МРНТИ: 06.01.29
JEL Classification: H54
DOI:https://doi.org/10.52821/2789-4401-2026-1-137-151

МЕМЛЕКЕТТІК ИНФРАҚҰРЫЛЫМНЫҢ КИБЕРҚАУІПСІЗДІК ДЕҢГЕЙІН БАҒАЛАУ ӘДІСТЕРІ МЕН МОДЕЛЬДЕРІ

Т. Ш. Миркасимова [1,2*], С. А. Адилжанова[1]
[1]Әл-Фараби атындағы ҚазҰУ, Алматы, Қазақстан
[2]Нархоз Университеті, Алматы, Қазақстан

АҢДАТПА

Мақалада цифрлық тәуекелдердің өсуі және киберқауіптердің күрделенуі жағдайында мемлекеттік инфрақұрылымның киберқауіпсіздігін қамтамасыз ету мәселелері қарастырылады.

Зерттеудің мақсаты Қазақстанның ұлттық жағдайларына бейімделген ISO/IEC 27001, NIST SP 800-53, FAIR, CMMI және Mitre ATT&CK халықаралық стандарттарына негізделген интеграцияланған киберқауіпсіздік архитектурасын әзірлеуге бағытталған.

Зерттеу әдістемесі қолданыстағы киберқауіпсіздікті бағалау модельдерін жүйелік және салыстырмалы талдауды, ICS/SCADA орталарында қауіп-қатерді модельдеуді және реттеуші көздердің мазмұнын талдауды қамтиды.

Зерттеудің бірегейлігі/құндылығы. Ғылыми жаңалық-технологиялық, ұйымдастырушылық және аналитикалық компоненттерді біріктіретін киберқауіпсіздіктің тұжырымдамалық архитектурасын қалыптастыру. Ұсынылған модель мемлекеттік инфрақұрылымның кибер тұрақтылық деңгейін арттыра отырып, фрагменттелген қорғау шараларынан тәуекелдерді басқарудың тұтас жүйесіне көшуді қамтамасыз етеді.

Нәтижелер халықаралық стандарттарды біріктіру мемлекеттік жүйелердің кибер тұрақтылығын арттыратынын және оқиғаларды бақылау мен оларға жауап берудің тиімді моделін құруға ықпал ететінін көрсетеді.

Түйін сөздер: мемлекеттік инфрақұрылым, киберқауіпсіздік, қорғаныс архитектурасы, тәуекелдерді басқару, ISO/IEC 27001, NIST.

КІРІСПЕ

Цифрландырудың қазіргі дәуірінде мемлекеттік Инфрақұрылым экономиканың, әлеуметтік саланың және мемлекеттік басқару жүйелерінің жұмыс істеуінің негізін құрайды. Оның жұмысының тиімділігі ұлттық қауіпсіздік пен мемлекеттің тұрақты дамуының ажырамас бөлігіне айналатын киберқауіпсіздік деңгейіне тікелей байланысты. Цифрлық тәуелділіктің өсуі киберинциденттер санының артуымен қатар жүреді, бұл маңызды объектілерді қорғауға жүйелі көзқарасты қажет етеді.

Қазіргі киберқауіптер үйлестірудің жоғары деңгейімен және техникалық күрделілігімен сипатталады, соның ішінде өнеркәсіптік басқару жүйелеріне (ICS/SCADA), энергетикалық және телекоммуникациялық желілерге, қаржы және денсаулық сақтау мекемелеріне шабуылдар. Бір сектордың бұзылуы басқа салаларға әсер ететін тізбекті реакцияны тудыруы мүмкін, бұл мемлекеттік инфрақұрылым элементтерінің жүйелі өзара тәуелділігін растайды.

Осы сын-қатерлерге жауап ретінде көп деңгейлі қорғаныс пен тәуекелдерді басқаруды қамтамасыз ететін мемлекеттік инфрақұрылымның біртұтас киберқауіпсіздік архитектурасын құру талап етіледі. Мұндай архитектура физикалық, технологиялық, ұйымдастырушылық және аналитикалық деңгейлерді біріктіруі керек, соның ішінде оқиғаларды бақылау үшін IDS/IPS, SIEM және SOAR жүйелерін пайдалану және процестердің жетілуін талдау және жақсарту үшін ISO/IEC 27001, NIST Cybersecurity Framework, FAIR, ROSI, CMMI және MITRE att&CK халықаралық стандарттарын қолдану.

Ұсынылған архитектура тұжырымдамасы иерархиялық принцип бойынша құрылады, мұнда әр деңгей нақты функцияны орындайды - физикалық активтерді қорғаудан бастап деректерді стратегиялық талдауға және шешім қабылдауға дейін. Бұл тәсіл кибер тұрақтылықтың ұлттық моделінің негізін құра отырып, инфрақұрылымның технологиялық ғана емес, басқарушылық тұрақтылығын да қамтамасыз етеді.

Зерттеудің өзектілігі Қазақстанның мемлекеттік инфрақұрылымдарының ерекшеліктеріне бейімделген тәуекелдерді бағалау мен басқарудың кешенді әдістерін әзірлеу қажеттілігімен айқындалады. Құрылымдық архитектураны енгізбестен және осалдықтарды үнемі бағаламай, киберқауіптерге ұзақ мерзімді төзімділікті қамтамасыз ету мүмкін емес.

Зерттеудің мақсаты халықаралық стандарттарға негізделген және ұлттық жағдайларға бейімделген мемлекеттік инфрақұрылымның киберқауіпсіздік деңгейін бағалаудың интеграцияланған әдістемелік моделін әзірлеу және негіздеу болып табылады.

Жұмыстың ғылыми жаңалығы маңызды объектілердің қауіпсіздігін жүйелі талдау үшін халықаралық құрылымдар мен жетілу модельдерін біріктіретін Киберқауіпсіздіктің интеграцияланған архитектурасын қалыптастырудан тұрады. Зерттеудің практикалық маңыздылығы мемлекеттік инфрақұрылымның энергетикалық, көліктік, телекоммуникациялық және өзге де секторларында киберқауіптерді жобалау, мониторингілеу және басқару кезінде әзірленген сәулет пен модельдерді қолдану мүмкіндігінде көрінеді.

Осылайша, мемлекеттік инфрақұрылымның киберқауіпсіздік архитектурасын қалыптастыру ұлттық тұрақтылықты қамтамасыз етудің стратегиялық бағыты болып табылады және үздік халықаралық тәжірибелер мен тәуекелдерді бағалаудың ғылыми негізделген әдістеріне негізделген техникалық, ұйымдастырушылық және талдамалық шешімдердің үйлесімін талап етеді.

Зерттеу барысында маңызды объектілердің киберқауіпсіздігіне қойылатын талаптарды анықтайтын негізгі халықаралық стандарттар мен модельдер қарастырылды. Ақпараттық қауіпсіздікті басқару жүйелерін құруға негіз болатын ISO/IEC 27001 және NIST SP 800-53 стандарттары үлкен маңызға ие [1][2].

Зерттеу жұмысы ең алдымен қолжетімді ғылыми әдебиеттер мен киберқауіпсіздік саласындағы негізгі нормативтік-құқықтық құжаттарды мұқият талдауға негізделді. Авторлар ақпараттық қауіпсіздікті басқаруда кеңінен танылған халықаралық стандарттар мен ұсынымдарға сүйенді. ISO / IEC 27001 ақпараттық қауіпсіздік менеджменті жүйесін (ISMS) құруға, енгізуге және жетілдіруге қойылатын талаптарды белгілейді. Стандарт ақпараттық активтердің құпиялылығын, тұтастығын және қолжетімділігін қорғауға жүйелі тәсілді қамтамасыз етеді. Ол ұйымдарға тәуекелдерді үздіксіз бағалауға және оқиғаларға төзімділікті арттыруға мүмкіндік беретін «жоспарлау – орындау – тексеру – әрекет» процесс циклін қамтамасыз етеді [1].

