Information about the authors

Zhanna Bakirbayevna Sadirmekova – leading researcher at Q University, associate professor, Republic of Kazakhstan; e-mail: Janna_1988@mail.ru. ORCID: https://orcid.org/0000-0002-7514-9315.

Bayangali Khayerberliuly Abdygalym – master of technical sciences, Phd student of the Department of Information Systems, L.N. Gumilyov Eurasian National University, Software engineer at "Q" University, Republic of Kazakhstan; e-mail: bayangali.abd@gmail.com. ORCID: https://orcid.org/0009-0001-8872-7428.

Madina Aralbayevna Sambetbayeva* – PhD, associate professor of the Department of Information Systems, L.N. Gumilyov Eurasian National University, leading researcher at Q University, Republic of Kazakhstan; e-mail: sambetbayeva_ma_1@enu.kz. ORCID: https://orcid.org/0000-0001-9358-1614.

Roman Taberkhan – master of technical sciences, Phd student of the Department of Information Systems, L.N. Gumilyov Eurasian National University; e-mail: rn_82@bk.ru. ORCID: https://orcid.org/0000-0002-3375-4947.

Indira Askarbekovna Karbozova – Senior Lecturer of the Department of Information and Communication Technologies, Taraz International University named after Sherkhan Murtaza, Republic of Kazakhstan; e-mail: karbozovaindira77@gmail.com. ORCID: https://orcid.org/0000-0002-7514-9315.

Received 05.01.2026
Revised 20.02.2026
Accepted 23.02.2026

https://doi.org/10.53360/2788-7995-2026-1(21)-12

ҒТАХР: 81.93.29

К.М. Сагиндыков[1] ,Ф.Б. Тебуева[2], Н.Ж. Мукушева[13]*
[1]Л.Н. Гумилёв атындағы Еуразия ұлттық университеті,
0100008, Қазахстан Республикасы, Сәтпаев көшесі, 2. Астана қ.
[2]Солтүстік-Кавказ федеральдық университеті,
355017, Россия, Ставрополь қ., Пушкина көшесі, 1,
*e-mail: nazym9_1@mail.ru

КИБЕРФИЗИКАЛЫҚ ЖҮЙЕЛЕРГЕ ЖАСАЛАТЫН КӨПВЕКТОРЛЫ ШАБУЫЛДАР: МЕХАНИЗМДЕРІ, АНЫҚТАУ ЖӘНЕ ҚОРҒАУ МЫСАЛДАРЫ

***Аңдатпа*:** *Мақалада киберфизикалық жүйелерде (КФЖ) жүзеге асырылатын көпвекторлы кибершабуылдарға кешенді және тереңдетілген шолу ұсынылады. Зерттеу барысында КФЖ архитектурасының негізгі алғышарттары, ақпараттық және операциялық технологиялар (IT/OT) тоғысындағы қауіп-қатер модельдері, сондай-ақ кибер және физикалық әсерлерді үйлестіру механизмдері егжей-тегжейлі талданады. Шабуылдардың негізгі түрлері, атап айтқанда жалған деректерді енгізу (FDI/FDIA), өнеркәсіптік басқару жүйелері мен PLC-лерге бағытталған зиянды программалар, supply-chain шабуылдары, ransomware, қызмет көрсетуден бас тарту (DoS) шабуылдары, insider-қатерлер және тікелей физикалық араласу жүйеленеді. Олардың бірыңғай компрометация сценарийі аясында өзара байланысы мен күшейту әсері көрсетіледі.*

Ашық ғылыми зерттеулер мен салалық есептерге сүйене отырып, Stuxnet, Украинаның энергетикалық инфрақұрылымына жасалған шабуылдар, CrashOverride/Industroyer, TRITON/Trisis және өнеркәсіптік ортадағы ransomware инциденттері талданады. Сонымен қатар «Шабуыл түрі – КФЖ қабаты» қағидатына негізделген тәуекелге бағдарланған матрица ұсынылады. IT/OT оқиғаларын корреляциялау және машиналық оқыту әдістерін қолдану арқылы аномалияларды анықтаудың тәжірибелік пайплайны сипатталады.

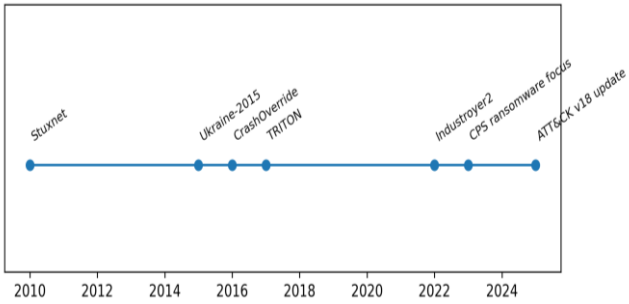
Жұмыс КФЖ архитектурасын, көпвекторлы операциялардың өмірлік циклін және СТ РК ISO/IEC 27001, NIST, ISA/IEC 62443, MITRE ATT&CK for ICS стандарттарына сәйкес инженерлік қорғаныс шараларын бейнелейтін кестелер, схемалар мен графиктерді қамтиды.

