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

2. Инциденты информационной безопасности: выявление, расследование и реагирование // https://selectel.ru/blog/security-incidents/ (дата обращения: 23.03.2025)
3. Что такое SIEM ? // https://www.microsoft.com/ru-ru/security/business/security-101/what-is-siem (дата обращения: 25.03.2025)
4. План реагирования на инциденты кибербезопасности: что это и почему он нужен каждой организации // https://ddos-guard.ru/blog/plan-reagirovaniya-na-incidenty-kiberbezopasnosti (дата обращения: 25.03.2025)
5. Отакулов Артур Собирович Способы реагирования на инциденты информационной безопасности // E-Scio. 2020. №1 (40). URL: https://cyberleninka.ru/article/n/sposoby-reagirovaniya-na-intsidenty-informatsionnoy-bezopasnosti (дата обращения: 31.03.2025).
6. Русскевич Евгений Александрович Понятие вредоносной компьютерной программы // Актуальные проблемы российского права. 2018. №11 (96). URL: https://cyberleninka.ru/article/n/ponyatie-vredonosnoy-kompyuternoy-programmy (дата обращения: 31.03.2025).
7. Голубятников Артем Олегович DDOS-АТАКИ И МЕТОДЫ БОРЬБЫ С НИМИ // E-Scio. 2022. №10 (73). URL: https://cyberleninka.ru/article/n/ddos-ataki-i-metody-borby-s-nimi (дата обращения: 31.03.2025).
8. Что такое социальная инженерия ? // https://www.kaspersky.ru/resource-center/definitions/what-is-social-engineering (дата обращения: 31.03.2025)

УДК 004.056

MITM ШАБУЫЛЫ (АДАМНЫҢ ОРТАДАҒЫ ШАБУЫЛЫ)

Қартбай Елнұр Ғалымжанұлы
Тынарбай Назым Исламбекқызы
shattik59@gmail.com,tynarbayn@gmail.com
Л.Н.Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультеті
Ақпараттық қауіпсіздік жүйелері кафедрасының студенттері, Астана, Қазақстан
Ғылыми жетекші: Казиева Назым Магидулловна

Аңдатпа

Бұл мақалада Man-in-the-Middle (MITM) шабуылының негізгі түрлері, орындалу механизмдері және олардың қауіпсіздікке тигізетін ықпалы қарастырылған. MITM шабуылы желідегі деректер алмасуға араласу арқылы ақпаратты ұрлау немесе өзгертуге мүмкіндік береді. MITM шабуылын жүзеге асыру үшін ARP-spoofing, DNS-spoofing, SSL-stripping сияқты әдістер кеңінен қолданылады. Бұл зерттеу аясында Kali Linux жүйесінде Bettercap құралы арқылы ARP-spoofing шабуылының орындалу тәсілдері зерттеліп, трафикті ұстап алу және өзгерту процестері көрсетілген. Сонымен қатар, MITM шабуылынан қорғану жолдары, HTTPS, VPN, ARP-қорғаныс механизмдері және жүйелік қауіпсіздік шаралары талданды. Бұл зерттеу MITM шабуылдарының механизмдерін тереңірек зерттеу негінде желілік қауіпсіздікті күшейту бағыттары анықталған.

Кілт сөздер: MITM шабуылы, ARP-spoofing, Kali Linux жүйе, Better Cap құралы, желілік қауіпсіздік.

Кіріспе. Қазіргі таңда ақпараттық қауіпсіздік кибершабуылдардың қарқынды дамуына байланысты маңызды мәселелер туындалуда. Ақпараттық технологиялардың дамуы "Man-in-the-Middle" (MITM) шабуылының жиі орын алуына ықпал етеді. Бұл шабуыл кезінде қаскүнем

екі тарап арасындағы деректердің алмасуына араласып, ақпараттар ұрлануға немесе оны өзгертуге мүмкіндіктер алады. MITM шабуылы қаржы ұйымдарына, мемлекеттік мекемелерге, жеке кәсіпорындарға, тіпті қарапайым пайдаланушыларға да қауіп төндіреді [1, 2].