АҚШ ұлттық стандарттар және технологиялар институты әзірлеген NIST SP 800-53-ұйымдастырушылық, техникалық және процедуралық қауіпсіздік шараларының кең каталогы. Құжат қол жеткізуді басқаруды, оқиғаларға жауап беруді, желілер мен деректерді қорғауды және тәуекелге бағытталған тәсіл принциптерін қамтитын 300-ден астам бақылау механизмдерін қамтиды. Стандарт икемді қорғаныс жүйелерін құру және ақпараттық қауіпсіздік процестерінің жетілуін бағалау үшін қолданылады [3].

Талдаудың нәтижесі көрсетілген стандарттар киберқауіптерді бағалау және басқару үшін әдіснамалық базаны қамтамасыз ететіні анықталды, алайда Қазақстанның Мемлекеттік инфрақұрылымдық жүйелерінің жұмыс істеу ерекшеліктері мен ұлттық жағдайларына бейімделуді талап етеді.

ЗЕРТТЕУДІҢ НЕГІЗГІ БӨЛІМІ

Зерттеу әдістемесі. Зерттеудің әдіснамалық негізі Мемлекеттік инфрақұрылымның киберқауіпсіздігін бағалау әдістері мен модельдерін жүйелі зерттеуге бағытталған. Мақсатқа жету үшін халықаралық модельдерді (FAIR, ROSI, NIST CSF, CMMI, MITRE ATT&CK, STRIDE) аналитикалық салыстыру, ICS/SCADA жүйелеріндегі осалдықтарды анықтау үшін қауіптерді модельдеу, сондай-ақ нормативтік және ғылыми дереккөздердің контент-талдауы (ISO/IEC 27001, NIST SP 800-53, ENISA) қолданылды [4][5][6].

Бұл тәсілдерді кешенді пайдалану теориялық және қолданбалы талдаудың үйлесімін қамтамасыз етті, бұл модельдерді жетілу дәрежесі, халықаралық стандарттармен Интеграция және Қазақстанның ұлттық жағдайларына бейімделу бойынша жіктеуге мүмкіндік берді.

Зерттеу әдістері киберқауіпсіздік деңгейін бағалауға және мемлекеттік маңызды инфрақұрылым тәуекелдерін басқаруға бағытталған теориялық және практикалық тәсілдердің жиынтығын қамтиды. Аналитикалық салыстыру, қауіп-қатерді модельдеу, нормативтік және ғылыми дереккөздердің мазмұнын талдау қолданылады. Сараптамалық бағалау мен сценарийлік талдауға негізделген сапалық әдістер де, статистикалық деректерді өңдеуге, осалдық көрсеткіштерді өлшеуге және қорғаныс шараларының тиімділігіне бағытталған сандық әдістер де қолданылады. Мұндай кешенді тәсіл киберқауіпсіздік жағдайын жан-жақты бағалауды қамтамасыз етеді және оны арттыру бойынша практикалық ұсыныстарды әзірлеуге ықпал етеді.

Киберқауіпсіздіктің жетілдірілген модельдері

NIST Cybersecurity Framework (CSF) – киберқауіпсіздік жетілуінің ең танымал модельдердің бірі. Оны АҚШ ұлттық стандарттар және технологиялар институты (NIST) ұйымдарға ақпараттық қауіпсіздік тәуекелдерін басқаруға көмектесу үшін әзірледі. CSF киберқауіпсіздік стратегияларын әзірлеу үшін негіз ретінде пайдаланылады және кез келген масштабты ұйымдастырудың икемді құралы болып табылады.

NIST CSF моделі бес негізгі функциядан тұрады:

1. Сәйкестендіру: бұл функция маңызды жүйелер мен деректер контекстінде киберқауіптерді түсінуге және басқаруға бағытталған.
2. Қорғау: қауіпсіздік оқиғаларынан болатын зиянды азайтуға көмектесетін шаралар мен процестерді қамтиды.
3. Анықтау: киберқауіптерді уақтылы анықтауға бағытталған.
4. Жауап беру: қауіпсіздік оқиғаларына жауап беру үшін ұйым қабылдауы керек әрекеттерді қамтиды.
5. Қалпына келтіру: кибершабуылдардан кейін қалыпты жұмысын қалпына келтіру шаралары [3].

1 - сурет. NIST Киберқауіпсіздік Жүйесі (CSF)және оның санаттары
Ескерту: Сурет [3] дереккөзінен алынған

Киберқауіпсіздік қатерлерінің үнемі дамып келе жатқан жағдайында ұйымдарға киберқауіпсіздік тәуекелдерін басқару бағдарламаларын басқару үшін сенімді, бірақ икемді құрылым қажет. Ұлттық Стандарттар Институтының (NIST) Киберқауіпсіздік Жүйесі (CSF) дәл осындай маяк болып табылады, ол киберқауіптерді анықтауға, қорғауға, анықтауға, әрекет етуге және қалпына келтіруге құрылымдық және қолдануға болатын тәсілді қамтамасыз етеді. CSF бес функциядан тұрады – идентификациялау, қорғау, анықтау, жауап беру және қалпына келтіру. Функциялар төмендегі 2-кестеде сипатталған.

1-кесте. Киберқауіпсіздікті бағалау әдістерін салыстырмалы талдау

Функция	Сипаттамасы
Identify (Идентификациялау)	Бұл функция жүйелер, активтер, деректер мен мүмкіндіктерге қатысты киберқауіпсіздік тәуекелдерін түсіну мен басқаруға бағытталған.
Protect (Қорғау)	«Protect» функциясы маңызды қызметтердің үздіксіздігін қамтамасыз ету мақсатында тиісті қорғаныс шараларын әзірлеу және енгізуге бағытталған.
Detect (Анықтау)	Бұл функция киберқауіпсіздік инциденттерінің пайда болуын уақтылы анықтауға қажетті іс-шараларды әзірлеу мен іске асыруға басымдық береді.
Respond (Жауап беру)	Аталған бөлім анықталған киберқауіпсіздік инциденттеріне жедел әрекет етуге арналған іс-қимылдарды әзірлеу мен жүзеге асыруға бағытталған.
Recover (Қалпына келтіру)	«Recover» функциясы киберқауіпсіздік инциденттері нәтижесінде бұзылған қызметтер мен мүмкіндіктерді қалпына келтіру және ұйымның тұрақтылығын қамтамасыз ету мақсатында жоспарлар мен іс-шараларды әзірлеу және енгізу жолдарын сипаттайды.
Ескерту: [3] дереккөзі негізінде құрастырылған	

Әрбір CSF функциясы қауіпсіздікті қамтамасыз ету үшін қажетті нақты процестер мен технологияларды сипаттайтын көптеген санаттар мен ішкі санаттарды қамтиды. CSF моделі ұйымға өзінің қауіпсіздік жүйелерінің қазіргі жетілу деңгейін анықтауға және осы салада одан әрі дамуды жоспарлауға мүмкіндік береді.

Capability Maturity Model Integration (CMMI) - бұл киберқауіпсіздікті басқару процестерін қоса, ұйымдағы процестердің жетілуін бағалау үшін қолданылатын модель. CMMI жобалар мен процестерді басқару сапасын жақсарту үшін жасалған, бірақ кейінірек ақпараттық қауіпсіздік саласында да қолданыла бастады.