Түйін сөздер: *көпвекторлы шабуылдар, FDI, supply-chain, ransomware, TRITON, Industroyer, аномалияларды анықтау.*

Кіріспе

Киберфизикалық жүйелер (КФЖ) есептеу, коммуникациялық және физикалық компоненттерді басқарудың бірыңғай контурына біріктіреді. Бұл жерде цифрлық әрекеттер

тікелей материалдық процестерге әсер етеді [1]. Мұндай жүйелерге өнеркәсіптік басқару жүйелері (ICS/SCADA), энергетикалық жүйелер, көлік кешендері, су тазарту жүйелері, «ақылды» ғимараттар сонымен қатар медициналық құрылғылар жатады. Байланыстылықтың артуы, IIoT-құрылғыларын енгізу және АТ мен ОТ-тың конвергенциясы процестердің тиімділігі мен бақыланымдылығын арттырады. Бірақ-та ол шабуыл бетінің артыуынада әкеледі [16]. Дәстүрлі корпоративтік АТ-желілерден айырмашылығы, КФЖ уақытша кідірістерге, қолжетімділікке және пайдаланудың қауіпсіздігіне қатаң талаптар қояды және де талап етеді. Сондықтан классикалық қорғаныс шараларының көпшілігі бейімдеуді қажет етеді [4]. Киберфизикалық жүйелерге бағытталған көпвекторлы шабуылдарға қатысты негізгі инциденттері мен маңызды кезеңдері (1 сурет).



Сурет 1 − Киберфизикалық жүйелерге бағытталған көпвекторлы шабуылдарға қатысты негізгі инциденттері мен маңызды кезеңдері (ашық дереккөздерден жинақталған)

1-суреттегі хронология жекелеген, жоғары мамандандырылған операциялардан APT-науқандары мен жаппай шабуылдардың үйлесіміне көшу үрдісін көрсетеді. Бұл КФЖ-ны қорғау стратегиясы физикалық әсері бар күрделі, нысаналы сценарийлерді де, сондай-ақ өндіріс тәуелді болатын АТ-сервистердің компрометациясы арқылы ауқымды тоқтап қалуларға әкелуі мүмкін шабуылдарды да қамтуы тиіс екенін білдіреді.

Материалдар мен әдістер

КФЖ қауіпсіздігі бойынша жүйелі шолулар компоненттер мен домендердің (кибер, физикалық және олардың түйісуі) әртүрлілігін, сондай-ақ қауіп-қатерлер мен қарсы шаралардың бірмәнді модельдеріне қажеттілікті атап өтеді [1]. Humayed және әріптестерінің еңбектерінде «қауіпсіздік перспективасы – CPS компоненттері – жүйелер кластары» координаталары аясында қауіп-қатерлерді, осалдықтарды, шабуылдарды және қорғаныс шараларын біріктіретін құрылым (framework) ұсынылған [1]. Бұл тәсіл зерттеу нәтижелері мен тәжірибелық ұсынымдарды салыстыруға қолайлы (кесте 1).

Кесте 1 − КФЖ қауіпсіздігін зерттеудің негізгі бағыттары және оларға тән әдістер

Зерттеу аймағы	Негізгі қиындықтар	Типтік әдістер
Энергетикадағы FDI/FDIA шабуылдары	Bad-data detection-ды айналып өту, күйді бағалауды манипуляциялау	Күй модельдері, ML/DRL, өлшемдерді корреляциялау
ICS/PLC malware	Басқару логикасын өзгерту, физикалық процестерге жасырын әсер ету	Forensics, whitelisting, тұтастықты бақылау
Supply-chain	Сенімді жаңартулар мен жеткізушілердің компрометациясы	SBOM, қолтаңбалар, secure SDLC, аудит
ОТ ортадағы ransomware шабуылдары	Конфигурацияны шифрлау, қарапайым	Сегменттеу, offline-backup, EDR/IDS
Аномалияларды анықтау	Әлсіз сигналдық ауытқулар, шу/дрейф	Isolation Forest, автоэнкодерлер, сандық егіздер

Энергетика және «ақылды желілер» саласында өлшемдерді жалған алмастыру шабуылдарына (false data injection) қатысты жеке бағыт қалыптасты. Liu-Ning-Reiter (2009) классикалық еңбегінде жүйе конфигурациясы белгілі болған жағдайда, шабуылдаушы стандартты «жарамсыз өлшемдерді» анықтау әдістерін айналып өтетіндей инъекция векторын құра алатыны көрсетілді [2]. Осы тұжырымдама негізінде FDIA-ны анықтау әдістері

дамытылуда. Оның ішінде статистикалық тәсілдер, машиналық оқыту және терең оқыту (соның ішінде DRL-тәсілдер) бар [19-21] .

