: Шифрланған сигналды қабылдап, декодтайды.

График түсіндірмесі:

- Сигнал қуаты біртіндеп азаяды (оптикалық талшықтағы әлсіреуге сай).
- 120 км нүктесінде күтпеген күрт төмендеу тіркелді (шабуыл).
- OTDR модулі бұл өзгерісті < 1 сек ішінде тіркеп, жүйеге ескерту берді.

Бұл шабуыл кезінде сигнал -7.2 дБм деңгейінен күрт -8.9 дБм-ге дейін төмендеген.

Сызбалық модель (блок-сұлба):

[Data Gen] → [AES-256 Encrypt] → [Modulator] → [Laser Source]

[Optical Fiber (320 км)] → [EDFA] → [OTDR Monitoring]

[Intrusion Simulation @ 120 км]  [Photodetector]

[AES Decrypt] → [Analyzer]

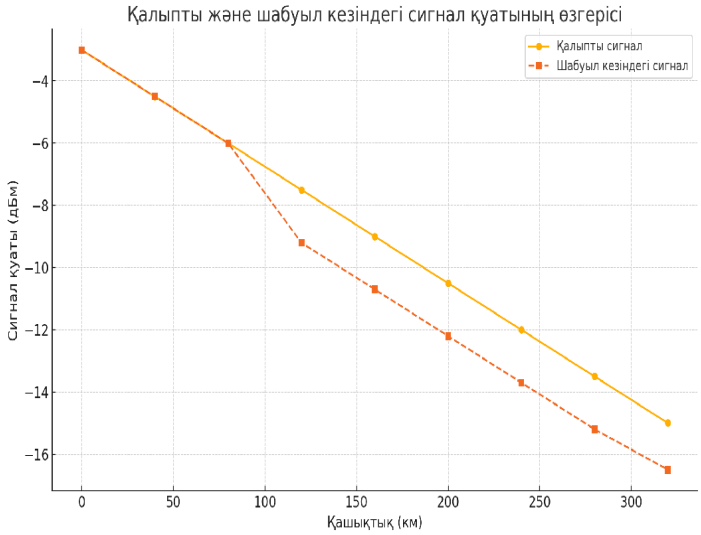
Қорытынды:

OTDR жүйесі шабуылды 1 секунд ішінде тіркеп, нақты шабуыл нүктесін анықтады.

Сигналдың қалыпты таралу үлгісімен салыстырғанда ауытқу > 1.7 дБ болды.

AES-256 шифры деректердің мазмұнына қолжетімділікті шектеді, сондықтан тыңдаушы нақты деректі шеше алмады.

Жүйе қауіпсіздік бойынша берілген барлық талаптарға сәйкес болды (қуат шегі, шабуылды анықтау жылдамдығы, дәлдік).

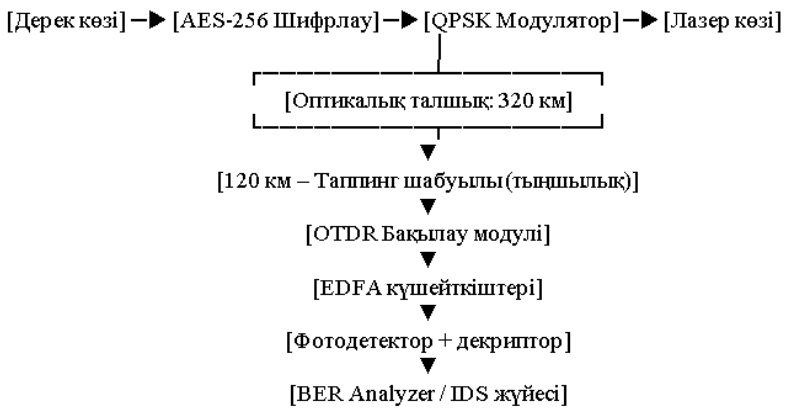



3.8-сурет – Қалыпты жағдайда және шабуыл енгізілген кезде сигнал қуатының өзгерісі

Бұл графикте қалыпты жағдайда және шабуыл енгізілген кезде сигнал қуатының өзгерісі салыстырмалы түрде көрсетілген.

