ҒТАМР 81.93.29 https://doi.org/10.52081/tst.2026.v03.i15.086

ӨНДІРІСТІК КОРПОРАТИВТІК ЖӘНЕ ТЕХНОЛОГИЯЛЫҚ ЖЕЛІЛЕРДІ СЕГМЕНТАЦИЯЛАУ АРҚЫЛЫ АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ

Бекетова Г.С., PhD, доцент
beketova_gs@mail.ru, https://orcid.org/0000-0001-7160-1514
Калбаев Т.С., 7М06101 «Ақпараттық жүйелер» ББП 2-ші курс магистранты
kalbayevt@gmail.com, https://orcid.org/0009-0004-0155-3341

«Алматы технологиялық университеті» АҚ, Алматы қ., Қазақстан

Аңдатпа. Мақалада өндірістік кәсіпорындардың корпоративтік және технологиялық желілерін сегментациялау арқылы ақпараттық қауіпсіздікті қамтамасыз ету мәселесі қарастырылады. Өндірістік процестерді цифрландыру және ақпараттық (IT) мен операциялық (OT) технологиялардың интеграциясы корпоративтік ортадағы киберқауіптердің технологиялық желілерге таралу ықтималдығын арттырады. Зерттеудің мақсаты – сегментацияға негізделген өндірістік желінің ақпараттық қауіпсіздік архитектурасын әзірлеу және оның негізгі қорғаныс механизмдерін негіздеу. Зерттеуде жүйелік және салыстырмалы талдау, желілік архитектураны модельдеу және тәуекелдерді бағалау әдістері қолданылды. Корпоративтік IT желісі, өндірістік DMZ, SCADA/HMI, басқару (PLC) және өріс деңгейлері мен қауіпсіздікті басқару аймағынан тұратын алты аймақты модель ұсынылды; ол VLAN, желіаралық экрандар, қолжетімділікті басқару тізімдері және «default deny» саясатына сүйенеді. IT және OT орталарын тікелей байланыстырудың орнына аралық DMZ мен басқарылатын байланыс арналары (conduits) қолданылатын сегменттелген архитектура қауіптің таралу аймағын шектейтіні негізделді. Сегментацияны енгізудің сегіз кезеңді алгоритмі және оның тиімділігін бағалау көрсеткіштері ұсынылды. Ұсынылған тәсілді өндірістік процестердің үздіксіздігін бұзбай, кезең-кезеңімен енгізуге болады. Модель өндірістік желілердің құпиялылығын, тұтастығын және қолжетімділігін қамтамасыз ететін ақпараттық қауіпсіздікті басқару жүйесінің техникалық негізі бола алады.

Тірек сөздер: өндірістік желі, ақпараттық қауіпсіздік, IT/OT, желілік сегментация, SCADA, PLC, DMZ, киберқауіпсіздік.

Кіріспе. Қазіргі өндірістік кәсіпорындардың цифрлық трансформациясы ақпараттық технологиялар мен операциялық технологиялардың өзара байланысын күшейтуде. Бұрын өндірістік басқару жүйелері көбінесе оқшауланған немесе шектеулі қолжетімді желілерде жұмыс істесе, қазіргі кәсіпорындар өндірістік деректерді корпоративтік ақпараттық жүйелерге, аналитикалық платформаларға, бұлттық сервистерге және қашықтан басқару құралдарына беру қажеттілігіне ие. IT/OT интеграциясы өндірістік процестердің тиімділігін арттыруға мүмкіндік бергенімен, бір мезгілде киберқауіпсіздікке қойылатын талаптарды күрделендіреді [1–3].

Операциялық технологиялар (Operational Technology, OT) физикалық процестерді бақылауға немесе басқаруға тікелей қатысатын аппараттық және бағдарламалық жүйелерді қамтиды. Оларға өнеркәсіптік басқару жүйелері (ICS), SCADA, DCS, PLC, HMI және өндірістік желілік құрылғылар жатады. NIST SP 800-82 Rev.3 құжаты OT жүйелерінің ақпараттық жүйелерден ерекшелігі олардың сенімділік, қолжетімділік, уақыттық сипаттамалар және физикалық қауіпсіздік талаптарымен тығыз байланысты екенін атап көрсетеді [1].

Өндірістік инфрақұрылымда ақпараттық қауіпсіздікті қамтамасыз ету тек жеке құрылғыларды қорғаумен шектелмеуі тиіс. Кибершабуылдың бір сегменттен екіншісіне таралу мүмкіндігін шектеу үшін желілік архитектураның өзінде қауіпсіздік механизмдерін қалыптастыру қажет. Осы тұрғыдан алғанда, желілік сегментация өндірістік киберқауіпсіздіктің маңызды техникалық шараларының бірі болып табылады.

Желілік сегментацияның негізгі мақсаты – біртекті немесе функционалдық жағынан ұқсас ресурстарды жеке қауіпсіздік аймақтарына бөліп, олардың арасындағы байланыстарды бақылау. NIST ұсыныстарына сәйкес сегментация физикалық немесе

логикалық түрде іске асырылуы мүмкін. Логикалық сегментацияда VLAN технологиясы қолданылса, физикалық сегментация жеке желілік құрылғыларды немесе физикалық байланыстарды пайдалануды көздейді [1, 4].

IEC 62443-3-2:2020 стандарты өндірістік автоматтандыру және басқару жүйелерінің қауіпсіздігін бағалау кезінде жүйені қауіпсіздік талаптары ұқсас аймақтарға (zones) және осы аймақтар арасындағы бақыланатын байланыс арналарына (conduits) бөлу тәсілін қарастырады. Бұл тәсіл өндірістік жүйенің әрбір бөлігінің қауіпсіздік деңгейін жеке бағалауға және тиісті қорғаныс шараларын таңдауға мүмкіндік береді.

Осы зерттеудің **объектісі** – өндірістік кәсіпорындардың корпоративтік және технологиялық компьютерлік желілері.

Зерттеу пәні – корпоративтік IT және технологиялық OT желілерін сегментациялау арқылы ақпараттық қауіпсіздікті қамтамасыз ету әдістері.

Зерттеудің мақсаты – өндірістік корпоративтік және технологиялық желілер үшін сегментацияға негізделген ақпараттық қауіпсіздік архитектурасын әзірлеу және оның негізгі қорғаныс механизмдерін негіздеу.