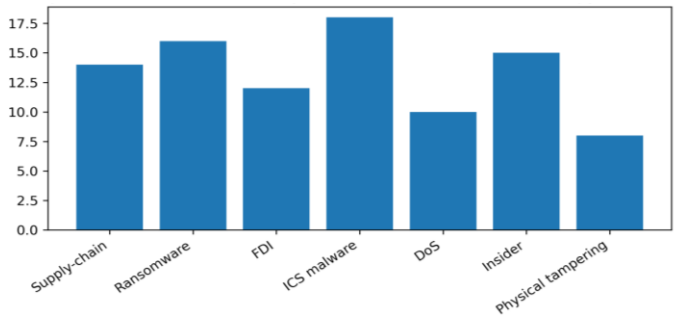
Өнеркәсіптік қауіпсіздікке арналған тәжірибиге негізделген жарияланымдар, академиялық зерттеулерді нақты инциденттерді егжей-тегжейлі талдаумен толықтырады. CrashOverride/Industroyer бойынша аналитикалық материалдар қосымша станциялар протоколдарын теріс пайдалану және зиянды программалық қамтамасыз етудің модульдік архитектурасын сипаттайды [12-14]. TRITON жөніндегі еңбектер Safety Instrumented Systems (SIS) жүйелеріне бағытталған шабуылдың бірегейлігін атап өтіп, келтірілетін зиянды safety-тәуекелдер жазықтығына көшіреді [9-11]. ОТ-ны қорғау жөніндегі NIST ұсынымдары және ISA/IEC 62443 тәсілі сегментацияға, тәуекелдерді басқаруға, қауіпсіз әзірлеуге және қорғалу деңгейлеріне қойылатын талаптарды рәсімдейді [4,5].

КФЖ архитектурасы әдетте көпқабатты болады (2 сурет). Олар физикалық процесс пен далалық құрылғылардан бастап контроллерлерге, диспетчерлеу деңгейіне және корпоративтік сервистерге дейін болады. Деректердің екіжақты алмасуы басқару мен телеметрияны қамтамасыз етеді. Алайда шабуылдың таралу арналарының пайда болуына әкеледі. Көпвекторлылық домендер шекараларының қиылысында мыналар пайда болады. АТ-сегменттің компрометациясы jump-server-ге, одан әрі инженерлік станцияға немесе SCADA жүйесіне қол жеткізуге мүмкіндік беруі мүмкін. Қауіптер мердігерлердің қашықтан қол жеткізуі, бұлттық интеграция және криптографиялық қорғанысы жоқ протоколдардың болуы салдарынан күшейе түседі.

Сурет 2 − КФЖ-ның эталондық архитектурасы (1-5 деңгейлер) және деректердің екіжақты алмасуы каскадты тәуекелдердің көзі ретінде

Нәтижелер және талдаулар

Тәуекелдерді тәжірибелік тұрғыда басқару үшін шабуылдарды әсер ету түрі және әсерге қол жеткізілетін архитектура деңгейі бойынша жіктеу маңызды. Төменде көпвекторлы шабуылдардың ең кең таралған кластары, шабуылдаушы тұрғысынан олардың күшті және әлсіз жақтары көрсетілген (3 сурет). Сондай-ақ КФЖ үшін тән тәуекел профилі қарастырылады.



Сурет 3 − КФЖ-ға бағытталған негізгі шабуыл векторларының үлестірімі (дереккөздерге шолу негізінде жасалған иллюстративтік синтез)

FDI-шабуылдары өлшеулерді немесе басқарушы әсерлерді алмастыруға бағытталады, соның салдарынан басқару жүйесі қате шешімдер қабылдайды [2, 19]. Күшті жағы – процесс моделі болған жағдайда жасырындылығы. Әлсіз жағы – өлшеу арналарына қол жеткізу және объект туралы терең білімнің қажеттілігі. Өлшеу қателері апаттық режимге немесе жабдықтың

көзге байқалмайтын деградациясына әкелуі мүмкін және жүйелер үшін тәуекел деңгейі жоғары болады.

КФЖ-дегі ransomware шабуылдары көбіне өндірістің АТ-сервистерге тәуелділігі арқылы ОТ ортасына әсер етеді [17, 18]. Күшті жағы -– тоқтап қалу әсерінің жылдам байқалуы. Әлсіз жағы – дұрыс ұйымдастырылған offline-резервтер мен сегментация болған жағдайда қалпына келтіру мүмкіндігі. Тоқтап қалуға төзімділігі шектеулі объектілер үшін тәуекел жоғары болады.

Жеткізу тізбегінің компрометациясы - ең қауіпті кластарының бірі болып есептеледі. Шабуылдаушы сенімді жаңартуларға немесе компоненттерге зиянды өзгерістерді енгізеді [18]. Күшті жағы – ауқымдылығы мен жасырындылығы. Әлсіз жағы – іске асырудың жоғары құны. ОТ жүйелерінің сенімділігі мен ұзақ өмірлік цикліне байланысты тәуекел өте жоғары болады.

Арнайы платформалар (Stuxnet, Industroyer, TRITON) контроллерлердің логикасын өзгертіп, физикалық процеске тікелей әсер ете алады [7-9,12,14]. Күшті жағы – физикалық әсердің болуы. Әлсіз жағы – әзірлеудің күрделілігі және объектіні терең білудің қажеттілігі. Критикалық объектілер үшін тәуекел өте жоғары болады.

