ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

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

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

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

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

2025
Астана

УДК 001(06)
ББК 72я631
F96

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

ISBN 978-601-08-5373-7

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

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

УДК 001(06)
ББК 72я431
F96

ISBN 978-601-08-5373-7

Л.Н. Гумилев атындағы Еуразия ұлттық университеті, 2025

СЕКЦИЯ 2

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ И КОММ УНИКАЦИОННЫЕ ТЕХНОЛОГИИ

Подсекция 2.2

Интеллектуальные информационные системы

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

Подсекция 2.3

Современные тенденции в программной инженерии и управлении в условиях цифровой индустрии

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

СЕКЦИЯ 3
ЕСТЕСТВЕННЫЕ НАУКИ

қауіпсіздік қосымшаларына сенімділігін көрсете отырып, осыиссаларды растайды. Болашақта kuznechik өнімділігін оңтайландыру үшін гибридті іске асыруды немесе аппараттық жеделдетуді зерттеуге болады.

Қолданылған әдебиеттер тізімі

1. RFC 2144: The CAST-128 Encryption Algorithm // Internet Engineering Task Force (IETF). – 1997. – URL: https://www.rfc-editor.org/rfc/rfc2144.txt.
2. RFC 7801: GOST R 34.12-2015 Block Cipher "Kuznyechik" // Internet Engineering Task Force (IETF). – 2016. – URL: https://www.rfc-editor.org/rfc/rfc7801.html.
3. ISO/IEC 18033-3 Standard: Information Technology – Security Techniques – Encryption Algorithms – Part 3: Block Ciphers // International Organization for Standardization (ISO). – Geneva, 2005.
4. Comparative Study of AES, Blowfish, CAST-128 and DES Encryption Algorithm // IOSR Journal of Engineering, Vol.6 Issue6, June 2016. – URL: https://www.iosrjen.org/Papers/vol6_issue6%20(part-1)/A066010107.pdf (дата обращения: 30.03.2025).
5. Profiling JVM Applications Remotely Using VisualVM // ITNEXT, June 2024. – URL: https://itnext.io/profiling-jvm-applications-remotely-using-visualvm-c0df9816aabf (дата обращения: 30.03.2025).

ӘӨЖ 004.056.5

ЖЕРГІЛІКТІ ЖЕЛІНІҢ ҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТЕТІН НЕГІЗГІ ПАРАМЕТРЛЕР

Акимбекова Дильназ Маратовна, Каиржанова Дильназ Жалғасқызы
akimbekovadilnaz@mail.ru, *dikairzhanova@gmail.com*
Л. Н. Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультеті Ақпараттық қауіпсіздік жүйесі кафедрасының 3 курс студенттері, Астана, Қазақстан
Ғылыми жетекші – Казиева Назым Магидулловна

Қазіргі заманғы желілер кибершабуылдарға жиі ұшырайды, олардың ішінде рұқсатсыз қол жеткізу, «қызмет көрсетуден бас тарту» (DoS/DDoS) шабуылдары және деректерді ұстап қалу сияқты қауіптер бар. Желілік құрылғылардың қауіпсіздігін қамтамасыз ету ақпаратты қорғаудың және ықтимал шабуылдардың алдын алудың негізгі шараларының бірі болып табылады.

Үйлердегі немесе үй желілеріндегі жергілікті желілерге (LAN) ерекше назар аударған жөн. Үй желілері – бұл жергілікті желілердің бір түрі; олар интернетке қосылған құрылғылардың кең және алуан түрін қамтуы мүмкін және оларды басқару оңай, сенімді және қауіпсіз болуы керек, әсіресе олардың иелері көбінесе техникалық дағдылары жоқ пайдаланушылар болғандықтан [1].

Көптеген жылдар бұрын үй желісі сымсыз желіге қосылған бірнеше ноутбуктан тұрған. Бүгінгі таңда оған смартфондар, сымсыз принтерлер, термостаттар, дыбыс датчиктері, түтін датчиктері, шамдар, камералар, теледидарлар, аудио жүйелері, ақылды динамиктер, тоңазытқыштар және тағы басқалар кіруі мүмкін. "Заттар интернеті" (IoT, Internet of Things) деп аталатын интернетке үйлесімді құрылғылардың көбеюі кез-келген электрониканы, соның ішінде әртүрлі сенсорларды желіге қосуға мүмкіндік береді. Қосылған құрылғылардың бұл

үлкен ауқымы мен әртүрлілігі үй желілерін жобалауда, басқаруда және қорғауда жаңа қоңыраулар тудырады [1].