Осы мақсатқа жету үшін келесі **міндеттер** қойылды:

- корпоративтік және технологиялық желілердің ерекшеліктерін талдау;
- IT/OT интеграциясынан туындайтын негізгі қауіптерді анықтау;
- өндірістік желілерді сегментациялау әдістерін зерттеу;
- қауіпсіздік аймақтары мен олардың арасындағы байланыстардың моделін қалыптастыру;
- VLAN, Firewall, ACL және DMZ механизмдерінің қолданылуын негіздеу;
- өндірістік желілерге арналған сегменттелген архитектураны ұсыну;
- ұсынылған архитектураның ақпараттық қауіпсіздікке әсерін бағалау.

Зерттеу барысында жүйелік талдау, салыстырмалы талдау, желілік архитектураны модельдеу, тәуекелдерді бағалау және қауіпсіздік талаптарын құрылымдау **әдістері** қолданылды.

Материалдар мен әдістер. Өндірістік желілерді зерттеу кезінде IT және OT орталарын функционалдық міндеттеріне қарай бөлу принципі қолданылды. Корпоративтік IT ортасына пайдаланушылардың жұмыс станциялары, файлдық серверлер, деректер базалары, корпоративтік қосымшалар, электрондық пошта және Интернетке шығатын сервистер жатқызылды.

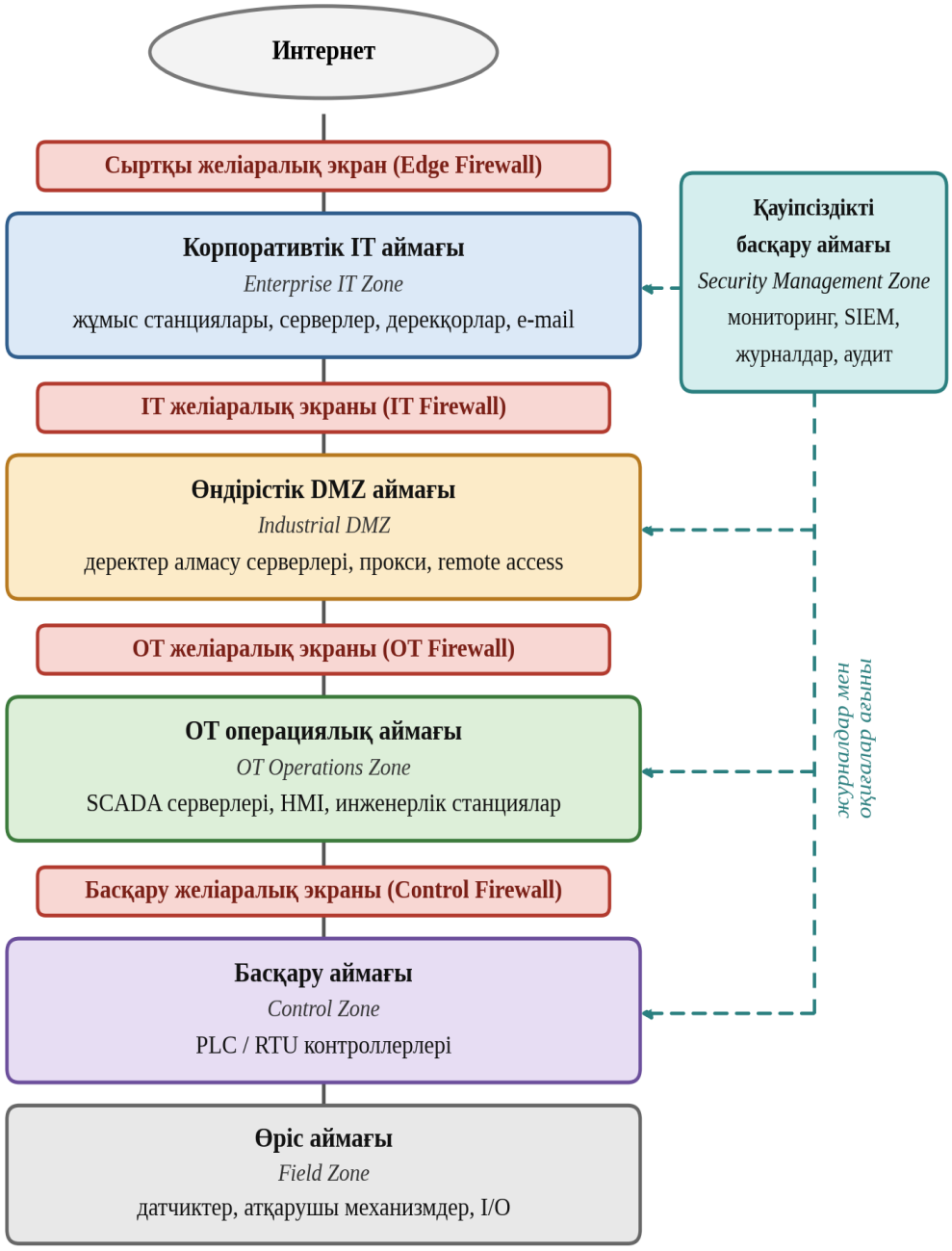
OT ортасына өндірістік процесті бақылау және басқару жүйелері енгізілді. Оның құрамына SCADA серверлері, HMI станциялары, PLC контроллерлері, инженерлік жұмыс станциялары және өндірістік Ethernet желілері кіруі мүмкін.

Өндірістік желілердің қауіпсіздік архитектурасын қалыптастыру кезінде қорғаныстың көпдеңгейлі тәсілі (defense-in-depth) қолданылды. Бұл тәсіл бойынша қауіпсіздік бір ғана желіаралық экранға тәуелді болмай, бірнеше өзара толықтыратын механизмдер арқылы қамтамасыз етіледі [5, 6].

Зерттеуде желіні төмендегідей негізгі сегменттерге бөлу ұсынылады:

1) **Enterprise IT Zone** – корпоративтік ақпараттық жүйелер орналасқан аймақ;
2) **Security Management Zone** – қауіпсіздікті басқару және мониторинг құралдары;
3) **Industrial DMZ** – IT және OT орталарын байланыстыратын аралық аймақ;
4) **OT Operations Zone** – SCADA, HMI және өндірістік серверлер орналасқан аймақ;
5) **Control Zone** – PLC және басқа өндірістік контроллерлер орналасқан аймақ;
6) **Field Zone** – датчиктер, атқарушы механизмдер және төменгі деңгейдегі өндірістік құрылғылар орналасқан аймақ.

Ұсынылатын архитектураның жалпы логикасы 1-суретте көрсетілген.