MITM шабуылдары көбінесе ашық және осал Wi-Fi желілерінде, шифрланбаған трафиктерде және әлсіз қорғаныс жүйелері бар желілік инфрақұрылымдарда орын алады. Қаскүнемдер ARP-spoofing, DNS-spoofing, SSL-stripping және басқа да әдістерді қолдану арқылы өз жәберіленуші желілік трафиктерін бақылап, қол жеткізе алады.

Бұл зерттеу жұмысында MITM шабуылының негізгі түрлері, олардың орындалу механизмдері және қауіпсіздікке тигізетін әсері талданды. Сондай-ақ, Kali Linux операциялық жүйесінде Bettercap құралын пайдалану арқылы ARP-spoofing шабуылының орындалу әдістері зерттеліп, шабуылдың орындалу кезеңдері мен қорғану әдістері қарастырылды.

Зерттеудің мақсаты - MITM шабуылдарының қауіптілігін көрсету, олардың орындалу әдістерін сипаттау және қорғаныс шараларын ұсыну.

Зерттеу әдістері. Зерттеу барысында жалпы ғылыми және арнайы таным, оның ішінде жүйелік талдау және синтез, теориялық жалпылау әдістері қолданылды.

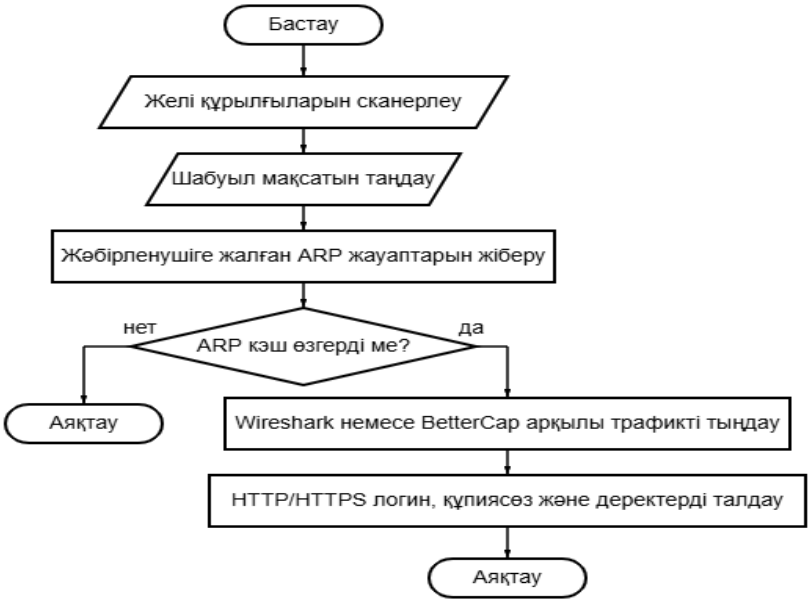
Талқылау және нәтижелер. Зиянкестер, шабуылдаушылар интернет-байланысын бақылау үшін әртүрлі тәсілдерді қоладанады [2]. Бұл әдістердің барлығы пайдаланушылардың деректерін ұрлауға, фишингтік шабуылдар жасауға, бұдан басқа жүйелерге кіруге мүмкіндік береді.

Қолданылатын әдістерге қарамастан, ортадағы адам шабуылдарының көпшілігі қарапайым әрекеттер тізбегін бақылайды. Мысалы: Алиса, Боб және Чак (шабуылдаушы) [3].

