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

тәсіл қажет: заманауи технологияларды және қауіпсіздік шараларын үздіксіз жетілдіру, сондай-ақ техникалық және ұйымдастырушылық шараларды үйлестіру ақпараттық инфрақұрылымды тиімді әрі сенімді қамтамасыз етеді.

Қолданылған әдебиеттер

1. Microsoft Azure Security Essentials. 2021. URL: https://learn.microsoft.com/en-us/azure/security/fundamentals/overview
2. «Как вести бизнес через облачные сервисы.» URL: https://secrets.tinkoff.ru/razvitie/oblachnye-servisy/
3. Нестеренко В.Р., Маслова М.А. «Современные вызовы и угрозы информационной безопасности публичных облачных решений и способы работы с ними». Научный результат. Информационные технологии. – Т.6, №1, 2021. – С.48-54. DOI: 10.18413/2518-1092-2021-6-1-0-6, URL: http://rrinformation.ru/journal/annotation/2375/
4. Миронова, А.О. «Применение методики оценки угроз безопасности информации». А.О. Миронова, Ю.Ю. Гончаренко, А.С. Гоголь, А.Н. Фролова // Энергетические установки и технологии. – 2021. – Т.7, №4, – С.71-75.
5. Облачные сервисы. URL:https://corporatefinanceinstitute.com/resources/knowledge/data-analysis/cloud-services/
6. Ожиганова, М.И. «Методы и средства проведения анализа угроз локальной вычислительной сети предприятия». М.И. Ожиганова, А.О. Шейко, Е.М. Исакова, А.О. Миронова // Цифровая трансформация науки и образования. Сборник научных трудов II Международной научно-практической конференции. 2021. – С.264-270.
7. Entra ID Diagram. URL: https://cdn-dynmedia-1.microsoft.com/is/image/microsoftcorp/Entra_ID_Diagram_new?resMode=sharp2&op_usm=1.5,0.65,15,0&wid=3840&hei=1500&qlt=100&fit=constrain
8. Azure Sentinel End-to-End Security. URL: https://gqadir.com/wp-content/uploads/2021/01/Azure-Sentinel-End-to-End-Security.png
9. Azure Key Vault Overview Diagram. URL: https://learn.microsoft.com/en-us/azure/key-vault/media/key-vault-whatis/azurekeyvault_overview.png

IOT ҚҰРЫЛҒЫЛАРЫНЫҢ ЖЕЛІДЕГІ ҚАУІПСІЗДІГІН ҚАЛАЙ ҚАМТАМАСЫЗ ЕТУГЕ БОЛАДЫ: СТРАТЕГИЯЛАР ЖӘНЕ PACKET TRACER КӨМЕГІМЕН МОДЕЛЬДЕУ

Т. Сахатбекқызы., Т.А.Бахтиярқызы
tokaniasgtbk@gmail.com , arujan081204@gmail.com
Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана қ., Қазақстан.
Ғылыми жетекші: Казиева Назым Магидулловна

Аңдатпа

Мақалада IoT құрылғыларының элементтерінің желідегі қауіпсіздігін қамтамасыз ету мәселесі қарастырылған. IoT инфрақұрылымына төнетін негізгі киберқауіптер мен олардың әсері талданып, қорғаныс стратегиялары ұсынылды. Қауіпсіздік шаралары ретінде шифрлеу, аутентификация, желілік сегментация және жаңартулардың маңыздылығы сипатталады. Сонымен қатар, Cisco Packet Tracer ортасында IoT құрылғыларының қауіпсіздігін модельдеу әдістері сипатталған. Ұсынылған шешімдер IoT жүйелерін қорғаудың тиімділігін арттыруға бағытталған.

Кілт сөздер: IoT қауіпсіздігі, желілік шабуылдар, шифрлеу, аутентификация, Firewall, Packet Traicer, желілік модельдеу, киберқауіптер, мәліметтерді қорғау.