1-сурет – Өндірістік корпоративтік және технологиялық желілерді сегментациялаудың ұсынылатын архитектурасы

Ұсынылған архитектурада корпоративтік және технологиялық желілер арасында тікелей маршруттау ұйымдастырылмайды. IT және OT орталары арасындағы қажетті ақпараттық алмасу Industrial DMZ арқылы жүзеге асырылады. Бұл тәсіл өндірістік ресурстарға корпоративтік желіден тікелей қол жеткізуді шектеуге мүмкіндік береді.

Желілік сегментацияның екінші деңгейі VLAN технологиясы арқылы орындалуы мүмкін. Өндірістік кәсіпорын үшін VLAN құрылымының ықтимал нұсқасы 1-кестеде келтірілген.

1-кесте – Өндірістік кәсіпорын желісінің VLAN құрылымы

VLAN	Сегмент	Негізгі ресурстар
VLAN 10	Corporate Users	Қызметкерлердің жұмыс станциялары
VLAN 20	Servers	Корпоративтік серверлер
VLAN 30	Security	Мониторинг және қауіпсіздік құралдары
VLAN 40	Industrial DMZ	Аралық серверлер
VLAN 50	SCADA	SCADA және HMI
VLAN 60	PLC	PLC/RTU контроллерлері
VLAN 70	Management	Желілік құрылғыларды басқару
VLAN 80	Guest/External	Қонақтық және сыртқы қолжетімділік

VLAN қолдану бір физикалық инфрақұрылым ішінде логикалық оқшауланған желілерді қалыптастыруға мүмкіндік береді. Алайда VLAN өздігінен толық қауіпсіздік механизмі болып саналмайды. Сегменттер арасындағы маршрутизацияны бақылау және рұқсат етілмеген трафикті блоктау үшін Firewall немесе Layer 3 деңгейіндегі ACL механизмдері қолданылуы қажет [1].

Сегментация тиімділігін арттыру үшін «default deny» қағидасын қолдану ұсынылады. Яғни сегменттер арасындағы барлық байланыстар бастапқыда тыйым салынады, кейін өндірістік процестің жұмыс істеуі үшін нақты қажетті байланыстар ғана рұқсат етіледі.

Мысалы, SCADA серверінің PLC контроллерлерімен байланысы қажет болса, Firewall ережесінде тек нақты SCADA серверінің IP мекенжайынан тиісті PLC мекенжайларына қажетті протокол мен порттарға рұқсат беріледі.

Сегменттер арасындағы рұқсат саясатының жалпы түрі 2-кестеде көрсетілген.

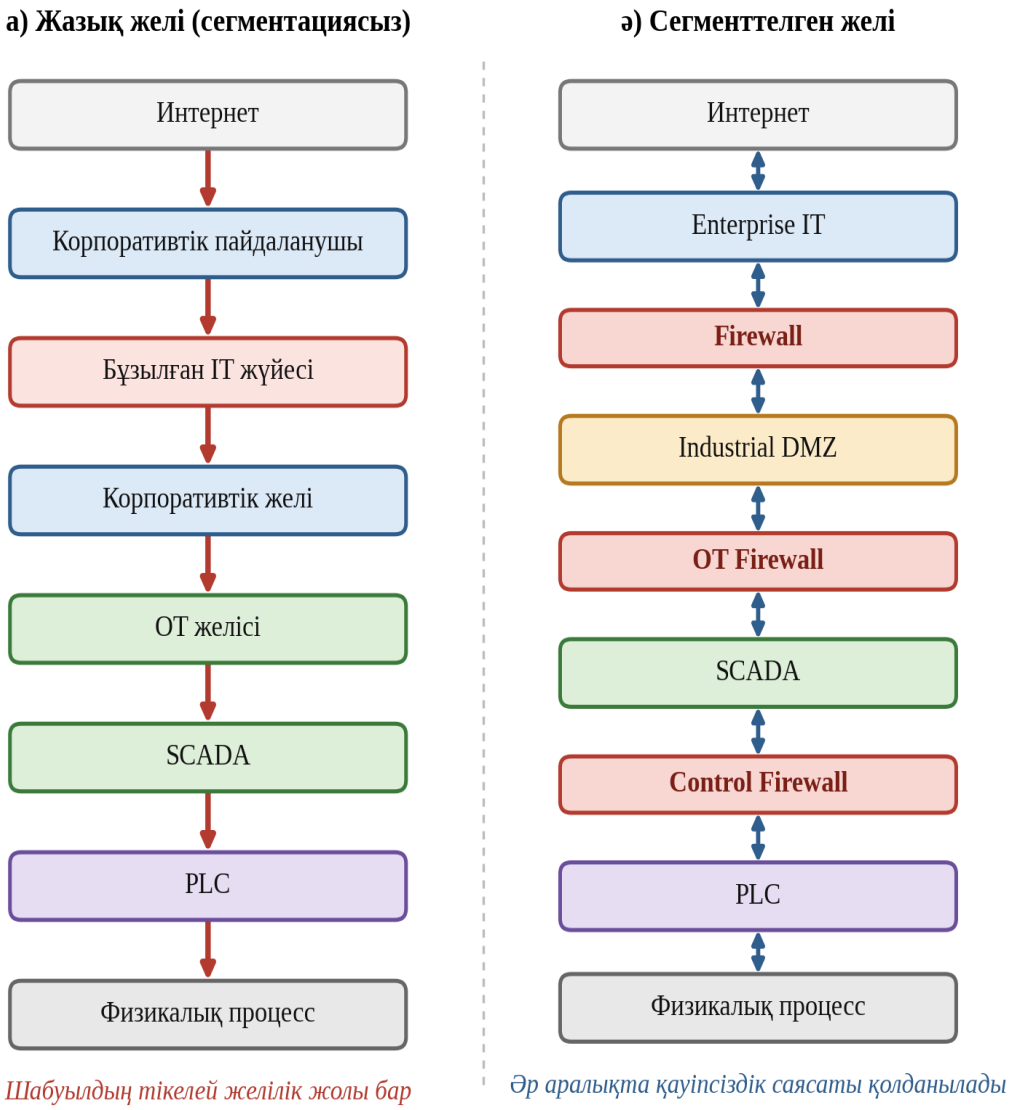
2-кесте – Сегменттер арасындағы рұқсат саясаты

Байланыс бағыты	Саясат
IT → OT	Тыйым салынады
IT → DMZ	Тек қажетті сервистерге рұқсат
DMZ → OT	Тек анықталған сервистерге рұқсат
OT → IT	Әдепкі бойынша тыйым салынады
SCADA → PLC	Қажетті басқару протоколдарына рұқсат
PLC → Internet	Тыйым салынады
Guest → OT	Толық тыйым салынады
Management → Network Devices	Әкімшілік протоколдарға шектеулі рұқсат

Бұл модельде желілік байланыстардың әрқайсысы жеке қауіпсіздік саясаты ретінде қарастырылады.

