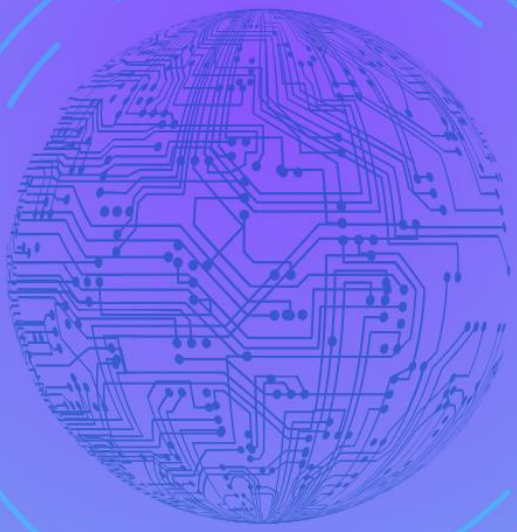
VOL 2 (18) 2025

JOURNAL OF SCIENCE AND RESEARCH



ASTANA

WWW.JSRJOURNAL.KZ

«Journal of Science and Research (JSR)»

зарегистрирован в Комитете информации Министерства информации и общественного развития Республики Казахстан
№ KZ41VPY00076697 от 01.09.2023 г.

Международный центр ISSN (ISSN-L): 3006-4325

Издается два раза в месяц.

ВЫПУСК № 2 (18), 2025 г.

Астана, 2025

www.jsrjournal.kz

СОДЕРЖАНИЕ

ОӘЖ 004

Шакенов Баглан Болатович
Ақпараттық технологиялар кафедрасының 2-курс магистранты,
Л.Н.Гумилев атындағы Еуразия ұлттық университеті
Қазақстан, Астана

ТЕЛЕКОММУНИКАЦИЯЛЫҚ ЖҮЙЕЛЕР КОНТЕКСТІНДЕ ЗАТТАР ИНТЕРНЕТІ (IOT) ҮШІН АҚПАРАТТЫҚ ҚАУІПСІЗДІК ҚАТЕРЛЕРІ МЕН ТӘУЕКЕЛДЕРІН БАҒАЛАУ

Аңдатпа: *Заттар интернеті (IoT) – қазіргі заманғы ақпараттық технологиялардың ең қарқынды дамып келе жатқан бағыттарының бірі. Бұл технология көптеген салаларда, соның ішінде өнеркәсіпте, денсаулық сақтауда, көлік және логистика жүйелерінде, сондай-ақ тұрмыстық құрылғыларда кеңінен қолданылады. Алайда, IoT экожүйесінің қарқынды дамуы көптеген жаңа ақпараттық қауіпсіздік қатерлерін тудырады. Мақалада телекоммуникациялық жүйелердегі Заттар интернетінің (IoT) қауіпсіздігіне байланысты негізгі қатерлер мен тәуекелдер қарастырылады. Ақылды құрылғылар мен желілік инфрақұрылымның осалдығы, деректердің рұқсатсыз қолжетімділігі, кибершабуылдардың жиілігі және стандарттардың жеткіліксіздігі талқыланады. Сонымен қатар, Mirai ботнеті сияқты нақты мысалдар негізінде IoT қауіпсіздігін бұзу сценарийлері қарастырылады.*

Кілт сөздер: *Заттар интернеті, ақпараттық қауіпсіздік, кибершабуылдар, IoT қатерлері, желілік қауіпсіздік.*

КІРІСПЕ

Ақылды құрылғылардың кең таралуы өнеркәсіп пен күнделікті өмірді түбегейлі өзгертуде, сондықтан Заттар интернетінің (IoT) ақпараттық қауіпсіздігіне байланысты қауіптер мен тәуекелдерді бағалау барған сайын маңызды бола түсуде. IoT – бұл датчиктермен, программалық жасақтамамен жабдықталған және желіге қосылу мүмкіндігі бар физикалық құрылғылардың кең желісі, бұл деректер алмасуға және әртүрлі қосымшаларды автоматтандыруға мүмкіндік береді. «Ақылды» үйлерден бастап өнеркәсіптік жүйелерге дейінгі салаларда қолданылатын бұл технологияның 2025 жылға қарай 55 миллиард құрылғыға жететіні болжануда. Сондықтан осы өзара байланысқан жүйелердің елеулі осалдықтарын ескере отырып, сенімді қауіпсіздік шараларын қабылдау бірінші кезектегі мәселе болып табылады.

Әсіресе, Заттар интернеті құрылғылары деректердің сыртқа таралуы, құрылғыларды басып алу және деректерді қауіпсіз сақтамау сияқты көптеген қауіпсіздік қатерлеріне тап болады. Мұндай қауіптер жеке деректердің бұзылуына және маңызды жүйелердің істен шығуына әкелуі мүмкін. Mirai ботнетінің шабуылы мен қосылған автомобильдерді бұзу сияқты резонанстық оқиғалар тиімді қауіпсіздік жүйелерін құрудың қаншалықты маңызды екенін көрсетеді. Әртүрлі IoT өнімдері үшін бірыңғай қауіпсіздік стандарттарының болмауы жағдайды одан әрі қиындатады. Бұл көптеген құрылғылардың жеткіліксіз қорғалуына және ескірген программалық жасақтаманың салдарынан оңай осал болуына әкеледі.

Заттар интернеті экожүйелеріндегі осалдықтарды анықтау және қауіпсіздік қатерлерін басқару үшін тәуекелдерді бағалау әдістері қажет. IoT Security Assurance Framework және NIST Cybersecurity Framework сияқты құрылымдар ұйымдарға қауіпсіздік деңгейін бағалауға және тәуекелдерді азайту шараларын енгізуге нұсқаулық береді. Дегенмен, үздіксіз мониторинг жүргізу және нормативтік талаптарға сәйкестікті сақтау сияқты мәселелер бұл орталарды қорғау бойынша күш-жігерді одан әрі қиындатады. Бұл қауіпсіздікке қатысты кешенді сәйкестік бағдарламаларын әзірлеу үшін мүдделі тараптардың бірлескен тәсілін қажет етеді, мұндай бағдарламалар жаңа қауіптер мен технологияларға бейімделуі тиіс.

Заттар интернеті дамыған сайын құрылғыларды аутентификациялау әдістерін жетілдіру, озық қауіпсіздік технологияларын енгізу және жеткізу тізбегінің қауіпсіздігін қамтамасыз ету маңызды бола түседі. Бұл өзара байланысқан жүйелерді қорғау стратегияларының болашағын айқындайтын негізгі факторлар болады. Сонымен қатар, саладағы реттеу мен өзін-өзі реттеу арасындағы тепе-теңдік туралы пікірталас та IoT ортасының қауіпсіз әрі орнықты болуына ықпал етпек. Осылайша, бұл инновациялық технологияның артықшылықтарын оның осалдықтары көлеңкелемейтіндей жағдай жасалады.

IOT ЭКОЖҮЙЕСІНЕ ШОЛУ

Заттар интернеті (IoT) – бұл датчиктермен, программалық жасақтамамен және басқа технологиялармен жабдықталған физикалық құрылғылардың кең желісі, олар Интернет арқылы қосылып, деректермен алмасуға мүмкіндік береді. Бұл өзара байланысқан жүйе тұрмыстық техникадан, мысалы, тоңазытқыштар мен термостаттардан бастап, заманауи өндірістік жабдықтар мен инфрақұрылымға дейінгі әртүрлі құрылғыларды қамтиды. IoT-тың негізгі мақсаты – осы құрылғылар арқылы деректер жинау, оларды өңдеу және талдау, бұл өз кезегінде процестерді автоматтандыруға және шешім қабылдау сапасын жақсартуға ықпал етеді.

IoT экожүйесі бірнеше негізгі компоненттерден тұрады:

Құрылғылар – ақпарат жинайтын және бір-бірімен байланысатын физикалық нысандар.

Коммуникациялық желілер – құрылғылар арасындағы деректер алмасуды қамтамасыз ететін байланыс арналары.

Деректер – IoT құрылғылары жинайтын ақпарат, оны кейіннен өңдеп, талдайды.

Қолданбалар – жиналған деректерді өңдейтін және оларды пайдалы функцияларды орындау үшін пайдаланатын программалық жасақтама.

Бұл өзара байланысқан желі құрылғылар арасында үздіксіз байланысты қамтамасыз етеді және көбінесе бұлттық есептеулерге сүйеніп, деректерді жинау мен талдауды тиімді жүргізуге мүмкіндік береді. Нәтижесінде, IoT әртүрлі салалардағы процестердің тиімділігін арттырып, жұмыс өнімділігін жақсартады.

IoT-тың қолданылу салалары

Заттар интернеті көптеген салаларда кеңінен қолданылады, соның ішінде:

Денсаулық сақтау – IoT құрылғылары өмірлік маңызды көрсеткіштерді бақылап, медициналық қызметкерлерге нақты уақыт режимінде хабар береді.

Ауыл шаруашылығы – климаттық жағдайлар мен топырақтың ылғалдылығын бақылау арқылы өнімділікті арттыру.

Логистика – интеллектуалды датчиктер мен байланысқан жүйелер арқылы жеткізу тізбегін оңтайландыру.

Ақылды үйлер – тұрмыстық құрылғыларды өзара байланыстырып, өмір сапасын арттыру.

Қоғамдық қауіпсіздік – бейнебақылау жүйелері мен төтенше жағдайларды анықтау механизмдерін жетілдіру.