Желіге әртүрлі кибершабуылдар бағытталуы мүмкін. Ең алдымен, желілік шабуылдар туралы айтуға болады. ARP Spoofing немесе ARP Poisoning арқылы шабуылдаушы желідегі құрылғылардың MAC-адрестерін өзгертіп, өзін заңды құрылғы ретінде көрсетіп, трафикті ұстап қалуы мүмкін. DHCP Starvation шабуылы кезінде заңды пайдаланушыларға IP мекенжай тағайындалмайтындай етіп, шабуылдаушы DHCP серверін жалған сұраныстармен толтырады. Сондай-ақ, Man-in-the-Middle (MitM) шабуылы желідегі құрылғылардың байланысын бұзып, барлық деректерді өз арқылы өткізуге мүмкіндік береді.

Құрылғыларға бағытталған шабуылдардың ішінде брутфорс арқылы роутер, сервер немесе IoT құрылғыларының логині мен паролін күшпен тауып алу әдісі кең таралған. SSH немесе Telnet хаттамалары арқылы рұқсатсыз кіруге әрекет жасау да ықтимал қауіптердің бірі болып табылады. Бұған қоса, Denial of Service (DoS немесе DDoS) шабуылдары серверді немесе роутерді шамадан тыс сұраныстармен жүктеп, қызметін тоқтатуы мүмкін.

IoT құрылғылары да осалдықтарға ұшырауы мүмкін. Егер олардың әдепкі логині мен паролі өзгертілмеген болса, шабуылдаушылар оларды оңай анықтап, желіге еніп кетуі мүмкін. Сонымен қатар, IoT құрылғылардың бағдарламалық жасақтамасында осалдықтар болса, шабуылдаушы оларды өз мүддесіне пайдаланып, құрылғыны басқаруы мүмкін. Кейбір жағдайларда зиянды ботнеттер осындай IoT құрылғыларды жұқтырып, оларды үлкен масштабтағы DDoS шабуылдарына қолданады.

Ақпарат ұрлау және тыңшылық шабуылдары да үлкен қауіп төндіреді. Packet Sniffing әдісімен желі трафигін тыңдау арқылы шабуылдаушы құпия ақпаратты, парольдерді немесе жеке мәліметтерді ұрлай алады. DNS Spoofing шабуылында желі қолданушылары жалған веб-сайттарға бағытталып, олардың деректерін зиянды серверлерге жіберу мүмкін.

Сондай-ақ, физикалық шабуылдар да қауіпсіздікке елеулі әсер етеді. Мысалы, кабельді үзу немесе қайта қосу арқылы шабуылдаушы желіні бұзуы мүмкін. Желілік құрылғыларға рұқсатсыз физикалық қолжетімділік алу арқылы конфигурацияны өзгерту немесе жабдықты зақымдау да ықтимал.

Осындай шабуылдарды болдырмау үшін VLAN, ACL, брандмауэр, күшті аутентификация, шифрлау сияқты қорғаныс шараларын қолдану қажет. Желіні үнемі бақылап, осалдықтарды уақытында жою қауіпсіздікті арттыруға көмектеседі.

Бұл мақалада маршрутизаторлар, коммутаторлар және IoT құрылғылары сияқты желілік құрылғыларды қорғаудың негізгі әдістері қарастырылады, сонымен қатар олардың Packet Tracer-де модельдену мүмкіндіктері талданады.

Негізгі қорғаныс құралдарының бірі – маршрутизаторлардағы кіруді басқару тізімдерін (Access Control Lists, ACL) пайдалану. ACL сізге қажет емес қосылымдарды бұғаттау арқылы кіріс және шығыс трафикті сүзуге мүмкіндік береді. ACL пайдалану жергілікті желіге сырттан кіруді шектеуге және рұқсатсыз қосылу қаупін азайтуға көмектеседі. Олар екі түрге бөлінеді:

- Стандартты ACL - трафикті тек дереккөздің IP-мекен-жайы бойынша сүзеді.
- Жетілдірілген ACL - пакеттерді дереккөз бен алушының IP мекенжайы, порт нөмірі және протокол арқылы сүзуге болады.

Желіні виртуалды жергілікті желілерге (VLAN) бөлу шабуылдардың таралу аймағын азайтуға және желідегі жүктемені азайтуға мүмкіндік береді. Мысалы, IoT құрылғыларына бөлек VLAN бөлу негізгі желінің бұзылу қаупін азайтады.