DoS-шабуылдары басқаруды бүркемелеу және байланыс сапасын төмендету үшін қолданылады. Күшті жағы – қарапайымдылығы, әлсіз жағы – көбіне физикалық әсерінің шектеулілігі. Кідірістерге қатаң талаптары бар жүйелерде тәуекел деңгейі орташа – жоғары.
Инсайдерлер мен конфигурация қателері сенімді деңгейде қол жеткізуді қамтамасыз етеді. Күшті жағы – процестерді жақсы білу, әлсіз жағы – адам факторына тәуелділік. Өзгерістерді басқару әлсіз болған жағдайда тәуекел деңгейі орташа – жоғары. Датчиктер мен атқарушы механизмдерге физикалық араласу цифрлық қорғанысты айналып өтуі мүмкін. Күшті жағы – кибер-периметрден тәуелсіздігі, әлсіз жағы – тікелей қол жеткізудің қажеттілігі. Тәуекел орташа, бірақ кибер-векторлармен үйлескен жағдайда критикалық деңгейге жетуі мүмкін.

Көпвекторлы шабуыл әрекеттер тізбегі ретінде жүзеге асырылады, мұнда әрбір кезең келесісіне дайындық жасайды, ал жекелеген векторлар параллель түрде іске қосылуы мүмкін (4 сурет). КФЖ-де технологиялық режимдермен синхрондау аса маңызды шабуылдаушы ауытқуларды анықтау қиынырақ болатын немесе қорғаныс тетіктері әлсірейтін сәттерді (қызмет көрсету, ауыстырып қосу, жаңартулар) таңдайды. Формализациялау үшін шабуыл графтары қолданылады және олар процессінің физикалық параметрлерімен кеңейтіледі.

Сурет 4 − Көпвекторлы шабуылдың өмірлік циклі (жалпыланған модель)

Енді көпвекторлық шабуылдарды кезеңдерін бөліп, атап айтқанда MITRE ATT&CK for ICS үшін оның тәсілдерін, әрекеттерін 2-кесте арқылы көрсетейік.

Кесте 2 − Шабуыл кезеңдерін тактикалармен/техникалармен сәйкестендіру (оның ішінде MITRE ATT&CK for ICS)

Кезең	Типтік тәсілдер	Countermeasures (мысал)
Барлау	Активтерді сканерлеу, конфигурацияны жинау, OSINT	ОТ активтерін түгендеу (инвентаризациялау), сканерлеуді мониторингтеу
Бастапқы қол жеткізу	Фишинг, VPN осалдықтары, supply-chain шабуылдары, USB тасымалдағыштар	MFA (көпфакторлы аутентификация), тасымалдағыштарды бақылау, жаңартуларды цифрлық қолтаңбамен растау
Көлденең (бүйірлік) қозғалу	RDP, jump-server-ді теріс пайдалану, тіркелу деректеріне қол жеткізу	Сегментация, PAM, әкімшілік арналарды шектеу
Жүйеде бекіну (тұрақты қолжетімділікті сақтау)	Бэкдорлар, конфигурацияларды өзгерту,микророграммаларды модификациялау	Тұтастықты бақылау, ақ тізімдеу (whitelisting)
Әсер етуі	PLC логикасын өзгерту, қорғаныс механизмдерін өшіру, шифрлау	Fail-safe режимдері, резервтеу, әрекет сценарийлері (playbooks)

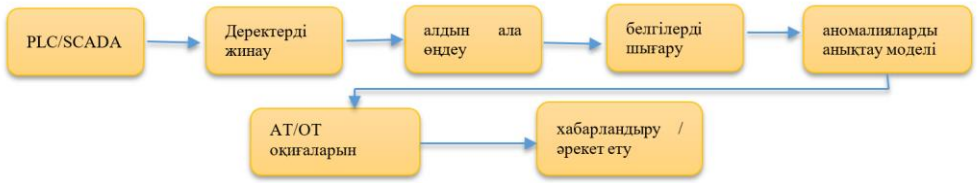
Stuxnet зиянды кодтың PLC логикасын өзгертіп, физикалық әсерлер тудыра алатынын дәлелдеген алғашқы мысалдардың бірі болды [7-8]. Жұқтыру векторларының комбинациясы (оның ішінде тасымалды дерек тасушылар), осалдықтарды пайдалану және технологиялық логиканы нысаналы түрде алмастыру көпвекторлы операциялардың жоғары күрделілігін көрсетеді.

Украинаның энергетикалық жүйесіне жасалған шабуылдар (2015/2016) кампаниялық сипатқа ие екенін көрсетті [15,16]. Ұзақ дайындық, фишинг, АТ-түйіндерді компрометациялау, SCADA-ға қол жеткізу және жойқын әрекеттер. CrashOverride/Industroyer қосалқы станциялардың өнеркәсіптік протоколдарын теріс пайдаланатын модульдік платформаны паш етті [12-14].