Қоршаған ортаны бақылау – ауа сапасын, су деңгейін және басқа да экологиялық көрсеткіштерді қадағалау.

Соңғы жиырма жылда IoT қарқынды дамып келеді, және болжамдарға сәйкес, 2025 жылға қарай бүкіл әлемде IoT құрылғыларының саны 55 миллиардқа жетеді. Мұндай жылдам өсу әртүрлі салаларда үлкен экономикалық мүмкіндіктер ашады, бұл IoT технологиясының цифрлық дәуірдегі маңызды технология ретінде көрсетеді.

Алайда, көптеген артықшылықтарына қарамастан, IoT киберқауіпсіздік саласында бірқатар күрделі мәселелерді туындатады. Қазіргі уақытта IoT технологиясына бөлінетін қаржының тек аз ғана бөлігі қауіпсіздік шараларына жұмсалады. Өзара байланысты құрылғылар экожүйесінің қарқынды дамуын ескере отырып, осы қауіпсіздік мәселелерін шешу IoT экожүйесінің тұтастығы мен қауіпсіздігін қамтамасыз етудің маңызды факторы болмақ.

Сурет 1. IoT құрылғыларының 2025 жылға арналған салалар бойынша таралу диаграммасы

IOT ЖҮЙЕСІНДЕГІ АҚПАРАТТЫҚ ҚАУІПСІЗДІККЕ ТӨНЕТІН КЕҢ ТАРАЛҒАН ҚАУІПТЕР

Заттар интернеті (IoT) құрылғылар арасындағы өзара әрекеттесу мен байланысты түбегейлі өзгертті. Алайда, бұл технология жеке адамдар мен ұйымдар үшін айтарлықтай қауіп төндіретін көптеген қауіпсіздік қатерлерін де алып келді. Осы қауіптерді түсіну IoT экожүйесінің қауіпсіздігін қамтамасыз ету үшін маңызды.

Деректердің сыртқа таралуы

IoT құрылғыларында жиналатын және сақталатын ақпаратқа рұқсатсыз тұлғалар қол жеткізген кезде деректердің сыртқа таралуы орын алады. Мұндай жағдайлар жеке деректердің, қаржылық ақпараттың және қызметтік мәліметтердің ашылуына әкелуі мүмкін. Мысалы, ақылды үйдегі қауіпсіздік камерасының осалдығы арқылы хакерлер үй желісіне еніп, жеке ақпаратты ала алады.

Құрылғыларды басып алу

Құрылғыны басып алу – бұл шабуылдаушының IoT құрылғысын иесінің рұқсатынсыз бақылауға алуы. Бұл DDoS (қызмет көрсетуден бас тарту) шабуылдарына, зиянды бағдарламаларды таратуға және басқа да қауіпті әрекеттерге әкелуі мүмкін. 2016 жылы Mirai ботнет шабуылы осы қауіптің ауқымын көрсетті: мыңдаған бұзылған IoT құрылғылары боттарға айналып, интернет-сервистердің жұмысын бұзды.

Желілік шабуылдар

IoT құрылғылары киберқылмыскерлер үшін желіге кіру нүктесіне айналуы мүмкін, бұл үлкен қауіпсіздік бұзылуларына әкеледі. Көптеген IoT құрылғылары жеткілікті қорғаныс шараларына ие емес, сондықтан олар осал болып табылады. Хакерлер HTTP, FTP сияқты қорғалмаған желілік хаттамаларды пайдаланып, деректерді шифрланбаған күйде ұстап, хабарламаларды ұстап қалып, рұқсатсыз қол жеткізе алады.

Құпиялылық мәселелері

IoT құрылғыларының кең көлемде деректер жинау мүмкіндігі жеке өмірге қатысты елеулі мәселелерді туындатады. Бұл құрылғылар көбінесе геолокациялық мәліметтерді, пайдаланушылардың мінез-құлқына қатысты деректерді және медициналық жазбаларды жинайды. Көп жағдайда бұл деректерді жинау пайдаланушының нақты келісімінсіз немесе деректерді қалай қолданатыны туралы ашық ақпаратсыз жүзеге асады. Рұқсатсыз қол жеткізу тыңшылық жасауға және деректердің ұрлануына әкелуі мүмкін.

Деректерді сақтау қауіпсіздігінің әлсіздігі

Көптеген IoT құрылғылары сенімді қауіпсіздік шараларымен жабдықталмаған, бұл оларды шабуылдарға осал етеді. Ескірген программалық жасақтама, әлсіз аутентификация әдістері және жеткіліксіз шифрлау сияқты осалдықтар сақталған деректерге рұқсатсыз қол жеткізуге мүмкіндік береді. Бұл деректердің сыртқа таралуына және құпия ақпараттың пайдаланылуына әкелуі мүмкін.

Қауіпсіздік стандарттарының жеткіліксіздігі

IoT құрылғыларын әртүрлі өндірушілер жасайтындықтан, бірыңғай қауіпсіздік стандарттары жоқ. Кейбір құрылғылар жоғары қауіпсіздік

шараларымен жасалса, басқаларында шығындарды азайту мақсатында қауіпсіздік екінші орынға қойылады. Бұл экожүйеде қорғау деңгейлерінің әркелкі болуына алып келеді, нәтижесінде тиімді қауіпсіздік шаралары мен хаттамаларын енгізу қиынға соғады.

Мониторинг пен жаңартудың қиындықтары

IoT құрылғыларының таралуы мен қашықтан орнатылуы олардың қауіпсіздігін бақылауды және жаңартуды қиындатады. Әсіресе алыс аймақтарда орналасқан құрылғылардың қауіпсіздік хаттамаларын жаңарту қиынырақ. Қолжетімділікті бақылаудың әлсіздігі мен нашар қауіпсіздік шаралары құрылғыларды осал етіп, хакерлердің әдепкі параметрлерді пайдалануына және кеңейтілген рұқсаттар алуына мүмкіндік береді.

Осы кең таралған қауіптерді түсіне отырып, IoT экожүйесінің мүдделі тараптары өз ортасын қорғау үшін алдын алу шараларын қабылдай алады. IoT құрылғыларының қауіпсіздігін күшейту және қатерлерді азайту кибершабуылдардың алдын алудың маңызды қадамы болып табылады.

IOT ОСАЛДЫҚТАРЫН АНЫҚТАУ

Заттар интернеті (IoT) құрылғылар мен олардың экожүйелеріне қауіп төндіретін көптеген осалдықтарды қамтиды. IoT технологиясы күнделікті өмірде кеңінен қолданылған сайын, бұл осалдықтарды түсіну тиімді киберқауіпсіздік шараларын әзірлеу үшін өте маңызды.

Көптеген IoT құрылғыларында сенімді қорғаныс жоқ, бұл оларды кибершабуылдарға осал етеді. Жиі кездесетін қауіпсіздік мәселелеріне әлсіз шифрлау, әдепкі құпия сөздерді пайдалану және жеткіліксіз аутентификация механизмдері жатады. Бұл факторлар киберқылмыскерлерге құрылғыларға оңай қол жеткізуге мүмкіндік береді, сондықтан IoT құрылғыларының қауіпсіздік хаттамаларын жақсарту аса маңызды.

Микропрограммалық және программалық жасақтамадағы осалдықтар

Ескірген программалық жасақтама мен жаңартылмаған микропрограммалық IoT құрылғылары үшін үлкен қауіп тудырады. Көптеген құрылғылар қауіпсіздік осалдығы бар ескірген нұсқаларда жұмысын жалғастырады. Өндірушілер қауіпсіздік жаңартуларын уақытында ұсынбаған жағдайда, бұл құрылғылар хакерлер үшін оңай нысанаға айналады. Осы қауіптерді азайту үшін тұрақты жаңартулар мен Микропрограмманы тиімді басқару қажет.

Стандарттаудың болмауы

IoT құрылғыларының стандарттарының жоқтығы бірыңғай қауіпсіздік шараларын әзірлеуді қиындатады. Әртүрлі құрылғылар әртүрлі деректерді беру технологияларын қолданады, бұл қорғаныс механизмдері мен хаттамаларын бірыңғай енгізуді қиындатады. Осындай әркелкілік қауіпсіздік жүйелеріндегі олқылықтарды тудырып, оларды киберқылмыскерлер пайдалануы мүмкін.

Экожүйе интерфейстерінің қорғалмауы

IoT құрылғылары жиі бұлттық сервистерге қосылады, бұл қосымша осалдықтарға әкелуі мүмкін. Қорғалмаған API интерфейстері құрылғыларға

рұқсатсыз қол жеткізу және оларды басқару қаупін тудырады. Қауіпсіз аутентификацияны қамтамасыз ету, шифрлауды күшейту және API үшін тиімді қауіпсіздік сүзгілерін енгізу IoT экожүйесін қорғаудың маңызды бөлігі болып табылады.

Әлсіз құпия сөздер және әдепкі баптаулар

IoT құрылғыларында стандартты, әлсіз немесе өзгертілмейтін құпия сөздерді пайдалану кибершабуылдарға жол ашады. Егер құрылғылар бастапқы конфигурациясында дұрыс бапталмаса, зиянкестер оларды оңай бұза алады. Сондықтан әдепкі пайдаланушы аттарын, құпия сөздерді және конфигурацияларды өзгерту шабуылға осалдықты айтарлықтай төмендетіп, құрылғының қауіпсіздігін арттырады.

