

Александр Дмитриевич Золотов – к.т.н., ассоциированный профессор кафедры «IT технологий»; Университет имени Шакарима города Семей, Республика Казахстан; e-mail: azol64@mail.ru.

Александр Игоревич Дворцевой – доцент кафедры тепловых электрических станций Новосибирского государственного технического университета.

Динара Ошановна Кожаметова – PhD, декан «Высшая школа искусственного интеллекта и строительства»; Университет имени Шакарима города Семей, Республика Казахстан; e-mail: dinara_kozhahmetova@mail.ru.

Авторлар туралы мәліметтер

Тұрсынхан Саятұлы Жылқыбаев* – техника ғылымдарының магистрі, «IT-технология» кафедрасының оқытушысы; Семей қаласының Шәкәрім атындағы университеті, Қазақстан Республикасы; e-mail: zhitosya@mail.ru. ORCID: <https://orcid.org/0000-0002-8918-527X>.

Айдана Дарханқызы Мендебаяева – техника ғылымдарының магистрі, Қазақстан Республикасы «Astana IT University» ЖШС деканатының маманы; e-mail: aid0904@mail.ru.

Александр Дмитриевич Золотов – т.ғ.к., «IT технология» кафедрасының қауымдастырылған профессоры; Семей қаласының Шәкәрім атындағы университеті, Қазақстан Республикасы; e-mail: azol64@mail.ru.

Александр Игоревич Дворцевой – Новосибир мемлекеттік техникалық университетінің жылу электр станциялары кафедрасының доценті.

Динара Ошановна Кожаметова – PhD, «Жасанды интеллект және құрылыс жоғары мектебі» декані; Семей қаласының Шәкәрім атындағы университеті, Қазақстан Республикасы; e-mail: dinara_kozhahmetova@mail.ru.

Information about the authors

Tursynkhan Zhylykybayev* – Master of Technical Sciences, lecturer of the Department «IT technologies»; Shakarim University of Semey, Republic of Kazakhstan; e-mail: zhitosya@mail.ru. ORCID: <https://orcid.org/0000-0002-8918-527X>.

Aidana Mendebayeva – Master of Technical Sciences, lecturer of the Department «Automatization, Information Technology and Urban Planning»; Shakarim University of Semey, Republic of Kazakhstan; e-mail: aid0904@mail.ru.

Alexandr Zolotov – Candidate of technical sciences, associate Professor of the Department «IT Technologies»; Shakarim University of Semey, Republic of Kazakhstan; e-mail: azol64@mail.ru.

Alexander Dvortsevov – Docent of Thermal Power Plants Department, Novosibirsk State Technical University.

Dinara Kozhakhmetova – PhD, dean of the «Graduate school artificial intelligence and construction»; Shakarim University of Semey, Republic of Kazakhstan; e-mail: dinara_kozhahmetova@mail.ru.

Received 29.08.2024

Revised 18.09.2024

Accepted 19.09.2024

[https://doi.org/10.53360/2788-7995-2024-4\(16\)-2](https://doi.org/10.53360/2788-7995-2024-4(16)-2)

FTAXP: 81.93.29



А.О. Закенова*, Ж.М. Алимжанова

Әл-Фараби атындағы Қазақ ұлттық университеті,
050040, Қазақстан Республикасы, Алматы қаласы, Әл-Фараби даңғылы, 71
*e-mail: zakenova99@list.ru

ВЕБ-КАМЕРАЛАРДЫҢ ЖАСЫРЫН БҰЗЫЛУЫН БОЛДЫРМАУДЫҢ ТИІМДІ ӘДІСТЕРІ

Андатпа: Бұл мақалада веб-камералардың азаматтық және мемлекеттік секторларға жасырын кіруін болдырмаудың тиімді әдістері қарастырылады. Сонымен қатар, веб-камералардың қауіпсіздік мәселелері туралы ақпаратты арттыруға бағыттталып, веб-камераларға бірнеше танымал шабуылдар, сондай-ақ азаматтық және үкіметтік секторларда-ғы веб-камералардың жасырын бұзылуына байланысты жоғары дәрежелі жағдайлар талқыланды. Веб-камераны бұзу-бұл пайдаланушылардың жеке өмірі мен қауіпсіздігін бұзу. Бұл мақала веб-камераны бұзудың себептері мен салдарын, сондай-ақ олардың зардап шегушілермен мен жалпы қоғамға әсерін талқылайды.