Кіріспе. XXI ғасыр цифрлық технологиялардың қарқынды дамыған дәуірі. IoT (Internet of Things) құрылғылары біздің күнделікті өміріміздің бір бөлігіне айналды. Ақылды үйлерден бастап өнеркәсіптік орындарға дейін IoT технологиялары процестерді автоматтандыруға және тиімділікті арттыруға көмектеседі. IoT құрылғылары қазіргі таңда шабуылдардың негізгі нысанына айналуда, өйткені олардың көпшілігі әлсіз қорғалған және желіге заңсыз қол жеткізуді жеңілдетеді.

Талқылаулар мен нәтижелер. IoT құрылғыларына төнетін қауіптер 2014 жылы Ресейде орын алған қызықты әрі үрей тудыратын жағдай хакерлердің әрекеті, желіде ол «Шайнекпен келген шабуыл» атты атақты жағдайдан көруге болады. Мұнда хакерлер интернетке қосылған кәдімгі ақылды шәйнектерді (смарт шәйнек) пайдаланып, Wi-Fi осал желісін пайдалану арқылы, интернет провайдерлердің серверлеріне шабуыл жасады. Нәтижесінде адамзаттың қарапайым тұрмыста қолданып жатқан шәйнектері хакерлік қаруға айналды!

IoT құрылғылары үлкен көлемде деректер жинайды, оның ішінде пайдаланушының жеке ақпараты, денсаулық көрсеткіштері, геолокациясы және күнделікті әдеттері болуы мүмкін. Бұл ақпарат хакерлердің қолына түссе, оны алаяқтық, бопсалау немесе басқа қылмыстық әрекеттер үшін қолдануы мүмкін. IoT тек тұрмыстық техникада ғана емес, өнеркәсіптік процестерде, денсаулық сақтау саласында және көлік жүйелерінде де жиі қолданылады. 2015 жылы Украинадағы энергетикалық инфрақұрылымға кибершабуыл жасалып, нәтижесінде бірнеше аймақтарда электр жарығы өшкендігін айтуға болады. Бұл шабуыл зиянды бағдарлама SCADA жүйелерін зақымдап, операторларға электр желілерін басқаруға мүмкіндік бермеді.

IoT құрылғыларының осалдықтарын жүйелі түрде қарастыру үшін негізгі қауіптер, олардың маңызы және Packet Tracer көмегімен модельдеу әдістері 1 кестеде сипатталған [1].

Кесте 1. IoT желі архитектурасының қауіпсіздік талдауы және қорғаныс стратегиялары

IoT желі элементі	Негізгі осалдылықтар	Төнетін қауіптер	Жүйедегі рөлі мен ықпалы	Packet Tracer көмегімен қорғау және модельду әдісі
Датчиктер (физикалық құрылғылар)	Әлсіз шифрлау, аутентификацияның жоқтығы	Деректерді ұстап қалу, жалған ақпарат енгізу	Деректерді бастапқы жинау көзі, сенсорлық ақпараттың дұрыстығын қамтамасыз етеді	Қауіпсіздік хаттамаларын (TLS, WPA2) қолдану, құрылғылардың қауіпсіздігін тестілеу
Басқару блоктары (IoT-шлюздер)	Фирмалық протоколдарға тәуелділік, әлсіз брандмауэр	Желілік шабуылдар, құрылғыларды басқаруды қолға алу	IoT құрылғыларының арасындағы деректерді үйлестіру және өңдеу орталығы	Брандмауэрді күшейту, IDS/IPS қолдану, виртуалды модельдеу

Желі инфрақұрылымы	Әлсіз Wi-Fi қауіпсіздігі, ашық порттар	MITM (Man-in-the-Middle) шабуылы, рұқсатсыз қол жеткізу	Құрылғылар арасындағы ақпарат алмасудың негізгі арнасы	VLAN сегментациясы, VPN пайдалану, Packet Tracer-де қауіптерді модельдеу