Нәтижелер және талқылау. Өндірістік желілерді сегментациялау мәселесін талдау көрсеткендей, IT және OT орталарын бір жазық желіге орналастыру кезінде қауіптің таралу аймағы кеңейеді. Мысалы, корпоративтік пайдаланушының жұмыс станциясы бұзылған жағдайда шабуылдаушы сол желілік сегментте орналасқан басқа ресурстарға желілік қолжетімділік алуға тырысуы мүмкін. Егер өндірістік басқару жүйелері осы желімен тікелей байланысты болса, қауіптің OT ортасына таралу мүмкіндігі пайда болады.

Қауіптің таралу бағыты мен сегментация енгізілгеннен кейінгі бақылау нүктелері 2-суретте салыстырмалы түрде көрсетілген. Сегментациясыз жазық желіде шабуыл Интернеттен бұзылған IT жүйесі арқылы корпоративтік желіге, одан OT желісіне, SCADA мен PLC-ге және физикалық процеске дейін тікелей жетуі мүмкін (2а-сурет). Сегментация енгізілген кезде бұл байланыс тізбегі бірнеше бақылау нүктелерімен бөлінеді (2ә-сурет).



2-сурет – Қауіптің таралу жолы: а) жазық желі; ә) сегменттелген желі

Осылайша шабуылдың бастапқы нүктесінен өндірістік басқару жүйесіне дейінгі тікелей желілік жол жойылып, әрбір аралықта қауіпсіздік саясаты қолданылады.

Бұл қорғаныстың көпдеңгейлі архитектурасына сәйкес келеді. NIST SP 800-82 Rev.3 желілік сегментация мен оқшаулауды OT орталарында defense-in-depth тәсілінің құрамдас бөлігі ретінде қарастырады. Құжатта физикалық және логикалық сегментация, VLAN, Firewall және басқа желілік оқшаулау құралдарын пайдалану арқылы коммуникацияларды шектеу ұсынылады [1].

IEC 62443-3-2 стандартының «zones and conduits» тұжырымдамасы да осы қағидаға негізделеді. Бірдей немесе ұқсас қауіпсіздік талаптары бар активтер бір зонаға біріктіріліп, олардың арасындағы коммуникациялар conduits арқылы басқарылуы тиіс.

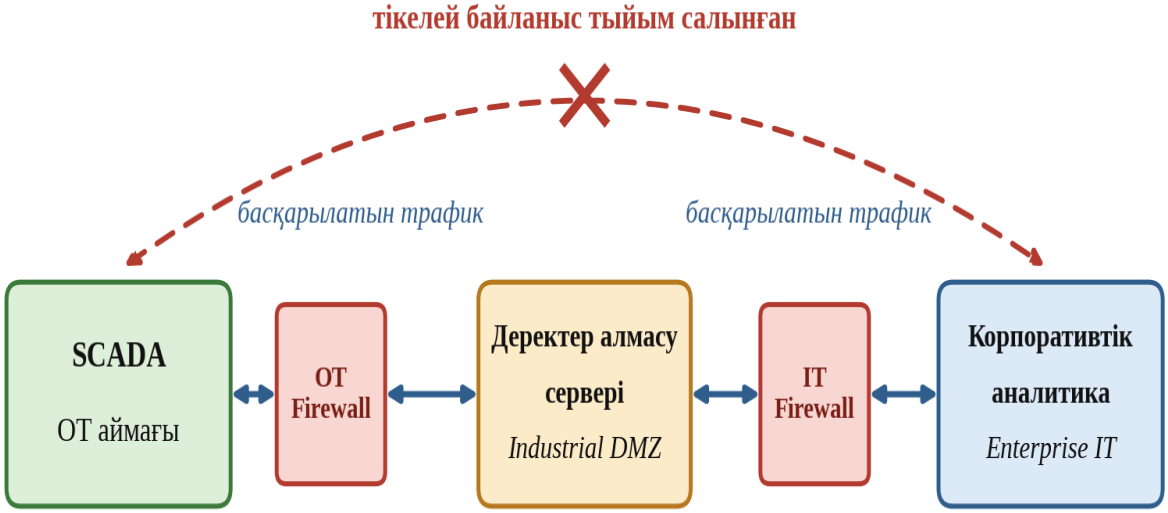
Осы принцип негізінде ұсынылған өндірістік архитектурада әрбір сегменттің өзінің қауіпсіздік мақсаты болады (3-кесте).

3-кесте – Өндірістік желі сегменттерінің қауіпсіздік міндеттері

Сегмент	Негізгі мақсаты	Негізгі қауіп
Enterprise IT	Корпоративтік процестерді қамтамасыз ету	Зиянды бағдарламалар, фишинг, рұқсатсыз қолжетімділік
Industrial DMZ	IT және OT арасында қауіпсіз ақпарат алмасу	Аралық серверлердің бұзылуы
OT Operations	Өндірісті бақылау	SCADA/HMI компрометациясы
Control	Өндірістік басқару	PLC-ге рұқсатсыз командалар
Field	Физикалық процеспен өзара әрекет	Құрылғыларды бұзу немесе манипуляциялау
Management	Инфрақұрылымды басқару	Әкімшілік есептік жазбалардың бұзылуы

Industrial DMZ сегменті ұсынылған архитектураның маңызды элементі болып табылады. DMZ корпоративтік және OT желілерін тікелей байланыстырудың орнына, деректерді алмасу үшін аралық орта қалыптастырады.

Мысалы, өндірістік деректерді корпоративтік аналитикалық жүйеге жіберу қажет болса, SCADA серверінен корпоративтік деректер базасына тікелей байланыс орнатудың орнына DMZ аймағында арнайы деректер алмасу серверін орналастыруға болады. Мұндай байланыс схемасы 3-суретте көрсетілген.



3-сурет – Industrial DMZ арқылы деректер алмасу схемасы

DMZ-де орналасқан серверлер үшін де минималды құқық қағидасы сақталуы тиіс. Сервер тек өзіне қажетті қызметтерге ғана қолжетімділік алуы қажет.