Құрылғылардың физикалық қауіпсіздігі

IoT құрылғыларына физикалық қол жеткізу олардың қауіпсіздігін бұзуы мүмкін. Егер зиянкестер құрылғыларға физикалық түрде қол жеткізе алса, оларды қайта жүктеп, аппараттық құрамын өзгертіп немесе зиянды программалық жасақтама орнатуы мүмкін. Сондықтан құрылғыларды рұқсатсыз араласудан қорғау үшін физикалық қауіпсіздік шараларын қолдану өте маңызды.

Зерттелген жағдайлар

Mirai ботнеті – IoT қауіпсіздігіне төнген маңызды қауіптердің бірі. Бұл зиянды бағдарлама көптеген ақылды құрылғылардың (камералар, маршрутизаторлар және т.б.) осал тұстарын пайдаланып, оларды басқару үшін қолданды. Осылайша, IoT құрылғылары жаппай ботнетке айналып, DDoS шабуылдарын іске асыруға мүмкіндік берді.

Бұл шабуыл IoT құрылғыларын бұзып, оларды желі инфрақұрылымына үлкен зиян келтіретін құралға айналдыруға болатынын дәлелдеді.

Кейіннен ФБР тергеу жүргізіп, Mirai ботнетінің жасаушыларын анықтады, бұл олардың қамауға алынуына әкелді. Қызықты жайт – кейінірек бұл кибершабуылшылар WatchTower деп аталатын IoT қауіпсіздік жүйесін әзірлеп, IoT құрылғыларына шабуыл жасайтын хакерлерді анықтауға көмектесті.

Jeep Cherokee автокөлігін бұзу

2015 жылы жүргізілген зерттеу қосылған көліктердің осалдықтарын көрсетті. Ақпараттық ойын-сауық жүйесінің осалдықтары арқылы хакерлер Jeep Cherokee автокөлігінің басқару жүйесін қашықтан бұзып, оны тежегіштері мен рөлін қадағалауға мүмкіндік алды.

Бұл жағдай автокөлік қауіпсіздігіне байланысты үлкен қауіптерді ашты. Автокөліктердегі бір-бірімен байланысқан жүйелер көптеген осалдықтарға жол ашуы мүмкін, сондықтан оларға сенімді киберқауіпсіздік шараларын енгізу қажеттілігі дәлелденді.

Ring бейнебақылау камераларындағы қауіпсіздік инциденттері

Ring қауіпсіздік камераларымен байланысты бірнеше инциденттер IoT құрылғыларының осалдығын тағы бір рет дәлелдеді.

Кейбір пайдаланушылар олардың камераларына рұқсатсыз қол жеткізілгенін хабарлады. Бір жағдайда бұзылған камералар арқылы бөгде адамдар балалармен сөйлескен, бұл жеке өмірдің қауіпсіздігіне қатысты үлкен алаңдаушылық туғызды.

Кейіннен Ring компаниясы жүйедегі осалдықтарды түзету үшін қауіпсіздік жаңартуларын шығарды. Бұл оқиға IoT құрылғыларын тұрақты жаңартып, қауіпсіздігін бағалау қажеттігін көрсетті.

IoT бұзуларының кең ауқымды салдары

IoT құрылғыларының таралуы киберқауіпсіздік қатерлерінің артуына әкелді. Әртүрлі инциденттер әлсіз құпия сөздер, шифрлаудың жоқтығы және тиімсіз қауіпсіздік хаттамалары сияқты кең таралған осалдықтарды көрсетті.

Мысалы, ақылды камералардың осалдықтарын пайдалану олардың кибершабуылшылар үшін желіге кіру қақпасына айналуына мүмкіндік берді. Тіпті қауіпсіздік мақсатында жасалған құрылғылардың өзі қауіпке айналуы мүмкін.

IoT қауіпсіздік ландшафты үздіксіз қадағалауды талап етеді, өйткені бұзылулардың салдары жеке деректердің ұрлануынан бастап физикалық қауіпке дейін жетуі мүмкін.

Бұл мысалдар IoT құрылғыларын жобалау және енгізу кезінде қауіпсіздік шараларын күшейту қажеттілігін, сондай-ақ пайдаланушылардың киберқауіпсіздікке қатысты хабардарлығын арттырудың маңыздылығын айқындайды.

БОЛАШАҚТАҒЫ ЗАТТАР ИНТЕРНЕТІНІҢ ҚАУІПСІЗДІК ТЕНДЕНЦИЯЛАРЫ

Заттар интернетінің (IoT) қауіпсіздік ландшафты технологиялар мен осы жүйелерге бағытталған қауіптер дамыған сайын жылдам өзгеріп жатыр. IoT құрылғылары әртүрлі секторларда кеңінен таралған сайын, олардың қауіпсіздігіне тән осалдықтарды жою маңызды міндетке айналады.

Қадағалау реттеуінің күшеюі

Заттар интернетінің қауіпсіздігі болашағын анықтайтын маңызды тенденциялардың бірі – қатаң нормативтік талаптардың пайда болуы. Үкіметтер тұтынушылар мен кәсіпорындарды қорғау үшін қауіпсіздік стандарттары мен ұсыныстарды әзірлеудің қажеттілігін түсініп отыр. Мысалы, Ұлыбританияның өнім қауіпсіздігі және телекоммуникациялық инфрақұрылым туралы заңы (PSTI) IoT өндірушілерінің нақты қауіпсіздік стандарттарына сәйкес жұмыс істеуін талап етеді, соның ішінде IASME IoT Cyber Scheme сияқты IoT киберқауіпсіздігі жөніндегі халықаралық ережелерге сәйкес келетін стандарттар бар.

Алдыңғы қатарлы қауіпсіздік технологияларын енгізу

IoT экожүйелері күрделенген сайын, жасанды интеллект (AI) және машиналық оқыту (ML) сияқты алдыңғы қатарлы қауіпсіздік технологияларына деген тәуелділік артады. Бұл технологиялар IoT желілеріндегі күдікті әрекеттерді мониторингтеуде және қауіпсіздік бұзылуын білдіретін аномалияларды анықтауда маңызды рөл атқаратын болады. Бұл

технологияларды интеграциялау қауіп-қатерлерді анықтау мүмкіндіктерін кеңейтеді және қауіпсіздік жүйелерінің жауап беру жылдамдығын арттырады.

Құрылғыларды аутентификациялау және шифрлауды жетілдіру

Болашақта IoT қауіпсіздік жүйелері сенімді аутентификация және шифрлау хаттамаларын қолданады деп күтілуде. Себебі, IoT құрылғылары жиі қауіпсіз емес хаттамалар арқылы байланысады, сондықтан сенімді шифрлау әдістерін және көпфакторлы аутентификацияны енгізу жеке деректерді қорғау мен рұқсатсыз қол жеткізуден қорғау үшін маңызды болады. Сонымен қатар, құрылғыларды қауіпсіз қосу үрдісі де дамып, барлық қосылған құрылғылардың желіге интеграциялану алдында қауіпсіздік стандарттарына сәйкес болуы қамтамасыз етіледі.

Жабдықтау тізбегінің қауіпсіздігіне көбірек көңіл бөлу

IoT құрылғылары бизнес операцияларының ажырамас бөлігіне айналған сайын, жабдықтау тізбегінің қауіпсіздігі маңызды бола түседі. Ұйымдар өздерінің жабдықтау тізбектеріндегі ықтимал осалдықтарды бақылап отыруы қажет, әсіресе рұқсатсыз IoT құрылғылары мен жабдықтау тізбегіне жасалатын шабуылдардың көбеюі жағдайында. Бұл тенденция өндірушілер, жеткізушілер және соңғы пайдаланушылар арасындағы бірігу мен қауіпсіздіктің барлық кезеңінде қамтылуын талап етеді.

Дамып келе жатқан киберқауіпсіздік стратегиялары

Киберқауіпсіздік қауіптерінің динамикалық сипатына қарсы тұру үшін, IoT қауіпсіздік стратегиялары үнемі дамып отыруы керек. Ұйымдар ықтимал осалдықтарды анықтап, оларды жоюдың тиімді стратегияларын енгізуге белсенді түрде қатысуы тиіс. Бұл бағдарламалық қамтамасыз етуді үнемі жаңартып отыруды, үнемі мониторинг жүргізуді және IoT экожүйесіндегі жаңа және пайда болған қауіптерге бейімделу үшін тәуекелдерді мұқият бағалауды қамтиды. IoT қауіпсіздігі – бұл бір реттік жұмыс емес, үздіксіз процесс екенін түсіну болашақ қауіпсіздік бастамаларының негізі болмақ.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1. Ganzha K. *Securing the IoT Landscape: Strategies for Safeguarding Connected Devices* // Technorely. – 2023. – November 23. – [Electronic resource]. URL: https://technorely.com/insights/securing-the-io-t-landscape-strategies-for-safeguarding-connected-devices

2. Oza C. *Legal Landscape of Internet of Things: A Critical Review of Privacy, Security, and Regulatory Challenges* // Lawful Legal. – 2024. – June 25. – [Electronic resource]. URL: https://lawfullegal.in/legal-landscape-of-internet-of-things-a-critical-review-of-privacy-security-and-regulatory-challenges/

3. Magnan C. *Unique Security Challenges of IoT Devices and Best Practices for Securing Them* // PECB Insights. – 2024. – November 15. – [Electronic resource]. URL: https://insights.pecb.com/unique-security-challenges-of-iot-devices-and-best-practices-for-securing-them/

4. Lima R. *IoT Security: 15 Types of Attacks with Real-World Examples* // InovaSense. – 2023. – October 23. – [Electronic resource]. URL: https://www.inovasense.com/15-types-of-attacks-with-real-world-examples/

5. Mirza D. *Top 10 IoT Device Vulnerabilities to Enhance IoT Security* // Host Duplex. – 2022. – December 15. – [Electronic resource]. URL: https://www.hostduplex.com/blog/top-iot-device-vulnerabilities/

УДК 69.003

Бейбітхан Қайсар Сейтжапарұлы
kaisar.beybitkhan@gmail.com
Л.Н. Гумилева атындағы ЕҰУ Құрылыс факультетінің 2 курс магистранті
(Астана қ.)
Ғылыми жетекші – Н. Т. Алибекова

BIM ДЕГЕНІМІЗ НЕ ЖӘНЕ ОНЫҢ ҚҰРЫЛЫС САЛАСЫНА ӘСЕРІ ҚАНДАЙ?

