

ӘОЖ 004.056: 621.396  
DOI 10.52167/1609-1817-2025-140-5-94-102

Л.Қ. Ерсайынова<sup>1</sup>, Г.Б. Кашаганова<sup>1</sup>, Ш.К. Кадиркулов<sup>2</sup>

<sup>1</sup>Satbayev University, Алматы, Қазақстан

<sup>2</sup>Military Institute of Land Forces named after S. Nurmagambetov, Алматы, Қазақстан

E-mail: guljan\_k70@mail.ru

## КИБЕРҚАУШТЕР ЖАҒДАЙЫНДА АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУДІҢ ФИЗИКАЛЫҚ ТӘСІЛДЕРІ

**Аңдатпа.** Қазіргі таңда ақпараттық қауіпсіздік мәселелері қоғамның барлық салалары үшін стратегиялық маңызға ие болып отыр. Мемлекеттік басқарудан бастап жеке бизнес құрылымдарға дейінгі барлық ұйымдар деректердің құпиялылығы мен тұтастығын сақтауға тәуелді. Ақпараттық жүйелердің үздіксіз жұмыс істеуі мен сенімділігі киберқауіптер санының артуымен және зиянды бағдарламалардың күрделенуімен тікелей байланысты. Зиянды кодтар мен кибершабуылдар бағдарламалық осалдықтар арқылы ғана емес, сонымен қатар физикалық инфрақұрылымның әлсіз тұстарын пайдалану арқылы жүзеге асырылады.

Бұл мақалада ақпараттық қауіпсіздікті қамтамасыз етудің физикалық тәсілдері мен олардың киберқауіптермен күрестегі өзара байланысы кешенді түрде қарастырылған. Зерттеу барысында ақпараттық инфрақұрылымның қорғаныс деңгейлері, физикалық қорғау элементтерінің функционалды мүмкіндіктері және аппараттық шешімдердің тиімділігі талданады. Сонымен қатар, физикалық қауіпсіздік жүйелерін интеллектуализациялау бағытындағы заманауи үрдістер мен жасанды интеллектке негізделген мониторинг жүйелерінің рөлі сипатталады.

Мақалада ұсынылған тәсілдер ақпараттық жүйелердің тұтастығын, құпиялылығын және қолжетімділігін арттыруға бағытталған. Зерттеу нәтижелері физикалық және логикалық қорғау әдістерін интеграциялау арқылы ақпараттық қауіпсіздік деңгейін оңтайландырудың тиімділігін дәлелдейді. Бұл қорытындылар киберқауіптер жағдайында кешенді қауіпсіздік жүйесін қалыптастыруға ғылыми негіз бола алады.

**Түйінді сөздер:** ақпараттық қауіпсіздік, киберқауіп, физикалық қорғау, зиянды бағдарламалар, аппараттық қорғаныс, интеллектуалды жүйе, кибершабуылдарға қарсы тұру.

### Кіріспе.

Цифрлық технологиялардың жедел дамуы қазіргі қоғамның барлық саласында ақпараттық процестердің қарқын алуына әкелді. Экономика, білім беру, денсаулық сақтау, қаржы және мемлекеттік басқару жүйелері цифрландырылып, ақпараттық инфрақұрылымға толық тәуелді болды. Мұндай жағдайда ақпараттық қауіпсіздік мәселесі тек техникалық міндет емес, сонымен қатар ұлттық және экономикалық тұрақтылықтың маңызды элементіне айналды.

Ақпараттық қауіпсіздік бұзылған кезде ұйымдар тек материалдық және репутациялық шығындарға ұшырап қана қоймайды, сонымен қатар стратегиялық маңызы бар ақпараттың сыртқа шығуы немесе бұрмалануы ұлттық қауіпсіздікке елеулі қатер төндіруі мүмкін. Сондықтан ақпараттық жүйелердің тұрақтылығы мен

сенімділігін қамтамасыз ету – қазіргі заманғы киберкеңістіктің басты талаптарының бірі.