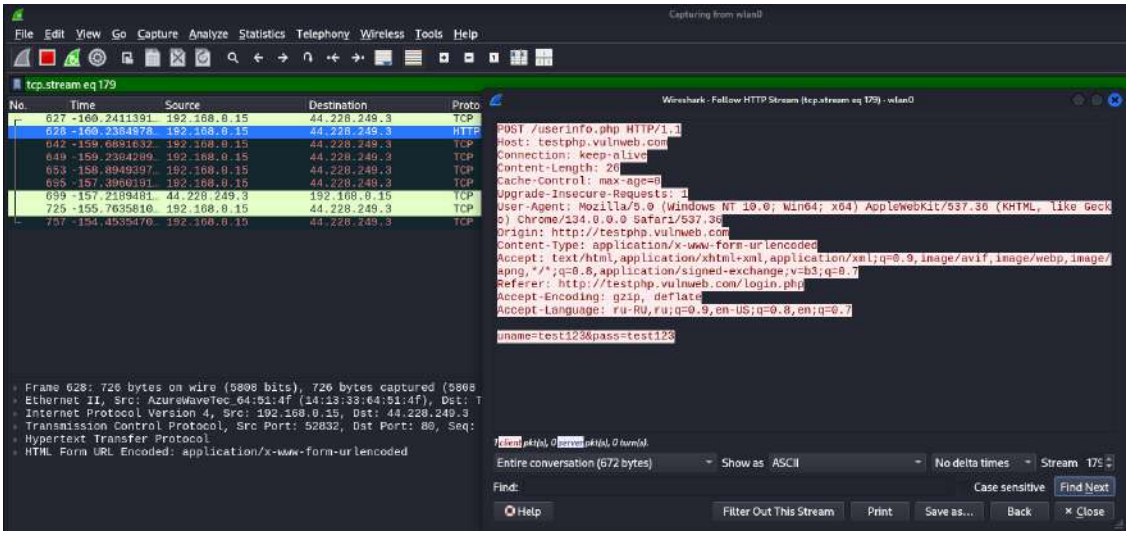
1. Чак Элис пен Бобтың байланысын тыңдайды.
2. Алиса Бобқа хабарлама жібереді.
3. Чак оны ұстап алып оқиды.
4. Чак хабарды өзгертіп, Бобқа жібереді.

«Ортадағы адам» (MITM) шабуылдары көбіне кибершабуылдың бастапқы кезеңдерінде қолданылады, яғни барлау, жүйеге кіру және зиянды әрекеттерді орындайды. Бұл әдіс арқылы шабуылдаушылар пайдаланушы мәліметтерін ұстап қалып, желідегі әрекеттерді бақылай алады.

MITM шабуылы желілік трафикті ұстап, оны өзгертуге немесе тыңдауға мүмкіндік беретін қауіпті кибершабуылдардың бірі болып табылады. Бұл шабуылдың ең көп таралған түрлерінің бірі - ARP Spoofing. Бұл әдіс жергілікті желіде орындалады және шабуылдаушыға трафикті өз құрылғысы арқылы өткізуге мүмкіндік береді (Сурет 1).



Сурет 1. "ARP Spoofing алгоритмі"



Сурет 2. Wireshark арқылы трафикті ұстап алу

Сурет 2. *arpspoof -i eth0 -t 192.168.0.15 192.168.0.1* командасын қолдану арқылы желілік трафикті ұстап алу және шабуыл жасау процестері сипатталған.

Bettercap - желілік трафикті талдауға, ARP спуфинг жасауға, Man-in-the-Middle (MITM) шабуылдарын орындауға арналған қуатты құрал (Сурет 3). Төменде көрсетілген әрекеттер Kali Linux-та Bettercap көмегімен жүзеге асырылған желілік шабуылды сипаттайды.

1. *bettercap -iface wlan0* команда арқылы WLAN интерфейсінде Bettercap қосылып, желіні бақылауға дайындық жасайды.
2. *net.probe on* команда желідегі барлық белсенді құрылғыларды анықтап, олардың IP, MAC және өндіруші (Vendor) ақпаратын жинау мүмкіндіктеріне ие.

3. *arp.spoof on* әрекет шабуылдаушыға өзін желілік шлюз ретінде көрсетуге мүмкіндік алады, маршрутизатор ARP спуфингтен қорғалмаған болса, шабуыл сәтті орындалып, толық дуплексті (full-duplex) трафик бағытын өзгерту мүмкіндігіне ие болады.

Сурет 3. Bettercap құралы арқылы желілік шабуыл

Ал Bettercap желі арқылы өтетін барлық трафикті тыңдап, оны талдауға кіріседі. Бұл әрекет барысында DNS сұраныстары мен жауаптары, HTTP трафигі, оның ішінде POST сұраныстары, логин мен пароль туралы мәліметтер ұсталып қалады (Сурет 4).