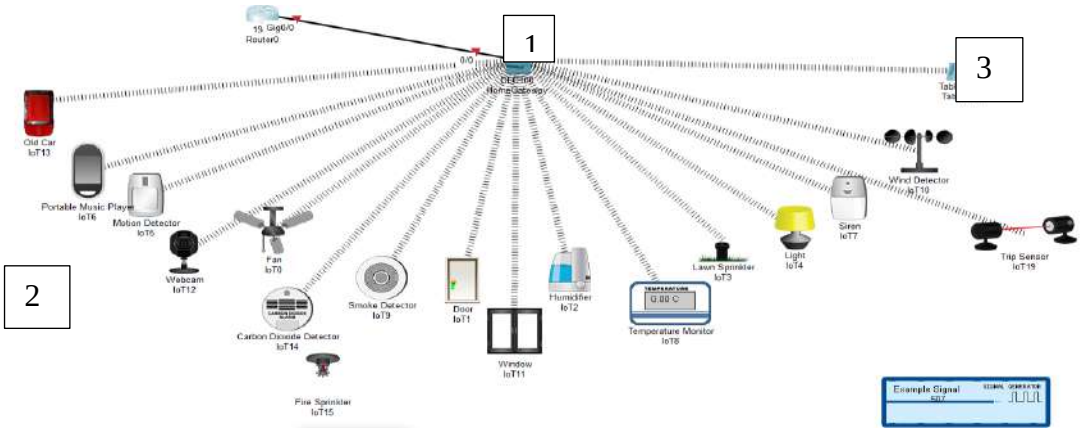
Packet Tracer көмегімен модельдеу

VLAN (Виртуалды жергілікті желі) бұл IoT құрылғыларын жеке желілерге бөлу.

VPN-интернеттегі деректерді шифрлайды және IP мекен жайын жасырады, осылайша қауіпсіз байланыс орнатады. 2018 жылы **Hapleton Bank** қаржы ұйымы қашықтан жұмыс істейтін қызметкерлерінің деректерін қорғау үшін **VPN қолданбаған**. Нәтижесінде, бір қызметкер **қоғамдық Wi-Fi желісіне** қосылып, шабуылдаушылар **банк жүйесіне рұқсатсыз кіріп**, клиенттердің **құпия қаржылық мәліметтерін ұрлаған.**

Packet Tracer-де ақылды үй (Smart home) IoT моделін жасау және қауіпсіздік баптаулары.

Бұл **Packet Tracer**-де модельденген **ақылды үй (Smart home) IoT желісінің топологиясы.** Сценарийде **бір Wi-Fi желісіне** қосылған әртүрлі **IoT құрылғылары** бар және олар **орталық шлюз (Home Gateway) арқылы бақыланады.**

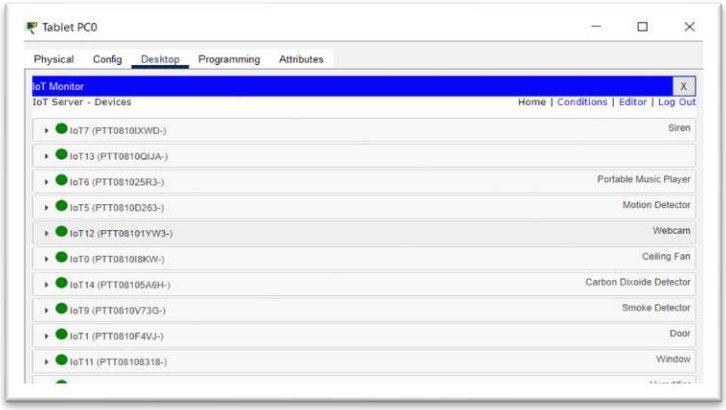


Сурет 1. Packet Traicer –де IoT құрылғыларын модельдеу топологиясы

1. Home Gateway (DCE100) – барлық IoT құрылғыларын байланыстыратын негізгі басқару құрылғысы. Бұл шлюз IoT құрылғылары мен қолданушылар арасында деректер алмасуды басқарады. Желінің негізгі қауіпсіздігін қамтамасыз етеді.