Веб-камераны бұзудың себептеріне хакерлерді ынталандыру, жеке ақпаратқа қол жеткізуге деген ұмтылыс, тыңшылық немесе тіпті қорқыту мен бопсалау жатады. Бұл шабуылдар қаржылық пайдаға, құпиялылықты бұзуға немесе жай ғана көңіл көтеруге байланысты болуы мүмкін.

Мақалада осалдықтарды пайдалану, фишингтік шабуылдар, зиянды бағдарлама және қашықтан қол жеткізу құралдарын қоса алғанда, шабуылдаушылар веб-камераларды бұзу үшін қолданатын әртүрлі әдістерді қарастырады.

Веб-камераны бұзудың салдары жойқын болуы мүмкін. Жәбірленушілер жеке өмірін жоғалтуға, құпиялылықты бұзуға, сондай-ақ олардың беделіне нұқсан келтіруге тап болады. Бұл сонымен қатар стресс пен мазасыздық сияқты психологиялық және эмоционалдық мәселелерге әкелуі мүмкін.

Веб-камераны бұзудың қоғамға әсері киберқауіпсіздік және жеке құрылғылар мен деректерді қорғауды күшейту қажеттілігі туралы сұрақтар туғызады. Бұл сонымен қатар пайдаланушыларға желідегі қауіпсіздік ережелері мен күшті парольдерді пайдалану туралы білім берудің маңыздылығын көрсетеді.

Түйін сөздер: веб-камера қауіпсіздігі, RAT, Clickjacking, азаматтық сектор, үкіметтік сектор.

Кіріспе

Қазіргі әлемде веб-камералар біздің күнделікті өміріміздің бір бөлігіне айналды. Олар азаматтық және үкіметтік аймақта бейнеконференциялар, онлайн хабарлар, бейнебақылау және басқа да көптеген мақсаттарда қолданылады. Дегенмен, веб-камераның кең таралуымен бірге олардың жасырын бұзылу қаупі артуда.

Зиянкестер веб-камераларға рұқсатсыз кіруге және тіпті оларды нақты ақпарат жинау үшін пайдалануға тырысуда, барған сайын тапқыр және шебер бола бастады. Жасырын веб-камераны бұзу ауыр зардаптарға әкелуі мүмкін, соның ішінде құпиялылықты бұзу, жеке басын ұрлау және бопсалау.

Веб-камера осалдығы – шабуылдаушыларға веб-камераға рұқсатсыз кіруге және оны иесінің келісімінсіз пайдалануға мүмкіндік беретін жүйенің, бағдарламалық құралдың немесе құрылғының әлсіздігі немесе кемшілігі.

Бұл веб-камераның қалаусыз іске қосылуына, пайдаланушының хабарынсыз суреттер мен бейнелердің жазылуына және басқа да құпиялылық пен қауіпсіздіктің бұзылуына әкелуі мүмкін.

Жасырын веб-камераны бұзу – бұл шабуылдаушы пайдаланушыны бақылау мақсатында компьютердің немесе басқа құрылғының веб-камерасына рұқсатсыз кіруге мүмкіндік беретін процесс [1].

Азаматтық және үкіметтік секторларда қолданылатын веб-камералар нақты талаптарға, ережелерге және оларды пайдалану мақсаттарына байланысты кейбір айырмашылықтарға ие. Осы секторларда қолданылатын веб-камералар арасындағы негізгі айырмашылықтарды 1-кестеден көре аламыз.

Маңызды фактор – бұл мәселе тек азаматтық сектормен ғана шектелмейді, ол құпия ақпаратты сақтайтын және шабуылдаушылар тарапынан нысанаға алынуы мүмкін мемлекеттік және мемлекеттік ұйымдарға да әсер етеді. Тиісінше, бұл зерттеу қоғамның барлық салаларында және веб-камералармен жұмыс істейтін ұйымдар үшін маңызды.

Материалдар мен тәсілдер

Киберқауіптердің армиясы барған сайын айлакер және бақыланбайтын шабуыл әдістерін көрсете отырып, жасырын веб-камера бұзудың алдын алу үшін осы салада зерттеу жүргізу өте маңызды.

Бұл зерттеу осалдықтарды анықтауға және пайдаланушылар мен ұйымдардың құқықтары мен құпиялылығын қорғау үшін веб-камера қауіпсіздігі бойынша ұсыныстар әзірлеуге бағытталған.

