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

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

Маратов Бауыржан Жанатович
maratov011@gmail.com
7М06306 “Ақпараттық қауіпсіздік жүйелері” мамандығы бойынша магистрант, Л.Н. Гумилев атындағы ЕҰУ, Астана, Қазақстан
Ғылыми жетекшісі - техника ғылымдарының кандидаты, доцент К.М. Сагиндыков

Қазіргі уақытта шабуылдаушылар корпоративтік желілерде орнатылған қорғаныс жүйелерін айналып өту немесе жүйенің осал тұстарын анықтау үшін әлеуметтік инженерия әдістерін жиі қолдануда.

Әлеуметтік инженерия – бұл әлеуметтану мен психологияны пайдалана отырып, белгілі бір нәтижеге жетуге бағытталған кеңістік, жағдайлар мен мүмкіндіктерді жасау әдістері мен технологияларының жиынтығы.

Әлеуметтік инженерия белгілі бір формада ежелгі заманнан бері қолданылып келеді. Мысалы, Ежелгі Рим мен Ежелгі Грецияда арнайы дайындықтан өткен риторларды жоғары бағалаған, олар өз қарсыластарын «қателіктеріне» сендіре алған. Бұл адамдар дипломатиялық келіссөздерге қатысып, мемлекеттік мәселелерді шешкен. Кейінірек әлеуметтік инженерияны ҰҚК сияқты арнайы қызметтер қолдана бастады. Олардың агенттері сәтті түрде өздерін басқа біреу ретінде таныстырып, мемлекеттік құпияларды білген [1].

Әлеуметтік инженерия әдістерін қолдану үлкен қаржылық шығындарды талап етпейді және оны жүзеге асырудың көптеген нұсқалары бар. Бұл әдістер зиянкестерге үлкен әрекет алаңын ұсынады.

Киберқауіпсіздік саласында құпия деректер мен желілерді қорғау көбінесе брандмауэр, шифрлау және антивирустық бағдарламалық қамтамасыз ету сияқты техникалық қорғанысқа бағытталған. Дегенмен, ұйымдық қауіпсіздікке төнетін ең кең таралған және қауіпті қатерлердің бірі бағдарламалық жасақтаманың осал тұстарын пайдаланатын хакерлерден емес, қызметкерлерді әлеуметтік инженерия арқылы манипуляциялайтын жеке тұлғалардан туындайды. Бұл психологиялық манипуляция адамдарды құпия ақпаратты ашуға, рұқсат етілмеген қол жеткізуге немесе қауіпсіздікке нұқсан келтіретін әрекеттерді орындауға алдауға бағытталған. Әлеуметтік инженерия тәуекелін тиімді азайту үшін қызметкерлерді қорғау және оқыту әдістері маңызды болып табылады.

Қызметкерлер әлеуметтік инженериядан қорғаныстың бірінші желісі ретінде осы шабуылдарды тану және оларға қарсы тұру үшін білім мен құралдармен қамтамасыз етілуі керек. Тиісті қорғаныс болмаса, ұйымдағы адамдар абайсызда шабуылдаушыларға құпия деректерге, жүйелерге немесе физикалық орындарға кіру мүмкіндігін бере алады. Әсері жойқын болуы мүмкін, соның ішінде қаржылық жоғалту, беделге нұқсан келтіру, заңды жауапкершіліктер және тұтынушы сенімінің жоғалуы.

Ұйымдар технологиялық қауіпсіздік шаралары маңызды болғанымен, компания активтерін қамтамасыз етуде адам элементі маңызды рөл атқаратынын мойындауы керек. Қызметкерлерді хабардар ету және қорғау стратегияларына инвестициялау арқылы бизнес әлеуметтік инженерлік шабуылдарға осалдығын айтарлықтай төмендете алады [2].

Әлеуметтік инженериямен күресудің негізгі оқыту әдістері:

1. Фишинг модельдеулері және хабардар ету науқандары

Қызметкерлерді фишингтік шабуылдар арқылы жүйелі түрде тестілеу оларға әдеттен тыс жіберушінің мекенжайлары, күдікті сілтемелер немесе жеке ақпаратқа арналған шұғыл сұраулар сияқты фишингтік электрондық хабарлардың жасырын белгілерін тануға көмектеседі. Бұл жаттығулар қызметкерлерге қырағылық танытуға және киберқылмыскерлердің мінез-құлқын манипуляциялау үшін қолданатын әдістерді түсінуге көмектеседі. Ақпараттық науқандар қажетсіз электрондық пошталарға, телефон

қоңырауларына немесе хабарламаларға деген дұрыс күмәнділікке ықпал етуі керек.