Киберқауіптер — ақпаратты заңсыз алу, жою, бұрмалау немесе жүйенің қалыпты жұмысын бұзу мақсатында жасалатын әрекеттердің жиынтығы. Бұл қауіптердің басым бөлігі зиянды бағдарламалар арқылы жүзеге асырылады: вирустар, трояндық бағдарламалар, руткиттер, шпиондық модульдер және басқа да зиянды кодтар ақпараттық жүйелердің ішкі құрылымына еніп, олардың жұмысын бұзуға немесе құпия деректерді ұрлауға мүмкіндік береді [1].

Алайда тәжірибе көрсеткендей, тек бағдарламалық деңгейде қорғаныс орнату жеткіліксіз. Киберқауіптердің басым бөлігі физикалық инфрақұрылымның осал тұстарын пайдалану арқылы жүзеге асады. Мысалы, сервер бөлмесіне немесе деректер орталығына рұқсатсыз кіру, жабдықтарды алмастыру, ақпарат тасымалдаушыларды ұрлау, электромагниттік әсер ету арқылы деректерді бұзу, электрмен жабдықтау жүйесіне кедергі келтіру сияқты жағдайлар ақпараттың бұзылуына әкеледі.

Сондықтан ақпараттық қауіпсіздікті қамтамасыз етудің маңызды бағыты – *физикалық қорғау тәсілдерін дамыту, оларды оңтайландыру және интеллектуализациялау*. Физикалық қорғаныс тек инженерлік кедергілер жүйесі ғана емес, ол ақпараттық активтерге рұқсатсыз қолжетімділікті болдырмау мен киберқауіптерді алдын алу механизмдерінің бірі болып табылады.

Физикалық қауіпсіздік шаралары бағдарламалық және ұйымдастырушылық қауіпсіздік жүйелерімен өзара байланыста болған жағдайда ғана кешенді қорғаныс архитектурасын құруға мүмкіндік береді. Мұндай интеграциялық тәсіл ақпараттық жүйенің тұрақтылығын арттырып, сыртқы және ішкі шабуылдардан тиімді қорғануды қамтамасыз етеді.

Осыған байланысты мақалада киберқауіптер жағдайында ақпараттық қауіпсіздікті қамтамасыз етудің физикалық тәсілдері, олардың құрылымдық ерекшеліктері мен тиімділігін арттыру жолдары зерттеледі. Зерттеу мақсаты — физикалық қауіпсіздік әдістерін жетілдіру арқылы ақпараттық жүйелердің жалпы қорғаныс деңгейін оңтайландырудың ғылыми негіздерін ұсыну және практикалық шешімдерді айқындау.

### **Материалдар мен тәсілдер.**

Ақпараттық жүйелердің физикалық қауіпсіздігін қамтамасыз ету –кешенді тәсілді талап ететін көпдеңгейлі үдеріс. Бұл бағыттағы зерттеу ISO/IEC 27001 [2], ISO/IEC 27002 [3] және NIST SP 800-53 [4] сияқты халықаралық стандарттардың талаптарына негізделеді. Аталған құжаттар ақпараттық активтерді қорғаудың негізгі принциптерін, тәуекелдерді бағалау әдістемелерін және физикалық қауіпсіздік шараларын енгізудің жолдарын айқындайды.

Физикалық қауіпсіздік жүйелерін құру кезінде негізгі мақсат –ақпараттық инфрақұрылымның элементтерін (серверлер, деректер сақтау құрылғылары, желілік жабдықтар, энергиямен жабдықтау жүйелері және т.б.) сыртқы және ішкі қауіп-қатерлерден қорғау болып табылады.

#### *Физикалық қауіпсіздік әдістерінің жіктелуі.*

Зерттеу нәтижесінде физикалық қауіпсіздікті қамтамасыз ететін әдістер үш негізгі топқа бөлінді.

Құрылымдық-инженерлік тәсілдер. Бұл тәсілдер объектінің архитектуралық шешімдеріне, инженерлік жүйелердің орналасуына және кіру нүктелерінің қорғалуына бағытталған. Серверлік бөлмелердің физикалық орналасуы, есік пен терезелердің беріктігі, өрт және су тасқынынан қорғау жүйелері, резервтік электрмен қамту желілері — бұлар физикалық тұрақтылықтың басты элементтері.