***Аңдатпа**: BIM (Building Information Modeling) — бұл құрылыс жобаларын жобалаудың, жүзеге асырудың және басқарудың заманауи әдісі. Бұл технология тек 3D модельдеумен шектелмейді, сонымен қатар ғимараттардың барлық өмірлік циклін қатысты физикалық және функционалдық мәліметтерді цифрлық түрде ұсынуға мүмкіндік береді. Мақалада BIM-нің артықшылықтары, құрылыс саласына әсері, оны енгізудегі қиындықтар және оларды шешу жолдары талқыланады. BIM технологиясы тиімділікті арттыруға, шығындарды азайтуға, тұрақтылықты қамтамасыз етуге және құрылыс жобаларының үйлесімділігін жақсартуға септігін тигізетіні көрсетілген. Сонымен қатар, BIM-ді сәтті енгізу үшін қажетті қадамдар сипатталған.*

***Кілттік сөздер:** BIM, құрылыс, цифрландыру, модельдеу, инновация, жоспарлау, тұрақтылық.*

Құрылыс саласы ұзақ уақыт бойы шығындардың артуы, мерзімдердің кешігуі және байланыстардың үзілуі сияқты маңызды мәселелермен бетпе-бет келуде. Мысалы, зерттеулер көрсеткендей, ірі құрылыс жобалары бастапқы жоспарланған бюджеттен 20%-ға артық шығындалады және 20%-ға ұзақ уақыт алады. Мұндай тиімсіздіктер трансформациялық шешімдерге деген сұраныстың артып отырғанын көрсетеді. Building Information Modeling (BIM) — құрылыс жобаларын жобалаудың, жүзеге асырудың және басқарудың жаңа тәсілін ұсынатын осындай шешім. BIM тек қана бағдарламалық құрал немесе 3D модель емес, ол — жерлердің физикалық және функционалдық сипаттамаларының цифрлық репрезентацияларын құру, басқару және бөлісуді қамтамасыз ететін кешенді процесс.

BIM (Building Information Modeling) дегеніміз не?

BIM — активтердің өмірлік циклі бойында, яғни бастапқы жобалаудан бастап құрылысқа, пайдалануға және техникалық қызмет көрсетуге дейінгі цифрлық репрезентацияларын 3D модельдер арқылы визуализациялауды білдіреді. Бұл процесс жобалық топтар арасында үздіксіз ынтымақтастықты қамтамасыз етіп, байланыс орнатуға, ақпарат алмасуға және жобаның шығындарын бақылауға мүмкіндік береді.

BIM-нің артықшылықтары:

- Жобаларды басқару жеңілдейді, дәстүрлі CAD әдістерінде жиі кездесетін кешігулер, қателіктер және түсініспеушіліктер қаупін азайтады.
- BIM жобалық топтарға архитектуралық, инженерлік және құрылыс процестеріне нақты уақыт режимінде шолу жасауға мүмкіндік береді.

- Бұл шешімдер қабылдаудың барлық кезеңдерін қолдайтын ортақ білім қоры ретінде қызмет етеді — бастапқы тұжырымдамадан бастап құрылысқа және ақырында демонтажға дейін.

Алғашында цифрлық макеттер жасау құралы ретінде пайда болған BIM бүгінде құрылыс жобаларының толық өмірлік циклін қамтитын трансформациялық процесс ретінде дамыды. Бұл эволюция құрылыс саласына тұрақтырақ тәсілдерді енгізуге, тиімділікті арттыруға және шығындарды азайтуға ықпал етеді.

BIM-нің технологиялық негізі

BIM тиімділігі оның жетілдірілген технологиялық негізіне байланысты. Autodesk Revit, ArchiCAD және Bentley Systems сияқты құралдар мамандарға ғимараттарды тек үш өлшемде визуализациялауға ғана емес, сондай-ақ нақты әлемдегі өнімділікті модельдеуге және құрылыс процесі барысында деректерді жан-жақты басқаруға мүмкіндік береді.

Бұл құралдар жобадағы барлық қатысушыларға ықтимал қиындықтарды алдын ала анықтап, оларды оңтайландыруға мүмкіндік беретін үздіксіз интеграцияны қамтамасыз етеді.

BIM-нің көптеген артықшылықтары

BIM көптеген және кең ауқымды артықшылықтарды ұсынады:

- Тиімділіктің артуы: BIM жұмыс процестерін оңтайландырып, қайталанатын жұмыстарды азайтады, бұл командаларға құнды тапсырмаларға назар аударуға мүмкіндік береді.
- Шығындарды азайту: Қателерді азайту және ресурстарды оңтайлы бөлу арқылы жалпы жобаның құны айтарлықтай төмендейді.
- Материалдардың ысырабын азайту: Дәл жоспарлау және визуализация материалдардың ысырабын азайтып, құрылыс саласындағы тұрақтылыққа ықпал етеді.
- Визуализацияның жақсаруы: Мүдделі тараптар жоба туралы нақты түсінік алады.
- Үйлестірудің жақсаруы: BIM дизайн және құрылыс топтарының ынтымақтастығын нығайтып, түсініспеушіліктерді азайтады.

Мысал: Бір ірі қалалық даму жобасы BIM-ді қолдану арқылы жобаның кешігуін 25%-ға, ал материал ысырабын 30%-ға қысқартты.

BIM-ді қолданудағы қиындықтар

BIM-нің артықшылықтарына қарамастан, оны енгізу бірқатар кедергілермен бетпе-бет келеді:

- Үйренудің күрделілігі: BIM-ді енгізу үшін айтарлықтай дайындық пен тәжірибе қажет.
- Бастапқы шығындардың жоғары болуы: BIM құралдары мен процестерін енгізу бастапқы кезеңде қымбатқа түсуі мүмкін.
- Мәдени өзгеріс: Ұйымдар ынтымақтастыққа негізделген көзқарасты қабылдап, өзгерістерге төтеп беруі керек.

Бұл қиындықтарды стратегиялық жоспарлау, кешенді оқыту бағдарламалары және BIM процестерін қолданыстағы жұмыс процестеріне біртіндеп интеграциялау арқылы жеңуге болады.

BIM-ді енгізу: қадамдық нұсқаулық

BIM-ді тиімді енгізу үшін құрылымдық тәсіл қажет:

- Айқын мақсаттар қою: BIM енгізу үшін нақты мақсаттар мен нәтижелерді анықтау.
- Толық жоспар жасау: BIM-ді жұмыс процестеріне интеграциялауға арналған жол картасын құру.
- Мүдделі тараптарды тарту: Барлық қатысушылар арасында ынтымақтастықты дамыту.
- Оқыту: Командаларды қажетті дағдылар мен біліммен қамтамасыз ету.

Біртіндеп интеграциялау: BIM процестерін біртіндеп енгізу.

BIM-нің жобаларды басқарудағы артықшылықтары

BIM жобаларды басқаруды интеграцияланған және ынтымақтастыққа негізделген тәсіл арқылы айтарлықтай жақсартады.

Мысал: Ауруханының құрылысы жобасында BIM архитектура, инженерия және мердігерлер арасындағы күш-жігерді үйлестіруді қамтамасыз етті, нәтижесінде қателер 40%-ға азайып, жеткізу мерзімдері жақсарды.

BIM технологиясы — заманауи құрылыстың негізі. Дегенмен, деректерді басқарудың үзіктілігі, күрделі құрылыс ортасы және желі инфрақұрылымдарының үйлесімсіздігі сияқты кедергілер оның толық таралуына кедергі келтіруде.

Алға жылжу үшін ұйымдық және ұлттық деңгейдегі инновациялар қажет. Деректер интерфейстері мен платформалық интеграция үшін бірыңғай стандарттарды белгілеу маңызды.

Құрылыс секторы тиімділік, тұрақтылық және инновацияны арттыру үшін BIM-нің әлеуетін толық іске асырып, болашақта ақылдырақ, төзімді құрылыс ортасын қалыптастыра алады.

Ұлыбританиядағы тұрғын үй құрылысы саласындағы инновациялар

Бұл бөлім Ұлыбританиядағы тұрғын үй құрылысы саласындағы инновацияларға қатысты жалпы контекстті кеңірек сипаттайды. 2016 жылы Фармер Ұлыбританиядағы құрылыс жұмыс күшінің моделіне шолу жасап, оны батыл түрде «Жаңғырту немесе жойылу: Саланың болашағын анықтайтын уақыт» деп атаған. Есепте ағымдағы жағдай қатаң сынға ұшырап, егер түбегейлі өзгерістер енгізілмесе, құрылыс саласы «айтарлықтай әлсіреуі» мүмкін деп көрсетілген (Farmer, 2016, 8-бет).