Сурет 4. Желі трафигін тыңдау (Sniffing)

Осылайша, шабуылдаушы ARP спуфинг және трафикті тыңдау әдістерін қолдана отырып, қорғалмаған HTTP аутентификациялық мәліметтерін оңай ұстап ала алады. Мұндай қауіптердің алдын алу үшін HTTPS пайдалану, ARP қорғау механизмдерін қосу және желідегі күдікті әрекеттерді бақылау үшін маңызды.

ARP спуфинг шабуылын орындау үшін бұл зерттеуде екі түрлі әдіс қолданылды: A**rpspoof** және **Bettercap құралы**. 1-кестеде осы әдістердің мүмкіндіктері салыстырмалы түрде көрсетілген [6].

Кесте 1. A**rpspoof** және **Bettercap құралдары**

Критерий	Arpspoof	Bettercap
Қолдану қарапайымдылығы	Қолдану үшін бірнеше команданы қолмен орындау қажет, сондай-ақ шабуылдың нысанын нақты көрсету талап етіледі.	Bettercap интерактивті интерфейсі бар, қолдануға ыңғайлы әрі қосымша функционалдары жеткілікті.
Желі құрылғыларын анықтау	Қолмен енгізілген IP мекенжайына ғана шабуыл жасайды, яғни автоматты түрде құрылғыларды анықтау мүмкіндігі жоқ, шабуылды дайындау уақыты ұзағырақ.	`net.probe on` командасын орындау арқылы желідегі барлық белсенді құрылғыларды автоматты түрде анықтап, жылдам шабуыл жасай алады.
Функционалдық мүмкіндіктер	Бұл құрал тек ARP спуфинг шабуылын іске асырып, трафикті қайта бағыттау үшін қолданылады.	Bettercap тек ARP спуфингпен шектелмейді, ол сонымен қатар DNS Spoofing, Sniffing және Man-in-the-Middle (MITM) шабуылдарын жүзеге асыра алады.
Трафикті бақылау (Sniffing)	Желідегі деректерді тыңдау үшін қосымша бағдарламалар (мысалы, Wireshark) қажет.	Bettercap өз ішінде трафикті ұстап, оны талдауға мүмкіндік береді.
Жасырындық деңгейі	Бұл әдіс қосымша құралдарды қажет ететіндіктен, шабуылды анықтау ықтималдығы жоғары.	Барлық процестерді орталықтандырылған түрде басқаруға мүмкіндік береді, бұл шабуылды тиімді орындауға және жасырын әрекет етуге көмектеседі.
Қорғану механизмдерінен айналып өту	Қарапайым шабуылдарды орындауға мүмкіндік береді, бірақ қорғанысы жоғары желілерге шабуылдау қиынырақ.	Бұл құрал динамикалық шабуылдарды орындауға, әртүрлі MITM әдістерін біріктіруге және қорғаныс механизмдерін айналып өтуге мүмкіндік береді.

Зерттеу барысында ARP спуфинг шабуылынан қорғану мақсатында ARP Saqshy бағдарламасы құрастырылды, бағдарлама шабуылды анықтайды және алдын алатын графикалық қосымшаны жасайды.

ARP Spoofing қорғаныс бағдарламасы және оның коды [7]

Біздің қарастырған қорғаныс құрылғысы қалай жұмыс істейді?

1. Желі туралы ақпаратты алады – роутердің IP және MAC-адресін анықтайды.

2. ARP-кэшті тексереді – роутердің MAC-адресі өзгергенін бақылайды.

3. Жаңартылған MAC-адреспен салыстырады – егер өзгеріс байқалса, шабуыл туралы ескертеді.

4. Ескерту береді – дыбыстық сигнал, экрандық хабарлама және жұмыс үстелі арқылы.

5. Желіні өшіреді – қауіп анықталса, интернет автоматты түрде өшіріледі.

6. ARP-кэшті тазалайды – қажет болғанда желіні қорғау үшін.

7. ARP-кестесін көрсетеді – arp -a командасына ұқсас желідегі құрылғылардың IP және MAC-адрестерін шығарады.

Ортадағы адам (MITM) шабуылдары желідегі осалдықтарды пайдаланып, пайдаланушылардың құпия мәліметтерін ұрлауға бағытталады. Мұндай шабуылдардан қорғану үшін киберқауіпсіздік шараларын сақтау өте маңызды.