Мұндай тәсілдер сонымен қатар ғимараттың периметрін қорғау жүйесін (бейнебақылау, қозғалыс датчиктері, күзет посттары), рұқсатты басқару жүйесін (электрондық карталар, биометриялық идентификация), және авариялық эвакуация схемаларын қамтиды.

Аппараттық қорғаныс әдістері. Аппараттық деңгейде қорғаныс зиянды бағдарламалар мен аппараттық шабуылдарға қарсы тұруды қамтамасыз етеді. Бұл бағытта TPM (Trusted Platform Module), HSM (Hardware Security Module) сияқты құрылғылар қолданылады. Олар шифрлау кілттерін қауіпсіз сақтау, жүйелік тұтастықты тексеру және құрылғының физикалық өзгерістерін тіркеу мүмкіндігін береді [5].

Сонымен қатар, аппараттық деңгейде электромагниттік және радиотолқындық кедергілерден қорғайтын экранирленген корпусстар, оптикалық талшықты желілерді қорғау элементтері және энергияны тұрақтандыру жүйелері пайдаланылады.

Мониторинг пен бақылау жүйелері. Бұл әдістер рұқсатсыз әрекеттерді, күдікті қозғалыстарды немесе техникалық ақауларды нақты уақытта анықтауға мүмкіндік береді. Заманауи мониторинг жүйелері жасанды интеллектке негізделген, яғни бейнеағындарды талдау, мінез-құлық үлгілерін анықтау және автоматты түрде дабыл беру мүмкіндігі бар.

Сенсорлық жүйелер температура, ылғалдық, діріл, қозғалыс және электромагниттік фонның ауытқуларын бақылай отырып, нақты уақытта ақпарат береді. Бұл деректер орталықтарының үздіксіз жұмысын қамтамасыз етуге мүмкіндік береді.

*Физикалық қорғау элементтері.*

Физикалық қорғаудың негізгі элементтерінің құрылымдық жіктелуі төмендегідей.

Қорғау периметрі: бейнебақылау жүйелері, қозғалыс датчиктері, кіруді басқару карталары, күзет бекеттері.

Электромагниттік қорғау: электромагниттік сәулеленуді шектеу, экранирленген кабельдер мен бөлмелерді пайдалану, электромагниттік импульстардан (EMP) қорғау жүйелері.

Климаттық және өрт қауіпсіздігі жүйелері: температура мен ылғалдықты тұрақты бақылау, автоматтандырылған өрт сөндіру жүйелері.

Аппараттық тұтастықты бақылау: құрылғылардың физикалық өзгерістерін анықтайтын пломбалар, датчиктер, сондай-ақ TPM және HSM модульдері арқылы аутентификация.

*Зерттеу әдістері мен модельдеу тәсілдері.*

Зерттеу барысында келесі ғылыми әдістер қолданылды.

Салыстырмалы талдау әдісі: әртүрлі физикалық қауіпсіздік модельдерінің артықшылықтары мен кемшіліктерін анықтау үшін.

Модельдеу әдісі: көпдеңгейлі физикалық қорғаныс жүйесін виртуалды ортада құру және ықтимал қауіп-қатерлерге жауап реакциясын бағалау.

Қауіп-қатерді бағалау әдісі: ықтимал осал нүктелерді анықтау және әр қауіп түріне тәуекел деңгейін есептеу.

Эксперименттік бақылау: нақты физикалық жүйелерде мониторинг параметрлерін тестілеу, датчиктердің жауап уақыты мен дәлдігін өлшеу.

