ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

ФИЗИКА-ТЕХНИКА ФАКУЛЬТЕТІ

«ФИЗИКАДАҒЫ ЗАМАНАУИ ТЕНДЕНЦИЯЛАР: ҒЫЛЫМ МЕН БІЛІМ ИНТЕГРАЦИЯСЫ»

Халықаралық ғылыми конференциясының материалдары

«СОВРЕМЕННЫЕ ТЕНДЕНЦИИ В ФИЗИКЕ:ИНТЕГРАЦИЯ НАУКИ И ОБРАЗОВАНИЯ»

Материалы международной научной конференции

«MODERN TRENDS IN PHYSICS: INTEGRATION OF SCIENCE AND EDUCATION»

Materials of the international scientific conference

Астана, 2024 ж

ОӘЖ 53.(075)
Н90

Ә43 Физикадағы заманауи тенденциялар: ғылым мен білім интеграциясы: Халықаралық ғылыми конференциясының материалдары (2024 жылдың 23 ақпаны, Астана, Қазақстан). – Астана: Л.Н. Гумилев атындағы ЕҰУ баспасы, 2024. – 555 б.

ISBN 978-601-337-957-9

«ФИЗИКАДАҒЫ ЗАМАНАУИ ТЕНДЕНЦИЯЛАР: ҒЫЛЫМ МЕН БІЛІМ ИНТЕГРАЦИЯСЫ» атты Халықаралық ғылыми-теориялық конференция материалдар жинағына кәсіптік-техникалық білім беруді жетілдіруде «Космологияның қазіргі мәселелері», «Техниканың дамуындағы физиканың рөлі», «Ядролық физика, жаңа материалдар мен технологиялар», «Радиоэлектроника мен телекоммуникацияның қазіргі даму тенденциялары», «Ғарыштық техника мен технологияларды дамытудың озық бағыттары», жоғары оқу орындарындағы кәсіби педагогика проблемалары «Университетте физика және астрономия білімінің даму тенденциялары», «Орта мектепте физиканы оқытудың тиімді педагогикалық технологиялары», «Жаратылыстану пәндері бойынша мұғалімдерді даярлау жүйесіндегі инновациялар», «Қазіргі ақпараттық және коммуникациялық технологиялар» және оларды шешу әдістері мен жолдары қарастырылған мақалалар жарияланған.

ОӘЖ53.(075)

КБЖ 22.3я73

ISBN 978-601-337-957-9

Білім алушы мұғаліммен өзара әрекеттесудің субъектісі мен объектісі ретінде таза кәсіби іс-әрекетте ғана емес, сонымен қатар педагогикада да жаңа білім, білік, практикалық дағдылар мен тұлғалық қасиеттерді осы процесте жасайды. Мұғалім студенттерге сыртқы көздерден ақпарат алуда қол жетімді тәсіл қажет екендігі туралы ескертуі керек. Тек жеткілікті тәжірибесі мен білімі бар адам ақпараттың сапасын дұрыс бағалай алады.

Турсунбоева Динара Турғунбойқызы
Физико-техникалық факультетінің магистранты
Л. Н. Гумилев атындағы Еуразия ұлттық университеті, Қазақстан

МУЛЬТИСЕРВИСТІК ЖЕЛІЛЕРДІҢ ЖЕЛІЛІК ДЕҢГЕЙІНЕ НЕГІЗДЕЛГЕН ДЕРЕКТЕРДІ ҚОРҒАУДЫҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІК ӘДІСТЕРІ

Аңдатпа.

Бұл жұмыс мультисервистік желілердің желілік деңгейіне негізделген ақпараттық қауіпсіздік пен деректерді қорғау әдістерін зерттеуге арналған. Мультисервистік желілер контекстінде қолданылатын әдістер мен олардың тиімділігіне жан-жақты шолу жасалынды. Атап айтсақ, деректерді шифрлау, виртуалды жеке желілер (VPN), брандмауэрлер және желіралық қалқан, идентификация және аутентификация, интрузияны анықтау жүйелері (IDS) және интрузияның алдын алу жүйелері (IPS) әдістері сияқты аспектілер қарастырылды. Жұмыс деректерді қорғаудың жоғары деңгейін қамтамасыз ету және мультисервистік желілердің тұрақты және қауіпсіз жұмысын қамтамасыз ету үшін практикалық ұсыныстар беруге бағытталған.