Зерттеу барысында сегментацияның тиімділігіне әсер ететін негізгі факторлар ретінде келесілер анықталды:

- активтерді дұрыс түгендеу;
- деректер ағындарын анықтау;
- желілік аймақтарды функционалдық және қауіпсіздік талаптарына сәйкес бөлу;
- сегменттер арасындағы байланыстарды құжаттау;
- Firewall ережелерін минималды қажеттілік қағидасы бойынша құру;
- әкімшілік қолжетімділікті бөлек басқару;
- журналдарды орталықтандырылған түрде жинау;
- желілік трафикті мониторингтеу;
- сегментация конфигурациясын тұрақты қайта қарау.

Сегментацияны енгізу алдында кәсіпорынның нақты ақпараттық ағындарын анықтау қажет. Бұл өте маңызды, себебі ОТ ортасында кейбір өндірістік құрылғылардың байланыстары толық құжатталмаған болуы мүмкін. NIST ұсыныстарына сәйкес сегменттер арасындағы қажетті коммуникацияларды анықтау үшін деректер ағындарын картаға түсіру маңызды болып табылады [1].

Сондықтан сегментацияны енгізудің ұсынылатын алгоритмі келесі кезеңдерден тұрады:

1-кезең – активтерді түгендеу. Барлық серверлер, жұмыс станциялары, PLC, SCADA, HMI, желілік құрылғылар және басқа өндірістік компоненттер анықталады.

2-кезең – деректер ағындарын анықтау. Қандай құрылғы қандай жүйемен, қандай протокол және қандай бағыт бойынша байланысатыны белгіленеді.

3-кезең – қауіпсіздік аймақтарын қалыптастыру. Ұқсас қауіпсіздік талаптары бар құрылғылар бір зонаға біріктіріледі.

4-кезең – conduits қалыптастыру. Аймақтар арасындағы қажетті байланыстар анықталады.

5-кезең – қауіпсіздік саясатын әзірлеу. Әр байланыс үшін рұқсат етілген source, destination, protocol және service анықталады.

6-кезең – Firewall/ACL конфигурациясы. Тек қажетті трафикке рұқсат беріліп, қалған байланыстар бұғатталады.

7-кезең – мониторинг және аудит. Firewall журналдары, желілік трафик, жүйелік журналдар және қауіпсіздік оқиғалары бақыланады.

8-кезең – тұрақты қайта бағалау. Жаңа активтер немесе өндірістік процестегі өзгерістер енгізілген сайын қауіпсіздік архитектурасы қайта қаралады.

Бұл алгоритм ақпараттық қауіпсіздікті бір реттік конфигурация емес, үздіксіз басқарылатын процесс ретінде қарастыруға мүмкіндік береді.

ISO/IEC 27001:2022 стандарты ақпараттық қауіпсіздікті басқару жүйесін тәуекелдерді басқаруға және ұйымның ақпараттық активтерінің құпиялылығы, тұтастығы және қолжетімділігін қамтамасыз етуге бағытталған жүйелік процесс ретінде қарастырады. Сондықтан желілік сегментацияны жеке техникалық шешім ретінде емес, кәсіпорынның жалпы ақпараттық қауіпсіздікті басқару жүйесінің техникалық бақылау шараларының бірі ретінде қарастырған жөн.

Сегментацияны тәуекелді бағалау нәтижелерімен байланыстыру үшін шартты тәуекел көрсеткішін (1) формуласы арқылы анықтауға болады:

$$R = P \times I, \tag{1}$$

мұндағы R – тәуекел деңгейі; P – қауіптің іске асу ықтималдығы; I – қауіптің ықтимал әсер ету деңгейі.

Егер белгілі бір ОТ активіне корпоративтік желіден тікелей қолжетімділік болса, P және I көрсеткіштері жоғары болуы мүмкін. Сегментация, Firewall және қолжетімділікті шектеу сияқты шаралар P мәнін төмендетуге бағытталады.

Сонымен қатар, қауіптің салдарын шектеу арқылы *I* көрсеткішіне де әсер етуге болады. Мысалы, SCADA сервері бұзылған жағдайда шабуылдаушының PLC желісіне тікелей өту мүмкіндігі болмаса, инциденттің өндірістік басқару деңгейіне таралу ықтималдығы шектеледі. ICS ортасында кибертәуекелдерді жүйелік деңгейде анықтау үшін тәуелділікті модельдеуге және Байес желілеріне негізделген әдістер ұсынылған [7]; (1) формуласы бұл әдістерге қарағанда қарапайым және сегментацияның әсерін алдын ала бағалауға арналған.

Өндірістік желілерде сегментацияны бағалау үшін келесі көрсеткіштерді қолдану ұсынылады:

- сегменттер саны;
- сегменттер арасындағы рұқсат етілген байланыстар саны;
- бұғатталған байланыстар үлесі;
- OT активтерінің корпоративтік желіден тікелей қолжетімділік деңгейі;
- рұқсат етілмеген трафик оқиғаларының саны;
- Firewall арқылы тіркелген қауіпсіздік оқиғалары;
- әкімшілік қолжетімділік арналарының саны;
- құжатталған және құжатталмаған деректер ағындарының арақатынасы.

Бұл көрсеткіштер сегментацияның техникалық жағдайын бақылаумен қатар, ақпараттық қауіпсіздікті басқару жүйесінің тиімділігін бағалауға мүмкіндік береді.

Зерттеудің маңызды нәтижелерінің бірі – корпоративтік және технологиялық желілер үшін бір ғана сегментация деңгейінің жеткіліксіз екендігін негіздеу. Біріншіден, корпоративтік IT және OT орталарын өзара бөлу қажет. Екіншіден, OT ішінде SCADA/HMI және PLC сияқты функционалдық деңгейлерді бөлу қажет. Үшіншіден, басқару сегменттеріне әкімшілік қолжетімділікті жеке қорғау қажет.

Осылайша үш деңгейлі сегментация моделін ұсынуға болады:

1-деңгей – IT/OT сегментациясы. Корпоративтік желі мен өндірістік желіні бөлу.

2-деңгей – OT ішіндегі функционалдық сегментация. SCADA, HMI және PLC желілерін бөлу.

3-деңгей – критикалық активтерді қорғау. Маңызды PLC, safety controller және басқа критикалық активтерге жеке қауіпсіздік саясатын қолдану.

Бұл тәсіл өндірістік желілерде defense-in-depth қағидасын іске асыруға мүмкіндік береді. Ғылыми зерттеулерде ICS сегментациясының өндірістік процестерге әсер ететін кибершабуылдардың домино әсерін шектеу құралы ретінде қолданылуы қарастырылған [8]. ICS киберқауіпсіздік құрылымдарын defense-in-depth өлшемдері бойынша бағалау жұмыстары да көпдеңгейлі қорғанысты негізгі талап ретінде қарастырады [9].