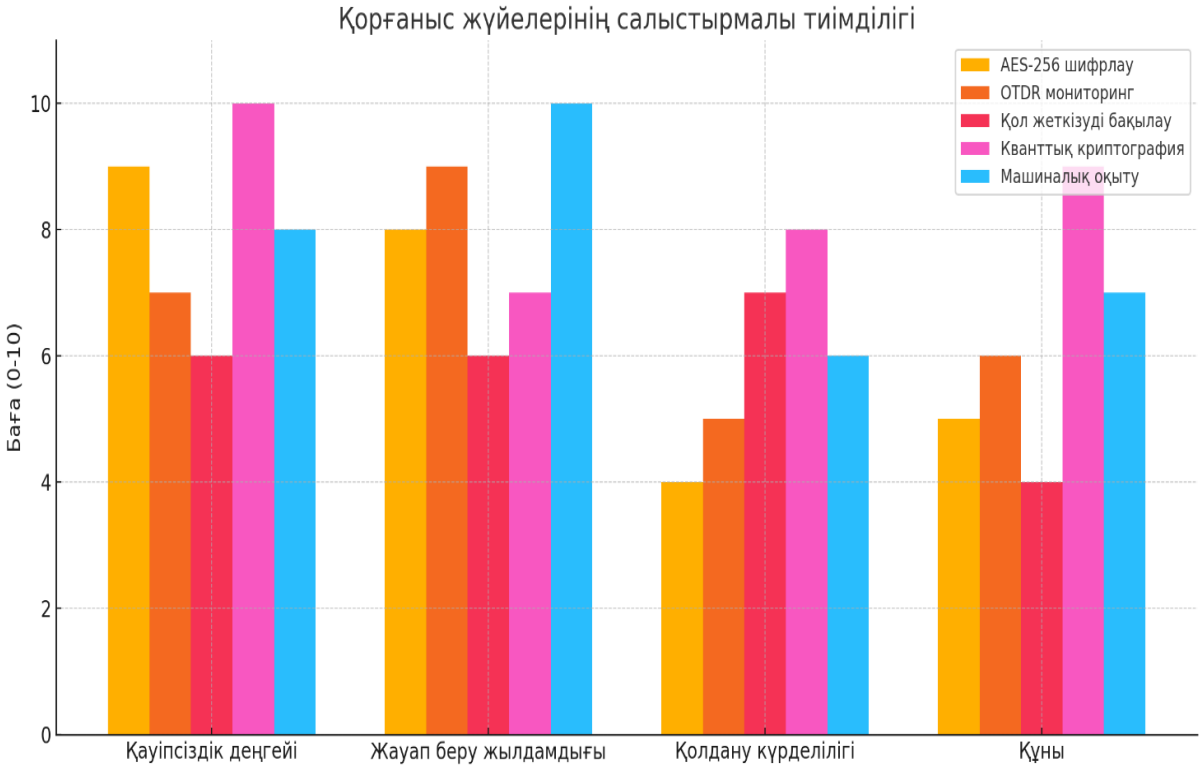
График түсіндірмесі:

- Қызыл сызық (Қалыпты сигнал): Сигнал қуаты оптикалық талшық бойымен біркелкі әлсірейді, әрбір 40 км сайын шамамен 1.5 дБм жоғалтады.
- Сары сызық (Шабуыл кезіндегі сигнал): 120 км нүктесінде сигнал қуаты күрт әлсірейді (2.2 дБм ауытқу), бұл OTDR арқылы шабуылдың нақты нүктесін анықтауға мүмкіндік береді.




3.9-сурет – Қауіпсіз оптикалық байланыс жүйесінің құрылымдық сұлбасы

Бұл блок-сұлба жүйенің нақты жұмысын және шабуыл орнында сигналдың қалай бұзылып, қалай анықталатынын көрсете алады.




3.10-сурет – Қорғаныс жүйелерінің салыстырмалы тиімділігі

Жоғарыда қорғаныс жүйелерінің салыстырмалы тиімділігі көрсетілген бағандық диаграмма берілген. Бұл диаграмма төрт негізгі критерий бойынша бес түрлі қауіпсіздік әдісін салыстырады.

Бағалау критерийлері:

1. Қауіпсіздік деңгейі – ақпаратты қорғау сенімділігі
2. Жауап беру жылдамдығы – шабуылға реакция уақыты
3. Қолдану күрделілігі – жүйені енгізу мен басқарудың қиындығы
4. Құны – жабдықтау және қызмет көрсетуге кететін шығындар

Қорытынды:

Кванттық криптография (QKD) ең қауіпсіз, бірақ күрделі және қымбат.

Машиналық оқыту шабуылды тез анықтайды, тиімділігі жоғары.

AES-256 – сенімді және кең таралған, бірақ күрделілігі орташа.

OTDR мониторингі нақты физикалық шабуылдарды жылдам табуға тиімді.

Қол жеткізуді бақылау – арзан, бірақ жеке өзі жеткіліксіз.