Кілт сөз: ақпараттық қауіпсіздік, мультисервистік желілер, шифрлау, идентификация, браундмауэр

Кіріспе

Қазіргі таңда цифрлық технологиялар біздің өміріміздің барлық салаларына мықтап енген кезде, ақпараттық қауіпсіздік мәселесі шешуші рөл атқарады. Күрделі және тармақталған өзара әрекеттесу құрылымдары болып табылатын мультисервистік желілердегі деректерді қорғау тақырыбы әсіресе өзекті болып табылады. Осы желілердің желілік деңгейінде ақпараттық қауіпсіздікті қамтамасыз ету әдістері деректердің құпиялылығын, тұтастығын және қол жетімділігін қорғауда маңызды рөл атқарады.

Мультисервистік желілер −ресурстарды тиімді пайдалануды қамтамасыз ететін және әртүрлі типтегі деректерге сапалы қызмет көрсететін әртүрлі қызметтер мен қолданбаларды қолдауға арналған желілік инфрақұрылымдар. Бұл желілер бірыңғай желілік инфрақұрылым арқылы дауыс, бейне, деректер, интернет қызметтері және т.б. сияқты әртүрлі қызметтерді тасымалдауды қолдайды [1,16 б].

Мультисервистік желілер әдетте трафиктің әртүрлі түрлері үшін әртүрлі кідірістерге, өткізу қабілеттілігіне және сенімділігіне қойылатын талаптарды қамтамасыз ете алатын технологияларды пайдаланады. Мысалы, олар жоғары өнімділік талаптары бар қолданбалар үшін оңтайлы қызмет сапасын қамтамасыз ету үшін Quality of Service (QoS) қолдауын жүзеге асыра алады.

Мультисервистік желілер сонымен қатар желіні виртуалдандыру тұжырымдамаларын, бағдарламалық жасақтамамен анықталған желілерді (SDN) және желіні басқаруды және конфигурациялауды жеңілдететін және өзгеретін қолданба талаптарына бейімделу икемділігін қамтамасыз ететін басқа технологияларды қамтуы мүмкін [1,19 б].

Бұл желілер қазіргі заманғы желілердің күрделілігінің артуы және қазіргі заманғы коммуникациялық жүйелердегі трафиктің әртүрлі түрлеріне қойылатын талаптардың артуы жағдайында сұранысқа ие бола бастады.

Зерттеу объектілері мен әдістері

Қазіргі уақытта мультисервистік байланыс желілеріндегі киберқауіпсіздік мәселесі ерекше өзектілікке ие болды. Себебі бұл желілер дауыстық байланыс, деректерді беру, бейнеконференциялар және басқа қызметтер сияқты байланыс қызметтерінің әртүрлі түрлерін қамтитын кешенді инфрақұрылым болып табылады. Мультисервистік байланыс желілері пайдаланушылардың құпия деректерін, коммерциялық ақпаратты, банктік деректерді және басқа да сезімтал ақпаратты қоса алғанда, үлкен көлемдегі ақпаратпен алмасады. Сондықтан бұл ақпаратты рұқсатсыз кіруден, араласудан немесе ұрлықтан қорғауды қамтамасыз ету маңызды. Сонымен қатар, жыл сайын шабуылдардың жалпы саны артып келеді [2, 51 б].