IT/OT интеграциясының қазіргі даму тенденциялары желілік архитектураға қойылатын талаптардың одан әрі күшеюіне алып келеді. Соңғы зерттеулер IT және OT интеграциясын коммуникация, өндірістік басқару, адам факторы және киберқауіпсіздік сияқты бірнеше өзара байланысты бағыттар арқылы қарастырады [10]. Оны практикада енгізу ұсыныстары IT/OT конвергенциясының қазіргі жай-күйін талдауға негізделеді [11]. Мұнай-газ нысандарындағы IT/OT конвергенциясы кезінде тәуекелдерді басқаруда адам факторын ескеру қажеттігі атап өтіледі [12], ал IT–OT конвергенциясына арналған салалық стандарттарға негізделген қауіпсіздік құрылымдары да ұсынылуда [13]. Сонымен қатар IT/OT конвергенциясы жағдайында сегментацияны нөлдік сенім (Zero Trust) қағидаттарымен толықтыру бағыты дамып келеді [14, 15]. Сондықтан өндірістік сегментация тек желілік құрылғыларды орналастыру мәселесі емес, ұйымның ақпараттық қауіпсіздігін басқару, активтерді басқару және өндірістік процестердің тұрақтылығын қамтамасыз ету мәселелерін біріктіретін кешенді міндет болып табылады.

SCADA жүйелерінің заманауи архитектуралары да желілік қосылымдардың кеңеюіне байланысты қауіпсіздік талаптарының артуын көрсетеді. Зерттеулерде SCADA жүйелерінің бұрынғы оқшауланған архитектуралардан қазіргі желілік және Интернетке

қосылған архитектураларға ауысуы олардың шабуыл бетінің кеңеюіне ықпал ететіні көрсетілген [16].

Сондықтан өндірістік желілер үшін ұсынылатын қауіпсіздік моделі келесі қағидаттарға негізделуі тиіс:

1) **Сегментация** – активтерді функционалдық және қауіпсіздік талаптарына қарай бөлу;

2) **Минималды қолжетімділік** – пайдаланушыға немесе жүйеге тек қажетті ресурстарға рұқсат беру;

3) **Default Deny** – анық көрсетілмеген байланыстарға тыйым салу;

4) **Defense-in-Depth** – бірнеше тәуелсіз қорғаныс деңгейін пайдалану;

5) **Мониторинг** – желілік трафик пен қауіпсіздік оқиғаларын тұрақты бақылау;

6) **Тұрақты аудит** – қауіпсіздік саясаты мен сегментация ережелерін кезеңдік қайта қарау;

7) **Қауіпсіздік талаптарын IT/OT өмірлік цикліне енгізу** – жаңа өндірістік жүйелерді жобалау кезінде қауіпсіздік талаптарын бастапқы кезеңнен ескеру.

Ұсынылған архитектураны өндірістік кәсіпорындарға енгізу кезінде маңызды мәселе – қолданыстағы OT жүйелерінің үздіксіздігін бұзбау. Кейбір өндірістік құрылғылар ұзақ уақыт бойы пайдаланылып, қазіргі заманғы қауіпсіздік механизмдерін толық қолдамауы мүмкін. Осы себепті сегментацияны енгізу кезінде өндірістік процестің қолжетімділігі бірінші кезектегі талаптардың бірі ретінде ескерілуі тиіс [1].

Сондықтан желілік қауіпсіздік шараларын енгізу өндірістік технологиялық процестермен келісіліп жүргізілуі қажет. Firewall ережелерін енгізу алдында нақты коммуникациялар анықталып, өзгерістерді тестілеу және кезең-кезеңімен енгізу жүзеге асырылуы тиіс.

Зерттеу нәтижелері сегментацияны дұрыс жобалау кезінде корпоративтік желідегі қауіптің OT ортасына таралу жолдарын қысқартуға, критикалық активтердің желілік оқшаулануын күшейтуге және желілік трафикті басқарудың ашық механизмін қалыптастыруға болатынын көрсетеді.

Қорытынды. Зерттеу барысында өндірістік корпоративтік және технологиялық желілерді сегментациялау арқылы ақпараттық қауіпсіздікті қамтамасыз ету мәселесі қарастырылды. IT және OT жүйелерінің өзара интеграциясы өндірістік процестерді цифрландыру үшін маңызды болғанымен, корпоративтік ортадан технологиялық ортаға киберқауіптердің таралуына жаңа мүмкіндіктер қалыптастырады.

Жүргізілген талдау өндірістік желілерді біртұтас жазық архитектурада орналастыру қауіптің таралу аймағын ұлғайтатынын көрсетті. Осыған байланысты корпоративтік IT, Industrial DMZ, OT Operations, Control және Field Zone деңгейлерінен, сондай-ақ қауіпсіздікті басқару аймағынан тұратын сегменттелген архитектура ұсынылды.

Ұсынылған модельдің негізгі ерекшелігі – корпоративтік және технологиялық желілер арасында тікелей байланысты болдырмау және қажетті ақпарат алмасуды басқарылатын аралық аймақ арқылы ұйымдастыру. Бұл тәсіл желіаралық экрандар, ACL, VLAN және мониторинг механизмдерімен толықтырылады.

Зерттеу нәтижесінде өндірістік желілерді қорғаудың негізгі принциптері анықталды: желілік сегментация, минималды қолжетімділік, default deny саясаты, defense-in-depth, деректер ағындарын бақылау және үздіксіз мониторинг.

IEC 62443 стандартындағы zones and conduits тұжырымдамасы өндірістік жүйелерді қауіпсіздік талаптарына сәйкес құрылымдауға мүмкіндік береді. NIST SP 800-82 Rev.3 ұсынымдары желілік сегментация мен оқшаулауды OT орталарын қорғаудың маңызды шараларының бірі ретінде қарастырады [1]. Ал ISO/IEC 27001:2022 талаптары желілік қауіпсіздік шараларын кәсіпорынның жалпы ақпараттық қауіпсіздікті басқару жүйесімен байланыстыруға мүмкіндік береді.

Осылайша, желілік сегментацияны тек техникалық конфигурация ретінде емес, өндірістік кәсіпорынның ақпараттық қауіпсіздігін басқару жүйесінің құрамдас бөлігі

ретінде қарастыру қажет. Сегментацияның тиімділігі активтерді түгендеу, деректер ағындарын анықтау, қауіпсіздік аймақтарын қалыптастыру, рұқсат саясатын әзірлеу және тұрақты мониторинг жүргізу процестерімен қамтамасыз етіледі.