TRITON/Trisis (HatMan) Safety Instrumented Systems (SIS) жүйелеріне бағытталған шабуылымен ерекшеленеді [9-11], бұл тәуекелдерді адамдардың және қоршаған ортаның қауіпсіздігі саласына көшіреді. Инцидент safety-контроллерлерге баратын арналарды бөлек бақылаудың және инженерлік станцияларды қатаң басқарудың қажеттілігін айқындайды.
Өнеркәсіптік ортадағы ransomware инциденттері көбіне АТ-сегменттен басталып, ОТ-тың АТ-сервистерге тәуелділігі салдарынан өндірістің тоқтауына әкеледі. Сондықтан қорғаныс offline-backup, оқшауланған қалпына келтіру жоспарын және объектіні қауіпсіз күйге көшіру рәсімдерін қамтуы тиіс.

Қортындылар

Көпвекторлы шабуылдарды анықтау АТ және ОТ оқиғаларын корреляциялауды талап етеді, өйткені жекелей алынған белгілер аз мәнді болып көрінуі мүмкін [6]. Тәжірибелық пайплайн телеметрияны жинауды, алдын ала өңдеуді, белгілерді (features) шығаруды, детекторларды қолдануды (мысалы, Isolation Forest) және жалған іске қосылуларды азайту үшін желілік және жүйелік логтармен корреляциялауды қамтиды (5 сурет).



Сурет 5 − КФЖ-дегі аномалияларды анықтаудың тәжірибелық пайплайны

КФЖ шабуылдарының тәсілдерімен оларды өзара салыстыруды 3-кесте арқылы сипаттап көресеттік.

Кесте 3 − Киберфизикалық жүйелердегі (КФЖ) шабуылдарды анықтау тәсілдерін салыстыру

Тәсіл	Артықшылықтары	Шектеулері	Қолдану аясы
Сигнатураға негізделген IDS	Белгілі шабуылдарды дәл анықтайды	Жаңа шабуыл техникаларын анықтай алмайды	Периметр және IOC (индикаторлар)
ML негізделген аномалиялар	Белгісіз сценарийлерді анықтайды	Деректер дрейфі және жалған іске қосылулар	Процесс телеметриясы
Тұтастықты бақылау	Конфигурация өзгерістеріне қарсы тиімді	Эталондық база қажет	PLC/RTU және инженерлік станциялар
Цифрлық егіз	Физикалық процестермен байланысы бар, түсіндірмелі	Калибрлеу құнының жоғары болуы	Сындарлы (қауіпсіздікке жауапты) объектілер

Көпвекторлы шабуылдар көпдеңгейлі қорғауды (defense-in-depth) және ОТ ортасының ерекшеліктерін (кідіріс шектеулері, пайдаланудағы қауіпсіздік, жабдықтың ұзақ өмірлік циклі) ескеретін тәуекелдерді басқаруды талап етеді. СТ РК ISO/IEC 27001 ұсынымдары ОТ-топологияларға, қауіп-қатерлерге және эксплуатациялық шектеулерді ескере отырып қарсы шараларға басымдық береді [3]. ISA/IEC 62443 стандарттары өмірлік циклді, сондай-ақ компоненттер мен жүйелерге қойылатын талаптарды айқындайды [5], ал MITRE ATT&CK for ICS қорғаныс бақылауларының шабуыл техникаларын қамту деңгейін верификациялауға

көмектеседі [6]. Тәжірибелық ең төменгі шаралар мыналарды тұралы. Олар аймақтар мен арналарды сегментациялау (DMZ, jump-серверлер), көпфакторлы аутентификация (MFA) және привилегияларды басқару (PAM), конфигурациялар мен микропрограммалардың (firmware) тұтастығын бақылау, OT-трафикті пассивті мониторингтеу, сондай-ақ safety-режимдерді ескеретін инциденттерге әрекет ету жоспары.

Кесте 4 − Көпвекторлы шабуылдар тәуекелін төмендетуге арналған қорғаныс шараларының чек-листі

Деңгей	Іс-шаралар	Әсері
Архитектуралық	Аймақтар/арналарды сегментациялау, DMZ, жеке jump-серверлер	Инцидентті оқшаулау
Қолжетімділік	MFA, PAM, мердігерлердің қашықтан қолжетімділігін бақылау	Есептік деректердің бұзылу қаупін төмендету
Конфигурация	Ақ тізім (whitelisting), тұтастықты бақылау, қауіпсіз жаңартулар	Зиянды кодты енгізу қаупін азайту
Деңгей	Іс-шаралар	Әсері
Мониторинг	OT IDS + SIEM корреляциясы, ескерту (алертинг)	Ерте анықтау
Тұрақтылық	Резервтеу, offline-backup, fail-safe рәсімдері	Тоқтап қалу мен залалды азайту
Ұйымдастырушылық	Оқыту, оқу-жаттығулар, жеткізушілер аудиті, өзгерістерді басқару	Қателіктерді азайту және дайындық деңгейін арттыру