Мультисервистік байланыс желілерінде вирустар, трояндық бағдарламалар, құрттар және бағдарламалық шабуылдардың басқа түрлері сияқты зиянды бағдарламалық жасақтаманың таралу қаупі жоғары. Бұл желінің бұзылуына, деректердің жоғалуына немесе тіпті бүкіл желілік инфрақұрылымның бұзылуына әкелуі мүмкін. Сонымен қатар, мультисервистік байланыс желілері көбінесе ұйымға зиян келтіру немесе оның ақпаратына рұқсатсыз қол жеткізу мақсатында шабуылдаушылар жүргізетін мақсатты шабуылдарға ұшырайды. Мұндай шабуылдар әртүрлі арналар арқылы, соның ішінде желілік протоколдар, қолданбалар, құрылғылар немесе тіпті физикалық әсерлер арқылы жасалуы мүмкін. Сондықтан да желілік деңгейде қорғау әдістерін қарастыру маңызды болып табылады.

Желілік деңгейде қорғау әдістері:

Деректерді шифрлау

Деректерді қорғаудың негізгі әдістерінің бірі − шифрлауды қолдану. Бұл әдіс математикалық алгоритмдерді қолдана отырып, бөгде адамдар үшін түсініксіз түрге айналдыру арқылы желі арқылы берілетін ақпараттың құпиялылығын қамтамасыз етеді. Мультисервистік желілерде шифрлау хаттамаларын желілік деңгейде қолдану деректерге рұқсатсыз қол жеткізуді болдырмай, берілетін ақпараттың құпиялылығын қамтамасыз етеді [2, 52 б].

Желілік деңгейде кеңінен қолданылатын шифрлау хаттамаларының мысалдары:

SSL/TLS (Secure Sockets Layer/Transport Layer Security): веб-трафикті қорғау үшін HTTPS пайдалану сияқты интернет арқылы деректерді қауіпсіз тасымалдауды қамтамасыз ету үшін қолданылады.

IPsec (Internet Protocol Security): желіде деректерді тасымалдау үшін пайдаланылатын IP пакеттерін қорғауды қамтамасыз етеді. IPsec туннельдеу немесе тасымалдау режимдерінде жұмыс істей алады. Бұл деректердің құпиялылығын, тұтастығын және түпнұсқалығын қамтамасыз етеді.

SSH (Secure Shell): жүйелерге қашықтан қол жеткізуді қорғау үшін қолданылады. Қашықтағы серверге қосылған кезде деректерді шифрлауды және аутентификацияны қамтамасыз етеді.

VPN (Virtual Private Network): қашықтағы түйіндер арасында шифрланған туннель жасайды. Бұл интернет сияқты өңделмеген желілер арқылы деректерді қауіпсіз тасымалдауға мүмкіндік береді.

WPA/WPA2/WPA3 (Wi-Fi Protected Access): деректерді шифрлау және құрылғылардың аутентификациясын қамтамасыз ету арқылы Wi-Fi сымсыз желілерінің қауіпсіздігін қамтамасыз ету үшін қолданылады [2, 54 б].

Виртуалды жеке желілер (VPN)

Виртуалды жеке желілер (VPN) желілік деңгейде қорғаудың тиімді әдісін ұсынады. VPN желідегі екі нүкте арасында шифрланған туннель жасайды. Бұл Интернет сияқты өңделмеген немесе сенімсіз желілер арқылы деректерді қауіпсіз тасымалдауды қамтамасыз етеді. Желілік деңгейді қорғау үшін VPN пайдаланудың кейбір негізгі аспектілері мен артықшылықтары[3, 248 б]:

Трафикті шифрлау: VPN желілері арқылы берілетін ақпаратты шифрлау арқылы деректердің құпиялылығын қамтамасыз етеді. Бұл, әсіресе, шабуылдаушылардың деректерді ұстап қалу қаупі бар қоғамдық желілерді пайдалану кезінде маңызды.

Аутентификация: VPN желіге қатысушылардың аутентификациясын жүргізуге мүмкіндік береді. Тек дұрыс рұқсат етілген пайдаланушылар желі ресурстарына қол жеткізе алады.

Цензура мен сүзуді айналып өту: VPN пайдаланушыларға кейбір елдерде немесе желілерде интернет-ресурстарға қол жеткізуге қойылған шектеулерді айналып өтуге мүмкіндік береді. Олар сондай-ақ жергілікті желі саясаткерлері белгілеген шектеулерді айналып өтуге көмектеседі.