Ұсынылған архитектураның практикалық маңызы – оны өндірістік кәсіпорындардың қолданыстағы желілік инфрақұрылымына кезең-кезеңімен енгізуге болатындығында. Болашақ зерттеулерде ұсынылған модельді нақты өндірістік желі стендінде тәжірибелік сынақтан өткізу, қауіп сценарийлерін модельдеу, желілік трафиктің өзгеруін талдау және сегментация енгізілгенге дейінгі және енгізілгеннен кейінгі тәуекел деңгейлерін сандық салыстыру қарастырылады.

Әдебиеттер:

[1] **Stouffer, K.,** Pease M., Tang C., Zimmerman T., Pillitteri V., Lightman S., Hahn A., Saravia S., Sherule A., Thompson M. Guide to Operational Technology (OT) Security. NIST Special Publication 800-82 Rev. 3. Gaithersburg: National Institute of Standards and Technology, 2023. DOI: 10.6028/NIST.SP.800-82r3.

[2] **Bhamare, D.,** Zolanvari M., Erbad A., Jain R., Khan K., Meskin N. Cybersecurity for industrial control systems: A survey // Computers & Security. – 2020. – Vol. 89. Article 101677. DOI: 10.1016/j.cose.2019.101677.

[3] **Maleh, Y.** IT/OT convergence and cyber security // Computer Fraud & Security. –2021.– No. 12. – P. 13-16. DOI: 10.1016/S1361-3723(21)00129-9.

[4] **Yatagha, R.,** Waedt K., Schindler J., Kirdan E. Security challenges and best practices for resilient IIoT Networks: Network Segmentation // INFORMATIK 2023. 2023. P. 2051–2070. DOI: 10.18420/inf2023_204.

[5] **Mell, P.,** Shook J., Harang R. Measuring and Improving the Effectiveness of Defense-in-Depth Postures // Proceedings of the 2nd Annual Industrial Control System Security Workshop. – 2016. DOI: 10.1145/3018981.3018986.

[6] **Fielder A.,** Li T., Hankin C. Defense-in-depth vs. critical component defense for industrial control systems // Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research. – 2016.– P. 1-10. DOI: 10.14236/ewic/ICS2016.1.

[7] **Rotibi, A.O.,** Saxena N., Burnap P., Reed C. System-level operational cyber risks identification in industrial control systems // Cyber-Physical Systems. – 2025. – Vol. 11.– No. 3. P. 265-296. DOI: 10.1080/23335777.2024.2373388.

[8] **Arief, R.,** Khakzad N., Pieters W. Mitigating cyberattack related domino effects in process plants via ICS segmentation // Journal of Information Security and Applications. – 2020.– Vol. 51. Article 102450. DOI: 10.1016/j.jisa.2020.102450.

[9] **Lima, E.P.** Rodriguez Esquerre V.F. Industrial Control System Cyber Security Frameworks: Assessment using Defense-in-Depth Criteria // International Journal of Information Security. – 2026. – Vol. 25. Article 99. DOI: 10.1007/s10207-026-01260-y.

[10] **Venanzi, R.** ,Di Modica G., Foschini L., Bellavista P. Towards IT/OT integration in industry digitalization: A comprehensive survey // Journal of Network and Computer Applications.– 2026. – Vol. 245. Article 104373. DOI: 10.1016/j.jnca.2025.104373.

[11] **Hantsch, C.,** Westner M., Matschi M. IT/OT-Konvergenz: Status-Quo und Umsetzungsempfehlungen // HMD Praxis der Wirtschaftsinformatik.– 2025. –Vol. 62.– P. 402-418. DOI: 10.1365/s40702-024-01111-1.

[12] **Imran, H.,** Turner C., Nassar S., Tran Y., Salama M. Human-centered cybersecurity risk management for IT/OT-converged oil and gas operating facilities // Computers & Security. – 2026. – Vol. 167. Article 104918. DOI: 10.1016/j.cose.2026.104918.

[13] **Schachinger, F.-K.,** Rosenstatter T., Pache U. PURITY – An Industry-Standard-Based Security Framework for IT-OT Convergence // IEEE Access.–2026.– Vol. 14.– P. 57014-57032. DOI: 10.1109/ACCESS.2026.3682366.

[14] **Slatvinska, V.,** Bevza V. Zero-Trust Architecture for Industrial IoT (IIoT): Protecting Critical Infrastructure in IT/OT Convergence // Scientific Papers of Donetsk National Technical University.– 2026. –DOI: 10.32782/2786-9024/v4i6(38).359304.

[15] **Purohit, S.,** Bridging IT and OT: Cybersecurity Risks, Zero-Trust Solutions, and Industrial Resilience in Oil & Gas Downstream // ASEAN Journal of Scientific and Technological Reports.– 2026.– Vol. 29.– No. 5. DOI: 10.55164/ajstr.v29i5.262008.

[16] **Yadav, G.,** Paul K. Architecture and security of SCADA systems: A review // International Journal of Critical Infrastructure Protection.–2021.–Vol. 34. Article 100433. DOI: 10.1016/j.ijcip.2021.100433.

References:

[1] **Stouffer, K.,** Pease M., Tang C., Zimmerman T., Pillitteri V., Lightman S., Hahn A., Saravia S., Sherule A., Thompson M. Guide to Operational Technology (OT) Security. NIST Special Publication 800-82 Rev. 3. Gaithersburg: National Institute of Standards and Technology, 2023. DOI: 10.6028/NIST.SP.800-82r3.

[2] **Bhamare, D.,** Zolanvari M., Erbad A., Jain R., Khan K., Meskin N. Cybersecurity for industrial control systems: A survey // Computers & Security. 2020. Vol. 89. Article 101677. DOI: 10.1016/j.cose.2019.101677.

[3] **Maleh, Y.** IT/OT convergence and cyber security // Computer Fraud & Security. 2021. No. 12. P. 13–16. DOI: 10.1016/S1361-3723(21)00129-9.

[4] **Yatagha, R.,** Waedt K., Schindler J., Kirdan E. Security challenges and best practices for resilient IIoT Networks: Network Segmentation // INFORMATIK 2023. 2023. P. 2051–2070. DOI: 10.18420/inf2023_204.

[5] **Mell, P.,** Shook J., Harang R. Measuring and Improving the Effectiveness of Defense-in-Depth Postures // Proceedings of the 2nd Annual Industrial Control System Security Workshop. 2016. DOI: 10.1145/3018981.3018986.