Есепте саладағы негізгі мәселелер ретінде мыналар көрсетілген:

- технологияның рөлін қабылдамауға байланысты өнімділіктің төмендігі;
- қартайған жұмыс күші, жаңа кадрлардың аз келуі және қайталанатын дағдарыстарға байланысты болашақтағы жұмыс күшінің тапшылығы;

- ұйымдардың ауқымын ұлғайтуға, тәуекелдерді бөлісуге және бизнесті жоспарлаудағы тұрақтылықты арттыруға кедергі келтіретін ынтымақтастық пен жетілдіру мәдениетінің болмауы;
- зерттеулер мен инновацияларға инвестицияның жетіспеушілігі.

Есепте жоғарыда аталған мәселелерді шешу үшін сыртқы өндіріс (off-site manufacturing) және BIM (Building Information Modeling) технологияларын қолдануға кеңес беріледі. Фармер былай дейді: «Қазір цифрландырудың мүмкіндіктерін пайдаланып, еңбекке негізделген әдістерге тәуелділік тәуекелдерін азайтатын уақыт келді» (ibid, 5-бет).

Алайда, Фармердің мәліметінше, құрылыс индустриясы инновацияларды кеңінен қабылдаудан бас тартып отыр: «Теріс көзқарастар... құрылыс дизайны мен құрылыс процесіндегі көптеген инновациялық тәсілдердің тәуекелді деп бағаланып, бірден қабылданбауына алып келеді... "Құрылыстың заманауи әдістері" немесе "заводтық дайындық" сияқты терминдер жиі күмәнмен қаралады» (ibid, 35-бет).

Lloyds Bank-тің «2018 жылғы тұрғын үй құрылысы туралы есебі» үй салушылар арасында инновацияларды қабылдаудың оң көрінісін ұсынады. Есепте тұрғын үй құрылысы секторы «жаңа үйлердің жеткізілуі, сапасы және қолжетімділігі мәселелерін шешуге, сондай-ақ өнімділік пен табыстылықты арттыруға мүмкіндік беретін жаңа құрылыс әдістерін енгізуге дайын екенін көрсетіп отыр» делінген (Lloyds Bank, 2018, 10-бет).

Lloyds Bank тұрғын үй құрылысында заманауи тәсілдерді атап өтеді, соның ішінде тұрғын үй компоненттерін құрылыс алаңынан тыс жерде дайындау және құрастыру, сондай-ақ болашақта робот-қыш қалаушылар мен 3D басып шығарылған үйлерді қолдану. Зерттеулерінің нәтижесінде, құрылыс компанияларының көпшілігі жаңа құрылыс әдістеріне инвестиция салатынын анықтаған, олардың ішінде модульдік үйлер (68%) көш бастап тұр.

Олар құрылыс компанияларының жаңа технологияларды қолдануындағы негізгі себептерді былайша сипаттайды: «Өнімділік, кірісті арттыру, құрылыс жеңілдігі, құрылыс стандарттарын жақсарту, энергия тиімділігін арттыру, қалдықтарды жою және тұтынушылар үшін қолжетімділік» (ibid, 10-бет).

Құрылыс әдістерінің көптеген жаңа түрлері қолжетімді. **NHBC Foundation** «Құрылыстың заманауи әдістерін» (Modern Methods of Construction, MMC) бес негізгі санатқа бөлген (NHBC Foundation, 2006).

Пайдаланылған әдебиеттер тізімі

1. NHBC (2013). Building Information Modelling: An introduction for house builders. Milton Keynes: NHBC.
2. Farmer, M. (2016). Modernise or Die: The Farmer Review of the UK construction labour market.
3. Abanda, F.H., Tah, J.H.M., Cheung, F.K.T. (2017). BIM in off-site manufacturing for buildings. Journal of Building Engineering, 14, pp. 89-102.

4. Ezcan, V., Isikdag, U., Goulding, J.S. (2013). BIM and Off-Site Manufacturing: Recent Research and Opportunities. CIB World Building Congress, Brisbane, Australia.
5. HM Government (2013). Construction 2025: Industrial Strategy.
6. Infrastructure and Projects Authority (2016). Government Construction Strategy 2016-20.
7. Autodesk (2018). What is BIM?
8. NBS (2017). NBS National BIM Report 2017.
9. Lloyds Bank (2018). Housebuilding Report 2018.
10. Wienerberger (2018). e4 Brick House Case Study.

udc 004.056

Malik Andassov
Computer Science and Engineering Master's student, Astana IT University
Kazakhstan, Astana

INNOVATIVE APPROACHES FOR SECURING PHYSICAL INFRASTRUCTURE: MODELS AND METHODS FOR MICROCONTROLLER-BASED SECURITY SYSTEMS RESILIENT TO CYBER-PHYSICAL ATTACKS

Abstract. *Modern society realizes the importance of physical infrastructure protection because of increasing advanced cyber-physical attack techniques. This document identifies modern approaches that strengthen protective microcontroller security systems power critical operations such as water supply management and industrial automation systems and electricity distribution networks. The subsequent analysis centers on a progressive security model based on relationships which protects hardware and firmware as well as networks and operation platforms. Reliability grows substantially against standard cyberattacks and physical adversities when attackers receive classification based on their access privileges and abilities and when security implementations occur in the first stages of system development. The practical field studies of water supply management and industrial IoT showcase operational success by enhancing threat identification capabilities together with diminishing operational downtime and enabling security solutions to scale smoothly. The final part of the article discusses AI-based predictive security and self-repairing systems and advanced cryptography adapted for microcontroller environments.*

Keywords: *AI, IoT, security systems, microcontroller.*

1.Introduction

Physical infrastructure depends on microcontrollers for critical operations throughout its entirety including water treatment facilities and related energy grids and fabrication lines and transportation systems. The devices carry out multiple operations which include gathering sensor information along with system controls and automated alert systems and remote system observation functions. The number of interconnected data-dependent systems has made cyber-physical attacks more likely to happen.

Key Motivations

Attacks on microcontrollers result in operational interruptions through plant shutdowns combined with hazardous operating parameter failures occurring in automated plants and municipal water pumps as well as energy substations.

Malicious tampering of devices will trigger hazardous environmental risks as well as life-threatening conditions because the altered equipment functions improperly.

Service interruptions coupled with security breaches cause both financial monetary loss and diminish customer trust in operators.

The article outlines new security methods which consolidate a multi-level security model linking relationships and threat categorization systems with early design implementations of resilience.

2.Background and Significance

2.1 The Role of Microcontroller-Based Systems

Modern infrastructure depends on microcontrollers which function as central control systems for numerous devices because of the following characteristics:

These systems work in environments where they have limited processing capabilities and small memory space alongside long-lasting operation periods.

Applications requiring rapid responses form a major category since they include robotic arm control systems and pressure valve activation examples.

Few deployments barring legacy and remote installations present simple update procedures.

2.2 Nature of Cyber-Physical Attacks

Cyber-attacks against microcontrollers combine both digital malicious activities with opportunities for physical system access to achieve their objectives.

Remote Intrusions: Exploiting networking protocols, firmware flaws, or unsecured access points.

Security Threats involving hardware manipulation occur when attackers manipulate microcontroller chips as well as their electronic connectors or develop electromagnetic signature-based side-channel attacks.

Attackers apply hybrid methods by amalgamating various vulnerabilities to accomplish sabotage such as malware that silences system logs before physical attackers adjust essential operational parameters.

The situation demands immediate action since a trivial security breach may spread rapidly between connected systems through robust defenses at different levels.

3. Hierarchical Security Modeling

3.1 Why a Hierarchical Approach?

Security measures implemented by traditional systems function independently within separate layers such as hardware or software or network elements which creates vulnerabilities for attackers to take advantage of. A Set-Based Hierarchical Relational Model implements security integration as it protects every layer so that:

The detecting of dependent hardware weaknesses that spread into software remains possible through simultaneous examination of both platforms.

Security infrastructure stays stable as the framework allows users to perform modular hardware substitutions along with protocol changes without causing disruption to the whole system.

3.2 Layers of the Model

Hardware Security Layer:

The secure bootloader system enables authentication of code that runs on the microcontroller platform. Security measures based on physical containers include components which detect unapproved open entries and environmental changes.

Firmware/Software Security Layer:

The continuous procedure which checks for alterations in firmware operation represents Runtime Integrity Checks. Security systems employ signature-based and behavior-based methods to detect irregular data movement and process order anomalies as part of an intrusion detection system.

Communication & Network Security Layer:

The system implements cryptographic protocols using AES-128 and elliptic curve algorithms meant for implementation on microcontrollers. Firewalls & Segmentation: Isolating critical microcontroller segments from less-trusted networks.

Attacker & Threat Modeling Layer:

Safety Surface Assessment: Collecting information about all operational ports together with protocols used and debug interfaces and all authorized access levels. Adaptive Defense provides a security system which adjusts its defense tactics through adaptive reconfiguration between elevated threats including encryption level increases and access control strengthening.

4. Classification of Attackers and Attacks

4.1 Attacker Taxonomy

Type 0 – No Direct Access: Attackers of this category only depend on social engineering and external reconnaissance alongside phishing tactics.

Type 1 – Indirect System Interaction: Attackers exploit insecure remote interfaces along with weak password policies to create minimal system access.