Қашықтан қол жеткізу: VPN офистен тыс жұмыс істейтін қызметкерлер үшін кәсіпорын желілеріне қауіпсіз қашықтан қол жеткізуді қамтамасыз етеді. Бұл әсіресе «телекоммуникация» технологиясы немесе қашықтан жұмыс істеу үшін өте маңызды.

Виртуалды желілерді құру: VPN қауіпсіз және тиімді байланысты қамтамасыз ете отырып, географиялық қашықтағы кеңселер немесе кәсіпорын филиалдары арасында виртуалды желілерді құруға мүмкіндік береді [3,250 б].

VPN күшті қорғаныс деңгейін қамтамасыз еткенімен, сенімді шифрлау протоколдарын пайдалану және желілік трафиктің қауіпсіздігін қамтамасыз ету үшін параметрлерді дұрыс реттеу маңызды.

Брандмауэрлер және желіаралық қалқан

Желілік деңгейде брандмауэрлер мен желіаралық қалқанды пайдалану трафикті басқаруға, зиянды деректер пакеттерін сүзуге және желілік ресурстарға рұқсатсыз кіруге жол бермейді. Яғни олар арқылы қандай деректер пакеттері өтуі мүмкін және қайсысы бұғатталуы керек екені анықталады [4, 130 б].

Брандмауэрлер мен желіаралық қалқан орындайтын негізгі аспектілер мен тапсырмалар:

Қол жеткізуді басқару: олар қандай желілік байланыстарға рұқсат етілгенін және қайсысына тыйым салынғанын анықтайды. Мұны IP мекенжайлары, порттар, хаттамалар және басқа параметрлер негізінде жасауға болады.

Трафикті сүзу: олар әртүрлі қауіпсіздік ережелері мен саясаттарына негізделген трафикті сүзе алады. Мысалы, файлдардың немесе қосымшалардың белгілі бір түрлерін бұғаттау, URL мекенжайларын сүзу, DDoS типті шабуылдардың алдын алу және басқа шаралар [5, 292 б].

NAT (network Address Translation): көптеген брандмауэрлер ішкі жергілікті IP мекенжайларын сыртқы жалпыға ортақ IP мекенжайына түрлендіру арқылы NAT орындайды. Бұл ішкі желі құрылымын сыртқы әлемнен жасыруға көмектеседі.

VPN қолдауы: көптеген брандмауэрлер vpn функционалдығын қамтамасыз етеді. Бұл қашықтағы қосылымдарға тағы бір қауіпсіздік қабатын қосады.

Логинг және бақылау: брандмауэрлер оқиғалар журналдарын жүргізеді және әкімшілерге желілік трафикті бақылауға, ықтимал қауіптерді анықтауға және өнімділікті талдауға мүмкіндік береді [5, 293 б].

Бұл қорғаныс желілік деңгейде қауіпсіздікті қамтамасыз ету үшін корпоративтік және үй желілерінде кеңінен қолданылады.

Идентификация және аутентификация:

Деректерді қорғаудың маңызды элементі − мультисервистік желілердегі пайдаланушылар мен құрылғыларды дұрыс анықтау және аутентификациялау. Бұл екі факторлы аутентификацияны және тұлғаны растаудың басқа заманауи әдістерін қолдануды қамтиды [6, 36 б].

Идентификация жүйеде пайдаланушының немесе құрылғының бірегей анықтамасын қамтиды. Мұны логин, сәйкестендіру нөмірі, электрондық пошта және т. б. сияқты параметрлерді қолдану арқылы жасауға болады. Әрбір пайдаланушы немесе құрылғы жүйеге оларды тануға және басқалардан ажыратуға мүмкіндік беретін бірегей идентификатор алады.

Аутентификация - бұл пайдаланушының немесе құрылғының тіркелген деректерінің түпнұсқалығын растау процесі. Бұл құпия сөзді енгізуді, биометриялық деректерді пайдалануды, таңбалауыштарды және басқа әдістерді пайдалануды қамтиды. Мұның ішінде

көп факторлы аутентификация (MFA) −құпия сөз, SMS коды және биометриялық деректер комбинациясы сияқты бірнеше түпнұсқалықты растау әдістерін қажет ететін қауіпсіз тәсіл.