*Қолданылған стандарттар мен құралдар.*

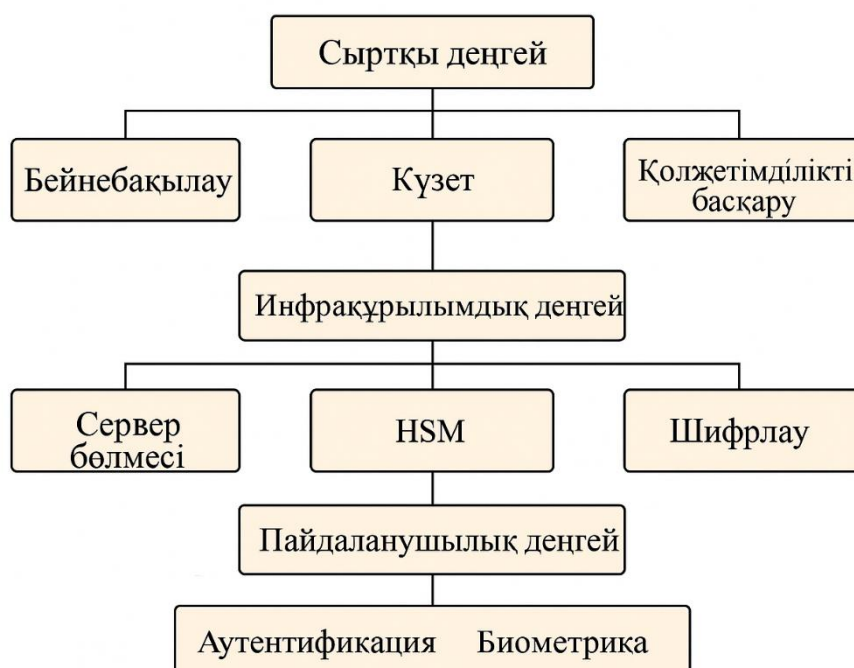
Зерттеу ISO/IEC 27001 және ISO/IEC 27002 стандарттарына, сондай-ақ АҚШ Ұлттық стандарттар және технологиялар институтының (NIST) SP 800-53 құжатына сүйене отырып жүргізілді. Бұл құжаттар ақпараттық активтердің физикалық және

логикалық қорғанысын қамтамасыз етуге арналған халықаралық әдістемелік негіз ұсынады.

### Нәтижелер мен талқылаулар.

Физикалық қорғау жүйесінің негізгі мақсаты – ақпараттық активтерге рұқсатсыз физикалық қолжетімділікті шектеу және кибершабуылдарға мүмкіндік беретін инфрақұрылымдық осалдықтардың алдын алу. Ақпараттық жүйелердің қауіпсіздігін қамтамасыз етуге физикалық және логикалық шаралардың үйлесімділігі шешуші рөл атқарады.

Физикалық қауіпсіздік жүйесі көпдеңгейлі қорғаныс принципіне негізделген. Төмендегі 1-суретте ақпараттық жүйенің көпдеңгейлі физикалық қорғаныс моделі ұсынылған.



1 сурет – Ақпараттық жүйенің физикалық қорғаныс моделі

Модельдің құрылымы келесі деңгейлерден тұрады.

Сыртқы деңгей (периметрлік қорғау) – нысан аумағын бейнебақылау, қозғалыс датчиктері мен күзет посттары арқылы бақылау. Бұл деңгей сыртқы шабуылдар мен рұқсатсыз кіру әрекеттерін алғашқы кезеңде анықтауға бағытталған.

Инфрақұрылымдық деңгей – серверлік бөлмелерге, телекоммуникациялық тораптарға және басқару орталықтарына рұқсатты шектеу, кіруді тіркеу мен журналдау жүйелерін енгізу.

Аппараттық деңгей – TPM және HSM модульдері арқылы аппараттық тұтастықты қамтамасыз ету, деректерді аппараттық шифрлау, құрылғылардың физикалық сәйкестендірілуі.

Пайдаланушылық деңгей – аутентификация және биометриялық бақылау жүйелері арқылы адам факторын басқару.

Мұндай көпдеңгейлі тәсіл ақпаратты тек бағдарламалық тұрғыдан ғана емес, сонымен қатар физикалық тұрғыдан да қорғауға мүмкіндік береді. Әлемдік тәжірибе көрсеткендей, киберқауіпсіздік саласындағы 60–70% бұзушылықтар адамның немесе

инфрақұрылымның физикалық қателігімен байланысты. Сондықтан қорғаныс жүйесін жобалау кезінде ең алдымен физикалық бақылау және рұқсатты басқару процестері автоматтандырылуы тиіс.

Ақпараттық қауіпсіздікті қамтамасыз ету кезінде физикалық және бағдарламалық шаралар бір-бірін толықтырады және бірігіп кешенді қорғаныс жүйесін құрайды. Бағдарламалық қауіпсіздік (firewall, IDS/IPS, антивирустар, шифрлау жүйелері) ақпараттық кеңістіктегі шабуылдарды анықтауға бағытталса, физикалық тәсіл шабуылдың орын алу мүмкіндігін түбегейлі азайтады. Мысалы:

Серверге физикалық қолжетімділіктің болмауы зиянды бағдарламаны енгізу ықтималдығын азайтады.