Көпвекторлы шабуылдар киберфизикалық жүйелер (КФЖ) қауіпсіздігінің жаңа бағытына айналды. лар жасырындықты, ауқымды әсерді және физикалық құралдарды біріктіріп, АТ және ОТ домендері арасында еркін ауыса алады. Архитектуралық алғышарттар мен нақты кейстерді (Stuxnet, Украинадағы шабуылдар, Industroyer, TRITON, ransomware) талдау ең ауыр мәселеселері контроллерлердің, safety-контурлардың және сенімді жабдықтау тізбектерінің компрометациясы кезінде туындайтынын көрсетеді. Тиімді қорғау кешенді тәсілді талап етеді. Олар сегментация, қолжетімділік пен тұтастықты бақылау, АТ/ОТ оқиғаларын корреляциялау, резервтеу, сондай-ақ АТ және ОТ мамандарының бірлескен жұмысы және қауіпсіздікті өмірлік цикл бойынша басқару қажеттігін талап етеді (СТ РК ISO/IEC 27001, NIST, ISA/IEC 62443).

Әдебиеттер тізімі

1. Cyber-Physical Systems Security – A Survey / A. Humayed et al // IEEE Internet of Things Journal. – 2017. – Vol. 4, № 6. – P. 1802-1831. https://arxiv.org/abs/1701.04525.
2. Liu Y. False Data Injection Attacks against State Estimation in Electric Power Grids / Y. Liu, P. Ning, M.K. Reiter // Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS 2009). – New York: ACM, 2009. – P. 21-32.
3. СТ РК ISO/IEC 27001-2023. Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. – Астана: Комитет технического регулирования и метрологии, 2023.
4. NIST SP 800-82 Rev. 3. Guide to Operational Technology (OT) Security. – Gaithersburg: National Institute of Standards and Technology, 2023. https://doi.org/10.6028/NIST.SP.800-82r3.
5. ISA/IEC 62443. Industrial Automation and Control Systems Security: Series of Standards. – Research Triangle Park: International Society of Automation, 2023. https://www.iec.ch/dyn/www/f?p=103:85:0::::FSP_LANG_ID:25 (дата обращения: 25.01.2026).
6. MITRE ATT&CK® Framework. Knowledge Base for Adversary Tactics and Techniques (ICS Domain). – Версия 18. – MITRE Corporation, 2025. https://attack.mitre.org (дата обращения: 25.01.2026).
7. Karnouskos S. Stuxnet Worm Impact on Industrial Cyber-Physical System Security / S. Karnouskos // Proceedings of the 37th Annual Conference of the IEEE Industrial Electronics Society. – Melbourne, 2011. – P. 4490-4494.
8. Langner R. To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve. – Hamburg: The Langner Group, 2011. – 32 p.

9. TRITON: How It Disrupted Safety Systems and Changed the Threat Landscape of Industrial Control Systems / A. Carcano et al // Black Hat USA 2018 Proceedings. – Las Vegas, 2018.
10. CISA. MAR-17-352-01 HatMan (TRITON/TRISIS) – Safety System Targeted Malware (Update A). – Washington, DC: Cybersecurity and Infrastructure Security Agency, 2017. https://www.cisa.gov (дата обращения: 25.01.2026).
11. Google Cloud Threat Intelligence. TRITON Threat Actor Profile and Detection Methods. – Google, 2023. https://cloud.google.com/security (дата обращения: 25.01.2026).
12. Dragos Inc. CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations. – Hanover: Dragos, 2017.
13. CISA. CrashOverride Malware Alert and Mitigations. – Washington, DC, 2017. https://www.cisa.gov (дата обращения: 25.01.2026).
14. ESET Research. Industroyer2: Industroyer Reloaded. – Bratislava: ESET, 2022. https://www.welivesecurity.com (дата обращения: 25.01.2026).
15. CISA. IR-ALERT-H-16-056-01: Cyber-Attack Against Ukrainian Critical Infrastructure. – Updated 20.07.2021. – Washington, DC. https://www.cisa.gov (дата обращения: 25.01.2026).
16. SANS Institute, E-ISAC. Analysis of the Cyber Attack on the Ukrainian Power Grid. – Bethesda, 2016.
17. Tuptuk N. Security of Smart Manufacturing Systems / N. uptuk, S. Hailes // Journal of Manufacturing Systems. – 2018. – Vol. 47. – P. 93-106. https://doi.org/10.1016/j.jmsy.2018.04.007.
18. Ransomware on Cyber-Physical Systems: Taxonomies, Case Studies, Security Gaps and Open Challenges / M. Benmalek et al // Computers & Security. – 2023. – Vol. 124.
19. Securing the Industrial Internet of Things against Ransomware Attacks // Journal of Network and Computer Applications. – 2023. – Vol. 212.
20. False Data Injection Attack in Smart Grid CPS: Issues and Detection Algorithms // Computers & Security. – 2023. – Vol. 122.
21. False Data Injection Attack in Smart Grid: Model and Detection Based on Deep Reinforcement Learning // Frontiers in Energy Research. – 2022. – Vol. 10.
22. ENIGMA: An Explainable Digital Twin Security Solution for Cyber-Physical Systems // Computers & Security. – 2023. – Vol. 123.
23. A Survey on Security-Enhancing Digital Twins: Models, Applications and Challenges // Computer Communications. – 2025. – Vol. 214.