Type 2 – Direct Physical Influence: Attackers carry out side-channel analysis or simultaneously manipulate hardware pins or surveil debug signals.

Type 3 – Full System Access: Users who maintain access within the organization system or achieve deep infiltration success.

Type 4 – Privileged/Root-Level Control: Organizations backed by state or possessing meaningful resources have successful stealth operation capabilities.

4.2 Classification of Cyber-Physical Attacks

Cyber Attacks: Malicious code insertion and backdoor installation happens through cellular updates known as firmware exploits.

Locking up the microcontroller occurs when its limited processing or memory resources become overwhelmed in Denial of Service (DoS) attacks.

Physical Attacks: Monitoring a system's power output and underobservation of electromagnetic signals allows attackers to recovery the cryptographic keys within. Internal circuit modification combined with component re-soldering and critical pathway shorting makes up device tampering.

Hybrid Attacks: An attacker targets software-hardware fusion vulnerabilities by executing firmware updates during physical protection circuit modification to conceal their unlawful modifications.

5.Methods and Algorithms for Cyber-Physical Resilience

5.1 Security-by-Design Principles

5.1.1 Requirements Analysis

Users should list every function the microcontroller performs before they associate these operations with potential points of attack. Security controls should direct themselves toward functions having both high-risk and high-impact characteristics.

5.1.2 Architectural Hardening

Physical unclonable functions (PUFs) together with onboard storage enable microcontroller power-up validation of system identity. The installation of code

updates must require signatures that verify their authenticity to protect against unauthorized code modifications.

5.1.3 Iterative Security Testing

Secure Penetration Tests enable attackers to simulate all types (0–4) to identify vulnerabilities before they affect the system. Testing under extreme conditions is important since microcontrollers mostly work in harsh operational environments requires stress and environmental tests to validate their performance under temperature and voltage fluctuations.

5.2 Adaptive Security Algorithms

Real-Time Intrusion Detection: The system starts with training on operational data until it learns normal patterns and later detects abnormal metrics such as sensors or CPU utilization variances. The implementation of self-learning systems let machines use machine learning algorithms to modify threshold values according to evolving infrastructure requirements.

Lightweight Cryptographic Suites: Devices should use AES-128 as their cryptographic standard because their limitations require this level of encryption security. Systems with hardware accelerators should be used to decrease computational workloads.

6. Experimental Validation

6.1 Water Supply Management

Watersupply stations regulated by microcontrollers are components of a municipal system that utilizes hierarchical security.

Implementation: Secure boot and firmware signing at each pump controller.

The system divides its communication network into separate domains for operator interfaces and remote devices. A system monitors sensor patterns by detecting anomalies in real-time.

Outcomes: The security measures reduced the number of unauthorized control attempts because attackers could not prove their firmware signatures were valid. Unexplained flow spike detection through anomaly detection systems stopped intentional overflows from occurring. The CPU performance of microcontroller operations remained intact at less than 5%.

6.2 Industrial IoT Deployment:

The industrial system linked robotic arms through microcontrollers to manage conveyor speeds as well as sensor results and track products throughout the workflow.

Security Measures: The supervisory controller established encryption-defense layers with all its connected microcontrollers. The system operates adaptation with machine learning algorithms which detect strange command sequences.

Results: The system detects compromised elements so it can partition them to stop attackers from spreading through the manufacturing line. Security incidents required less downtime because the security team rapidly found and responded to threats. The addition of new robotic workstations demanded a limited adjustment of the wide-scale security infrastructure parameters.

Conclusion

Protecting critical physical infrastructure infrastructure based on microcontroller systems requires developers to implement multiple defense strategies in advance. An attack defense system becomes stronger when security measures are implemented first during design thus advancing from hardware layers to network layers while adapting security measures to detect new threats.

Testing has demonstrated that the integrated security frameworks yield encouraging outcomes through their real-world implementations. Each application in the domain validates how a systematic approach to complete security implementation delivers increased value in water supply systems and industrial IoT deployments. The fundamental models provide organizations with adaptable guidelines to deliver infrastructure that incorporates protected microcontroller systems and achieves higher security levels and resilience through new technologies and threats.

References

1. Levshun, D. *Models, Algorithms, and Methodology for the Design of Microcontroller-Based Physical Security Systems Protected from Cyber-Physical Attacks.* Ph.D. Thesis, Université Paul Sabatier - Toulouse III & ITMO University, 2021.

2. Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. *Guide to Industrial Control Systems (ICS) Security (NIST Special Publication 800-82 Rev. 2).* National Institute of Standards and Technology, 2015.

3. Falliere, N., Murchu, L.O., & Chien, E. *"W32.Stuxnet Dossier."* Symantec Security Response, 2011.

4. Padilla, M., & Crompton, N. *"Securing Embedded Systems Against Side-Channel Attacks."* Microprocessors and Microsystems, vol. 55, 2017, pp. 28–38.

5. Ronen, E., O'Flynn, C., Shamir, A., & Weingarten, A. *"IoT Goes Nuclear: Creating a ZigBee Chain Reaction."* IEEE Symposium on Security and Privacy (SP), 2017, pp. 195–212.

6. Moradi, A., Paar, C., & Salmasizadeh, M. *"Side-Channel Attacks on Embedded Systems: A Survey."* Journal of Cryptographic Engineering, vol. 4, no. 2, 2014, pp. 89–108.

7. LeMay, E., Ford, M., Keefe, K., & Sanders, W. *"Model-Based Security Metrics Using ADversary VIew Security Evaluation (ADVISE)."* 2011 Eighth International Conference on Quantitative Evaluation of Systems, 2011, pp. 191–200.

8. IEC 62443 Series *Security for Industrial Automation and Control Systems.* International Electrotechnical Commission (IEC), various publication dates.

9. Zhang, P., & Green, B. *"Lightweight Cryptography for Microcontroller-Based IoT Systems: A Survey."* ACM Computing Surveys, vol. 53, no. 6, 2021, pp. 1–34.

10. Kotenko, I., & Ulanov, A. *"Agent-Based Modeling and Simulation of Cyber-Warfare between Malefactors and Security Agents in Internet."* Journal of Information Warfare, vol. 8, no. 3, 2009, pp. 1–18.

11. Skarmeta, A. F., Moreno, M. V., & Calero, F. J. *"Managing the Security of the IoT-Based Smart Grid."* Electronics, vol. 6, no. 2, 2017, pp. 30–45.

12. Sadeghi, A.-R., Wachsmann, C., & Waidner, M. *"Security and Privacy Challenges in Industrial Internet of Things."* Proceedings of the 52nd Annual Design Automation Conference, 2015, pp. 1–6.

УДК 3.7016.1

Rysbek Aigerim Sakenkyzy
2nd year student of Master`s degree
Kazakh National Women's Teacher Training University
(Almaty, Kazakhstan)

Kozhak Lazzat Muratkyzy
2nd year student of Master`s degree
Kazakh National Women's Teacher Training University
(Almaty, Kazakhstan)

USAGE OF AUTHENTIC VIDEO MATERIALS FOR THE DEVELOPMENT OF COMMUNICATIVE SKILLS

Annotation. *In the modern age of globalization, proficiency in a second or foreign language has become an essential talent. Communicative competence, which includes grammatical precision and the appropriate use of language in many social circumstances, is a primary objective in language education. Conventional pedagogical approaches, frequently emphasizing rote memory and grammatical exercises, have faced growing criticism for their inadequacy in equipping learners for authentic communication scenarios. In response, instructors have utilized real resources, especially video, as an effective instrument for enhancing communicating abilities. Genuine video materials—such as films, television programs, news segments, and digital videos—offer learners exposure to authentic language usage, cultural subtleties, and non-verbal communication signals. This article examines the advantages of employing authentic video materials in language acquisition, outlines practical methods for their incorporation into the classroom, and emphasizes current research validating their efficacy.*

Keywords:*authentic video materials, communicative skills, language learning, communicative competence, cultural competence, real-life language use, listening comprehension, speaking fluency, intercultural awareness.*

The Role of Authentic Video Materials in Language Learning

Authentic video resources are characterized as being produced for native speakers, as opposed to language learners. In contrast to scripted dialogues found in textbooks, these materials exemplify authentic language usage, incorporating idiomatic phrases, colloquialisms, and regional dialects. This authenticity is essential for cultivating communicative competence, as it enables learners to engage with language as it is utilized in real-life contexts.

A key benefit of utilizing real video resources is their capacity to deliver contextualized linguistic input. Krashen's Input Hypothesis (1985) posits that language acquisition transpires when learners encounter intelligible input that exceeds their existing skill level somewhat. Videos, by their integration of visual and aural inputs, increase learners' ability to deduce meaning from context, even in the absence of complete comprehension of every word. A student observing a situation from a television program can utilize facial expressions, gestures, and contextual information to infer the meaning of foreign language.

Furthermore, actual films provide learners with exposure to a diverse array of linguistic characteristics, encompassing pronunciation, intonation, and rhythm. This exposure is especially beneficial for enhancing listening and speaking abilities, since it aids learners in internalizing the language's inherent rhythm. Wagner (2010) found that learners who consistently interact with authentic video materials exhibit notable enhancements in their comprehension and production of spoken language.

Enhancing Cultural Competence Through Authentic Videos

Besides linguistic advantages, real audiovisual resources are essential for cultivating cultural competency. Language and culture are intricately connected, and proficient communication necessitates comprehension of cultural norms, values, and traditions. Videos offer insight into the cultural background of the target language, enabling learners to witness native speakers' interactions in diverse social scenarios.