2. IoT құрылғылары – әртүрлі смарт құрылғылар (терезе, есік, дабыл жүйелері, жарықтандыру, сенсорлар). Қауіпсіздік құрылғылары: қозғалыс детекторы (Motion Detector), веб-камера (Webcam), дабыл (Siren). Климаттық құрылғылар: температура датчигі (Temperature Monitor), ауа ылғалдандырғыш (Humidifier), жел сенсоры (Wind Detector). Үй автоматизациясы: желдеткіш (Fan), жарық шамы (Light), есік (Door), терезе (Window) Сурет 1.

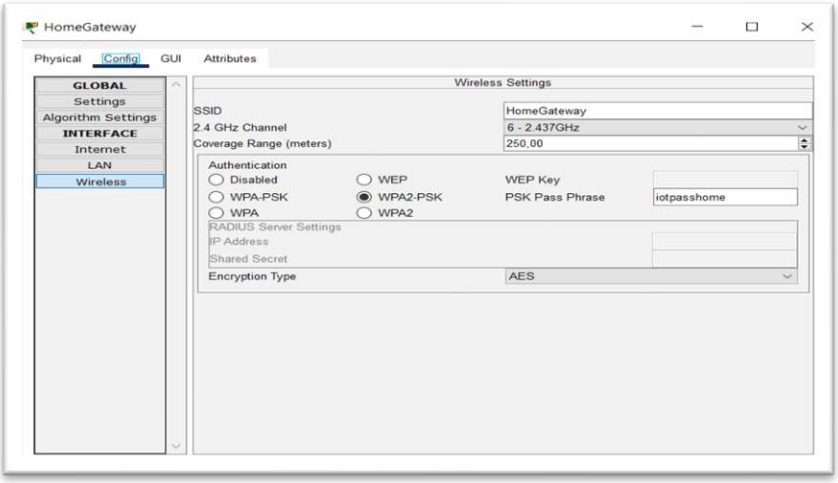
3 Планшет (Tablet PC) – IoT құрылғыларын қашықтан басқаруға және мониторинг жасауға мүмкіндік береді. Планшет Home Gateway-ге қосылып, арнайы интерфейс арқылы барлық құрылғылардың жұмысын көруге және басқаруға болады. Мысалы: қозғалыс сенсоры біреуді байқаса, планшетке хабарлама келеді. Суретте **Packet Tracer** ортасында әртүрлі IoT құрылғыларының планшетке қосылғанын көруге болады (сурет 2).



Сурет 2. IoT құрылғыларының қосылуы

IoT құрылғыларының осалдығы желідегі қорғалмаған құрылғылар арқылы хакерлердің бүкіл желіні бұзып кіруі.

IoT желісін құпия кілт орнату арқылы құрылғыларды ортақ желіге жалғап, «iotpasshome» паролін пайдаланып Home Gateway-ға қауіпсіз түрде қосылады. WPA2 - PSK аутентификациясы мен AES шифрлеуі деректердің қорғалуын қамтамасыз етеді, осылайша желідегі құрылғылардың қауіпсіздігі сақталады (сурет 3).



Сурет 3. WPA2-PSK аутентификациясы

Мысал ретінде құрылғылардың қозғалысына 2 команда бердім.

1 - команда. Қозғалыс анықталса ("person present"). Бұл шарт бойынша қозғалыс детекторы (IoT5) іске қосылғанда келесі әрекеттер орындалады:

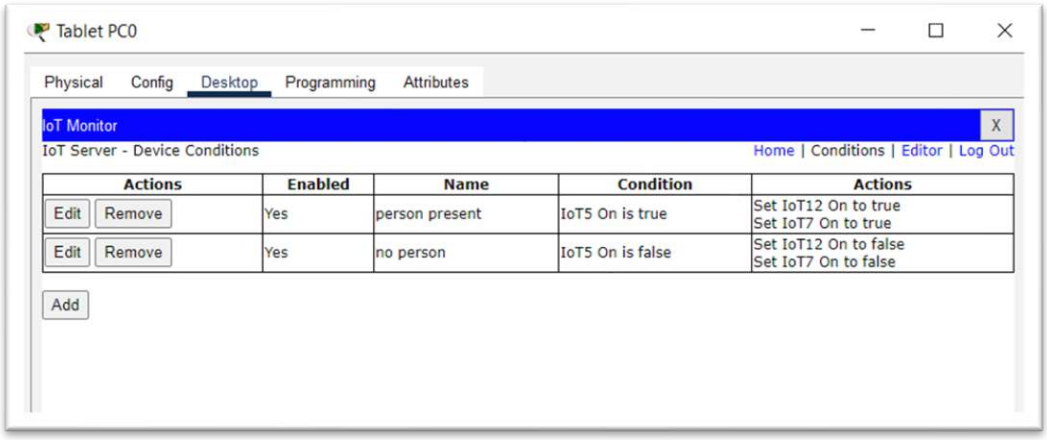
- ✓ Веб-камера (IoT12) жазба жүргізуді бастайды;
- ✓ Сирена (IoT7) дыбыс шығарады.