2. Қауіпсіздік саласындағы үздік тәжірибелер бойынша тренинг

Қызметкерлер құпия ақпаратты өңдеу кезінде ең жақсы тәжірибелерді қалай қолдану керектігін үйретуі керек. Бұған күшті құпия сөздерді орнату, ақпаратқа күдікті сұрауларды тану және құпия құжаттарды қауіпсіз жою бойынша нұсқаулар кіреді. Оқыту сонымен қатар құпия деректер мен жүйелерге қол жеткізуге арналған сұрауларды қалай өңдеу керектігін және сұраушының заңдылығын әрқашан тексеруді қамтуы керек, әсіресе олар сыртқы немесе бейтаныс болса.

3. Рөлдік оқыту

Ұйымдағы әртүрлі рөлдер әртүрлі әлеуметтік инженерлік шабуылдарға тап болуы мүмкін. Мысалы, басшылар мен жоғары деңгейлі қызметкерлер жиі фишингтік шабуылдарға ұшырайды, ал тұтынушыларға қызмет көрсететін қызметкерлер сылтауларға көбірек бейім болуы мүмкін. Оқытуды нақты жұмыс функцияларына бейімдеу қызметкерлердің ең ықтимал әлеуметтік инженерлік шабуыл түрлеріне дайын болуын қамтамасыз етеді.

4. Қауіпсіздік – бірінші мәдениетті құру

Проактивті қауіпсіздік мәдениеті әлеуметтік инженерлік шабуылдардың сәттілігін айтарлықтай төмендетуі мүмкін. Қызметкерлерді күдікті әрекеттер туралы дереу және кек алудан қорықпай хабарлауға шақырыңыз. Қызметкерлерге ықтимал қауіпсіздік тәуекелдері туралы алаңдаушылық білдіру үшін қауіпсіз орта жасау пайда болатын қауіптерге тезірек жауап беруді қамтамасыз етеді.

5.Үнемі біліктілікті арттыру курстары

Әлеуметтік инженерия тактикасының ландшафты үнемі дамып отырады. Шабуылшылар өз техникаларын үнемі жетілдіріп отырады, сондықтан қызметкерлерді оқыту бір реттік оқиға болмауы керек. Қызметкерлердің соңғы қауіптермен және олармен күресу жолымен жаңартылғанын қамтамасыз ету үшін біліктілікті арттыру курстары мерзімді түрде өткізілуі керек.

6. Симуляцияланған әлеуметтік инженерия сценарийлері

Қызметкерлер имитацияланған әлеуметтік инженерлік шабуылдарға жауап беруі керек болатын тікелей сценарийлерді іске қосу (жеке немесе онлайн болсын) қызметкерлерге жылдам шешім қабылдауға және үйренгендерін бекітуге көмектеседі. Бұл қызметкерлерге басқарылатын ортада нақты жағдайдың қысымын сезінуге мүмкіндік береді, бұл оларға нақты қауіпке тап болған кезде тиімді әрекет ету жолын жақсырақ түсінуге мүмкіндік береді.

7. Көп факторлы аутентификацияны (КФА) пайдалануды ынталандыру

Оқытумен тікелей байланысты болмаса да, көп факторлы аутентификацияны (КФА) енгізу әлеуметтік инженерлік шабуылдарының әсерін айтарлықтай төмендетеді. Тіпті шабуылдаушылар қызметкердің желіге кіру, тіркеу деректерін сәтті алса да, CIM қамтамасыз ететін қауіпсіздіктің қосымша деңгейі, рұқсатсыз кіруді қиындатады.

Оқытудың тиімділігін өлшеу

Оқыту үрдісін қамтамасыз ету жақсы нәтижеге жеткізуге жеткіліксіз - ұйымдар қауіпсіздік туралы хабардар ету бағдарламаларының тиімділігін үнемі бақылап отыруы қажет. Сәтті фишингтік модельдеу жылдамдығы, хабарланған қауіпсіздік оқиғаларының саны және қызметкерлердің кері байланысы сияқты көрсеткіштер оқу әрекеттерінің сәттілігі туралы құнды түсініктерді бере алады. Оған қоса, қауіпсіздіктің нақты бұзылуының немесе әлеуметтік инженерлік шабуылдардың әрекет ету үрдістерін қадағалау оқу процесінде жақсарту аймақтарын анықтауға көмектеседі [3].