Желілік деңгейде идентификация мен аутентификацияны қолданудың келесі артықшылықтары бар:

- Рұқсатсыз кірудің алдын алу: идентификация және аутентификация желілік ресурстарға рұқсатсыз кірудің алдын алу арқылы кіруді басқару механизмдерін қамтамасыз етеді.
- Белсенділікті бақылау: жүйе пайдаланушылардың белсенділігін олардың бірегей идентификаторлары негізінде бақылай алады. Бұл күдікті әрекеттерді бақылауды және анықтауды жеңілдетеді.
- Қауіпсіздік саясатын сақтау: идентификация және аутентификацияны пайдалану құпия сөзге қойылатын талаптар немесе белгілі бір аутентификация әдістерін қолдану сияқты қауіпсіздік саясаттарын орындауға мүмкіндік береді.
- Деректердің құпиялылығын қорғау: дұрыс аутентификацияны қамтамасыз ету құпия ақпаратқа рұқсатсыз кірудің алдын алуға көмектеседі [6, 38 б].

Бұл әдістерді брандмауэр және шифрлау сияқты желілік деңгейдегі басқа қауіпсіздік құралдарымен бірге қолдану сенімдірек қорғаныс механизмдерін жасайды.

Интрузияны анықтау (IDS) және интрузияны болдырмау (IPS) жүйелері

Интрузияны анықтау жүйелері (Intrusion Detection Systems, IDS) және интрузияның алдын алу жүйелері (Intrusion Prevention Systems, IPS) қауіпсіздіктің ықтимал қауіптерін анықтауға және оларға жауап беруге бағытталған маңызды желілік қорғаныс әдістері болып табылады [7,115 б]. Олардың негізгі сипаттамаларын қарастырайық:

Интрузияны анықтау жүйелері (IDS):

- IDS аномальды мінез-құлықты немесе ықтимал шабуылдарды анықтау үшін желілік трафик пен жүйелік журналдарды талдайды.
- Қолтаңбаны анықтау: желілік трафикте оларды анықтау үшін алдын ала анықталған қолтаңбаларды немесе белгілі шабуылдардың үлгілерін пайдаланады.
- IDS қауіптерді анықтайды, бірақ оларды блоктау үшін белсенді қадамдар жасамайды. Бұл жүйелер әкімшіні хабардар ете алады немесе кейінірек талдау үшін журналдар жасай алады [7,116 б].

Интрузияның алдын алу жүйелері (IPS):

- Шабуылдарды блоктау: нақты уақыттағы шабуылдарды белсенді түрде блоктауға немесе алдын алуға қабілетті.
- Динамикалық қолтаңбаны жаңарту: IPS қолтаңбаларды жаңарта алады, бұл оларға шабуылдар мен қауіптердің жаңа түрлерін тануға мүмкіндік береді.
- Терең пакеттік талдау: IPS IDS-ке қарағанда желілік трафикке тереңірек талдау жасайды және шабуылдарды жоғары деңгейде анықтап, бұғаттай алады [7,116 б].

IDS және IPS ұқсас ерекшеліктері:

- Деректерді жинау жүйелері: екі жүйе де желілік трафик, оқиғалар және ықтимал шабуылдар туралы деректерді жинайды.
- Ортақ мақсат −қауіпсіздікті қамтамасыз ету: IDS және IPS екеуі де желі мен жүйелердің қауіпсіздігіне нұқсан келтірмеуге бағытталған.

IDS және IPS пайдалану желінің қауіпсіздігін айтарлықтай жақсарта алады және шабуылдар туралы ескертеді. Ал IPS жағдайында оларды нақты уақытта бұғаттайды.