CMMI моделі бес жетілу деңгейінен тұрады:

1. Бастапқы деңгей (Initial): қауіпсіздік процестері жоқ немесе ретсіз және сәйкес келмейді.
2. Басқарылатын деңгей (Managed): киберқауіпсіздік процестері бақыланады және олардың тиімділігін бағалау үшін өлшенеді.
3. Белгілі бір деңгей (Defined): процестер стандартталған және құжатталған, олардың орындалуы жеке қызметкерлерге тәуелді емес.
4. Сандық басқарылатын деңгей (Quantitative Process Performance and Management) – Даму процестері өлшемдер мен көрсеткіштерді қамтитын сандық мәліметтермен өлшенеді және бақыланады. Ұйым осы сандық деректерді болжамды процестерді анықтау үшін пайдаланады. Сонымен қатар, ұйым тәуекелдерді тиімді басқару, процестерді тиімдірек ету және процестердегі кемшіліктерді түзету үшін деректерді пайдаланады.
5. Оңтайландыру деңгейі (Optimizing): ұйым деректерді талдау және енгізу нәтижелері негізінде өз процестерін үнемі жетілдіріп отырады [4].

CMMI ұйымдарға қауіпсіздік процестерінің жетілуін бағалауға және оларды жақсарту жоспарын құруға көмектеседі. Модель сонымен қатар үздіксіз жетілдіру процестерін қолдайды және ұзақ мерзімді дамуға баса назар аударады.

Кибер тәуекелге бағытталған модельдер

Бұл модельдер кибершабуылдармен байланысты тәуекелдерді бағалауға және олардың салдарын экономикалық талдауға бағытталған. Олар ұйымдарға шабуылдардың ықтималдығын және қауіпсіздік оқиғаларының қаржылық салдарын түсінуге көмектеседі.

FAIR (Factor analysis of Information Risk) - ең танымал және кеңінен қолданылатын кибер тәуекелге бағытталған модельдердің бірі. Бұл ұйымдарға ақпараттық қауіпсіздікке байланысты тәуекелдерді сандық бағалауға және басқаруға көмектеседі. FAIR моделінің негізгі міндеті - кибершабуылдың ықтималдығын бағалауға және оның ықтимал салдарын анықтауға көмектесу.

FAIR келесі негізгі элементтерге негізделген:

1. Қауіп: бұл ақпараттық жүйелерге жағымсыз салдар тудыруы мүмкін кез келген субъект.
2. Осалдық: бұл жүйеде оның қалыпты жұмысының бұзылуына қауіп төндіретін әлсіз жер.

3. Бақылау: бұл осалдықтарды азайту немесе жою үшін ұйым қабылдаған шаралар.

4. Ықтималдық: модель шабуылдың ықтималдығын қауіптің осалдықты қаншалықты пайдаланатындығына қарай бағалайды.

FAIR ықтималдық пен ықтимал зиянды өлшеу арқылы тәуекелдерді сандық бағалауды ұсынады. Бұл модель басқа тәсілдерден ерекшеленеді, өйткені ол шабуылдардың қаржылық салдарын дәл болжауға мүмкіндік беретін көрсеткіштерді қолданады. FAIR моделінің басты артықшылығы – тәуекелдерді бағалау және ресурстарды киберқауіпсіздікке бөлу туралы шешім қабылдау үшін басшылыққа нақты деректерді ұсыну мүмкіндігі. FAIR сонымен қатар басқа тәуекелдерді бағалау әдістемелерімен біріктірілуі мүмкін, бұл оны киберқауіпсіздікті басқарудың әмбебап құралына айналдырады [5].

Бұл модельдерді қолдану тәжірибесі Халықаралық және аймақтық жағдайлармен расталады. Мысалы, Қазақстанда ISO/IEC 27001 стандартының және NIST CSF элементтерінің қағидаттары мемлекеттік ақпараттық жүйелердің жетілуін бағалау үшін "Қазақстанның киберқауіпсіздік тұжырымдамасы (Қазақстанның кибер қалқаны)" шеңберінде енгізіледі. FAIR моделін АҚШ пен Еуропаның ірі қаржы институттары киберқауіптерді сандық бағалау үшін белсенді қолданады, ал Mitre att&CK әдістемесі энергетика және көлік саласындағы оқиғаларды тергеу кезінде қауіпсіздік мониторингі орталықтарында (SOC) қолданылады. Бұл мысалдар халықаралық модельдерді ұлттық киберқауіпсіздік стратегияларына біріктірудің тиімділігін көрсетеді.

Қауіп-қатерге негізделген қорғаныс модельдері

MITRE ATT&CK - шабуылдаушылар шабуылдарда қолданатын тактиканы, техниканы және процедураларды (TTPs) сипаттайтын кең мәліметтер базасы. Бұл модель нақты қауіптерді талдауға бағытталған және ұйымдарға шабуылдаушылардың мінез-құлқына негізделген тиімді қорғаныс шараларын жасауға көмектеседі.

MITRE ATT&CK келесі компоненттерден тұрады:

1. Тактика: шабуылдаушылар шабуылдың әртүрлі кезеңдерінде қол жеткізуге тырысатын мақсаттар, мысалы, деректерді жинау, артықшылықтар алу, желі ішінде қозғалу және т. б.

2. Техника: шабуылдаушылар өз мақсаттарына жету үшін қолданатын нақты әдістер. Мысалы, бұл осалдықтарды пайдалану, деректерді жинау үшін фишингті пайдалану немесе зиянды бағдарламаны енгізу болуы мүмкін.

3. Процедуралар: шабуылдаушылардың белгілі бір әдістерді қалай қолданатыны туралы егжей-тегжейлі сипаттамалар [6].

ATT&CK ұйымдарға олардың жүйелеріне қалай шабуыл жасалуы мүмкін екенін түсініп қана қоймай, сонымен қатар нақты қауіптерге негізделген қарсы шараларды әзірлеуге көмектеседі. Модель мониторинг жүйелерінде, қауіпсіздікті бағалау үшін және мамандарды оқыту кезінде қолданылады.

Қарастырылған модельдерді көрнекі түрде салыстыру үшін 3-кестеде олардың негізгі артықшылықтары, шектеулері және практикалық қолдану салалары көрсетілген.

2-кесте. Киберқауіпсіздікті бағалау және басқару модельдерін салыстырмалы талдау

Модель	Артықшылықтар	Шектеулер	Қолдану аясы
FAIR	Тәуекелдерді сандық бағалау, экономикалық интерпретация, ISO/NIST интеграциялау мүмкіндігі	Маңызды бастапқы деректерді қажет етеді, мамандарсыз енгізу қиын	Қаржылық тәуекелдерді талдау, АҚ стратегиялық жоспарлау
NIST CSF	Әмбебаптық, икемділік, халықаралық стандарттарға сәйкестік	Сандық баға бермейді, белгілі бір секторға бейімделуді қажет етеді	АҚ процестерін басқару, мемлекеттік және корпоративтік сектор
CMMI	Процестердің жетілуін бағалау, үздіксіз жетілдіруді қолдау	Іске асырудың күрделілігі, ұзақ бағалау циклі	АҚ процестерінің жетілуін бағалау
MITRE ATT&CK	Шабуыл тактикасы мен техникасының толық сипаттамасы, өзекті білім базасы	Техникалық аспектілерге назар аудара отырып, экономикалық әсерді ескермейді	Қауіп-қатерді талдау, SOC мамандарын оқыту
Ескерту: зерттеулер нәтижесінде авторлармен құрастырылған			

Модельдерді салыстырмалы талдау әртүрлі тәсілдерді – экономикалықтан мінез-құлыққа дейін интеграциялау тәуекелдерді жан-жақты бағалауды қамтамасыз ететінін және маңызды инфрақұрылымның киберқауіптерге төзімділігін арттыратынын көрсетті.