VPN (Virtual Private Network) пайдалану интернет арқылы берілетін деректерді шифрлау арқылы қорғауға мүмкіндік береді. IPsec VPN кәсіпорын мен үй желілерін қорғау үшін қолданылады, дегенмен Cisco Packet Tracer толық функционалдығы жоқ тек негізгі VPN эмуляциясын қолдайды.

IoT құрылғылары көбінесе әлсіз кірістірілген қорғанысқа ие, сондықтан оларды бөлек VLAN-ға орналастыру керек. Бұл құрылғылардың негізгі желімен өзара әрекеттесуін шектейді және олардың бұзылу қаупін азайтады. IoT құрылғыларының Интернетке қол жетімділігін шектеу үшін ACL пайдалану олардың осалдығын азайтуға мүмкіндік береді.

IoT құрылғыларының микробағдарламасын үнемі жаңартып отыру осалдықтарды жоюға мүмкіндік береді. Packet Tracer ішіндегі микробағдарламаны жаңарту эмуляцияланбайды, бірақ оны веб-интерфейс немесе SSH арқылы қолмен жасау керек. Secure Shell (SSH) - бұл салыстырмалы түрде қарапайым және арзан болатындай етіп жасалған қауіпсіз желілік байланыс протоколы [2].

IoT құрылғылары желінің әлсіз нүктесі болғандықтан, сондықтан олар үшін қосымша қорғаныс шаралары қабылданды. Жеке VLAN және оқшаулау: IoT құрылғылары бір-бірімен байланыса алады, бірақ негізгі желіге қосыла алмайды. IoT VLAN-ынан интернетке тікелей шығу шектелді. ACL арқылы: IoT құрылғылары тек басқару серверімен байланыса алады. Администратор ноутбугі ғана IoT құрылғыларын басқара алады. Қауіпсіздік саясаты: Желідегі барлық IoT құрылғылары статикалық IP мекенжайлармен конфигурацияланды. Белгісіз MAC мекенжайлары бар құрылғыларға желіге қосылуға тыйым салынды.

Күрделі құпия сөздерді және екі факторлы аутентификацияны (2FA) пайдалану желілік жабдықтың қауіпсіздігін арттырады. Деректердің жоғалуын және желінің тоқтап қалуын болдырмау үшін келесі шаралар қолданылды. Резервтік көшірме жасау: Желі құрылғыларының конфигурациясы тұрақты түрде сақталады. Маңызды деректерді сақтау үшін серверге қол жеткізу шектелді. Қауіпсіз қашықтықтан басқару: Барлық әкімшілік әрекеттер тек SSH арқылы жүзеге асырылады.Барлық пайдаланушылар үшін күшті пароль саясаты енгізілді.

Желілік құрылғылардың қауіпсіздігін қамтамасыз ету үшін бірқатар шаралар қабылданды:

Брандмауэр (ACL) маршрутизаторда: Қауіпсіздік ережелері арқылы рұқсат етілмеген трафикті бұғаттау. Әкімшіге (Admin) тек өз құрылғысынан SSH арқылы маршрутизаторға қосылуға рұқсат беру. және IoT құрылғылары мен серверге тек белгілі IP мекенжайларынан ғана қосылуға мүмкіндік беру арқылы жалпы қауіпсіздікті қамтамасыз етеміз.

Желі сегментациясы (VLAN): Негізгі құрылғыларды (ноутбук, сервер, компьютер) жеке VLAN-ға орналастыру. IoT құрылғыларын бөлек VLAN-да оқшаулау, олардың ішкі желіге қолжетімділігі шектелді.

Портқа негізделген VLAN артықшылықтары:

- Орнатудың қарапайымдылығы. Ethernet порттарын топтастыру негізінде виртуалды желілерді құру көп жұмысты қажет етпейді, белгілі бір VLAN-ға кіретін әрбір Ethernet портына бірдей VLAN идентификаторын тағайындау жеткілікті.
- Хосттардың физикалық қозғалысынсыз желінің логикалық топологиясын өзгерту мүмкіндігі. Ethernet портының параметрлерін осы порттың параметрлерінде басқа VLAN идентификаторын көрсету арқылы өзгерту жеткілікті (мысалы, техникалық бөлімнің VLAN идентификаторын сату бөлімінің VLAN идентификаторына өзгерту) және жұмыс станциясы бірден жаңа VLAN ресурстарын пайдалануға мүмкіндік алады [3].

Қауіпсіз қашықтан басқару: Telnet-ті өшіріп, тек SSH арқылы маршрутизатор мен коммутаторларға қосылу қамтамасыз етілді. Күшті парольдер енгізу және барлық басқару интерфейстеріне рұқсатты шектеу.