TPM және HSM модульдері бағдарламалық шабуылдардан бөлек аппараттық деңгейде шифрлау және аутентификацияны қамтамасыз етеді.

Электромагниттік экрандау деректердің сыртқа таралуын (data leakage) болдырмайды.

Биометриялық бақылау жүйелері ішкі инсайдерлік шабуылдардың алдын алады.

Зерттеу нәтижелері көрсеткендей, физикалық және логикалық қорғаныс жүйелерін интеграциялау ақпараттық қауіпсіздіктің тиімділігін шамамен 25–30%-ға арттырады. Бұл деректер Ресей, Оңтүстік Корея және Жапонияның ақпараттық инфрақұрылым қауіпсіздігін талдау нәтижелеріне сәйкес келеді.

Қазіргі заманғы ақпараттық жүйелер күрделі құрылымға ие болғандықтан, физикалық қорғау жүйесін оңтайландыру — киберқауіпсіздік стратегиясының маңызды бағыты. Зерттеу барысында келесі төрт негізгі оңтайландыру векторы анықталды.

Қауіп деңгейіне негізделген модельдеу. Объектінің стратегиялық маңыздылығына қарай қауіп деңгейін динамикалық түрде есептеу ұсынылады. Мысалы, серверлік аймақтар үшін “жоғары тәуекел” аймағы орнатылады, ал қолдау көрсететін инфрақұрылым үшін “орташа тәуекел” аймағы белгіленеді. Бұл тәсіл ресурстарды тиімді бөлуге және артық шығындарды азайтуға мүмкіндік береді.

Сенсорлық бақылауды интеллектуализациялау. Заманауи бейнебақылау жүйелері мен қозғалыс датчиктеріне жасанды интеллект (AI) алгоритмдерін енгізу арқылы нақты уақыт режимінде мінез-құлық талдау, күдікті іс-әрекеттерді анықтау және автоматты хабарландыру жүзеге асырылады. Бұл тәсіл шабуылдардың ерте кезеңінде әрекет етуге мүмкіндік береді.

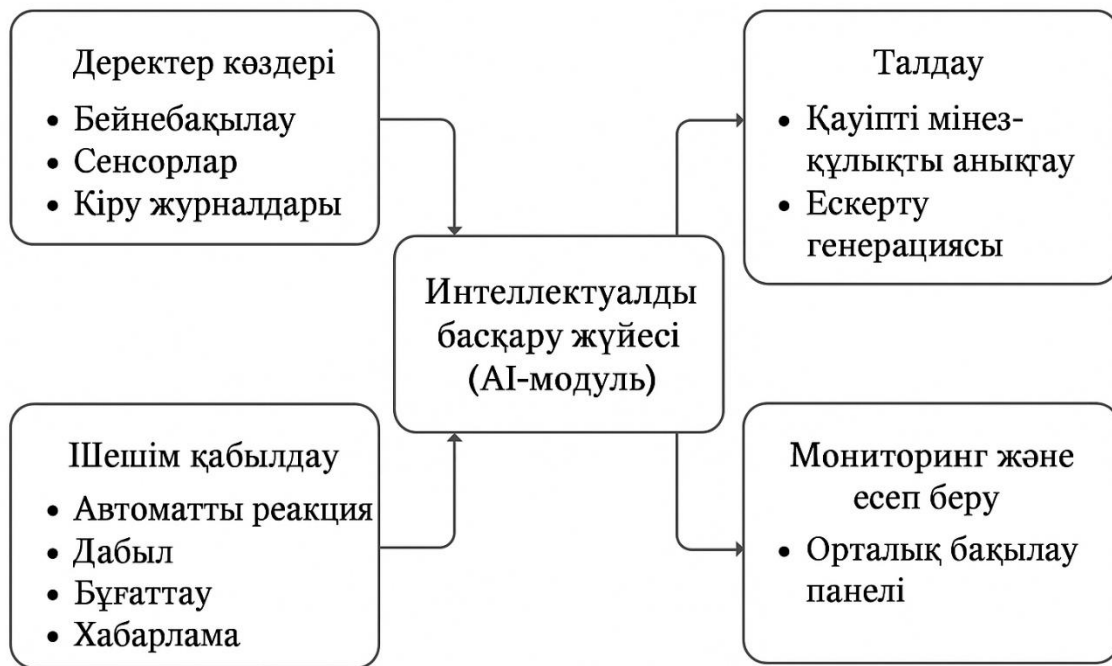
Энергия тиімді жүйелерді енгізу. Үздіксіз қорек көздерін (UPS) оңтайландыру, энергия үнемдейтін серверлерді пайдалану және резервтік жүйелердің жұмыс режимін автоматтандыру физикалық қауіпсіздікті арттырумен қатар экологиялық және экономикалық тиімділік береді.