Қорытынды. Ең алдымен, **қауіпсіз желіге қосылу** басты шарт болып табылады. Белгісіз немесе ашық Wi-Fi желілеріне қосылу үлкен қауіп төндіреді, сондықтан WPA2/WPA3 қорғанысы бар маршрутизаторларды қолдану керек. Сонымен қатар, **VPN қызметін пайдалану** желідегі трафикті шифрлап, оны үшінші тараптардың бақылауынан қорғайды. **Желідегі мәліметтерді шифрлау** да маңызды рөл атқарады. HTTPS қосылымдарын ғана пайдалану, электрондық пошта мен хабарламаларды түпкілікті шифрлауды қосу ақпараттың қауіпсіздігін арттырады. **DNS сұрауларын шифрлау** арқылы DNS-спуфинг сияқты шабуылдардың алдын алуға болады.

Қауіпсіздікті күшейтудің тағы бір маңызды аспектісі - **жүйелік жаңартуларды уақытылы орнату** және **антивирус пен брандмауэрді белсенді ұстау**. Бұл зиянды бағдарламалар мен шабуылдарды ерте анықтауға көмектеседі.

Бұдан бөлек, **құпиясөздерді қауіпсіз сақтау және қайта пайдаланбау** үшін құпиясөз менеджерін қолдану қажет. **Көп факторлы аутентификацияны (MFA) енгізу** есептік жазбалардың қосымша қорғалуын қамтамасыз етеді. Желілік қауіпсіздікті арттыру үшін **нөлдік сенім принципін (Zero Trust)** қолдану қажет, яғни жүйеге кірген пайдаланушылар мен құрылғыларға автоматты түрде сенім білдірудің орнына, әрбір кіру әрекеті мұқият тексерілуі тиіс. Сонымен қатар, **желілік белсенділікті бақылау** арқылы күдікті әрекеттерді ерте анықтап, шабуылдардың алдын алуға болады.

Жалпы, жоғарыда аталған әдістерді қолдану желілік қауіпсіздікті күшейтіп, MitM шабуылдарынан тиімді қорғануға мүмкіндік береді. Киберқауіпсіздік - бұл бір реттік емес, үздіксіз процесс, сондықтан әрбір пайдаланушы өзінің жеке деректерін қорғауға жауапкершілікпен қарауы қажет.

Пайдаланылған әдебиеттердің тізімі

1. John Martinez. Man-in-the-Middle (MITM) Attack: Definition, Examples & More: https://www.strongdm.com/blog/man-in-the-middle-attack 03.01.2025 (Время посещения 20.03.2025)
2. Man-in-the-middle attack: https://encyclopedia.kaspersky.com/glossary/man-in-the-middle-attack/ (Время посещения 21.03.2025)
3. Jeff Petters. Man-in-the-Middle: советы по обнаружению и предотвращению: https://habr.com/ru/companies/varonis/articles/526632 05.11.2020 (Время посещения 20.03.2025)
4. ARP Мағынасы Kazakh: https://goong.com/kk/word/arp-мағынасы--kazakh/ (Время посещения 22.03.2025)
5. Защита от MITM атак: Примеры инструменты и советы: https://sky.pro/wiki/javascript/zashita-ot-mitm-atak-primery-instrumenty-i-sovety/ (Время посещения 25.03.2025)
6. ARP Spoofing: https://www.prosec-networks.com/en/blog/arp-spoofing/ (Время посещения 29.03.2025)
7. Kartbay Yelnur & Tynarbay Nazym. ARP Saqshy: https://github.com/Elikon0106/ARP-Saqshy/tree/main (Время создания 28.03.2025)

ӘОЖ 004.056

ӘЛЕУМЕТТІК ИНЖЕНЕРИЯ ҚАУІПСІЗДІККЕ ҚАТЕР РЕТІНДЕ: ҚЫЗМЕТКЕРЛЕРДІ ҚОРҒАУ ЖӘНЕ ОҚЫТУ ӘДІСТЕРІ