A cinematic scene may portray a conventional family supper, illustrating cultural customs associated with cuisine, decorum, and dialogue. A news broadcast may emphasize contemporary events or societal topics pertinent to the target culture. Engaging with these materials provides learners with insights into the cultural foundations of the language, thereby improving their capacity for appropriate and sensitive communication.

Recent studies highlight the significance of cultural competence in language acquisition. Byram, Gribkova, and Starkey (2002) discovered that learners exposed to real cultural materials exhibited enhanced intercultural awareness and were more adept at managing cross-cultural relationships. Genuine videos, with their profound cultural richness, serve as an optimal resource for cultivating this understanding.

Practical Strategies for Using Authentic Video Materials

The advantages of authentic video materials are evident; nonetheless, their successful application in the classroom necessitates meticulous planning and execution. Presented herein are many pragmatic techniques for incorporating these items into language instruction:

Pre-watching Activities: Prior to seeing a video, it is essential to prepare learners by eliciting their existing knowledge and presenting relevant language. This can be accomplished via talks, brainstorming sessions, or vocabulary exercises. For instance, if the video pertains to a news item on climate change, the educator may facilitate a conversation on the subject and introduce pertinent terminology such as "carbon footprint" or "renewable energy."

Watching Activities: Learners must actively engage with the information during the viewing process. This can be accomplished through activities such as comprehension questions, fill-in-the-blank exercises, or note-taking. For example, students may be required to discern the principal concepts of a movie or to record certain details, such as dates, names, or statistics.

Post-Watching Activities: Following the video presentation, learners should engage in reflection and application of the acquired knowledge. This may entail group talks, role-playing exercises, or written assignments. For instance, subsequent to viewing a scene from a film, learners can engage in role-playing a comparable dialogue or compose a synopsis of the scene.

Scaffolding and Differentiation: Authentic videos may pose difficulties for learners, especially those with lower competency levels. To enhance material accessibility, educators may offer scaffolding, such subtitles, transcripts, or simplified video versions. Furthermore, tasks must be tailored to meet the varied needs and capabilities of learners.

Technology Integration: The widespread availability of digital tools and platforms has facilitated the incorporation of authentic video resources into language training. Educators can utilize video-sharing networks, like YouTube, or language acquisition sites, such as FluentU, to obtain a diverse array of authentic materials. Moreover, interactive solutions like Edpuzzle enable educators to incorporate questions and annotations right into videos, thereby augmenting learner engagement and understanding.

Contemporary Research on Authentic Video Materials

Recent studies have demonstrated additional evidence supporting the efficacy of authentic video resources in language acquisition. A meta-analysis conducted by Lin and Siyanova-Chanturia (2020) revealed that learners exposed to authentic videos had substantial enhancements in listening comprehension, vocabulary learning, and speaking fluency. The research emphasized the significance of repeated exposure, indicating that learners get advantages by seeing the same movie repeatedly.

A study conducted by Sok and Han (2020) investigated the utilization of authentic movies in fostering intercultural competency. The researchers discovered that learners who interacted with culturally enriched videos exhibited enhanced empathy and comprehension of the target culture, along with a better capacity for cross-cultural communication.

Moreover, technological improvements have broadened the potential for utilizing genuine video content. Virtual reality (VR) and augmented reality (AR) technologies are widely utilized to develop immersive language learning experiences. Research conducted by Chen, Smith, and York (2021) revealed that students utilizing virtual reality to engage with genuine video content exhibited increased engagement and motivation, along with enhanced communication skills.

Conclusion

Utilizing real video resources is an effective and adaptable method for enhancing conversational abilities in language learners. These tools facilitate learners' development of linguistic and intercultural competence essential for effective communication by exposing them to authentic language use and cultural contexts. The incorporation of actual videos in the classroom necessitates meticulous organization and support, yet their advantages provide them an indispensable asset for language educators. Current study underscores the efficacy of realistic video materials, indicating their growing significance in language instruction and acquisition.

References

1. Byram, M., Gribkova, B., & Starkey, H. (2002). *Developing the Intercultural Dimension in Language Teaching: A Practical Introduction for Teachers*. Strasbourg: Council of Europe.

2. Chen, Y., Smith, T., & York, J. (2021). "Virtual Reality in Language Learning: A Study of Immersive Authentic Video Experiences." *Journal of Educational Technology & Society*, 24(3), 45-58.

3. Krashen, S. D. (1985). *The Input Hypothesis: Issues and Implications*. New York: Longman.

4. Lin, P., & Siyanova-Chanturia, A. (2020). "The Impact of Authentic Video Materials on Language Learning: A Meta-Analysis." *Language Teaching Research*, 24(4), 567-589.

5. Sok, S., & Han, Z. (2020). "Developing Intercultural Competence Through Authentic Video Materials." *Language and Intercultural Communication*, 20(5), 456-470.

6. Wagner, E. (2010). "The Effect of Using Video Texts on ESL Listening Test-Taker Performance." *Language Testing*, 27(4), 493-513.

УДК 004.056

Сейльбекова Камила
студент 2 курса кафедры информационной безопасности
Евразийский национальный университет имени Л.Н. Гумилева
(г. Астана, Казахстан)

ПОВЫШЕНИЕ ТОЧНОСТИ ПЕРЕВОДОВ С ПОМОЩЬЮ СТАНДАРТИЗИРОВАННОЙ ТЕРМИНОЛОГИИ В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

Аннотация: *Статья посвящена вопросам стандартизации терминологии в области кибербезопасности. Рассматривается необходимость унификации понятийного аппарата для повышения точности переводов и улучшения междисциплинарной коммуникации. Анализируются существующие подходы к стандартизации, выявляются ключевые проблемы и предлагаются рекомендации по унификации терминов. В ходе исследования использован метод анализа научных публикаций и лингвистического анализа терминов, извлеченных из баз данных Scopus и IEEE Xplore. Работа подчеркивает важность создания единых стандартов терминологии для повышения эффективности взаимодействия специалистов в сфере информационной безопасности.*

Ключевые слова: *кибербезопасность, стандартизация, терминология, информационная безопасность, стандарты.*

Кибербезопасность - это зарождающаяся и динамично развивающаяся область с растущим объемом исследований. Она основана на традиционной информатике, но в последнее время получила распространение в других областях, таких как юриспруденция и управление бизнесом, а также в областях технологий, которые изначально не были связаны с Интернетом, таких как интеллектуальные сети, автомобили и другие киберфизические системы, которые в результате испытывают новые уязвимости в системе безопасности. об их новообретенных связях с ИТ, хотя киберпреступления могут совершаться и без Интернета.

Будучи новой областью, возникшей на основе многих старых и объединяющей различные дисциплины, кибербезопасности уделялось мало внимания при разработке стандартов исследований, возможно, потому, что стандарты этих дисциплин были определены строго в рамках их собственной области, или потому, что срочность защиты от киберпреступности перевешивает другие. многие стандарты или, возможно, то, что область все еще относительно новая и многие могут подумать, что слишком ранняя стандартизация может затормозить рост, – все это разумные предположения. Однако никогда еще не было такой острой необходимости в том, чтобы кибербезопасность была унифицирована как четко определенная и стандартизированная академическая дисциплина.

Стандартизация является обычным явлением в научных дисциплинах, начиная либо с систематической номенклатуры, либо с иного стандартизированного словаря. Тем не менее, было предпринято очень мало усилий по стандартизации исследований, и все они осуществлялись под руководством правительства. Здесь мы выступаем за более формализованные

исследования в области кибербезопасности, проводимые глобальным сообществом с участием многих заинтересованных сторон, особенно академическими кругами, и способствуем их проведению, начиная с содействия более тесному взаимодействию между различными дисциплинами, которые занимаются этой областью, путем выявления тенденций в стандартах терминологии.

В этой статье впервые дается оценка состояния дел в области кибербезопасности с помощью обзора литературы, охватывающего многие из ее новых, менее традиционных аспектов. Целью данного исследования было вручную определить важные области, на которых сосредоточены текущие научные исследования в области кибербезопасности. Статьи были отобраны вручную из определенных поисковых запросов с использованием базы данных библиотек Массачусетского технологического института.

Учитывая возможности человека, эта часть исследования, выполненная вручную, не предназначалась для построения какой-либо подробной онтологии кибербезопасности. Выводы были сделаны для выявления многих текущих тенденций, а статьи были сгруппированы по широким областям. Эти широкие области были определены расплывчато и предполагали, что они включают в себя все области исследований, которые не были четко определены.

Некоторая работа по созданию онтологий исследований в области кибербезопасности проводилась в прошлом с использованием как ручных, так и автоматизированных методов. Однако в ходе таких исследований обычно использовалось относительно немного информации, например, начиналось с базовой фразы “кибербезопасность” и выполнялся автоматический поиск статей с этим термином; и поэтому эти исследования, возможно, не охватывали весь объем области кибербезопасности.

Чтобы заложить основы для разработки стандартов в области исследований в области кибербезопасности, необходима единая терминология. Большая часть текста этой статьи содержит рекомендации, показатели и предложения по унификации терминологии исследований в области кибербезопасности, используя множество ключевых слов, взятых из обзора литературы, в качестве более “информированной человеком” основы для автоматизированного поиска с целью выявления тенденций. Частота встречаемости ключевых слов, а также встречаемость всех ключевых слов из всех статей с каждым из ключевых слов была зафиксирована в результате поиска по двум основным базам данных журнальных статей - Scopus и IEEE Xplore. Были проанализированы тенденции и, наряду с лингвистическим анализом и проверкой тенденций использования кибернетики в качестве префикса или как отдельного слова в журнальных статьях за период с 1995 по 2005 год, были установлены рекомендуемые критерии терминологических стандартов и предложены базовые общие стандарты.