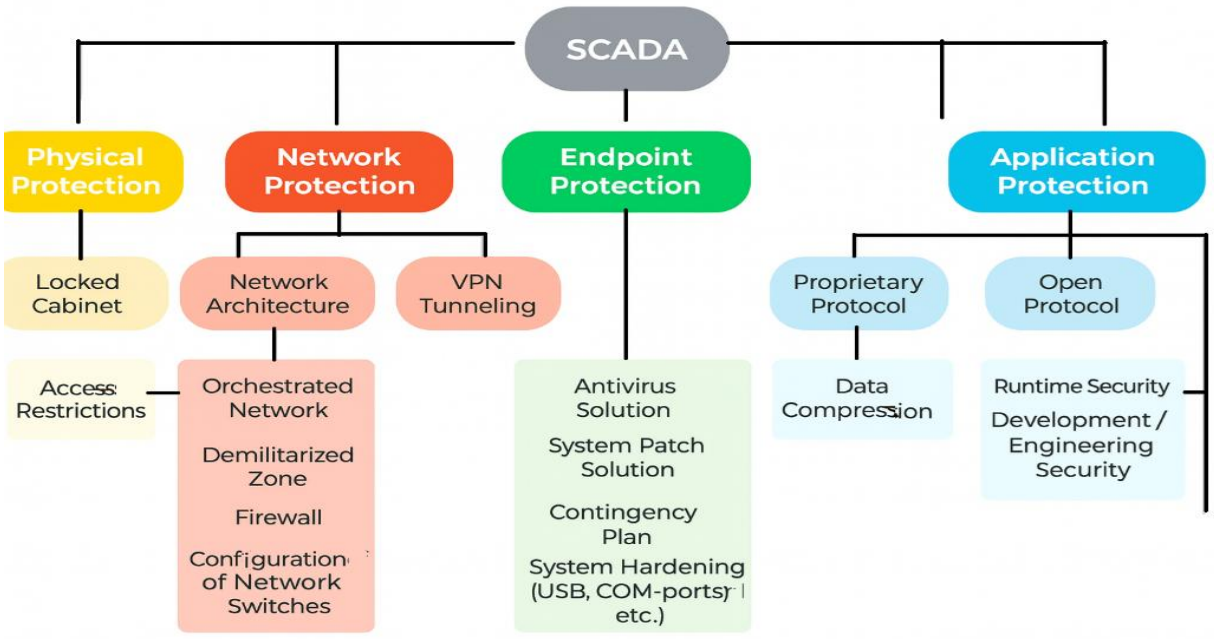
Мемлекеттік инфрақұрылымға төнетін негізгі қауіптер

Мемлекеттік инфрақұрылымға төнетін негізгі қатерлер сыни жүйелердің ақпараттық-коммуникациялық технологияларға тәуелділігінің артуымен байланысты. Ең маңызды тәуекелдердің қатарына энергетикалық, көліктік, қаржылық және телекоммуникациялық желілерге кибершабуылдар, зиянды бағдарламалық жасақтаманың таралуы, әлеуметтік инженерия әдістерін қолдану, сондай-ақ құпия деректердің ағуы жатады. Бұл факторлар ұлттық қауіпсіздікке, мемлекеттік институттардың тұрақтылығына және елдің экономикалық тұрақтылығына әлеуетті қауіп төндіреді.

Өнеркәсіптік басқару жүйелерінің қауіпсіздігі (ICS — Industrial Control Systems) энергетика, көлік, сумен жабдықтау және өнеркәсіптегі технологиялық процестердің мониторингі мен басқарылуын қамтамасыз ететін аппараттық-бағдарламалық кешендерді қорғауға бағытталған. Бұл жүйелер инфрақұрылымның маңызды объектілерінің жұмыс істеуінің негізі болып табылады, олардың жұмысының бұзылуы ауыр экономикалық және әлеуметтік салдарға әкелуі мүмкін.

ICS ішкі жүйелеріне SCADA (Supervisory Control and Data Acquisition), үлестірілген процестерді басқару жүйелері (DCS) және бағдарламаланатын логикалық контроллерлер (PLC) кіреді. Олар деректерді жинауды, қашықтан басқаруды және технологиялық операцияларды автоматтандыруды қамтамасыз етеді.

Алайда, мұндай жүйелердің едәуір бөлігі заманауи киберқауіпсіздік талаптарын ескермей жасалған. Олардың ұзақ өмірлік циклі және бастапқыда сыртқы желілерден шектеулі оқшаулануы Интернетке қосылу және АТ инфрақұрылымымен интеграциялау кезінде жоғары осалдыққа әкелді. Кіріктірілген қорғаныс механизмдерінің болмауы ICS және SCADA-ны деректердің тұтастығын, жабдықтың қауіпсіздігін және өндірістік процестердің үздіксіздігін қамтамасыз ету үшін кешенді шараларды енгізуді талап ететін жоғары қауіпті объектілерге айналдырады [7].



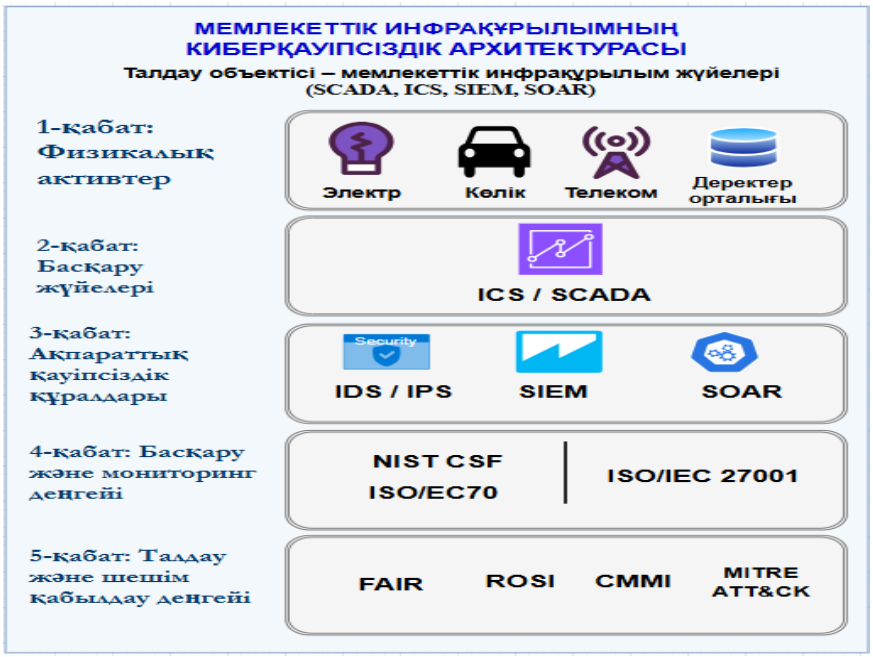
2 - сурет. SCADA security архитектурасы

Ескерту: Сурет [7] дереккөзі негізінде құрастырылған

SCADA security күрделі өндірістік процестерді автоматтандыру және басқару үшін қажетті бақылау және деректерді жинау жүйелерін қорғауға бағытталған. Бұл желілер коммуналдық қызметтерде, өндірісте және тасымалдауда маңызды рөл атқарады. SCADA жүйелері нақты уақыт режимінде деректерді жинауға, процестерді бақылауға және жедел басқаруға арналған. Ашық архитектуралар мен IP негізіндегі коммуникациялардың енгізілуімен SCADA жүйелерінің киберқауіптерге осалдығы артты. Бұл қауіпсіздік хаттамаларын операциялық тұтастық пен қоғамдық қауіпсіздікті қамтамасыз ету үшін өте маңызды етеді.

Мемлекеттік инфрақұрылымның киберқауіпсіздік архитектурасы

Зерттеу нәтижесінде маңызды жүйелердегі тәуекелдерді қорғау мен басқарудың көп деңгейлі жүйесін көрсететін мемлекеттік инфрақұрылымның киберқауіпсіздігінің тұжырымдамалық архитектурасы жасалды. Архитектура ISO/IEC 27001 және NIST Cybersecurity Framework халықаралық стандарттарының принциптеріне, сондай-ақ FAIR, ROSI, CMMI және MITRE ATT&CK әдістемелік тәсілдеріне негізделген, бұл оның ғылыми негізділігі мен практикалық қолданылуын қамтамасыз етеді.