Сондай-ақ, әлеуметтік инженерия әдістері классикалық бұзу әдістерінен айырмашылығы ескірмейді. Қорғаныс саласында да, шабуылда да жаңа трендтер мен жаңалықтарды үнемі бақылап отыру қажет, өйткені олар арқылы қажетті әрекеттерді жүзеге асыруға болады.

Дегенмен, барлық әлеуметтік инженерлер алаяқтар емес. Олар бәсекелестердің шабуылы немесе қара пиардан кейін компанияның беделін қалпына келтіруге көмектесуі мүмкін. Мысалы, психологиялық әдістер, анонимді пікір қалдырушының деректерін алып, оны қажетсіз пікірлер мен жалған ақпаратты жоюға итермелеу үшін қолданылады.

Әлеуметтік инженерлер форумдарға тіркеліп, теріс пікірдегі аудиториямен диалог жүргізеді және нейролингвистикалық прогрраммалау техникаларын қолданып, олардың пікіріне әсер етеді.

Қауіптің алдын алу тәсілдерін анықтау үшін, киберқылмыскерлер не істей алатынын және оны қалай жүзеге асыратынын түсіну қажет [4].

Біріншіден, адаммен хат алмасу арқылы сенімге кіріп, болашақ шабуылдарға қажет болатын ақпаратты білуге болады. Мысалы, басқа қызметкерлердің телефон нөмірлері мен электрондық пошталары, желінің конфигурациясы, қорғаныс құралдарының нұсқалары сияқты мәліметтер.

Екіншіден, күдік тудырмайтын «жұмыс кестесі», «шот бойынша қарыз», «жұмыстан босату» сияқты зиянды файлды ашқан кезде, компьютерге жұқпалы файл орнатылады. Нәтижесінде қылмыскер жүйеге қол жеткізе алады.

Тағы бір шабуыл әдісі – «кері әлеуметтік инженерия». Мұндай шабуылдың мысалы ретінде қорғалатын аймаққа тазалаушы ретінде кіруді айтуға болады. Сіз қабырғадағы техникалық қолдау нөмірін өзіңіздің нөміріңізге ауыстырасыз, содан кейін кішігірім ақау жасайсыз. Бір күннен кейін, көңілсіз пайдаланушы сізге қоңырау шалып, өз білімін «білікті маманмен» бөлісуге дайын болады. Авторизацияңыз күдік тудырмайды, өйткені адам кімге және не үшін хабарласқанын біледі.

Әлеуметтік инженерия салдарынан құпия ақпараттың таралу ықтималдығын азайту үшін келесі ережелерді сақтау қажет:

- Ақпараттық қауіпсіздік мамандары орындалатын, жүйелік және басқа да файлдарға арналған кеңейтімдері бар файлдарды жіберуге тыйым салуы қажет. Сондай-ақ, компьютерлік сауаттылықты арттыру мақсатында персоналмен нұсқаулықтар өткізілуі керек.
- Хатқа қосымша немесе сілтеме келген жағдайда, жіберушінің мекенжайын, хаттың кеңейтімін мұқият тексеріп, файлды антивирустық бағдарламалық қамтамасыз ету арқылы сканерлеу қажет.
- Қылмыскермен байланысқа түспеу маңызды, себебі ол әңгіме барысында келесі құрбанына шабуыл жасау үшін қажетті ақпаратты алуы мүмкін.

Әлеуметтік инженерия бүгінгі күні ұйымдардың алдында тұрған ең жасырын қауіпсіздік қатерлерінің бірі болып қала береді. Ол адам психологиясын пайдалана отырып, оны тіпті ең озық техникалық қорғаныс құралдарының алдын алуға тырысатын шабуыл векторына айналдырады. Күшті, қызметкерлерді қорғау және оқыту бағдарламаларына инвестициялау арқылы, ұйымдар әлеуметтік инженерлік шабуылдарды танитын және оларға қарсы тұруға жақсырақ дайындалған, қауіпсіздікті білетін, жұмыс күшін құра алады. Қызметкерлер киберқылмыскерлер қолданатын тактиканы түсінгенде және оларға тиімді әрекет ету құралдары берілгенде, олар осы дамып келе жатқан қауіптерден ұйымның бірінші және ең тиімді қорғаныс желісі болады [5].