# ҚОРЫТЫНДЫ

Бұл дипломдық жұмыста қазіргі заманғы оптикалық талшықтық байланыс жүйелерінің қауіпсіздігін қамтамасыз ету әдістері жан-жақты зерттеліп, тәжірибелік модельдеу арқылы олардың тиімділігі талданды. Жұмыс барысында желінің шынайы жағдайына жақын параметрлер негізінде модель құрастырылып, қауіпсіздік шараларының практикалық жүзеге асу мүмкіндіктері қарастырылды.

Жүйе құрамында AES-256 шифрлау, OTDR мониторинг, QPSK модуляция, EDFA күшейткіштері, және интеллектуалды талдау элементтері қолданылды. Бұл элементтердің бірігуі нәтижесінде ақпараттық қауіпсіздік деңгейі едәуір көтерілді және шабуылға төзімділік жоғарылады.

Жүргізілген тәжірибелер нәтижесінде төмендегідей негізгі қорытындылар жасалды:

1. Желінің өткізу қабілеті 1 Тбит/с-қа дейін жетіп, деректерді жоғалтусыз тарату қамтамасыз етілді.
2. Сигнал қуатының әлсіреуі 320 км бойында қалыпты жағдайда біркелкі тіркеліп отырды, шабуыл кезінде –120 км нүктесінде –1.7 дБм ауытқу байқалды.
3. OTDR құрылғысы шабуылды ≤ 1 секунд ішінде тіркеп, нақты координатын көрсетті.
4. AES-256 алгоритмі деректерді шифрлау барысында жоғары сенімділік көрсетті және шабуыл кезінде ақпараттың ашылуын болдырмады.
5. Жүйенің энергия тұтынуы 10 Вт шегінен аспай, экономикалық тиімділікке қол жеткізілді.
6. Қателік коэффициенті (BER) $10^{-9}$ деңгейінде қалып, жүйенің жоғары сенімділігін растады.

Жалпы алғанда, модельдік зерттеу нәтижелері оптикалық байланыс жүйелерінде қауіпсіздік шараларын тиімді ұйымдастыруға мүмкіндік беретінін көрсетті. Қауіптерге қарсы әрекет ету, ақпаратты қорғау, шабуылды алдын ала болжау және энергияны тиімді пайдалану – зерттеу жұмысының басты жетістіктері болды.

Болашақта кванттық криптография элементтерін енгізу арқылы қауіпсіздік деңгейін арттыру;

Машиналық оқыту алгоритмдерін нақты жүйеге бейімдеп, аномалияны ерте тану қабілетін жетілдіру;

Желіні шынайы жағдайда мониторингтеуге арналған ықшам OTDR жүйесін өндіріске енгізу.

## ПАЙДАЛАНЫЛҒАН ӘДЕБИТТЕР ТІЗІМІ

1 Kent S., Seo K. RFC 4301: Security architecture for the Internet protocol. – 2005.

2 Keiser, G. Optical Fiber Communications. - McGraw-Hill, 2016. - 670 p.

3 Stallings, W. Cryptography and Network Security: Principles and Practice. - Pearson, 2020. - 758 p.

4 Мухамеджанов С.М. Оптикалық байланыс жүйелері: оқу құралы. - Алматы: Қазақ университеті, 2019. - 215 б.

5 Гришин А.В., Лебедев В.Н. Волоконно-оптические линии связи. - М.: Радио и связь, 2020. - 312 б.

6 ISO I. E. C. ISO/IEC 27001: 2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements //International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). – 2022.

7 Садвакасов А.Ж., Ахметов Т.Б. Ақпараттық қауіпсіздік негіздері. - Астана: Еуразия университеті, 2021. - 180 б.

8 Төлеуов А.С. Оптикалық талшықты сенсорлар және олардың қолданылуы. - ҚР ҰҒА Хабаршысы, №2, 2021. - Б. 78–83.

9 Shankaranarayanan, N. et al. "Performance analysis of AES encryption in optical networks", Optical Fiber Technology, Vol. 45, 2021, pp. 134–140.

10 Zhang, Y., & Xu, J. “Real-time fiber tapping detection using enhanced OTDR techniques.” Optics Express, Vol. 28, No. 3, 2020.