3 - сурет. Мемлекеттік инфрақұрылымның киберқауіпсіздік архитектурасы
Ескерту: авторлармен құрастырылған

Модель өзара байланысты бес деңгейден тұрады, олардың әрқайсысы инфрақұрылымның тұрақтылығы мен қауіпсіздігін қамтамасыз етуде өзіндік функцияны орындайды:

1. Физикалық деңгей-негізгі активтерді (энергетика, көлік, телекоммуникация желілері және деректер орталықтары) қамтиды.
2. Басқару жүйелерінің деңгейі (ICS/SCADA) — физикалық және цифрлық ортаны байланыстыра отырып, технологиялық процестерді бақылау мен бақылауды қамтамасыз етеді.
3. Ақпараттық қауіпсіздік құралдарының деңгейі (IDS/IPS, SIEM, SOAR) - киберқауіптерді анықтауға, алдын алуға және корреляциялауға жауап береді.
4. Басқару және мониторинг деңгейі (NIST CSF, ISO/IEC 27001) - тәуекелдерді басқару және стандарттарға сәйкестікті бақылау бойынша ұйымдастырушылық-нормативтік шаралар жүйесін қалыптастырады.
5. Аналитикалық-басқару деңгейі (FAIR, ROSI, CMMI, MITRE ATT&CK) — тәуекелдерді стратегиялық бағалауды, деректерді талдауды және оңтайлы басқару шешімдерін әзірлеуді қамтамасыз етеді.

Ұсынылған архитектура технологиялық, ұйымдастырушылық және аналитикалық компоненттерді бір модельге біріктіру арқылы кибер тұрақтылыққа жүйелік және иерархиялық тәсілді көрсетеді. Оның практикалық құндылығы ұлттық инфрақұрылымның әртүрлі секторларына бейімделу және мемлекеттік ақпараттық жүйелерді киберқорғау тиімділігін арттыру қабілетінде жатыр.

Автоматтандырылған қауіпсіздікті бақылау және басқару жүйелері

Кибершабуылдар санының үнемі өсуі және зиянкестердің әдістерінің күрделенуі жағдайында қауіпсіздікті бақылау мен басқарудың автоматтандырылған жүйелері ақпараттық жүйелерді қорғаудың маңызды элементтеріне айналады. Бұл жүйелер қауіптерді тез анықтауға, олардың алдын алуға және оқиғаларға минималды ресурстармен жауап беруге мүмкіндік береді. Мұндай жүйелердің негізгі компоненттерінің ішінде мыналарды атап өтуге болады: интрузияны анықтау және алдын алу жүйелері (IDS/IPS), SIEM жүйелері (қауіпсіздік ақпараты және оқиғаны басқару), сондай-ақ оқиғаларды басқару және кибершабуылдарға жауап беру құралдары (SOAR).

Интрузияны анықтау және алдын алу жүйелері (IDS/IPS)

Анықтау жүйелері (IDS — Intrusion Detection System) және кіруді болдырмау (IPS — Intrusion Prevention System) белсенділікті бақылауды және шабуылдардан қорғауды қамтамасыз ететін желілік қауіпсіздіктің негізгі элементтері болып табылады. IDS желілік трафикті талдайды, күдікті әрекеттерді анықтайды және деректерді беру процесіне араласпай әкімшіге хабарлайды. IDS негізгі түрлеріне мыналар жатады:

- Желілік IDS (NIDS) — желінің белгілі бір сегментіндегі трафикті талдайды және портты сканерлеу әрекеттерін, DDoS шабуылдарын және осалдықтарды пайдалануды анықтайды.
- Хост IDS (HIDS) — оқиғалар журналдарын, рұқсат етілмеген өзгерістерді және кіру әрекеттерін бақылай отырып, Жеке құрылғылар немесе серверлер деңгейінде жұмыс істейді.

Қауіптерді анықтау екі тәсілмен жүзеге асырылады:

- Қолтаңба бойынша-трафикті белгілі шабуыл үлгілерінің базасымен салыстыру;
- Ауытқулар негізінде-жүйенің қалыпты мінез-құлқынан ауытқуларды анықтау.

IPS IDS-ке ұқсас жұмыс істейді, бірақ одан әрі белсенді жауап береді: күдікті трафикті блоктайды, деректерді бағыттауды өзгертеді немесе нақты уақыттағы ресурстарға қол жеткізуді шектейді. IPS-тің негізгі функцияларына трафикті талдау, шабуылдардың автоматты түрде алдын-алу және кейінгі талдау үшін оқиғалар журналын жүргізу кіреді.

IDS/IPS-ті басқа қорғаныс құралдарымен — брандмауэрлермен, антивирустармен және SIEM жүйелерімен біріктіру заманауи қауіптерге кешенді қарсы тұруды қамтамасыз ететін көп деңгейлі киберқауіпсіздік архитектурасын жасауға мүмкіндік береді [8].

ЗЕРТЕУ НӘТИЖЕЛЕРІ (ҚОРЫТЫНДЫЛАР)

Киберқылмыскерлер мен террористік ұйымдар мемлекеттік инфрақұрылым нысандарына ерекше қызығушылық танытады, себебі мұндай нысандарға жасалған шабуылдар тұтас мемлекеттің қызметін бұғаттауға, халық арасында дүрбелең туғызуға және айтарлықтай экономикалық залал келтіруге қабілетті. Киберқылмыскерлердің негізгі уәжі, әдетте, қаржылық пайда табу болса, террористік топтар көбінесе саяси немесе идеологиялық мақсаттарды көздеп, мемлекетті дестабилизациялауға ұмтылады.

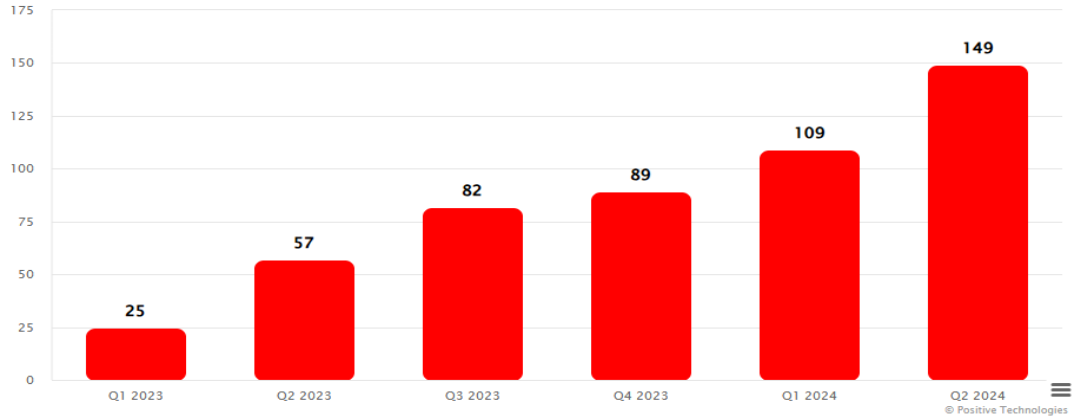
ТМД елдеріндегі өзекті киберқауіптер

Positive Technologies деректері мен ашық дереккөздерге негізделген 2023 және 2024 жылдың ТМД елдері үшін өзекті киберқауіптер нәтижелері зерттеліп, жарияланған есеп мәліметтері:

- 2024 жылдың II тоқсанында ТМД елдеріне жасалған кибершабуылдар саны 2023 жылдың осы кезеңімен салыстырғанда 2,6 есе өсті.
- Барлық шабуылдардың 73%-ы Ресейге, 8%-ы Қазақстанға, 7%-ы Беларуське түсті.
- Көбінесе мемлекеттік мекемелерге (18%), өнеркәсіпке (11%) және телекоммуникацияға (10%) шабуыл жасалады.
- Шабуылдардың негізгі әдістері-зиянды бағдарлама және әлеуметтік инженерия.
- ТМД-дағы DDoS-шабуылдардың үлесі орташа әлемдік деңгейден едәуір жоғары-8% қарсы 18% [10].