Бұл механизм бөлмеге адам кірген кезде қауіпсіздік шараларын автоматты түрде іске қосады.

2 – команда. Қозғалыс анықталмаса ("no person") егер қозғалыс детекторы (IoT5) ешқандай қозғалыс тіркемесе, онда келесі әрекеттер орындалады:

- ✓ Веб-камера (IoT12) өшіріледі.
- ✓ Сирена (IoT7) дабыл беруді тоқтатады.

Бұл шарт қажетсіз құрылғылардың жұмысын шектеу арқылы энергияны үнемдеуге және жүйенің тиімділігін арттыруға бағытталған. Осылайша, аталған екі команда арқылы қауіпсіздік жүйесі автоматтандырылып, қажетсіз қуат тұтыну азайтылады (сурет 4).

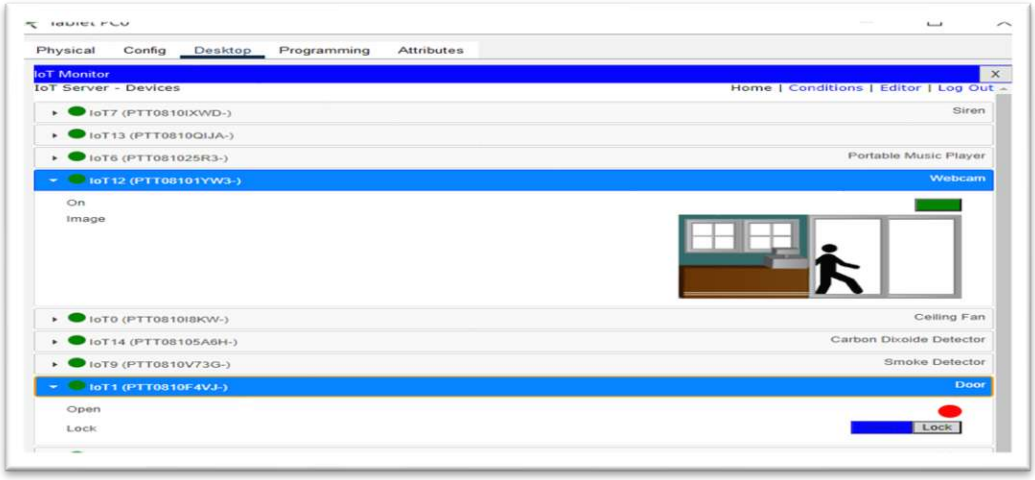


Сурет 4. Ереже орнату

Енді осы конфигурацияны тексеру барысында **Alt** батырмасын басып, қозғалыс детекторын (IoT5) іске қостым. Нәтижесінде:

- ✓ Сирена (IoT7) автоматты түрде іске қосылды.
- ✓ Веб-камера (IoT12) адам кіргені туралы белгі жіберді.

Бұл жүйе офлайн режимде қауіпсіздікті бақылауға мүмкіндік береді. Яғни, интернетсіз-ақ детектор, сирена және камера өзара әрекеттесіп, қауіпсіздік шараларын автоматты түрде іске асырады (сурет 5).



Сурет 5. Қауіпсіздік жүйесін тексеру

Көрсетілген мысалдардан IoT құрылғылары арқылы қауіпсіздікті бақылауға болатынын көрдік. Бірақ мұндай жүйенің тұрақты әрі қауіпсіз жұмыс істеуі үшін арнайы желілік конфигурацияларды орындау керек. Төменде осыған қажетті негізгі қадамдар берілген.