Зерттеу нәтижелері

Қорытындылай келе, деректерді қорғаудың жоғары деңгейін қамтамасыз ету және мультисервистік желілердің тұрақты және қауіпсіз жұмысын қамтамасыз ету үшін келесі практикалық шараларды жүзеге асыру ұсынылады:

Деректерді шифрлау:

- Берілетін ақпаратты қорғау үшін желілік деңгейде деректерді шифрлаудың күшті алгоритмдерін енгізу.
- Шифрлау кілттерін үнемі жаңартып отыру және шифрлау тиімділігін бақылау.

Виртуалды жеке желілер (VPN):

- Қашықтағы кеңселер мен мобильді құрылғыларды орталық желіге қауіпсіз қосу үшін VPN пайдалану.
- VPN протоколдарын үнемі жаңартып отыру және қосылым қауіпсіздігін бақылау.

Брандмауэрлер және желіаралық қалқан:

- Трафикті сүзу және ережелерге негізделген кіруді басқару үшін брандмауэрлерді орнату.
- Ауытқулар мен ықтимал шабуылдарды анықтау үшін брандмауэрлерді қолдана отырып, желілік трафикті бақылау.

Идентификация және аутентификация:

- Қол жеткізу қауіпсіздігінің деңгейін арттыру үшін екі факторлы аутентификация тетіктерін енгізу.
- Күдікті әрекеттерді анықтау үшін тіркелген деректерін үнемі жаңартып отыру және пайдаланушылардың белсенділігін бақылау.

Интрузияны анықтау (IDS) және интрузияны болдырмау (IPS)жүйелері:

- Желідегі қалыптан тыс мінез-құлықты ерте анықтау үшін интрузияны анықтау жүйелерін дамыту.
- Қауіптерге автоматты түрде жауап беру және шабуылдарды блоктау үшін кірудің алдын алу жүйелерін орнату.

Қызметкерлерді үнемі жаңарту және оқыту:

- Деректер қауіпсіздігі және желілік қауіпсіздік мәселелері бойынша қызметкерлерге тұрақты тренингтер өткізу.
- Қызметкерлердің қауіпсіздік саясатын түсінуін және олардың белсенді сақталуын қамтамасыз ету.

Қауіпсіздік мониторингі және аудиті:

- Желідегі оқиғаларды үнемі қадағалап отыру үшін қауіпсіздікті бақылау жүйелерін енгізу.
- Осалдықтарды анықтау және қауіпсіздік стандарттарына сәйкестігін тексеру үшін тұрақты қауіпсіздік аудиттерін жүргізу.

Деректердің сақтық көшірмесін жасау және қалпына келтіру:

- Деректердің сақтық көшірмесін үнемі жасау және оларды қауіпсіз жерлерде сақтау.
- Оқиғалардан кейін кепілдендірілген жылдам қалпына келтіру үшін деректерді қалпына келтіру процедураларын тексеру.

Осы ұсыныстарды қолдану тәуекелдерді азайту және маңызды кәсіпорын деректерін қорғауды қамтамасыз ету арқылы мультисервистік желілер үшін сенімді және қауіпсіз ортаны құруға көмектеседі.

Мультисервистік желілердің желілік деңгейіндегі ақпараттық қауіпсіздік әдістері деректерді сенімді қорғауды қамтамасыз етуде шешуші рөл атқарады. Шифрлауды, брандмауэрлерді, идентификацияны және басқа технологияларды қамтитын біріктірілген тәсіл күрделі және динамикалық желілік орта жағдайында деректердің тұтастығын, құпиялылығын және қолжетімділігін қамтамасыз ету үшін қажет. Желілік деңгейде қорғаудың заманауи әдістерін енгізу мультисервистік желілер дәуірінде ақпараттық қауіпсіздікті қамтамасыз ету стратегиясының ажырамас бөлігі болып табылады. Әр түрлі мультисервистік желілер арасындағы қорытынды таңдау ұйымның нақты қажеттіліктері мен талаптарына, соның ішінде қауіпсіздік деңгейіне, өнімділікке, ауқымдылыққа және бюджеттік шектеулерге байланысты болады.