Киберқылмыстың негізгі ошақтары

ТМД елдеріне зиянкестердің қызығушылығы тоқсаннан тоқсанға артып келеді. Сонымен, 2024 жылдың II тоқсанында 2023 жылдың сәйкес кезеңіне қарағанда 2,6 есе көп шабуылдар тіркелді (3-суретті қараңыз). Біздің мәліметтеріміз бойынша, ТМД ұйымдарына бағытталған барлық шабуылдардың 73% - ы Ресейдің үлесіне тиді. Екінші және үшінші орында — Қазақстан (8%) және Беларусь (7%). Шабуылдаушылардың осы мемлекеттерге деген қызығушылығы, соның ішінде Ресей, Беларусь және Қазақстанмен байланысты деректер мен қызметтерді сату, тарату және сатып алу туралы дарквебте көптеген хабарландырулармен расталады. Бұл туралы толығырақ "көлеңкелі аймақтарды талдау" бөлімінен оқыңыз.



4-сурет. Табысты кибершабуылдарды тоқсан бойынша бөлу
Ескерту: [10] дереккөзінен алынған

Қазақстан NCSI рейтингінде Беларусь, Молдова, Әзірбайжан және Ресейден кейін 78-ші орында. Киберқауіпсіздікті арттыру үшін 2023 жылы "Қазақстанның кибер қалқаны" бағдарламасы шеңберінде Ұлттық үйлестіру орталығын дамытуды және киберполигон құруды көздейтін 2023-2029 жылдарға арналған цифрлық трансформация және киберқауіпсіздік тұжырымдамасы бекітілді.

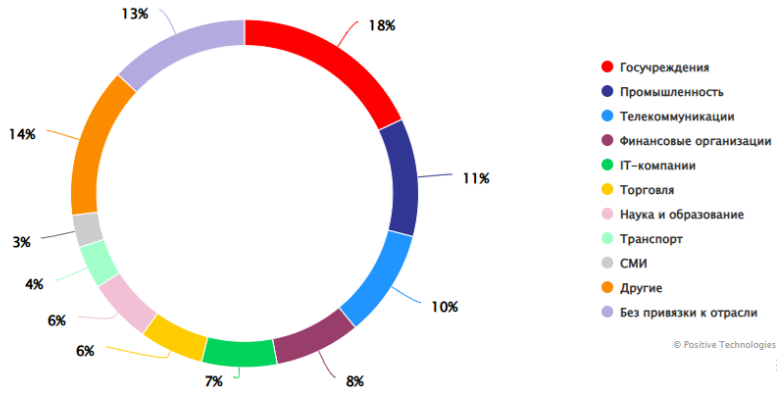
2023-2024 жылдары Қазақстандағы шабуылдардың негізгі мақсаттары БАҚ (19%), мемлекеттік мекемелер (12%), қаржы секторы (12%) және телекоммуникациялар (7%) болды. 2023 жылдың аяғынан бастап DDoS шабуылдарының толқыны тәуелсіз БАҚ-қа түсіп, журналистиканы қорғау мәселелері бойынша қоғамдық пікірталас тудырды.

Шабуылдардың шамамен 65%-ы зиянды бағдарламалармен, 53%-ы әлеуметтік инженериямен, ал 35%-ы деректердің бұзылуымен жүрді.

5-сурет. Қазақстанға жасалған шабуылдар бойынша жиынтық статистика
Ескерту: [10] дереккөзінен алынған

Шабуылдардың құрбандары мен салдары

2023 жылы және 2024 жылдың бірінші жартысында ТМД елдеріндегі шабуылдардың ең көп саны мемлекеттік мекемелерге (18%), өнеркәсіпке (11%) және телекоммуникацияға (10%) ұшырады. Бұл үш сала бірнеше себептерге байланысты зиянкестер үшін ең үлкен қызығушылық тудырады. Біріншіден, осы салалардағы ұйымдар ел экономикасы үшін стратегиялық маңызды, сондықтан геосаяси шиеленіс жағдайында олар бірінші кезекте кибершабуылдарға ұшырайды. Екіншіден, мемлекеттік, өнеркәсіптік және телекоммуникациялық компанияларда үлкен көлемдегі құпия ақпарат, ең алдымен дербес деректер мен коммерциялық құпия сақталады. Оларға әртүрлі санаттағы зиянкестер бағытталған — көлеңкелі нарықтардағы деректерді сатушылардан бастап, барлау жинайтын мемлекеттік кибершпиондарға дейін.



6-сурет. Ұйымдар арасындағы құрбандар санаттары
Ескерту: [10] дереккөзі негізінде құрастырылған

Ұйымдарға жасалған сәтті шабуылдардың негізгі салдары-құпия ақпараттың таралуы (41%) және негізгі қызметтің бұзылуы (37%). Жеке тұлғаларға жасалған шабуылдар 69% жағдайда құпия ақпараттың ағып кетуімен және 32% жағдайда тікелей қаржылық шығындармен аяқталды.

Қорытынды

Киберқауіпсіздікті тиімді қамтамасыз ету үнемі бақылауды, қорғаныс жүйелерін үнемі жаңартуды және тез өзгеретін қауіп ландшафтына бейімделуді қажет етеді. Заманауи кибершабуылдар жоғары жылдамдықпен және күрделілікпен дамиды, бұл интеллектуалды технологияларды, автоматтандырылған анықтау жүйелерін (IDS/IPS), оқиғаларды талдауды (SIEM) және жауап беруді (SOAR) қолдануды қажет етеді.

Мемлекеттік инфрақұрылым тұрақтылығының негізгі факторы техникалық, ұйымдастырушылық және талдамалық шараларды біріктіретін интеграцияланған киберқауіпсіздік архитектурасын қалыптастыру болып табылады. Жасанды интеллект пен машиналық оқыту әдістерін енгізу қауіптерді анықтауды автоматтандыруға, жауап беру уақытын қысқартуға және адам факторын азайтуға мүмкіндік береді. Сонымен қатар, қауіпсіздік мәдениетін дамыту және қызметкерлердің біліктілігін арттыру маңызды рөл атқарады, бұл ақпаратты қорғауға жауапты көзқарасты қалыптастыруға ықпал етеді.

Практикалық ұсыныстар:

- Салалық тәуекелдер мен сыни жүйелердің ерекшеліктерін ескере отырып, Киберқауіпсіздіктің стратегиялық жоспарларын әзірлеу және енгізу;
- Тәуекелдерді және оқиғаларға дайындықты үнемі бағалау;
- Халықаралық ынтымақтастық пен киберқауіптер туралы деректермен алмасуды күшейту;
- Заманауи қорғаныс технологияларына инвестиция салу-IDS / IPS, SOAR, SIEM және аналитикалық платформалар;
- Операцияларды жедел бақылау және үйлестіру үшін орталықтандырылған инциденттерге жауап беру командаларын (CERT/CSIRT) құру.

Зерттеудің негізгі ғылыми тұжырымдары халықаралық стандарттар мен әдіснамалық модельдерді (ISO/IEC 27001, NIST, FAIR, CMMI, MITRE ATT&CK) кешенді қолдану кибер тұрақтылық деңгейін арттыруға және Мемлекеттік инфрақұрылымдық жүйелердегі инциденттерге жауап берудің тиімді жүйесін қалыптастыруға ықпал ететінін растайды.

Әрі қарайғы зерттеулердің болашағы интеллектуалды киберқауіпсіздік архитектураларын дамытумен, жасанды интеллект технологияларын, цифрлық егіздерді және нақты уақыттағы киберқауіпсіздіктерді болжау және алдын алу үшін болжамды талдауды біріктірумен байланысты.