Кесте 1 – Азаматтық және үкіметтік секторларда қолданылатын веб-камералар айырмашылықтары

	Мақсаты	Қауіпсіздік және құпиялылық:	Сапа және сенімділік:
Азаматтық сектор	Жеке және коммерциялық мақсаттарда қолданылады. бейнеконференциялар, онлайн кездесулер, онлайн оқыту, тікелей эфир және бетпе-бет сөйлесу үшін қолданылады.	Жеке өмір мен қауіпсіздік азаматтық сектордағы маңызды аспектілер болып табылады, Пайдаланушылар веб-камера параметрлерін және құпиялылық мүмкіндіктерін басқара алады.	Веб-камералар сапасы мен функционалдығы жағынан әр түрлі. Олар жалпы пайдалануға арналған және әртүрлі бағамен қол жетімді.
Үкіметтік сектор	Қауіпсіздікті бақылау, Көпшілік жиналыстар мен тыңдаулар, мемлекеттік органдармен байланыс, қашықтан жұмыс істеу және ресми үкіметтік іс-шараларға арналған телеконференциялар сияқты әртүрлі мақсаттарда қолданылады.	Мемлекеттік органдар көбінесе қауіпсіздік пен құпиялылыққа қатаң талаптар қояды. Мемлекеттік мақсатта пайдаланылатын Веб-камералар құпия ақпаратты қорғауды қамтамасыз ететін және рұқсатсыз кіруге жол бермейтін ережелерге бағынуы мүмкін.	М органдарға олардың коммуникацияларының сенімділігі мен қауіпсіздігін қамтамасыз ету үшін шифрлау сияқты жетілдірілген мүмкіндіктері бар жоғары сапалы веб-камералар қажет. Бұл веб-камералар белгілі бір стандарттар мен сертификаттарға сәйкес.

Веб-камераларды бұзу әдістері олардың қалай қолданылатынына және шабуылдаушылар қандай осалдықтарды пайдалана алатынына байланысты әртүрлі болуы мүмкін. Міне, веб-камераны бұзудың негізгі 3 әдіске бөліп қарастырайық:

- Зиянды бағдарламалар және қашықтан қол жеткізу құралдары

Хакерлер жәбірленушінің веб-камерасын бақылау үшін зиянды бағдарламалар мен қашықтан қол жеткізу құралдарын жиі пайдаланады. Зиянды бағдарламалық жасақтаманы заңды қосымшалар немесе тіркемелер ретінде жасыруға болады, сондықтан интернеттен файлдарды жүктеу кезінде абай болу керек.

- Фишингтік шабуылдар

Фишинг хакерлердің веб-камераларға кіруінің кең таралған әдісі болып қала береді. Пайдаланушыларды зиянды сілтемелер арқылы өтуге немесе жеке ақпарат беруге алдау арқылы хакерлер құрылғыларды бұзып, рұқсатсыз кіре алады.

- Осалдықтарды пайдалану

Ескірген бағдарламалық жасақтама және қауіпсіздік осалдықтары хакерлер үшін кіру нүктесі бола алады. Олар пайдаланушының веб-камерасын және басқа да құпия ақпаратты бақылау үшін осы әлсіз жерлерді пайдаланады. Бағдарламалық жасақтаманы үнемі жаңартып отыру және күшті парольдерді пайдалану бұл тәуекелдерді азайтады.

Сонымен қатар Thermax көмегімен камераны бұзу тәсіліне тоқталсақ:

Алғашқы сипатталатын қашықтықтан басқару құралын пайдаланып жүйедегі трояндық ат шабуылы. Қашықтан басқару құралы (RAT) – әдетте пайдаланушыны білмей компьютерді жасырын бақылау үшін қолданылатын бағдарлама. RAT пайдаланушы енгізген әрбір пернені басуды түсіре алады, сонымен қатар хосттың веб-камерасына кірген кезде бейнені жасырын түрде жаза алады. RATs ноутбукты бақылауда және ұрыны жасырын суретке түсіру арқылы ұрлықтан қалпына келтіруде маңызды рөл атқаруы мүмкін болса да, RAT-ті шабуылдаушы жәбірленушінің суреттері мен бейнежазбаларын білмей түсіру үшін де пайдалана алады. Пайдаланушылар RAT-ты өз компьютеріне білмей әр түрлі тәсілдермен орната алады: вирус жұққан қосымшаны ашып, жүктеу сілтемесіне өту арқылы, берілген рұқсаттары бар жаңа құралдар тақтасын орнатып, т.б. RAT орнатылғаннан кейін, шабуылдаушы хосттың веб-камера бағдарламалық жасақтамасына оңай қол жеткізе алады және кез-келген уақытта веб-камераны қосады [3].