Коммутаторлардағы MAC мекенжайларын сүзу рұқсат етілмеген құрылғыларды блоктауға мүмкіндік береді. Желіде қолданушылар мен құрылғылардың рұқсатсыз әрекеттерін болдырмау үшін келесі шаралар енгізілді: MAC-мекенжайлар бойынша бақылау (Port Security). Әрбір портқа белгілі бір MAC-мекенжайлар ғана қосыла алады. Бөгде құрылғы қосылған жағдайда порт автоматты түрде бұғатталады. Жеке интерфейстерден басқа, MAC-адрес интерфейстер тобын немесе тіпті барлық желілік интерфейстерді анықтай алады [4].

Қол жеткізуді бөлу: Администратор (ноутбук) - маршрутизатор, коммутатор және серверге толық қолжетімділікке ие. Кәдімгі пайдаланушылар (PC, Laptop) - серверге тек HTTP/HTTPS арқылы қосыла алады. IoT құрылғылары - тек өз VLAN ішінде байланыса алады, негізгі желіге кіре алмайды. Жүйелік оқиғаларды бақылау: Барлық маңызды оқиғалар syslog-серверге тіркеледі. SSH арқылы әрбір кіру әрекеті журналға жазылады.

Операциялық жүйеде, құрылғыда немесе қолданбада орын алатын оқиғаларды журналдау - ақпараттық қауіпсіздікті қамтамасыз ету процесінің ажырамас бөлігі. Қауіпсіздік журналдарындағы оқиғалардың болуына қарай желіге шабуыл жасау әрекетін алдын ала анықтауға болады. Егер оқиға орын алса, журналдағы жазбалар оны тергеуге көмектесе алады. Сондықтан қолданбалы деңгейдегі Syslog хаттамасы ақаусыз жұмыс істеуі керек. Ірі желілерде оқиғаларды жинау үшін әдетте барлық құрылғылар мен қолданбалардан оқиғаларды алатын орталық Syslog сервері қолданылады. Хакер белгілі бір құрылғыны бұзуға тырысады. Егер ол сәтті болса, онда құрылғыдағы оқиғалар журналын тазалай алады. Алайда бұл оқиғалар туралы жазбалар орталық Syslog серверінде сақталады [5].

Әрекетті бақылау үшін желі оқиғаларын түсіретін syslog серверін конфигурациялауға болады.

ACL пайдалану күдікті трафикті блоктауға көмектеседі, бірақ жетілдірілген талдау үшін Snort сияқты интрузияны анықтау жүйелерін (IDS) қолданған дұрыс. Алайда, Packet Tracer IDS-ке қолдау көрсетілмейді.

Журналдар арқылы хабарландыруларды эмуляциялау қауіпті анықтауды автоматтандыруға мүмкіндік береді. Желідегі кез келген күдікті әрекеттерді ерте анықтау үшін бақылау шаралары енгізілді. Желілік трафикті бақылау: Packet Tracer Simulation Mode арқылы нақты уақытта трафикті талдау. Қауіпті немесе рұқсат етілмеген трафикті автоматты түрде бұғаттау үшін ACL ережелері енгізілді. Желі құрылғыларының жұмысына мониторинг: SNMP көмегімен құрылғылардың жұмысын бақылау. Syslog сервері арқылы қауіпсіздік оқиғаларын жинау.

Практикалық жұмыстың нәтижесінде біз осындай қорытындыға келеміз:

Ақпараттық қауіпсіздікті қамтамасыз ету мақсатында желіде қатаң қолжетімділік саясаты енгізілді. Бұл саясат құрылғылар арасындағы өзара әрекеттестікті реттеп, маңызды желілік түйіндерге рұқсатты пайдаланушылардың рөлі мен құрылғылардың функционалдық мүмкіндіктеріне сәйкес шектейді.

Әкімші қолжетімділігі:

Желіні басқару және бақылау үшін әкімшінің ноутбугіне кеңейтілген рұқсаттар берілген. Әкімші маршрутизаторға SSH протоколы арқылы қосыла алады, бұл оған желіні қашықтан басқаруға мүмкіндік береді. Сонымен қатар, әкімші коммутаторға SSH және SNMP арқылы қосылып, оның параметрлерін өзгерте алады және желілік трафикті бақылай алады.

Серверге әкімші тек басқару мақсатында қосыла алады. Бұл қосылу SSH және HTTP арқылы жүзеге асырылады, ал басқа хаттамаларға шектеу қойылған. IoT құрылғыларына әкімшінің қолжетімділігі жоқ, себебі олар басқа VLAN-да оқшауланған.