[6] **Fielder, A.,** Li T., Hankin C. Defense-in-depth vs. critical component defense for industrial control systems // Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research. 2016. P. 1–10. DOI: 10.14236/ewic/ICS2016.1.

[7] **Rotibi, A.O.,** Saxena N., Burnap P., Reed C. System-level operational cyber risks identification in industrial control systems // Cyber-Physical Systems. 2025. Vol. 11, No. 3. P. 265–296. DOI: 10.1080/23335777.2024.2373388.

[8] **Arief, R.,** Khakzad N., Pieters W. Mitigating cyberattack related domino effects in process plants via ICS segmentation // Journal of Information Security and Applications. 2020. Vol. 51. Article 102450. DOI: 10.1016/j.jisa.2020.102450.

[9] **Lima, E.P.,** Rodriguez Esquerre V.F. Industrial Control System Cyber Security Frameworks: Assessment using Defense-in-Depth Criteria // International Journal of Information Security. 2026. Vol. 25. Article 99. DOI: 10.1007/s10207-026-01260-y.

[10] **Venanzi, R.,** Di Modica G., Foschini L., Bellavista P. Towards IT/OT integration in industry digitalization: A comprehensive survey // Journal of Network and Computer Applications. 2026. Vol. 245. Article 104373. DOI: 10.1016/j.jnca.2025.104373.

[11] **Hantsch, C.,** Westner M., Matschi M. IT/OT-Konvergenz: Status-Quo und Umsetzungsempfehlungen // HMD Praxis der Wirtschaftsinformatik. 2025. Vol. 62. P. 402–418. DOI: 10.1365/s40702-024-01111-1.

[12] **Imran, H.,** Turner C., Nassar S., Tran Y., Salama M. Human-centered cybersecurity risk management for IT/OT-converged oil and gas operating facilities // Computers & Security. 2026. Vol. 167. Article 104918. DOI: 10.1016/j.cose.2026.104918.

[13] **Schachinger, F.-K.,** Rosenstatter T., Pache U. PURITY – An Industry-Standard-Based Security Framework for IT-OT Convergence // IEEE Access. 2026. Vol. 14. P. 57014–57032. DOI: 10.1109/ACCESS.2026.3682366.

[14] **Slatvinska, V.,** Bevza V. Zero-Trust Architecture for Industrial IoT (IIoT): Protecting Critical Infrastructure in IT/OT Convergence // Scientific Papers of Donetsk National Technical University. 2026. DOI: 10.32782/2786-9024/v4i6(38).359304.

[15] **Purohit, S.,** Bridging IT and OT: Cybersecurity Risks, Zero-Trust Solutions, and Industrial Resilience in Oil & Gas Downstream // ASEAN Journal of Scientific and Technological Reports. 2026. Vol. 29, No. 5. DOI: 10.55164/ajstr.v29i5.262008.

[16] **Yadav, G.,** Paul K. Architecture and security of SCADA systems: A review // International Journal of Critical Infrastructure Protection. 2021. Vol. 34. Article 100433. DOI: 10.1016/j.ijcip.2021.100433.

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПУТЁМ СЕГМЕНТАЦИИ ПРОИЗВОДСТВЕННЫХ КОРПОРАТИВНЫХ И ТЕХНОЛОГИЧЕСКИХ СЕТЕЙ

Бекетова Г.С., PhD, доцент
Калбаев Т.С., магистрант 2 курса ОП 7М06101 «Информационные системы»

АО «Алматинский технологический университет», г. Алматы, Казахстан

Аннотация. В статье рассматривается обеспечение информационной безопасности производственных предприятий путём сегментации корпоративных и технологических сетей. Цифровизация производственных процессов и интеграция информационных (IT) и операционных (OT) технологий повышают вероятность распространения киберугроз из корпоративной среды в технологические сети. Цель исследования – разработка архитектуры информационной безопасности производственной сети на основе сегментации и обоснование её основных механизмов защиты. Применены системный и сравнительный анализ, моделирование сетевой архитектуры и оценка рисков. Предложена модель из шести зон: корпоративная IT-сеть, промышленная DMZ, уровни SCADA/HMI, управления (PLC) и полевой уровень, а также зона управления безопасностью; в ней используются VLAN, межсетевые экраны, списки контроля доступа и политика «default deny». Обосновано, что сегментированная архитектура с промежуточной DMZ и контролируемыми каналами связи (conduits) вместо прямого соединения IT- и OT-сред ограничивает область распространения угроз. Предложены восьмиэтапный алгоритм внедрения сегментации и показатели оценки её эффективности. Предложенный подход можно внедрять поэтапно, не нарушая непрерывности производственных процессов. Модель может служить технической основой системы управления информационной безопасностью, обеспечивающей конфиденциальность, целостность и доступность производственных сетей.

Ключевые слова: производственная сеть, информационная безопасность, IT/OT, сегментация сети, SCADA, PLC, DMZ, кибербезопасность.

ENSURING INFORMATION SECURITY THROUGH SEGMENTATION OF INDUSTRIAL CORPORATE AND TECHNOLOGICAL NETWORKS

Beketova G.S., PhD, associate professor
Kalbayev T.S., 2nd-year Master's student of the EP 7M06101 «Information Systems»

JSC «Almaty Technological University», Almaty, Kazakhstan

Annotation. The article addresses the problem of ensuring the information security of industrial enterprises through the segmentation of corporate and technological networks. The digitalization of production processes and the integration of information technologies (IT) and operational technologies (OT) increase the likelihood that cyber threats will spread from the corporate environment to technological networks. The aim of the study is to develop a segmentation-based information security architecture for an industrial network and to substantiate its main protection mechanisms. Systems analysis, comparative analysis, modelling and risk assessment were used. A six-zone model is proposed, comprising the enterprise IT network, an industrial DMZ, the SCADA/HMI level, the control (PLC) level, the field level and a security management zone; it relies on VLANs, firewalls, access control lists and a default-deny policy. It is shown that a segmented architecture with an intermediate DMZ and controlled communication channels (conduits), instead of a direct connection between IT and OT environments, limits the area over which threats can spread. An eight-stage algorithm for implementing segmentation and indicators for assessing its effectiveness are proposed. The model can serve as the technical basis of an information security management system that ensures the confidentiality, integrity and availability of industrial networks.

Keywords: industrial network, information security, IT/OT, network segmentation, SCADA, PLC, DMZ, cybersecurity.