ӘДЕБИЕТТЕР ТІЗІМІ

1. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. Online Browsing Platform (OBP). URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

2. National Institute of Standards and Technology. NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations. 2020. URL: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

3. Device42 Freshworks Inc. (2025). NIST CSF Categories: Description, Examples, and Best Practices. URL: https://www.device42.com/compliance-standards/nist-csf-categories/

4. CMMI Institute. CMMI® for Development, Version 2.0. 2018. URL: https://cmmiinstitute.com/cmmi/dev

5. FAIR Institute. Factor Analysis of Information Risk (FAIR) Model. Standard Artifact | Version 3.0. 2025. All Rights Reserved.

7. MITRE Corporation. (2024). MITRE ATT&CK® – A Knowledge Base of Adversary Tactics and Techniques Based on Real-World Observations.

8. Palo Alto Networks. What Are the Differences Between OT, ICS, & SCADA Security? Cyberpedia/Network Security/OT and IoT Security. 2025. URL: https://www.paloaltonetworks.com/cyberpedia/ot-vs-ics-vs-scada-security

9. Eurobyte Company Blog. (2025). What Do IDS and IPS Mean in Information Security? URL: https://eurobyte.ru/articles/chto-znachit-ids-i-ips-v-informaczionnoj-bezopasnosti/

10. European Commission. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. 2016.

11. Positive Technologies. (2024). Current Cyber Threats in CIS Countries 2023–2024. Leader in Effective Cybersecurity. URL: https://ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-v-stranah-sng-2023-2024/#id1

12. The White House. (2018). National Cyber Strategy of the United States of America.

13. Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). The impact of information security breaches: Has there been a downward shift in costs? Journal of Computer Security, 10(3), 211–230.

14. Smith, R. (2021). Critical Infrastructure Protection: A Comprehensive Approach to Cybersecurity. Cybersecurity Journal.

15. Kaspersky Lab. (2014). Stuxnet: The First Victims.

16. Kaspersky Lab. (2021). Dark Chronicles: The Consequences of the Colonial Pipeline Attack.

17. Investopedia. (n.d.). Risk Analysis: Definition, Types, Limitations, and Examples. Retrieved from https://www.investopedia.com/terms/r/risk-analysis.asp

18. SecurityScorecard. (n.d.). Qualitative vs. Quantitative Cybersecurity Risk Assessment: What's the Difference? Retrieved from https://securityscorecard.com/blog/qualitative-vs-quantitative-risk-assessment/

19. ISACA. (2021). Risk Assessment and Analysis Methods. ISACA Journal, 2021(2). Retrieved from https://www.isaca.org/resources/isaca-journal/issues/2021/volume-2/risk-assessment-and-analysis-methods

20. Riskaware. (n.d.). How to Measure Cybersecurity Risk: Key Metrics and Best Practices. Retrieved from https://riskaware.io/how-to-measure-cybersecurity-risk/

21. Amirkhanov, B., Amirkhanova, G., Kunelbayev, M., Adilzhanova, S., & Tokhtassyn, M. (2025). Evaluating HTTP, MQTT over TCP and MQTT over WEBSOCKET for digital twin applications: A

comparative analysis on latency, stability, and integration. International Journal of Innovative Research and Scientific Studies (IJIRSS), 8(1), 679–694. https://doi.org/10.53894/ijirss.v8i1.4414

22. Adilzhanova, S., Kunelbayev, M., Amirkhanova, G., Zhussupov, Y., & Tortay, A. (2025). Development of a data collection and storage system for remote monitoring and detection of security threats in the enterprise. International Journal of Innovative Research and Scientific Studies, 8(2), 176–196. https://doi.org/10.53894/ijirss.v8i2.5136

23. Zeeshan Ali & Miin-Shen Yang. (2024). Improving Risk Assessment Model for Cybersecurity Using Robust Aggregation Operators for Bipolar Complex Fuzzy Soft Inference Systems. Mathematics (MDPI). https://doi.org/10.3390/math12040582

24. Lakhno, V., Bereke, M., Adilzhanova, S., et al. (2022). Genetic algorithm for solving the problem of scaling a cloud-oriented object of informatization. Journal of Theoretical and Applied Information Technology, 100(6).

25. Mirkassimova, T., Adilzhanova, S., Astaubaeva, G., & Mukhamedzhanova, G. (2025). Methods of information security risk analysis and assessment. KazATK, 138(3). https://vestnik.alt.edu.kz/index.php/journal/article/view/2675

26. Uandykova, M., Mirkasimova, T., Astaubaeva, G., Mukhamedzhanova, G., & Eleukulova, A. (2024). The advantages and necessity of integrating the Jira course into the educational program. KazATK, 133(4), 235–253. https://doi.org/10.52167/1609-1817-2024-133-4-235-253

27. Adilzhanova, S., Igilmanov, A., Tyulepberdinova, G., Salmanova, A., & Amirkhanova, G. (2024). The use of log analysis to identify DoS attacks and determine user behavior during the development of a digital twin of a food industry enterprise. KazATK, 136(1), 96–107. https://doi.org/10.52167/1609-1817-2025-136-1-96-107

28. Uandykova, M. K., Astaubayeva, G. N., Mukhamejanova, G. S., & Mirkassimova, T. S. (2025). Innovative methods for developing decision support systems (DSS) in economic development management. Bulletin of "Turan" University, (1), 55–70. (In Kazakh). https://doi.org/10.46914/1562-2959-2025-1-1-55-70

29. Uandykova, M., Baitenova, L., Mukhamejanova, G., Yeleukulova, A., & Mirkassimova, T. (2024). Java coding using artificial intelligence. Frontiers in Computer Science, 6, 1473870. https://doi.org/10.3389/fcomp.2024.1473870

30. Uandykova, M., Baitenova, L., Astaubaeva, G., Mirkassimova, T., & Mukhamedzhanova, G. (2024). Model of Innovation-Based Economy Within the New Paradigm During the Relevant Economic Transformation. In Modeling and Simulation of Social-Behavioral Phenomena in Creative Societies (MSBC 2024), Communications in Computer and Information Science, vol. 2211. Springer, Cham. https://doi.org/10.1007/978-3-031-72260-8_12

REFERENCES

1. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. Online Browsing Platform (OBP). URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

2. National Institute of Standards and Technology. NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations. 2020. URL: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

3. Device42 Freshworks Inc. (2025). NIST CSF Categories: Description, Examples, and Best Practices. URL: https://www.device42.com/compliance-standards/nist-csf-categories/

4. CMMI Institute. CMMI® for Development, Version 2.0. 2018. URL: https://cmmiinstitute.com/cmmi/dev

5. FAIR Institute. Factor Analysis of Information Risk (FAIR) Model. Standard Artifact | Version 3.0. 2025. All Rights Reserved.

6. MITRE Corporation. (2024). MITRE ATT&CK® – A Knowledge Base of Adversary Tactics and Techniques Based on Real-World Observations.

7. Palo Alto Networks. What Are the Differences Between OT, ICS, & SCADA Security? Cyberpedia/

Network Security/OT and IoT Security. 2025. URL: https://www.paloaltonetworks.com/cyberpedia/ot-vs-ics-vs-scada-security

8. Eurobyte Company Blog. (2025). What Do IDS and IPS Mean in Information Security? URL: https://eurobyte.ru/articles/chto-znachit-ids-i-ips-v-informaczionnoj-bezopasnosti/

9. European Commission. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. 2016.

10. Positive Technologies. (2024). Current Cyber Threats in CIS Countries 2023–2024. Leader in Effective Cybersecurity. URL: https://ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-v-stranah-sng-2023-2024/#id1

11. The White House. (2018). National Cyber Strategy of the United States of America.

12. Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security, 10*(3), 211–230.