Әдебиеттер:

1. Шаров В. Базовые технологии мультисервисных сетей, ж. Сети и телекоммуникации – М.; 2006. – 336 с.
2. Агеев С.А., Бушуев А.С., Егоров Ю.П. Концепция автоматизации управления информационной безопасностью в защищенных мультисервисных сетях специального назначения – Автоматизация процессов управления, 2011 – 50-57 с

3. Рыжкова А.Е. Виртуальные частные сети VPN как концепция реализации защищенных корпоротивных сетей. Системы управления, сложные сети. 2021. 248-251 с
4. Болдырихин Н.В., Бельчикова Д.А., Закут М. Анализ современных технологий межсетевого экранирования. Издательство: ГНИИ «Нацразвитие». Высокие технологии и инновации в науке: сборник избранных статей Международной научной конференции. Санкт-Петербург, 2020. 129-134 с
5. Мезенцева М.А. Применение межсетевых экранов. Международная научно-техническая конференция молодых ученых БГТУ Им. В.Г. Шухова, посвещенная 170-летию со дня рождения В.Г. Шухова. Сборник докладов. Том Часть 13. Белгород, 2023. 291-294 с
6. Таланов С.Б. Управление информационной безопасностью в мультисервисных сетях связи. Цифровая экономика: региональный аспект, 2019. 35-39 с
7. Глущенко М.В., Ширяев А.А., Глушенко С.А. IDS/IPS-системы обнаружения и предотвращения вторжений. Концепция «общества знаний» в современной науке сборник статей по итогам Международной научно-практической конференции. 2019. 115-117с

Н.А. Черепанов[1] *магистрант,* **С.Д. Тулеуов**[1]*, студент,* **Т.С. Рахимгалиев**[1] *студент,*
М.А. Жұман[1] *студент,* **А.К. Нурмаханова**[2] *сеньор-лектор*
[1]*Карагандинский университет имени академика Е.А. Букетова*
[2] *Алматинский технологический университет*

УСТАНОВКИ ПО ИЗМЕРЕНИЮ СПЕКТРОВ ЛЮМИНЕСЦЕНЦИИ НА БАЗЕ МОНОХРОМАТОРА МДР-23 С ИСПОЛЬЗОВАНИЕМ СОВРЕМЕННЫХ ПОДХОДОВ В АВТОМАТИЗАЦИИ ПРОЦЕССОВ.

Аннотация: В данных материалах приведены результаты автоматизации процесса измерения спектров люминесценции на базе монохроматора МДР-23. Для ускорения процесса создания установки и понижения ее стоимости использованы современные подходы автоматизации процессов. Использована платформа Arduino и программная среда разработки LabVIEW для создания управляющей программы. Это практичное решение позволяет существенно снизить затраты и обеспечивает эффективность в измерениях образцов с низким квантовым выходом.

Ключевые слова: Спектр люминесценции, монохроматор, Arduino Uno, автоматизация.

Введение

Методы, основанные на измерении характера взаимодействия излучения с веществом, является широко используемыми в научных исследованиях, медицине и биологии, в лазерных и телекоммуникационных технологиях. Не смотря на наличие большого количества различных приборов, существуют различные ограничения в их использовании. Одним из существенных ограничений является их стоимость. Спектральные прибора содержащие оптические, механические и электронные компоненты являются дорогим оборудованием. Поэтому использование спектральных приборов, собранных в лаборатории, и автоматизация процессов оптических измерений остается актуальной задачей.

Современное развитие микроконтроллерной техники и информационных технологий позволяет производить автоматизацию измерительных и технологических процессов с незначительными временными и финансовыми усилиями. За последние 10-15 лет на рынке появилось большое количество программно-аппаратных платформ с открытым исходным кодом позволяющих быстро программировать и использовать микроконтроллерные и микропроцессорные устройства. К таким платформам относятся Raspberry Pi, BeagleBoard, Arduino и т.д. [1]. Среди вышеуказанных моделей платформа Arduino является наиболее простой, недорогой и с разнообразными функциональными и техническими характеристиками. Тем не менее, простота Arduino находит свое место во многих проектах