1. Құпия сөздерді орнату және SSH конфигурациялау құрылғылардың қауіпсіздік арттыру үшін мықты құпия сөздер орнатылады және SSH қосылады > service password-encryption. Барлық құпия сөздерді шифрлау > crypto key generate rsa modulus 2048 – RSA кілтін генерациялау > transport input ssh Telnet-ті өшіріп, тек SSH қолдану.

2. VLAN құру және IoT құрылғыларын бөлу IoT құрылғылары үшін жеке VLAN орнату арқылы қауіпсіздік күшейтіледі > vlan 10. Жаңа VLAN құру > name IoT Devices – VLAN атауын беру > interface Gigabit Ethernet 0/1. Интерфейсті таңдау > switchport mode access. Портты қолжетімді режимге қою > switchport access vlan 10. Портты VLAN 10-ға қосу.

3. VPN (Virtual Private Network) конфигурациясы VPN IoT құрылғылары мен пайдаланушылар арасындағы қауіпсіз байланысты қамтамасыз етеді > crypto isakmp key VPNKey123 address 0.0.0.0 VPN кілтін орнату > crypto ipsec transform-set. MYSET esp-aes 256 esp-sha-hmac. Шифрлау параметрлерін орнату > crypto map VPNMAP 10 ipsec-isakmp – VPN картасын құру > set peer <Remote_IP> Қашықтағы құрылғыны анықтау > set transform-set MYSET. Шифрлау параметрлерін тағайындау > interface Gigabit Ethernet 0/0. VPN картасын интерфейске тағайындау > crypto map VPNMAP. VPN картасын қосу.

4. ACL (Access Control List) құру IoT құрылғыларына сыртқы қолжетімділікті шектеу үшін ACL пайдаланылады > access-list 100 permit tcp 192.168.10.0 0.0.0.255 any eq 22 – SSH арқылы рұқсат беру > access-list 100 deny ip any any – Басқа барлық трафикке тыйым салу > interface GigabitEthernet0/0 – Интерфейсті таңдау > ip access-group 100 in – ACL-ді кіріс трафигіне қолдану.

5. AAA (Authentication, Authorization, and Accounting) орнату IoT_Router жүйесіне кіруді басқару үшін AAA конфигурациясы орындалады > aaa authentication login default local – Аутентификацияны қосу > aaa authorization exec default local – авторизацияны қосу > aaa accounting exec default start-stop group tacacs+ – Бақылауды орнату.

6. NAT (Network Address Translation) конфигурациясы IoT құрылғыларының сыртқы желіге қауіпсіз қосылуын қамтамасыз ету үшін NAT қолданылады > ip nat inside source list 1 interface GigabitEthernet0/0 overload – NAT қызметін қосу.

Осы шаралар IoT құрылғыларының қауіпсіздігін күшейтіп, желіге рұқсатсыз қолжетімділіктің алдын алады

Қорытынды. IoT технологиясының қарқынды дамуы 2025 жылға қарай нарық көлемін 53,8 миллиард долларға дейін арттырады. Бұл өсім өнеркәсіптік автоматтандыруға сұраныстың ұлғаюымен байланысты. Алайда, IoT құрылғыларының қауіпсіздігі маңызды мәселе болып қалады, өйткені олардың 98% шифрланбаған трафикті пайдаланады, бұл кибершабуылдар мен деректер ұрлығын арттырады. Осы қауіптерді болдырмау үшін сенімді киберқауіпсіздік стратегиялары қажет. Желілік тренажерлер, мысалы, Packet Tracer, қауіпсіздік механизмдерін сынап, оқтайландыруда тиімді құрал бола алады. Шифрлау технологияларын енгізу, қауіпсіздік хаттамаларын жетілдіру және экожүйені қорғау тұрақты мониторингпен қамтамасыз етілуі тиіс.