Келесі веб-камера арқылы Adobe Flash ортасындағы Clickjacking көмегімен жасалатын шабуыл түріне келетін болсақ, Clickjacking – бұл пайдаланушының веб-сеансын түсіру үшін frames қолданылатын зиянды әдіс. Clickjacking шабуылдаушыға жәбірленушінің зиянсыз

шертулерін ұстап алуға және оларды JavaScript көмегімен немесе JavaScript көмегін пайдаланбай-ақ ішкі кадрлар болып табылатын мақсатты веб-беттерге жіберуге мүмкіндік береді [4].

Құрылғының камерасы бұзылса не болуы мүмкін?

Рұқсат етілмеген бақылау. Камераға кірген шабуылдаушы оны сізді немесе айналаңызды бақылау үшін пайдалана алады. Ол сіздің жеке немесе іскери әңгімелеріңізді жаза алады, интернет-банкингті пайдалануды немесе жеке деректерді енгізуді жаза алады. Бұл сіздің жеке өміріңізді бұзады және сезімтал ақпараттың ағып кетуіне, қаржылық шығындарға және басқа да жағымсыз салдарға әкелуі мүмкін. Егер шабуылдаушылар бұзылған камерамен түсірілген айыптау материалдарын ала алса, оларды бопсалау үшін қолдана алады. Ешбір жағдайда қауіп-қатерге бой алдырмаңыз және зиянкестердің талаптарын орындамаңыз. Оның орнына құқық қорғау органдарына жүгіну керек [5].

Нәтижелер

Веб-камераны бұзудың қиындықтары мен сипаттамалары назар аударуға және талдауға тұрарлық бірқатар маңызды аспектілерді қамтиды. Олардың кейбірін толығырақ қарастырайық:

- Құпиялылықты бұзу: негізгі мәселелердің бірі-пайдаланушылардың жеке өмірін бұзу. Веб-камераны бұзу шабуылдаушыларға адамның жеке кеңістігіне қол сұғуға, оны орынсыз сәттерде бақылауға және оның келісімінсіз бейне жазуға мүмкіндік береді.
- Тыңшылық және барлау: веб-камераларды тыңшылық және барлау үшін пайдалануға болады. Зиянкестер құнды ақпарат жинау арқылы белгілі бір адамдардың, ұйымдардың немесе мекемелердің қызметін бақылау мақсатында веб-камераларға қол жеткізе алады.
- Қауіпсіздікті бұзу: веб-камераны бұзу пайдаланушының компьютеріне немесе желісіне ауыр шабуылдардың алғашқы қадамы болуы мүмкін. Зиянкестер жүйеге кеңірек кіру үшін веб-камераға кіруді пайдалана алады.
- Техникалық аспектілер: веб-камераны бұзу әртүрлі тәсілдермен жүзеге асырылуы мүмкін, соның ішінде зиянды бағдарламаларды (малвари) пайдалану, бағдарламалық жасақтаманың осалдығы, желілік трафикті ұстап қалу және басқа да техникалық әдістер..
- Заңнама және жаза: веб-камераны бұзудың құқықтық аспектілері де маңызды. Құқық бұзушылар, егер олардың әрекеттері киберқауіпсіздік және жеке өмір туралы заңдарды бұзса, қылмыстық жауапкершілікке тартылуы мүмкін [6].

Осы сипаттамалар мен мәселелерді зерттеу және түсіну веб-камералардың бұзылуын болдырмаудың және пайдаланушылардың жеке өмірін қорғаудың тиімді стратегияларын әзірлеу үшін маңызды.

Мұндай шабуылдардан қорғау үшін негізгі қауіпсіздік шараларын сақтау маңызды, мысалы:

- Осалдықтарды жою үшін операциялық жүйені және бағдарламалық құралды үнемі жаңартып отырыңыз.
- Зиянды бағдарламаны анықтау және блоктау үшін антивирустық бағдарламалық құрал мен брандмауэрді пайдаланыңыз.
- Электрондық хаттардағы тіркемелерді ашқанда және сенімсіз көздерден файлдарды жүктеп алған кезде абай болыңыз.
- Веб-камера жұмысын үздіксіз бақылаңыз және қажет болса, оны пайдаланбаған кезде физикалық немесе бағдарламалық түрде өшіріңіз.
- Интернетке қосылған құрылғылардың стандартты құпия сөздері мен логиндерін өзгертуді және күшті және бірегей құпия сөздерді пайдалануды ұмытпаңыз [7].