К.М. Сагиндыков[1] ,Ф.Б. Тебуева[2], Н.Ж. Мукушева[*]
[1]Евразийский национальный университет имени Л.Н. Гумилева,
010008, Республика Казахстан, г. Астана, ул. Сатпаева, 2
[2]Северо-Кавказский федеральный университет,
355017, Россия, г. Ставрополь, ул. Пушкина, 1,
[*]e-mail: nazym9_1@mail.ru

МНОГОВЕКТОРНЫЕ АТАКИ НА КИБЕРФИЗИЧЕСКИЕ СИСТЕМЫ: МЕХАНИЗМЫ, ОБНАРУЖЕНИЕ И ПРИМЕРЫ ЗАЩИТЫ

В статье представлен комплексный и углублённый обзор многовекторных кибератак, реализуемых в киберфизических системах (КФС). В ходе исследования подробно анализируются ключевые архитектурные предпосылки КФС, модели угроз на стыке информационных и операционных технологий (IT/OT), а также механизмы координации кибер- и физического воздействия. Систематизируются основные типы атак, включая внедрение ложных данных (FDI/FDIA), вредоносное программное обеспечение для промышленных систем управления и PLC, атаки на цепочки поставок (supply-chain), ransomware, атаки отказа в обслуживании (DoS), инсайдерские угрозы и прямое физическое вмешательство. Показаны их взаимосвязь и эффект усиления в рамках единого сценария компрометации.

Опираясь на открытые научные исследования и отраслевые отчёты, рассматриваются кейсы Stuxnet, атаки на энергетическую инфраструктуру Украины, CrashOverride/Industroyer, TRITON/Trisis, а также инциденты ransomware в промышленной среде. Кроме того, предложена риск-ориентированная матрица, основанная на принципе «Тип атаки – уровень КФС». Описан практический пайплайн выявления аномалий с использованием корреляции IT/OT-событий и методов машинного обучения.

Работа включает таблицы, схемы и графики, отражающие архитектуру КФС, жизненный цикл многовекторных операций, а также инженерные меры защиты в соответствии со стандартами СТ РК ISO/IEC 27001, NIST, ISA/IEC 62443 и MITRE ATT&CK for ICS.

Ключевые слова: *многовекторные атаки, FDI, supply-chain, ransomware, TRITON, Industroyer, обнаружение аномалий.*

K.M. Sagindykov[1] ,F.B. Tebueva[2], N.Zh. Mukusheva[*]
[1]L.N. Gumilyov Eurasian National University,
0100008, 2 Satpayev Street, Astana, Republic of Kazakhstan.
[2]North Caucasus Federal University,
355017, 1 Pushkina Street, Stavropol, Russia
[*]e-mail: nazym9_1@mail.ru

MULTI-VECTOR ATTACKS ON CYBER-PHYSICAL SYSTEMS: MECHANISMS, DETECTION, AND PROTECTION EXAMPLES

The article presents a comprehensive and in-depth review of multi-vector cyberattacks implemented in cyber-physical systems (CPS). The study provides a detailed analysis of the key architectural prerequisites of CPS, threat models at the intersection of information technology and operational technology (IT/OT), as well as the mechanisms for coordinating cyber and physical impacts. The main types of attacks are systematized, including false data injection (FDI/FDIA), malware targeting industrial control systems and PLCs, supply-chain attacks, ransomware, denial-of-service (DoS) attacks, insider threats, and direct physical interference. Their interconnection and amplification effects within a unified compromise scenario are demonstrated.

Based on open scientific studies and industry reports, the paper analyzes notable cases such as Stuxnet, cyberattacks on Ukraine's energy infrastructure, CrashOverride/Industroyer, TRITON/Trisis, and ransomware incidents in industrial environments. In addition, a risk-oriented matrix based on the principle «Attack Type – CPS Layer» is proposed. A practical anomaly-detection pipeline using IT/OT event correlation and machine-learning methods is described.

The work includes tables, diagrams, and graphs illustrating CPS architecture, the lifecycle of multi-vector operations, and engineering security measures aligned with the standards ST RK ISO/IEC 27001, NIST, ISA/IEC 62443, and MITRE ATT&CK for ICS.

Key words: *multi-vector attacks, FDI, supply-chain, ransomware, TRITON, Industroyer, anomaly detection.*

Авторлар туралы мәліметтер

Каким Молдабекович Сагиндыков – «Ақпараттық қауіпсіздік» кафедрасының т.ғ.к., доценті, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана қ., Қазақстан; e-mail: sagindykov_km@enu.kz. ORCID: https://orcid.org/0000-0003-3315-798X.

Фариза Биляловна Тебуева – ф-м.ғ докторы,есептеу математикасы және кибернетика кафедрасының профессоры, «Солтүстік Кавказ федералдық университеті» ФГАОУ ВО, Ставрополь қ., Ресей Федерациясы; e-mail: ftebueva@ncfu.ru. ORCID: https://orcid.org/0000-0001-9324-9259.