Қолданылған әдебиеттер тізімі:

1. **Packet Tracer - Adding IoT devices to Smart Homes** - Cisco Networking Academy
2. **Introduction to the Internet of Things - Cisco Networking Academy**
3. Bruce Sinclair. IoT Inc: How Your Company Can Use the Internet of Things to Win in the Outcome Economy. 2017. 304 p.
4. Gurutech Networking Training. *Introduction to IoT Connecting & Simulating IoT Devices in Packet Tracer IoT Registration Server.*Қолжетімді:https://youtu.be/qbh7SzCfM1o?si=yK3R25fwXpcw1fyi
5. Techno Brunch. *Smart Security System using Packet Tracer | IoT application | Anti Theft system using Packet Tracer.*Қолжетімді:https://youtu.be/42DCkx36Uv8?si=Fkrbiq5FO8xTRk8a
6. Analyzing Docker Vulnerabilities through Static Analysis.
7. Internet of Things (IoT) Security With Blockchain Technology: A State-of-the-Art Review

8. Markets and Markets – Global Market Research Reports and Consulting

ПОВЫШЕНИЕ ПРОИЗВОДИТЕЛЬНОСТИ РАЗРАБОТЧИКОВ С ПОМОЩЬЮ ИНТЕГРИРОВАННЫХ ИСКУССТВЕННЫХ ИНТЕЛЛЕКТОВ И СООБРАЖЕНИЯ КИБЕРБЕЗОПАСНОСТИ

Серғазы Мәди
saitamenter@gmail.com
Кафедра систем информационной безопасности, факультет информационных технологий, Евразийский национальный университет им. Л.Н. Гумилева, Астана, Казахстан
Научный руководитель – PhD, старший преподаватель Токсеит Динара

Аннотация

Стремительное развитие искусственного интеллекта (ИИ) привело к появлению новых инструментов для повышения производительности разработчиков, особенно в области кибербезопасности. Cursor AI, помощник по программированию на базе искусственного интеллекта, предназначен для оптимизации разработки программного обеспечения путем предоставления предложений по коду в режиме реального времени, поддержки отладки и повышения безопасности. В этом обзоре рассматривается влияние разработки Cursor AIon, ориентированной на кибербезопасность, подчеркивается ее роль в повышении эффективности, сокращении количества ошибок и внедрении методов безопасного кодирования. В статье рассматриваются существующие помощники по кодированию, управляемые ИИ, сравниваются их функциональные возможности и оценивается уникальный вклад Cursor AI в разработку безопасного программного обеспечения. Кроме того, обсуждаются потенциальные риски, связанные с кодированием с помощью ИИ, и предлагаются стратегии снижения рисков для обеспечения надежности и безопасности.

Кибербезопасность остается серьезной проблемой, поскольку уязвимости программного обеспечения продолжают развиваться. Традиционные методы программирования требуют тщательной отладки и аудита безопасности, что делает разработку программного обеспечения трудоемким и сложным процессом. Помощники по программированию на базе искусственного интеллекта, такие как Cursor AI, меняют мир, предлагая интеллектуальные рекомендации, выявляя угрозы безопасности и помогая в отладке. Эти инструменты помогают разработчикам более эффективно писать защищенный код, снижая вероятность человеческой ошибки и повышая общую целостность программного обеспечения.

В этой статье рассматривается, как Cursor AI помогает разработчикам писать более безопасный код, сокращая количество ошибок, повышая осведомленность о безопасности и ускоряя процесс разработки. Кроме того, в ней оцениваются потенциальные риски и этические проблемы, связанные с кодом, созданным с помощью искусственного интеллекта, что гарантирует, что такие инструменты остаются активами, а не обязательствами при разработке безопасного программного обеспечения.

Cursor AI интегрируется с широко используемыми средами разработки и обеспечивает поддержку разработчиков в режиме реального времени. Он обеспечивает интеллектуальное автозавершение, помогая программистам писать более точный код, сводя к минимуму синтаксические и логические ошибки. Инструмент также обладает возможностями автоматической отладки, что позволяет разработчикам быстрее выявлять и устранять проблемы. Помимо повышения производительности, Cursor AI способствует повышению