13. Smith, R. (2021). Critical Infrastructure Protection: A Comprehensive Approach to Cybersecurity. *Cybersecurity Journal.*

14. Kaspersky Lab. (2014). Stuxnet: The First Victims.

15. Kaspersky Lab. (2021). Dark Chronicles: The Consequences of the Colonial Pipeline Attack.

16. Investopedia. (n.d.). Risk Analysis: Definition, Types, Limitations, and Examples. Retrieved from https://www.investopedia.com/terms/r/risk-analysis.asp

17. SecurityScorecard. (n.d.). Qualitative vs. Quantitative Cybersecurity Risk Assessment: What's the Difference? Retrieved from https://securityscorecard.com/blog/qualitative-vs-quantitative-risk-assessment/

18. ISACA. (2021). Risk Assessment and Analysis Methods. *ISACA Journal,* 2021(2). Retrieved from https://www.isaca.org/resources/isaca-journal/issues/2021/volume-2/risk-assessment-and-analysis-methods

19. Riskaware. (n.d.). How to Measure Cybersecurity Risk: Key Metrics and Best Practices. Retrieved from https://riskaware.io/how-to-measure-cybersecurity-risk/

20. Amirkhanov, B., Amirkhanova, G., Kunelbayev, M., Adilzhanova, S., & Tokhtassyn, M. (2025). Evaluating HTTP, MQTT over TCP and MQTT over WEBSOCKET for digital twin applications: A comparative analysis on latency, stability, and integration. *International Journal of Innovative Research and Scientific Studies (IJIRSS), 8*(1), 679–694. https://doi.org/10.53894/ijirss.v8i1.4414

21. Adilzhanova, S., Kunelbayev, M., Amirkhanova, G., Zhussupov, Y., & Tortay, A. (2025). Development of a data collection and storage system for remote monitoring and detection of security threats in the enterprise. *International Journal of Innovative Research and Scientific Studies, 8*(2), 176–196. https://doi.org/10.53894/ijirss.v8i2.5136

22. Zeeshan Ali & Miin-Shen Yang. (2024). Improving Risk Assessment Model for Cybersecurity Using Robust Aggregation Operators for Bipolar Complex Fuzzy Soft Inference Systems. *Mathematics (MDPI).* https://doi.org/10.3390/math12040582

23. Lakhno, V., Bereke, M., Adilzhanova, S., et al. (2022). Genetic algorithm for solving the problem of scaling a cloud-oriented object of informatization. *Journal of Theoretical and Applied Information Technology, 100*(6).

24. Mirkassimova, T., Adilzhanova, S., Astaubaeva, G., & Mukhamedzhanova, G. (2025). Methods of information security risk analysis and assessment. *KazATK, 138*(3). https://vestnik.alt.edu.kz/index.php/journal/article/view/2675

25. Uandykova, M., Mirkasimova, T., Astaubaeva, G., Mukhamedzhanova, G., & Eleukulova, A. (2024). The advantages and necessity of integrating the Jira course into the educational program. *KazATK, 133*(4), 235–253. https://doi.org/10.52167/1609-1817-2024-133-4-235-253

26. Adilzhanova, S., Igilmanov, A., Tyulepberdinova, G., Salmanova, A., & Amirkhanova, G. (2024). The use of log analysis to identify DoS attacks and determine user behavior during the development of a digital twin of a food industry enterprise. *KazATK, 136*(1), 96–107. https://doi.org/10.52167/1609-1817-2025-136-1-96-107

27. Uandykova, M. K., Astaubayeva, G. N., Mukhamejanova, G. S., & Mirkassimova, T. S. (2025). Innovative methods for developing decision support systems (DSS) in economic development management. *Bulletin of "Turan" University, (1),* 55–70. (In Kazakh). https://doi.org/10.46914/1562-2959-2025-1-1-55-70

28. Uandykova, M., Baitenova, L., Mukhamejanova, G., Yeleukulova, A., & Mirkassimova, T. (2024). Java coding using artificial intelligence. *Frontiers in Computer Science, 6,* 1473870. https://doi.org/10.3389/fcomp.2024.1473870

29. Uandykova, M., Baitenova, L., Astaubaeva, G., Mirkassimova, T., & Mukhamedzhanova, G. (2024). Model of Innovation-Based Economy Within the New Paradigm During the Relevant Economic Transformation. In *Modeling and Simulation of Social-Behavioral Phenomena in Creative Societies (MSBC 2024), Communications in Computer and Information Science, vol. 2211.* Springer, Cham. https://doi.org/10.1007/978-3-031-72260-8_12

METHODS AND MODELS FOR ASSESSING THE CYBERSECURITY LEVEL OF STATE INFRASTRUCTURE

T. Sh. Mirkassimova[1,2]*, S. A. Adilzhanova[1]
[1]Al-Farabi Kazakh National University, Almaty, Kazakhstan
[2]NARXOZ University, Almaty, Kazakhstan

ABSTRACT

The article examines the challenges of ensuring the cybersecurity of state infrastructure amid increasing digital risks and the growing sophistication of cyber threats.

Purpose: The study aims to develop an integrated cybersecurity architecture based on international standards — ISO/IEC 27001, NIST SP 800-53, FAIR, CMMI, and MITRE ATT&CK — adapted to the national context of Kazakhstan.

Methodology: The research employs a systemic and comparative analysis of existing cybersecurity assessment models, threat modeling in ICS/SCADA environments, and an examination of relevant regulatory frameworks and guidelines.

Originality/Value: The originality of the study lies in the development of a conceptual cybersecurity architecture that integrates technological, organizational, and analytical components. The proposed model facilitates a shift from fragmented protective measures to a holistic risk management system, thereby enhancing the cyber resilience of state infrastructure.

Findings: The findings demonstrate that integrating international frameworks significantly improves the cybersecurity and resilience of governmental systems and contributes to establishing an effective model for incident monitoring and response.

Keywords: state infrastructure, cybersecurity, defense architecture, risk management, ISO/IEC 27001, NIST.

МЕТОДЫ И МОДЕЛИ ОЦЕНКИ УРОВНЯ КИБЕРБЕЗОПАСНОСТИ ГОСУДАРСТВЕННОЙ ИНФРАСТРУКТУРЫ

Т. Ш. Миркасимова[1,2]*, С. А. Адилжанова[1]
[1]Казахский национальный университет имени аль-Фараби, Алматы, Казахстан
[2]Университет Нархоз, Алматы, Казахстан

АННОТАЦИЯ

Статья посвящена анализу проблем обеспечения кибербезопасности государственной инфраструктуры в условиях роста цифровых рисков и усложнения киберугроз.

Цель исследования: разработка интегрированной архитектуры кибербезопасности, основанной на международных стандартах — ISO/IEC 27001, NIST SP 800-53, FAIR, CMMI и MITRE ATT&CK — с адаптацией к национальным условиям Казахстана.

Методология: в исследовании применяются системный и сравнительный анализ существующих моделей оценки кибербезопасности, моделирование угроз в средах ICS/SCADA, а также анализ нормативно-правовых актов и руководящих документов.

Оригинальность/ценность: научная новизна работы заключается в разработке концептуальной архитектуры кибербезопасности, объединяющей технологические, организационные и аналитические компоненты. Предложенная модель обеспечивает переход от фрагментарных мер защиты к целостной системе управления рисками, что способствует повышению киберустойчивости государственной инфраструктуры.

Результаты: проведённое исследование показало, что интеграция международных фреймворков существенно усиливает кибербезопасность и устойчивость государственных систем, а также способствует созданию эффективной модели мониторинга и реагирования на инциденты.

Ключевые слова: государственная инфраструктура, кибербезопасность, архитектура защиты, управление рисками, ISO/IEC 27001, NIST.

АВТОРЛАР ТУРАЛЫ

Миркасимова Толкын Шабденбековна – Нархоз университеті, Алматы, Қазақстан Республикасы, e-mail: tolkyn.mirkasimova@narxoz.kz, ORCID: https://orcid.org/0009-0003-1594-4012*

Адилжанова Салтанат Альмуханбетовна – әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан Республикасы, e-mail: asaltanat81@gmail.com, ORCID: https://orcid.org/0000-0003-1768-064X