Осы шараларды орындау сіздің жасырын веб-камераңызды бұзу қаупін азайтады.

Ноутбуктің Веб-камераларын зиянды бағдарламалар мен құқық қорғау органдары жасырын түрде іске қоса алады. Сол себепті, американдықтардың 59% пайызы қадағалауды болдырмау үшін веб-камераларды қолмен жабуды жөн көреді. Дегенмен, қолмен жасалған мұқабалар адам қателіктеріне бейім – себебі 200 пайдаланушыдан сұхбат алғаннан кейін, олардың 61,5%-ы кейде веб-камераны қолданғаннан кейін мұқабаны қайта жабуды ұмытып кететіні анықталған. Байқағандарыңыздай шабуылдардан қорғануда қауіпсіздікке толық кепілдікті ешқандай жолмен сақтай алмаймыз сол себептен мүмкіндігі жоғары деген

антивирустық бағдарламаларды орнатып жаңартып отыру ең тиімді жолы болып есептеледі [8].

Талқылау

Компьютерлік технологиялар адам өмірінің барлық салаларында кеңінен қолданылады.

Біз үшін антивирустық бағдарламалар арқылы қорғану ыңғайлы. Ең жақсы антивирустық бағдарламаны 2 – кесте арқылы анықтап көрейін. Бұл, ең алдымен, кез-келген мекеменің жұмысын оңтайландыруға және шығындарды азайтуға мүмкіндік береді [9].

Кесте 2 – Веб-камера қорғауға арналған антивирустық бағдарламалардың техникалық сипаттамалар

Аты	ESET Internet Security	Bitdefender	ShieldApps Webcam Blocker	Avast Antivirus
Веб-сайттың мекен-жайы	https://www.spysheiter.com/	https://a.pr-cy.ru/www.bitdefender.com/	https://shieldapps.com/products/shieldapps-webcam-blocker/	https://www.avira.com/ru
Веб-сайтты жүктеу жылдамдығы	0.15 сек – тексерілген сайттардың 93%-дан жылдамырақ.	1.75 сек – тексерілген сайттардың 16%-дан жылдамырақ.	1.36 сек – быстрее чем 22% проверенных сайтов.	0.41 сек – тексерілген сайттардың 74%-дан жылдамырақ.
Домен жасы	?	-	12 жыл	-
Технологиялар	Google Analytics Google Tag Manager	Adobe Experience Manager CloudFlare Facebook Google Analytics Google Tag Manager jQuery Java	AdRoll Apache Facebook Google Analytics Google Font API Google Tag Manager TweenMax jQuery Twitter Bootstrap WordPress WordPress PHP	Google Analytics Google Tag Manager
SSL-сертификат	Сайт https арқылы қол жетімді. Сертификат 05.01.2022 дейін жарамды.	Сайт https арқылы қол жетімді. Сертификат 24.11.2021 дейін жарамды.	Сайт https арқылы қол жетімді. Сертификат 18.01.2023 дейін жарамды	Сайт https арқылы қол жетімді. Сертификат 21.06.2023 дейін жарамды.
Доменнің аяқталуы	-	-	Домен 13.02.2023 дейін ұзартылды	-
Сервер орны	Америка Құрама Штаттары	Америка Құрама Штаттары	Канада	Нидерланды
HTML бетінің өлшемі	12 КБ	15КБ	14КБ	33КБ
Веб-сайтты бағалау	84,09/100	83,72/100	84,78/100	93,33/100
Сыни қателер	191 қате	3 қате.	53 қате.	179 қате.
Ескертулер	5 ескерту табылды.	4 ескерту табылды	21 ескерту табылды	20 ескерту табылды

2 – кесте бойынша анализ нәтижесінде веб-камера қорғауға арналған антивирустық бағдарламалардың ішінен техникалық сипаттамаларына қарай отыра ен тиімді ESET Internet Security антивирустық бағдарламасы болды. Басқа антивирустық бағдарламалардан артықшылығы: Көп деңгейлі қорғаныс:

- Бағдарлама бірнеше деңгейде қорғауды қамтамасыз етеді, соның ішінде антивирустық қорғау, фишингтік шабуылдардан қорғау, зиянды бағдарламалардан қорғау

және онлайн қауіптерден қорғау. Бұл қауіптердің кең ауқымын анықтауға және блоктауға мүмкіндік береді.