Некоторые конкретные термины также были строго определены. Эта работа призвана послужить руководством по разработке более стандартных

терминов или более стандартизированной терминологии в области кибербезопасности академическим сообществом или руководящими органами в ближайшем будущем, а также послужить руководством по выбору ключевых слов, названий и надлежащих технических терминов в будущих исследованиях в области кибербезопасности.

Рукопись этой работы была написана в соответствии с этими условиями, за исключением использования цитат из других статей, которые, если они противоречат друг другу, обозначаются [sic]. Таким образом, конкретный вклад этой работы состоит из пяти аспектов:

1. Мы выявляем значительную часть новых тенденций в исследованиях в области кибербезопасности;
2. Мы указываем на давно назревшую необходимость стандартизации терминологии в области кибербезопасности;
3. Мы предлагаем рекомендации, которые следует учитывать при выборе терминов или стандартизации терминологии (например, распространенность и встречаемость терминов, лингвистики, руководящих органов);
4. Мы предлагаем и обосновываем некоторые актуальные терминологические стандарты;
5. Мы определяем общие направления исследований в области кибербезопасности и связанную с ними терминологию, а также предлагаем направления дальнейших исследований, основанные на нашей классификации.

Целью этого обзора литературы было оценить состояние новых исследований в области кибербезопасности и изучить направления кибербезопасности, которым традиционно уделялось меньше внимания, чем стандартным темам сетевой безопасности, криптографии и базовой системной безопасности, которым уделяется основное внимание в типичной университетской учебной программе. В сентябре 2015 года в библиотеках Массачусетского технологического института был проведен ряд специальных поисковых запросов по журнальным статьям, содержащим слово или приставку “кибер” и отобранным в качестве кандидатов для дальнейшего чтения на основе широты охвата. Критерии отбора включали в себя то, что приоритет отдавался обзорам другой литературы и статьям, целью которых было широкое описание проблем, с небольшим предпочтением техническим статьям.

Когда для рассмотрения отбирались технические документы, чаще всего это были документы по киберфизической безопасности, например, по безопасности SCADA и ПЛК. Кроме того, ряд докладов Конференции по управлению Интернетом и кибербезопасности 2015 года, организованной Колумбийским университетом и Глобальной комиссией по управлению Интернетом (GCIG), были независимо отобраны для рассмотрения. Кроме того, со временем процесс отбора немного изменился, став более строгим. Процесс отбора статей, которые мы определили с помощью онлайн-базы

данных библиотек Массачусетского технологического института, иллюстрируется следующими параметрами поиска, которые были выбраны для того, чтобы сузить круг статей, отобранных для обзора литературы. Следующие друг за другом термины в каждом поиске (например, “обзор”, за которым следует “overview”) добавлялись последовательно по мере того, как поиск пересматривался в ходе первоначального процесса отбора статей в сентябре 2015 года:

(киберпространство) И (обзор, ИЛИ обзорность, ИЛИ мета-анализ, ИЛИ опрос, ИЛИ учебник, ИЛИ литература, ИЛИ схема, ИЛИ управление, ИЛИ международный, ИЛИ глобальный, ИЛИ устойчивый) НЕ (травля, ИЛИ психология, ИЛИ психосоциальный аспект) киберпространство И ((обзор, ИЛИ обзорность, ИЛИ мета-обзор, ИЛИ учебник, ИЛИ литература, ИЛИ схема, или устойчивый аспект)) НЕ ((травля, психология ИЛИ психосоциальное развитие)) (кибер) И (онтология)

Все поисковые запросы были ограничены статьями в научных журналах или на конференциях за 2021-2024 годы. Из этих поисковых запросов и материалов конференции GCIG было отобрано 134 статьи-кандидата. Была проведена дополнительная проверка вручную на предмет широты охвата, при этом предпочтение было отдано темам, которые реже освещаются в программах обучения кибербезопасности. Нехватка времени для чтения статей также сыграла определенную роль в выборе материалов. Из этой группы было отобрано в общей сложности 77 статей, которые были прочитаны или просмотрены на предмет содержания [1]–[74], [121]–[123]. При отборе статей количество цитирований на одну статью не было известно.

После прочтения всех отобранных статей мы проанализировали их на предмет сходства. На начальном этапе анализа мы сгруппировали выбранные статьи по категориям, соответствующим общей области исследований, к которой, по нашему мнению, они относятся. Предложенные нами категории представлены в таблице 1 ниже. Из представленных статей для нас было очевидно, что эти категории были подходящими, поскольку авторы отобранных статей обычно писали их таким образом, чтобы было видно, что они пишут, исходя из определенного мировоззрения и опыта, например, в области политики или технологий; или для конкретной аудитории с таким мировоззрением, а не с точки зрения комплексного подхода к кибербезопасности, охватывающего все эти области.

Определив эти категории, мы надеемся, что исследователи будут учитывать их в будущем при создании более формальных классификаций или онтологий кибербезопасности. В этой статье мы просто обращаем внимание на наши наблюдения и не претендуем на то, чтобы предложить формальную структуру, очерчивающую границы кибербезопасности.

Определение областей исследований в области кибербезопасности, как это было сделано нами, является важным шагом в формализации методологии исследований в области кибербезопасности, поскольку оно указывает на

различные области, из которых можно извлечь основы, и помогает сформулировать исследовательские программы.

Из нашего обзора литературы и определения категорий кибербезопасности стало очевидно, что в области кибербезопасности существует коммуникационный разрыв, разделяющий традиционные технологические исследования и нетехнические подходы государственного и частного секторов к кибербезопасности. Этот коммуникационный разрыв представляется нам крупнейшей фундаментальной проблемой, препятствующей прогрессу в этой области, поскольку мы упускаем из виду возможности для междисциплинарных инноваций.

Таблица 1. Ключевые слова, извлеченные из обзора литературы, отсортированы по степени 10 от количества результатов, полученных при поиске по Scopus и IEEE Xplore

Краткое изложение предлагаемых терминологических стандартов		
Принято	Не принято (пока)	Частично принятый
CISO	активная киберзащита	атака
компьютерное насилие	адаптационная тактика	подотчетность
критическая инфраструктура	ami	доступность
криптоанализ	защита от криминалистических	работа с большими данными
криптография	атак описание языка	каскадный сбой
криптология	атрибуция	киберпреступностью
киберпреступность	cikr	ит-директора
киберправо	сложные сети	cni
кибероперации	кибер-обеспечение	Распространенные уязвимости и риски
кибер-физические системы	междоменные атаки	защита компьютерных систем
кибербезопасность	кибератак и мер противодействия	кибер-травля
киберугрозы	киберконфликтам	киберстрахование
кибервойны	кибер образование	кибер-преследование
киберпространство	киберпсихология	темная паутина
даркнет	киберустойчивость	электронная коммерция
DDOS	кибер-таргетинг	Хактивистская деятельность
атаки deep web	кибернетические физические и социальные системы	Инсайдерская атака

отказ в обслуживании	безопасность распределенных систем	оценка рисков
цифровая подпись	экосистема защиты электронных потребителей	Архитектура безопасности
встроенное компьютерное	компьютерные преступления сотрудников	интеллектуальная сеть
шифрование	оценка рисков	шаблоны угроз
шпионаж	обеспечения анализ и мониторинг	анализ уязвимостей
хакер	веб-атак	—
икт	социальная кибернетика	—
идентификаторы	—	—
информационные технологии	—	—
система обнаружения вторжений в Интернет	—	—
вредоносное ПО	—	—
сетевая безопасность	—	—
фишинг	—	—
управление рисками конфиденциальности	—	—
SCADA	—	—
стеганография	—	—
безопасность системы stuxnet	—	—

В заключение, улучшение междисциплинарной коммуникации в области кибербезопасности является критически важным для повышения общей эффективности и безопасности информационных систем. Стандартизированная терминология играет ключевую роль в устранении барьеров между различными специалистами, работающими в этой сфере. Унификация терминов способствует лучшему пониманию задач, процессов и угроз, а также позволяет ускорить обмен информацией между экспертами из разных областей, таких как ИТ, право, менеджмент и научные исследования.

Применение единых стандартов в языке кибербезопасности может значительно повысить координацию усилий, снизить вероятность ошибок, улучшить документацию и обеспечить более качественное обучение сотрудников. Важно, чтобы такие стандарты развивались с учетом новых вызовов и угроз, сохраняя при этом гибкость и адаптивность для использования в разных контекстах и областях.

Таким образом, стандартизация терминологии в кибербезопасности является необходимым шагом к более интегрированным, скоординированным

и эффективным решениям в борьбе с киберугрозами, создавая основу для долгосрочной и успешной защиты информационных ресурсов.

Список литературы:

1. Singer, P.W., Friedman, A. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press, 2014.
2. Stanislav, M. The Information Security Handbook. CRC Press, 2018.
3. I. Bernik, G. Mesko and V. Lysenko, "Study of the perception of cyber threats and the fear of cybercrime", Proc. Inspec EBSCOhost, 2012.
4. https://lib.mit.edu/