Назым Жумагельдыевна Мукушева* – «Ақпараттық қауіпсіздік» кафедрасының докторанты; Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана қ., Қазақстан; e-mail: nazym9_1@mail.ru. ORCID: https://orcid.org/0009-0001-5015-3617.

Сведения об авторах

Каким Молдабекович Сагиндыков – к.т.н., доцент кафедры «Информационная безопасность», Евразийский национальный университет имени Л.Н. Гумилёва, г. Астана. Казахстан; e-mail: sagindykov_km@enu.kz. ORCID: https://orcid.org/0000-0003-3315-798X.

Фариза Биляловна Тебуева – доктор ф-м.н, профессор кафедры вычислительной математики и кибернетики, ФГАОУ ВО «Северо-Кавказский федеральный университет», г. Ставрополь, Российская Федерация; e-mail: ftebueva@ncfu.ru. ORCID: https://orcid.org/0000-0001-9324-9259.

Назым Жумагельдыевна Мукушева – докторант кафедры «Информационная безопасность», Евразийский национальный университет имени Л.Н. Гумилёва, г. Астана. Казахстан; e-mail: nazym9_1@mail.ru. ORCID: https://orcid.org/0009-0001-5015-3617.

Information about the authors

Kakim Moldabekovich Sagindykov – Candidate of Technical Sciences (Ph.D.), Associate Professor of the Department of Information Security, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan; e-mail: sagindykov_km@enu.kz. ORCID: https://orcid.org/0000-0003-3315-798X.

Fariza Bilyalovna Tebuyeva – Doctor of Physical and Mathematical Sciences, Professor of the Department of Computational Mathematics and Cybernetics, North Caucasus Federal University, Stavropol, Russian Federation; e-mail: ftebueva@ncfu.ru. ORCID: https://orcid.org/0000-0001-9324-9259.

Nazym Zhumageldyevna Mukusheva* – PhD student (Doctoral student) of the Department of Information Security, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan; e-mail: nazym9_1@mail.ru ORCID: https://orcid.org/0009-0001-5015-3617.

Редакцияға енуі 06.01.2026
Өңдеуден кейін түсуі 20.02.2026
Жариялауға қабылданды 23.02.2026

https://doi.org/10.53360/2788-7995-2026-1(21)-13

IRSTI: 55.47.03

Z.A. Kutpanova[1], D.O. Kozhakhmetova[2]*, K.M. Suleymenov[3], G.N. Baiseitov[4], D.N. Shandronov[5]

[1]Astana IT University, 010000, Kazakhstan, Astana,Mangilik El, 55/11
[2]Shakarim University,
071412, Kazakhstanst, Semey, Glinka, 20 A
[3]L.N. Gumilyov Eurasian National University,
10000, Kazakhstan, Astana, Stepaeva 2
[4]R&D Center «Kazakhstan Engineering»,
010000, Kazakhstan Astana, Auezov Str. 2
[5]Military Engineering Institute of Radio Electronics and Communications,
Almaty, Kazakhstan, Zandosova, 53
*e-mail: d.kojahmetova@shakarim.kz

OPTIMIZATION OF FLIGHT TRAJECTORIES OF UNMANNED AERIAL VEHICLES WITH GIVEN FINAL CONDITIONS

Abstract: *The article considers the urgent problem of optimizing the flight trajectory of unmanned aerial vehicles (UAVs) with given final conditions. An approach to constructing the optimal UAV trajectory along successive sections using approximation by a fifth-degree polynomial is presented. A mathematical model is developed that takes into account the features of using local inertial coordinate systems on each section of the trajectory. A motion optimization method is proposed based on minimizing the quadratic functional characterizing both the accuracy of reaching specified points and the energy costs for control. The solution to the optimization problem is obtained using analytical design of the optimal controller. Analytical expressions are given for determining the optimal lateral acceleration of the UAV, ensuring the required positioning accuracy with minimal energy costs. Features of coordinate transformation between trajectory sections to ensure continuity of motion are considered. A practical example of calculating the optimal UAV trajectory with given initial conditions is given.*

Key words: *unmanned aerial vehicle, trajectory optimization, polynomial approximation, inertial coordinate systems, quadratic functional, optimal control, segmented trajectory*.

Introduction

Unmanned aerial vehicles (UAVs) are increasingly required to execute complex multi-stage missions under strict constraints on positioning accuracy, timing, and energy consumption. Typical missions include area reconnaissance, payload delivery, monitoring tasks, and return-to-base operations, each imposing specific kinematic and dynamic requirements. The successful execution of such missions critically depends on the quality of trajectory planning and control algorithms.

Trajectory planning for UAVs must account for physical and operational constraints, including flight dynamics, actuator limitations, time restrictions, and safety margins. In practical applications, inefficient trajectory generation may lead to excessive energy consumption or violation of mission constraints, resulting in incomplete task execution. These challenges become particularly