- Жетілдірілген нақты уақыттағы қорғау: ESET Internet Security бағдарламасы қауіптерді олар пайда болған кезде бірден анықтау және блоктау үшін құрылғыны және желі әрекетін бақылайтын нақты уақыттағы қорғауды ұсынады.

- Вирусқа қарсы және шпиондық бағдарламаға қарсы мүмкіндіктер: Бағдарлама тек вирустардан қорғауды қамтамасыз етіп қоймайды, сонымен қатар шпиондық бағдарламаларды, трояндарды, руткиттерді және басқа зиянды бағдарламаларды анықтауға және жоюға қабілетті [10].

Қорытынды

Қорытындылай келе, веб-камераларды жасырын бұзу – бұл соңғы уақытта көптеген тақырыптарға ене бастаған құбылыс, өйткені веб-камера мүмкіндіктерін жеке зиянкестер де, мемлекеттік органдар да қолданады. Киберқауіпсіздік әлеміндегі маңызды тұрақтылардың бірі-шабуылдаушылардың мотивациясының әртүрлілігі. Оларға ақша табуға деген ұмтылыс, интрига, билікке деген құштарлық немесе тіпті ойын-сауық себеп болуы мүмкін. Мотивтердің бұл әртүрлілігі веб-камераны бұзу мәселесін күрделі және жан-жақты етеді. Нәтижесінде жеке тұлғалар да, ұйымдар да өздерінің веб-камералары мен жеке ақпараттарын қорғау үшін шаралар қабылдауы керек.

Веб-камераларды бұзу ауыр зардаптарға әкеледі. Бұл құпиялылықтың бұзылуына, психологиялық және эмоционалдық мәселелерге, сондай-ақ ықтимал қаржылық шығындарға әкелуі мүмкін. Жәбірленушілер бопсалауға және беделін жоғалтуға тап болуы мүмкін. Сондықтан веб-камералардың бұзылуын болдырмау және құрылғыларды қорғау қаншалықты маңызды екенін атап өту маңызды.

Бұл тұрғыда, қорғаныс шаралары біздің киберқауіпсіздігіміздің ажырамас бөлігіне айналуға. Пайдаланушылар антивирустық бағдарламалық жасақтаманы пайдалануы, бағдарламаларды үнемі жаңартып отыруы, күшті парольдер жасауы және пайдаланылмаған кезде веб-камераларды жабу арқылы физикалық қауіпсіздікке назар аударуы керек. Сонымен қатар, пайдаланушыларға киберқауіпсіздік ережелері туралы білім беру веб-камераның бұзылуымен күресудің маңызды аспектісіне айналуға.

Әдебиеттер тізімі

1. Preventing Covert Webcam Hacking in the Civilian and Governmental Sectors / A. Sydney Jones et al // International Conference on Computational Science and Computational Intelligence (CSCI). – 2016. <https://doi.org/10.1109/CSCI.2016.0190>.
2. M. Asim Tech, Camera Hacking Using Termux. – 2022. <https://www.masimtech.com/2022/01/Camera-Hacking-Using-Termux.html>.
3. Kharb L. RAT: Remote Administrative Trojan / L. Kharb, S. Singh // Techniques To Avoid Webcam Hacking. Pallavi Suresh Poojary. – 2019. – P. 50-53.
4. Preventing Covert Webcam Hacking in the Civilian and Governmental Sectors / A.S. Jones et al // International Conference on Computational Science and Computational Intelligence (CSCI). – 2016. <https://doi.org/10.1109/CSCI.2016.0190>.
5. Adhikarla E. Face Mask Detection on Real / E. Adhikarla, B.D. Davison // Proceedings of the Conference on Information Technology for Social Good. – 2021. <https://doi.org/10.1145/3462203.3475903>.
6. Proceedings of the ACM on Interactive / Y. Do et al // Wearable and Ubiquitous Technologies/ – 2021. – № 154. – Vol. 5. – P. 1-21. <https://doi.org/10.1145/3494983>.
7. Fa Zh. Civilian Characteristics and Casualties Of Terrorist Attacks in Public Places / Zh. Fa, W. Song-Chun, S. Zhi-Hua // ICCMS '20: Proceedings of the 12th International Conference on Computer Modeling and Simulation. – 2020. – P. 109-114. <https://doi.org/10.1145/3408066.3408070>.
8. Wisiecka K. Comparison of Webcam and Remote Eye Tracking / K. Wisiecka, I. Krejtz, D. Sromek // ETRA '22: Symposium on Eye Tracking Research and Applications. – 2022. – № 32. – P. 1-7. <https://doi.org/10.1145/3517031.3529615>.
9. Adhikarla E. Face Mask Detection on Real-World Webcam Images / E. Adhikarla, B.D. Davison // Proceedings of the Conference on Information Technology for Social Good. – 2021. – P. 139-144. <https://doi.org/10.1145/3462203.3475903>.