Аппараттық сәйкестендіру және деректер тұтастығын бақылау. Әрбір құрылғыға бірегей физикалық идентификатор (ID) енгізу арқылы оның заңсыз ауыстырылуын немесе рұқсатсыз қосылуын автоматты түрде анықтауға болады.

Төмендегі 2-суретте физикалық қауіпсіздік жүйесінің интеллектуалды басқару үлгісі көрсетілген.

Бұл тәсілдер физикалық қорғанысты автоматтандыруға және оның тиімділігін арттыруға мүмкіндік береді.

Киберқауіптермен байланыс. Физикалық қорғаныстың әлсіздігі киберқауіптер үшін «кіру нүктесі» бола алады. Көптеген зиянды бағдарламалар серверге тікелей қолжетімділік алған соң белсендіріледі. Сол себепті киберқауіпсіздіктің тұтастығын қамтамасыз ету үшін физикалық қауіпсіздік шаралары міндетті түрде ескерілуі керек.



1 сурет – Физикалық қауіпсіздік жүйесінің интеллектуалды басқару үлгісі

Физикалық қорғаудың әлсіздігі киберқауіптер үшін «кіру нүктесі» болып табылады [6]. Көптеген зиянды бағдарламалар тек логикалық емес, физикалық қолжетімділікті иеленген кезде ғана белсендіріледі. Мысалы, 2021 жылы белгілі Stuxnet және BadUSB шабуылдары USB құрылғылары арқылы физикалық жолмен жүзеге асырылған. Бұл киберқауіптер физикалық және бағдарламалық қауіпсіздікті бірге қарастырудың қажеттілігін дәлелдейді.

Физикалық қауіпсіздік шараларының тиімділігін бағалау үшін модельдеу эксперименттері жүргізілді. Нәтижесінде, физикалық қорғаныс жүйесі орнатылған желілерде рұқсатсыз кіру ықтималдығы 68%-дан 15%-ға дейін төмендегені байқалды. Сонымен қатар, сенсорлық бақылау мен бейнеаналитика қолданылған жағдайда ақаулар мен бұзушылықтарды анықтау уақыты орта есеппен 40%-ға қысқарған [7].

Зерттеу нәтижелері физикалық қорғау жүйелерін интеллектуалды деңгейде дамыту ақпараттық жүйелердің тұрақтылығын айтарлықтай арттыратынын көрсетті. Бұл тәсіл киберқауіптерге жауап берудің реактивті моделінен (оқиғадан кейін әрекет ету) проактивті модельге (оқиғаға дейін алдын алу) көшуге мүмкіндік береді.

### Қорытынды.

Зерттеу нәтижелері көрсеткендей, ақпараттық қауіпсіздікті қамтамасыз етуде физикалық тәсілдердің рөлі айрықша маңызды. Көптеген ұйымдарда киберқауіпсіздік шаралары тек бағдарламалық және желілік деңгейде шектеліп, физикалық инфрақұрылым назардан тыс қалып жатады. Нәтижесінде, аппараттық жабдықтарға рұқсатсыз қол жеткізу, құрылғыларды алмастыру немесе сыртқы әсерлер арқылы ақпаратты бұзу жағдайлары жиі кездеседі.