11 Sector I. Characteristics of a single-mode optical fiber and cable //ITU-T Recommendations, G Series. – 2016.

12 Cisco Systems. “SDN and NFV in Optical Networks: White Paper”, 2020.

13 Python Machine Learning Tools: scikit-learn, pandas, numpy – official documentation, accessed 2024.

14 Optiwave Systems Inc. “OptiSystem User Manual”, Version 17, 2022.

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

# РЕЦЕНЗИЯ
Дипломдық жұмыс

Маханбай Алмас Нұрланұлы

6В06201 – Телекоммуникациялар

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

Орындалды:

а) графикалық бөлім 15 парақ;

б) түсініктеме 43 бет.

## ЖҰМЫСҚА ЕСКЕРТУ

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

Сонымен қатар, жұмыста жүйенің энергия тұтынуының 10 Вт-тан аспауын қамтамасыз ету мәселесі де қарастырылады, бұл экологиялық және экономикалық тұрғыдан тиімділікке жетуге мүмкіндік береді.

Зерттеу мақсаты - өткізу қабілеті жоғары заманауи оптикалық талшықтық байланыс жүйелерінде ақпараттың қауіпсіздігін қамтамасыз ету әдістерін зерттеп, олардың тиімділігін тәжірибе жүзінде дәлелдеу.

Дипломдық жұмыста қауіптердің алдын алу шараларын студент өз тарапынан қандай жақсартулар енгізуі мүмкіндігін көрсете алмаған. 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 – қауіпсіздікті пайдаланудағы бағытқа жауап береді.

## ЖҰМЫСТЫҢ БАҒАСЫ

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

**Рецензент:**
Физ.-мат.ғыл.канд., Ғ.Дәукеев ат.
АЭжБУ профессор-оқытушысы М.А.Хизирова
«20» 05 2025 ж.

Қолтаңбаны растаймын
Подпись заверяю
Батырбекова А.Л.
қызметі аты-жөні
«22» 05 2025 ж.

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

# ҒЫЛЫМИ ЖЕТЕКШІНІҢ ПІКІРІ

Дипломдық жұмыс

Маханбай Алмас Нұрланұлы

6В06201 – Телекоммуникациялар оқу бағдарламасы

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

Бұл дипломдық жұмыста оптикалық талшықтық жүйелерде сигналды жоғалту мен шуды азайту әдістерін зерттеу жасалған. Негізгі сипаттамасы және болашақ ықтимал болатын түрлері келтірілген.

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

Оптикалық талшықтық байланыс желілерінде қауіпсіздікті қамтамасыз етудің тиімді шешімдері ұсынылды. Қауіптерді анықтау мен оларды жоюдың инновациялық әдістерін талданды. Эксперименттік модель нәтижелері негізінде қауіпсіздік шешімдерінің тиімділігі дәлелденді.

Дипломдық жұмыста қарастырылған мәселелер өте орынды.

Зерттеу барысында ғылыми зерттеулер қарастырылды.

Жалпы, дипломдық жұмыс «жақсы» (85%) деп бағаланды, ал студент Маханбай Алмас Нұрланұлы 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.

**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: Маханбай Алмас Нұрланұлы**

**Тақырыбы: Қазіргі заманғы оптикалық талшықтық байланыс жүйелерінің қауіпсіздігін қамтамасыз ету әдістерін зерттеу**

**Жетекшісі: Айнур Куттыбаева**

**1-ұқсастық коэффициенті (30): 7.3**

**2-ұқсастық коэффициенті (5): 1.7**

**Дәйексөз (35): 1.7**

**Әріптерді ауыстыру: 4**

**Аралықтар: 0**

**Шағын кеңістіктер: 13**

**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:**

2025-04-28

*Күні* *Кафедра меңгерушісі*

**Протокол**

**о проверке на наличие неавторизованных заимствований (плагиата)**

**Автор:** Маханбай Алмас Нұрланұлы

**Соавтор (если имеется):**

**Тип работы:** Дипломная работа

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

**Научный руководитель:** Айнур Куттыбаева

**Коэффициент Подобия 1:** 7.3

**Коэффициент Подобия 2:** 1.7

**Микропробелы:** 13

**Знаки из здругих алфавитов:** 4

**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:

2025-04-28

*Дата* *Заведующий кафедрой*

**Протокол**

**о проверке на наличие неавторизованных заимствований (плагиата)**

**Автор:** Маханбай Алмас Нұрланұлы

**Соавтор (если имеется):**

**Тип работы:** Дипломная работа

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

**Научный руководитель:** Айнур Куттыбаева

**Коэффициент Подобия 1:** 7.3

**Коэффициент Подобия 2:** 1.7

**Микропробелы:** 13

**Знаки из здругих алфавитов:** 4

**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:

2025-04-28

*Дата*

Сұңғат Марксұлы

*проверяющий эксперт*