10. Sowjanya P.L. Image Encryption Using Secure Force Algorithm With Affine Transform For Wsn / P.L. Sowjanya, K.S. Lorraine // Webology. – 2022. – Vol. 19, № 1. <http://www.webology.org>.

А.О. Закенова*, Ж.М. Алимжанова

Казахский национальный университет имени аль-Фараби,
050040, Республика Казахстан, Алматы, проспект аль-Фараби, 71

*e-mail: zakenova99@list.ru

ЭФФЕКТИВНЫЕ МЕТОДЫ ПРЕДОТВРАЩЕНИЯ СКРЫТОГО ВЗЛОМА ВЕБ-КАМЕР

В данной статье рассматриваются эффективные способы предотвращения проникновения веб-камер в гражданский и государственный сектор. Кроме того, в целях повышения осведомленности о проблемах безопасности веб-камер обсуждались несколько громких атак на веб-камеры, а также громкие случаи скрытого взлома веб-камер в гражданском и государственном секторах. Взлом веб-камеры является нарушением конфиденциальности и безопасности пользователей. В этой статье рассматриваются причины и последствия взлома веб-камер, а также их влияние на жертв и общество в целом.

Причинами взлома веб-камеры могут быть поощрение хакеров, желание получить доступ к личной информации, шпионаж или даже угрозы и шантаж. Эти атаки могут быть мотивированы финансовой выгодой, вторжением в частную жизнь или просто развлечением. В статье рассматриваются различные методы, используемые злоумышленниками для компрометации веб-камер, включая использование уязвимостей, фишинговые атаки, вредоносное ПО и инструменты удаленного доступа. Последствия взлома веб-камеры могут быть разрушительными. Жертвы сталкиваются с утратой частной жизни, нарушением конфиденциальности, а также возможным ущербом для их репутации. Это также может привести к психологическим и эмоциональным проблемам, таким как стресс и тревожность.

Влияние взломов веб-камер на общество поднимает вопросы о кибербезопасности и необходимости усиления защиты личных устройств и данных. Это также подчеркивает важность образования пользователей о правилах безопасности в сети и использовании надежных паролей.

Ключевые слова: безопасность веб-камеры, RAT, Clickjacking, гражданский сектор, правительственный сектор.

A.O. Zakenova*, Zh. Alimzhanova

Al-Farabi Kazakh National University,
050040, Republic of Kazakhstan, Almaty, Al-Farabi Avenue, 71

*e-mail: zakenova99@list.ru

EFFECTIVE WAYS TO PREVENT HIDDEN HACKING OF WEBCAMS

This article discusses effective ways to prevent the intrusion of webcams into the civil and public sectors. In addition, several high-profile attacks on webcams, as well as high-profile cases of covert breaches of webcams in the civilian and government sectors, were discussed in an effort to raise awareness of webcam security issues. Hacking a webcam is a violation of privacy and security of users. This article discusses the causes and consequences of webcam hacking, as well as their impact on victims and society at large.

Reasons for hacking a webcam include encouraging hackers, the desire to access personal information, espionage, or even threats and blackmail. These attacks may be motivated by financial gain, invasion of privacy, or simply for fun. The article examines the various methods attackers use to compromise webcams, including exploiting vulnerabilities, phishing attacks, malware, and remote access tools.

The consequences of hacking a webcam can be devastating. Victims face loss of privacy, violation of confidentiality, as well as possible damage to their reputation. It can also lead to psychological and emotional problems such as stress and anxiety.

The impact of webcam hacks on society raises questions about cybersecurity and the need to strengthen the protection of personal devices and data. It also highlights the importance of educating users about network security rules and the use of strong passwords.

Key words: web-cam security, RAT, Clickjacking, civil sector, government sector.