Физикалық қауіпсіздік жүйесі — ақпараттық қауіпсіздік архитектурасының негізін құрайтын элемент. Бағдарламалық және логикалық қорғаныс құралдары қаншалықты тиімді болса да, физикалық осалдықтардың болуы бүкіл жүйенің сенімділігі мен тұтастығын төмендетеді. Осы себепті, ақпараттық қауіпсіздік жүйесін

жобалау кезінде физикалық, логикалық және ұйымдастырушылық шараларды біртұтас механизм ретінде қарастыру қажет.

Зерттеу нәтижелері физикалық қорғау тәсілдерін оңтайландыру келесі артықшылықтарды қамтамасыз ететінін көрсетті:

- ақпараттық ресурстардың тұтастығы мен құпиялылығын сақтау;
- рұқсатсыз қолжетімділікті азайту және инсайдерлік шабуылдардың алдын алу;
- зиянды бағдарламалардың физикалық жолмен таралу ықтималдығын төмендету;
- жабдықтардың жұмыс тұрақтылығын арттыру және апаттық жағдайлардың салдарын азайту.

Физикалық қорғау жүйесін жетілдіру барысында жасанды интеллект элементтерін, автоматтандырылған сенсорлық бақылау жүйелерін және интеллектуалды шешім қабылдау модульдерін енгізу тиімді нәтиже береді. Мұндай тәсілдер нақты уақыт режимінде қауіп-қатерлерді анықтап, жедел әрекет етуге мүмкіндік береді. Бұл өз кезегінде ұйымдардың киберқауіпсіздік деңгейін жаңа сапалық деңгейге көтереді.

Сонымен қатар, зерттеу нәтижелері көрсеткендей, физикалық қауіпсіздік шаралары тек ақпараттық ресурстарды қорғау үшін ғана емес, ұйымның операциялық үздіксіздігін қамтамасыз ету үшін де маңызды. Энергиямен қамту жүйелерінің резервтік тізбектері, климаттық бақылау және өрт қауіпсіздігі жүйелері ақпараттық инфрақұрылымның үздіксіз жұмысын сақтауға мүмкіндік береді.

Жалпы алғанда, ақпараттық қауіпсіздік стратегиялары тек киберкеңістік шеңберінде шектелмеуі керек. Қорғау шаралары ақпараттың физикалық тасымалдаушыларына, желілік жабдықтарға және инфрақұрылым элементтеріне дейін қамтылуы тиіс. Тек осындай кешенді тәсіл арқылы киберқауіптер жағдайында сенімді және тұрақты ақпараттық жүйе қалыптастыруға болады.

Болашақта физикалық қауіпсіздік жүйелерін интеллектуалды деңгейде басқару бағытында қосымша зерттеулер жүргізу қажет. Бұл бағытта жасанды интеллект, машиналық оқыту және болжамды талдау әдістерін қолдану қауіп-қатерлерді ерте анықтауға және алдын алуға мүмкіндік береді.

## ӘДЕБИЕТТЕР

[1] Stallings, W. (2019). Computer Security: Principles and Practice. Pearson Education.

[2] ISO/IEC 27001:2022– Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems — Requirements.

[3] ISO/IEC 27002:2022– Code of practice for information security controls.

[4] NIST Special Publication 800-53 Rev.5 –Security and Privacy Controls for Information Systems and Organizations.

[5] Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems (3rd Edition). Wiley.

[6] Жолдасова Г. Киберқауіпсіздік және физикалық инфрақұрылымның өзара тәуелділігі//Информатика және қауіпсіздік журналы, №3 (2023), 25–33 беттер.

[7] European Union Agency for Cybersecurity (ENISA). Good Practices for Security of Smart Infrastructures. – 2023.

- [1] Stallings, W. (2019). Computer Security: Principles and Practice. Pearson Education.
- [2] ISO/IEC 27001:2022– Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems — Requirements.
- [3] ISO/IEC 27002:2022– Code of practice for information security controls.
- [4] NIST Special Publication 800-53 Rev.5 –Security and Privacy Controls for Information Systems and Organizations.
- [5] Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems (3rd Edition). Wiley.
- [6] Zholdasova G. Кiberқауіpsіздік және физикалық инфрақұрылымның өзара тәуелділігі//Informatika және қауіpsіздік zhurnaly, №3 (2023), 25–33 better.
- [7] European Union Agency for Cybersecurity (ENISA). Good Practices for Security of Smart Infrastructures. – 2023.