Жұмыс қорытындысы бойынша, әлеуметтік инженерия көмегімен жасалатын шабуылдардың негізгі әдістері ұсынылды. Сонымен қатар, осы типтегі шабуылдардың алдын алу үшін негізгі принциптер тұжырымдалды, және сол принциптер негізінде персоналды дайындау қажет.

Қолданылған әдебиеттер тізімі

1. Әлеуметтік инженерия және әлеуметтік хакерлер / М.В. Кузнецов, И.В. Симдянов. СПб.: БХВ-Петербург, 2007.

2. Positive research. Практикалық қауіпсіздік бойынша зерттеулер жинағы. [Электрондық ресурс]. Қол жеткізу режимі: https://www.ptsecurity.com/upload/ptru/analytics/Positive-Research-2017-rus.pdf/

3. Алдау өнері / Кевин Митник, Уильям Саймон. М.: ВМиК МГУ баспа бөлімі. МАКС Пресс баспасы, 2018.

4. Whitman, M. E., & Mattord, H. J. (2020). *Principles of Information Security* (6th ed.). Cengage Learning.

5. Symantec Corporation**. (2020). *2019 Internet Security Threat Report*. Symantec.

- A detailed annual report that highlights trends in cybersecurity threats, including social engineering. It provides real-world case studies and advice on securing employees from these types of attacks. [Link: https://www.broadcom.com/company/newsroom/press-releases?filtr=internet-security-threat-report]

УДК: 004.056.5

WEBSOCKET ПРОТОКОЛЫНДАҒЫ ОСАЛДЫҚТАРДЫ ТАЛДАУ

Магзумов Алихан Маратұлы
alihan.magzumov@mail.ru
Л.Н.Гумилев атындағы ақпараттық қауіпсіздік факультетінің магистрантты
Ғылыми жетекші – Ж.Сауханова

Аннотация: Бұл мақалада WebSocket протоколының осалдықтарын зерттеу және талдау әдістері қарастырылады. Нақты шабуыл мысалдары негізінде WebSocket байланыстарының қауіпсіздік мәселелері талданып, олардың ақпараттық жүйелерге ықтимал әсері бағаланады. Сондай-ақ осалдықтарды пайдаланудың негізгі әдістері мен оларды анықтау жолдары көрсетіледі. WebSocket байланыстарын қорғау және шабуылдардың алдын алу бойынша ұсыныстар беріледі. Мақала ақпараттық қауіпсіздік саласындағы мамандарға, зерттеушілерге және веб-қосымшалар әзірлеушілеріне арналған.

Кілт сөздер: Веб-қосымша, Интернет-ресурс, Websocket, қауіпсіздік, осалдық, ақпарат жинау.

Ақпараттық қауіпсіздіктегі осалдық - шабуылдаушылар қолдана алатын ақпараттық активтің немесе бақылау мен басқарудың әлсіз жақтары. Ақпараттық қауіпсіздіктің осалдықтарының жіктелуі өте көп. Соның ішінде веб-қосымшалардағы Websocket осалдықты ескерген жөн. Өйткені бұл қосымшаның және онымен байланысты деректердің құпиялылығына, тұтастығына және қол жетімділігіне нұқсан келтіруі мүмкін қауіпсіздік қатерлері мен шабуылдарына жол береді.

WebSocket осалдықтарын және олардың веб-қосымшалар үшін салдарын зерттеу әдістемесі теориялық талдауды және қауіпсіздік әдістерін әзірлеуді біріктіретін кешенді тәсілді қамтиды.

WebSocket – бұл екі жақты нақты уақыттағы деректер алмасуды қамтамасыз ететін хаттама. Ол веб-қосымшалардағы жылдамдық пен тиімділікті арттырады, бірақ сонымен бірге жаңа қауіпсіздік қатерлерін де тудырады. WebSocket хаттамасының ерекшелігі – тұрақты қосылым орнату арқылы сервер мен клиент арасында үздіксіз байланыс жасауында. Бұл механизм дәстүрлі HTTP сұраныс-жауап үлгісінен ерекшеленеді және дұрыс қорғалмаған жағдайда осалдықтарға жол ашады.