Авторлар туралы мәліметтер

Айжан Оразбекқызы Закенова* – «Ақпараттық жүйелер» кафедрасының магистранты; Өл-Фараби атындағы Қазақ ұлттық университеті; e-mail: zakenova99@list.ru

Жанна Муратбековна Алимжанова – физика – математика ғылымдарының кандидаты, профессор; Өл-Фараби атындағы Қазақ ұлттық университеті; e-mail: zhannamen@mail.ru

Сведения об авторах

Айжан Оразбеккызы Закенова* – магистрант кафедры «Информационные системы»; Казахский национальный университет имени аль-Фараби; e-mail: zakenova99@list.ru

Жанна Муратбековна Алимжанова – кандидат физико-математических наук, профессор; Казахский национальный университет имени аль-Фараби; e-mail: zhannamen@mail.ru

Information about the authors

Aizhan Orazbekkyzy Zakenova* – Master's student of the department of Information systems; Al-Farabi Kazakh National University; e-mail: zakenova99@list.ru

Zhanna Muratbekovna Alimzhanova – candidate of physics and mathematics, professor; Al-Farabi Kazakh National University; e-mail: zhannamen@mail.ru

Редакцияға енуі 24.04.2024

Өңдеуден кейін түсуі 07.10.2024

Жариялауға қабылданды 08.10.2024

[https://doi.org/10.53360/2788-7995-2024-4\(16\)-3](https://doi.org/10.53360/2788-7995-2024-4(16)-3)



FTAXP: 50.43.15

Д.О. Кожаметова*, А.Ж. Адылканова, Р.Н. Назаров

Семей қаласының Шәкәрім атындағы университеті,
071412, Қазақстан Республикасы, Семей қ., Глинка к-сі, 20 А

*e-mail: dinara_kozhahmetova@mail.ru

АЙҚЫН ЕМЕС ОРТАДА МҰНАЙДЫ ТЕРЕҢ ӨҢДЕУ ТЕХНОЛОГИЯЛЫҚ НЫСАННЫҢ ЖҰМЫС РЕЖИМДЕРІН ОПТИМИЗАЦИЯЛАУ

Андатпа: Мақалада қондырғы жұмысын басқаруды оптимизациялау үшін көпкритерийлік жағдайында модельдеу әдістері мен тәсілдері қарастырылды. Мұнайды терең өңдеу технологиялық кешендерінің тиімділігін математикалық модельдеу негізінде шешім қабылдау арқылы арттыру тәсілдері келтірілді. Мамандардан келіп түскен ақпаратты алып өңдеу әдісіні expertтік бағалау тәсілінің құрылымдық сұлбасы құрылып, зерттеу нысанына талдау жасалынды.

Айқын емес ортада технологиялық кешеннің математикалық сипатын жетілдіру кезінде, expertтер көрсеткішті көлемдік бағалай алмаған жағдайда, expertтік бағалау әдісін пайдалану мәселелері зерттелді. Лингвистикалық тәсіл негізінде, сапалы ақпарат көмегімен айқын емес ортада expertтік сауалнаманы ұйымдастырып жүргізуге мүмкіндік беретін expertтік бағалау әдісі қарастырылды.

Жинаған сапалы ақпарат және зерттеу нәтижелері негізінде реактордың математикалық моделі құрылып, құрылған модель негізінде технологиялық жүйенің тиімді жұмыс режимін таңдау үшін басқару тапсырмалары қалыптастырылды. Алынған expertтік ақпарат негізінде каталитикалық крекинг блогы реакторының кірістік параметр жұмысын сипаттайтын мәліметтер қоры ережесі құрылып лингвистикалық айнымалылары жасақталды.

Айқын емес ортада каталитикалық крекинг құрылғы қондырғысының технологиялық үрдісін басқару мысалында шешім қабылдаудың көпкритериалдық есебінің математикалық қойылымы алынды. Ұсынылып отырған, маман-expertтердің тәжірибесі мен білімі негізінде алынған алгоритм, шешім қабылдаушы тұлғаға процессті тиімді басқаруға және дұрыс жұмыс режимін таңдауға мүмкіндік береді.

Түйін сөздер: Айқын емес логика, expertтік бағалау, шешім қабылдау, оптимизациялау алгоритмі, математикалық модель, каталитикалық крекинг.

Кіріспе

Қазақстанның экономикалық дамуына мұнай өңдеу және мұнай химиялық үрдістері маңызды роль атқарады. Елімізде соңғы жылдары октан саны жоғары бензинге сұраныс