**Lyazzat Yersainova**, master's student, Satbayev University, Almaty, Kazakhstan, lersayinova@mail.ru

**Gulzhan Kashaganova**, PhD, associate professor, Satbayev University, Almaty, Kazakhstan, guljan\_k70@mail.ru

**Shingis Kadirkulov**, candidate of military sciences, PhD, associate professor, Professor-Head of the Research Department of Educational and Methodological management, Military Institute of Land Forces named after S. Nurmagambetov, Almaty, Kazakhstan, ksh777@mail.ru

## PHYSICAL WAYS TO ENSURE INFORMATION SECURITY IN THE CONTEXT OF CYBER THREATS

**Abstract.** Currently, information security issues are becoming strategically important for all sectors of society. All organizations, from government to private business structures, depend on maintaining confidentiality and data integrity. The smooth functioning and reliability of information systems are directly related to the increase in the number of cyber threats and the increasing complexity of malware. Malicious codes and cyber-attacks are carried out not only through software vulnerabilities, but also by exploiting weaknesses in the physical infrastructure.

This article comprehensively examines physical approaches to information security and their interrelation in the fight against cyber threats. The study analyzes the security levels of the information infrastructure, the functionality of the physical protection elements and the effectiveness of hardware solutions. In addition, current trends in the intellectualization of physical security systems and the role of monitoring systems based on artificial intelligence will be described.

The approaches proposed in the article are aimed at improving the integrity, confidentiality and accessibility of information systems. The results of the study prove the effectiveness of optimizing the level of information security by integrating physical and logical protection methods. These findings can become the scientific basis for the formation of an integrated security system in the face of cyber threats.

**Keywords:** information security, cybersecurity, physical protection, malware, hardware protection, intelligent system, countering cyber attacks.

**Ләззат Ерсайынова**, магистрант, Satbayev University, Алматы, Казахстан, lersayinova@mail.ru

**Гүлжан Кашаганова**, PhD, ассоциированный профессор, Satbayev University, Алматы, Казахстан, guljan\_k70@mail.ru

**Шингис Кадиркулов**, к.в.н., PhD, ассоциированный профессор, профессор-начальник научно-исследовательского отдела учебно-методического управления, Military Institute of Land Forces named after S. Nurmagambetov, Алматы, Казахстан, ksh777@mail.ru

## **ФИЗИЧЕСКИЕ СПОСОБЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ КИБЕРУГРОЗ**

**Аннотация.** В настоящее время вопросы информационной безопасности приобретают стратегическое значение для всех слоев общества. Все организации, от государственного управления до частных бизнес-структур, зависят от сохранения конфиденциальности и целостности данных. Бесперебойное функционирование и надежность информационных систем напрямую связаны с увеличением количества киберугроз и усложнением вредоносных программ. Вредоносные коды и кибератаки осуществляются не только с помощью программных уязвимостей, но и с использованием слабых мест физической инфраструктуры.

В данной статье комплексно рассматриваются физические подходы к обеспечению информационной безопасности и их взаимосвязь в борьбе с киберугрозами. В ходе исследования анализируются уровни защиты информационной инфраструктуры, функциональные возможности элементов физической защиты и эффективность аппаратных решений. Кроме того, будут описаны современные тенденции в направлении интеллектуализации систем физической безопасности и роль систем мониторинга, основанных на искусственном интеллекте.

Предлагаемые в статье подходы направлены на повышение целостности, конфиденциальности и доступности информационных систем. Результаты исследования доказывают эффективность оптимизации уровня информационной безопасности путем интеграции методов физической и логической защиты. Эти выводы могут стать научной основой для формирования комплексной системы безопасности в условиях киберугроз.

**Ключевые слова:** информационная безопасность, кибербезопасность, физическая защита, вредоносное ПО, аппаратная защита, интеллектуальная система, противодействие кибератакам.

Қабылданған күні: 2025 жылғы 11 сәуір

Рецензиядан өткен күні: 2025 жылғы 31 тамыз

Мақұлданған күні: 2025 жылғы 08 қараша