Қауіпсіздік шаралары ретінде SSH қолданылады, бұл деректердің шифрланған байланысын қамтамасыз етеді және Telnet-ке қарағанда анағұрлым қауіпсіз болып табылады. Желілік құрылғыларға кіру парольмен қорғалған, ал SNMP қызметі тек әкімшіге рұқсат етілген.

Пайдаланушылардың қолжетімділігі:

Кәдімгі пайдаланушылардың желіге қосылу мүмкіндігі шектеулі. Олар серверге HTTP протоколы арқылы қосылып, ондағы қызметтерді пайдалана алады.

Маршрутизаторға, коммутаторға және IoT құрылғыларына пайдаланушылардың қолжетімділігі жоқ. Бұл желінің тұрақтылығын қамтамасыз ету және пайдаланушылардың маңызды желілік құрылғыларға әсер ету мүмкіндігін болдырмау үшін жасалған.

Қауіпсіздік мақсатында пайдаланушылардың желілік құрылғыларға SSH арқылы қосылу әрекеттері бұғатталған. Серверге қосылу тек HTTP арқылы жүзеге асырылады, ал SSH қолжетімді емес. Сонымен қатар, коммутаторда MAC-мекенжай бойынша бақылау механизмі енгізілген, бұл рұқсат етілмеген құрылғылардың желіге қосылуын шектейді.

Серверге қолжетімділік:

Сервер әкімші мен пайдаланушылардың сұраныстарын өңдейді. Пайдаланушылар HTTP арқылы сұраныстар жібере алады, ал әкімші тек SSH арқылы қосыла алады. IoT құрылғыларының сервермен байланысы шектелген, бұл ACL (Access Control List) көмегімен жүзеге асырылады.

Сервердің қауіпсіздігін қамтамасыз ету үшін тек қажетті порттар ашық. HTTP және SSH порттарынан басқа барлық кіріс трафигі бұғатталған. ACL ережелері IoT құрылғыларынан серверге келетін сұраныстарды қабылдамайды, осылайша ықтимал қауіптерді азайтады. Сонымен қатар, сервер конфигурациясының резервтік көшірмесі жасалады, бұл істен шыққан жағдайда жүйені қалпына келтіруді жеңілдетеді.

IoT құрылғыларының қолжетімділігі:

IoT құрылғылары оқшауланған VLAN ішінде орналасқан және олардың желіге қосылу мүмкіндіктері шектелген. Олар тек Home Gateway арқылы байланыс орнатуға рұқсат етілген. Мысалы, бейнебақылау камерасы тек белгілі IP-мекенжайларға бейне ағын жібере алады, ал басқа құрылғылармен өзара әрекеттесе алмайды.

IoT құрылғыларына интернетке шығуға тыйым салынған. Сонымен қатар, олар сервермен немесе басқа VLAN-дармен байланыса алмайды. Бұл олардың ықтимал шабуыл нысаны болуын болдырмау үшін маңызды шара болып табылады.

Қауіпсіздік шаралары ретінде ACL арқылы шектеулі қолжетімділік орнатылды. IoT құрылғылары жеке VLAN ішінде оқшауланған, бұл олардың басқа желілерге кіру мүмкіндігін шектейді. Сонымен қатар, сыртқы құрылғылардың IoT желісіне кіруіне толық тыйым салынған.

Қолданылған әдебиеттер тізімі

1. Andrew S. T., Nick F., David W. Computer Networks // Pearson Education Limited. – 2021. – ISBN 978-1-292-37406-2. - С. 18-20.
2. Столлингс У. Network Security Essentials: Applications and Standards // Prentice Hall. – 2011. – ISBN 978-0-13-610805-4. - С. 162.
3. Лапонина О.Р. Основы сетевой безопасности. Часть 1. Межсетевые экраны // Национальный Открытый Университет «ИНТУИТ». - 2014. - С. 41.
4. Олифер В.Г., Олифер Н.А. Компьютерные сети: принципы, технологии, протоколы. 2-е изд. // Учебник для вузов. - С. 419.
5. Бирюков А.А. Информационная безопасность: защита и нападение // ДМК Пресс. – 2023. – №3. – С. 138.

УДК 004

РАЗРАБОТКА И ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ МЕТОДА И ИНСТРУМЕНТА ДЛЯ ВЫЯВЛЕНИЯ ФЕЙКОВЫХ НОВОСТЕЙ В СОЦИАЛЬНЫХ СЕТЯХ

Аскаров Абылай Дарханулы
askarovabylay@yandex.kz