АҚПАРАТТЫҚ-КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР
ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ
INFORMATION AND COMMUNICATION TECHNOLOGIES

АҚПАРАТТЫҚ ҚАУІПСІЗДІК. ДЕРЕКТЕРДІ ҚОРҒАУ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. ЗАЩИТА ИНФОРМАЦИИ
INFORMATION SECURITY. INFORMATION PROTECTION

DOI 10.51885/1561-4212_2024_4_150
МҒТАА 81.93.29

А.С. Канжекеев[1], А.А. Конырханова[1], Т. Толғанбайұлы[2]
[1]Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана қ., Қазақстан
*E-mail: aidyn-94-10@mail.ru**
E-mail: konyrkhanova_aa@enu.kz
[2]ЖШС «QazCloud», Астана қ., Қазақстан
E-mail: talant.kz@mail.ru

КИБЕРФИЗИКАЛЫҚ ЖҮЙЕЛЕР: КИБЕРҚАУІПСІЗДІК ҚАТЕРЛЕРІ, ШАБУЫЛДАРДЫ ТАЛДАУ ЖӘНЕ МАҢЫЗДЫ ИНФРАҚҰРЫЛЫМДЫ ҚОРҒАУ ӘДІСТЕРІ

КИБЕРФИЗИЧЕСКИЕ СИСТЕМЫ: УГРОЗЫ КИБЕРБЕЗОПАСНОСТИ, АНАЛИЗ АТАК И МЕТОДЫ ЗАЩИТЫ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

CYBER-PHYSICAL SYSTEMS: CYBERSECURITY THREATS, ATTACK ANALYSIS AND CRITICAL INFRASTRUCTURE PROTECTION METHODS

Аңдатпа. *Мақалада физикалық және кибернетикалық компоненттерді біріктіретін маңызды инфрақұрылымның негізгі элементтері ретінде киберфизикалық жүйелер қарастырылады. Зерттеу мақсаттарының бірі киберфизикалық жүйелер саласындағы өзекті мәселелерді анықтау болып табылады. Осы типтегі жүйелер энергетика, көлік, денсаулық сақтау және өнеркәсіп сияқты салаларда кеңінен қолданылады, бұл олардың қазіргі қоғамның жұмыс істеуі үшін маңыздылығын көрсетеді. Мақалада соңғы 10 жылдағы киберфизикалық жүйелерге жасалған кибершабуылдарды талдау, энергетикалық желілер мен сумен жабдықтау жүйелері сияқты маңызды нысандарға жасалған шабуылдардың көбеюі көрсетілген. Зиянды программалар, SQL инъекциялар, MITM, спуфинг және DDoS сияқты кибер шабуыл түрлері қарастырылады және антивирустық бағдарламалық жасақтаманы пайдалану, желіні сегментациялау, деректерді шифрлау және көп факторлы аутентификация сияқты қорғаныс шаралары ұсынылады. Зерттеу нәтижелері маңызды инфрақұрылымды қорғау және қоғам мен экономика үшін ауыр зардаптардың алдын алу үшін киберфизикалық жүйелердің киберқауіпсіздігін күшейту қажеттілігін көрсетеді.*

Түйін сөздер: *киберфизикалық жүйелер, кибершабуыл, SCADA жүйесі, IoT, киберқауіпсіздік.*

Аннотация. *В данной статье рассматриваются киберфизические системы как ключевые элементы критической инфраструктуры, объединяющие физические и кибернетические компоненты. Одно из целей исследование было необходимо определить актуальные вопросы в сфере киберфизических системы. Системы этого типа находят широкое применение в таких отраслях, как энергетика, транспорт, здравоохранение и промышленность, что подчеркивает их важность для функционирования современного общества. Статья содержит анализ кибератак на киберфизические системы за последние 10 лет, выявляя рост числа атак на критически важные объекты, таких как энергосети и системы водоснабжения. Рассмотрены типы атак, включая вредоносное ПО, SQL-инъекции, MITM, спуффинг и DDoS, а также предложены меры защиты, такие как использование антивирусного ПО, сегментация сети, шифрование данных и многофакторная аутентификация. Выводы исследования подчеркивают необходимость усиления*

кибербезопасности киберфизических систем для защиты критической инфраструктуры и предотвращения серьезных последствий для общества и экономики.

Ключевые слова: *киберфизические системы, кибератака, SCADA-система, IoT, кибербезопасность***.**

Abstract. *This paper examines cyber-physical systems as key elements of critical infrastructure that integrate physical and cyber components. One of the objectives of the study was to identify current issues in the field of Cyber-Physical Systems. These systems are widely used in industries such as energy, transportation, healthcare, and manufacturing, highlighting their importance for the functioning of modern society. The paper analyzes cyber-attacks on cyber-physical systems over the past 10 years, revealing an increase in attacks on critical assets such as power grids and water supply systems. The types of attacks, including malware, SQL injection, MITM, spoofing, and DDoS, are discussed, and protective measures such as the use of antivirus software, network segmentation, data encryption, and multi-factor authentication are proposed. The findings highlight the need to strengthen the cybersecurity of cyber-physical systems to protect critical infrastructure and prevent serious consequences for society and the economy.*

Keywords: *cyber-physical systems, cyber attack, SCADA system, IoT, cyber security.*

Кіріспе. Қазіргі таңда әлемде киберфизикалық жүйелерге жасалған кибершабуылдардың саны өскенін байқап отырмыз. Зерттеудің негізгі мақсаты соңғы 10 жылда киберфизикалық жүйелерге жасалған кибершабуылдарды талдау, олардың ерекшеліктерін анықтау және қолданыстағы қорғаныс әдістерінің тиімділігін бағалау болды. Бұл ретте электр энергетикасы, атом өнеркәсібі, газ және мұнай өндіру сияқты маңызды секторларға жасалған шабуылдарға ерекше назар аударылды.

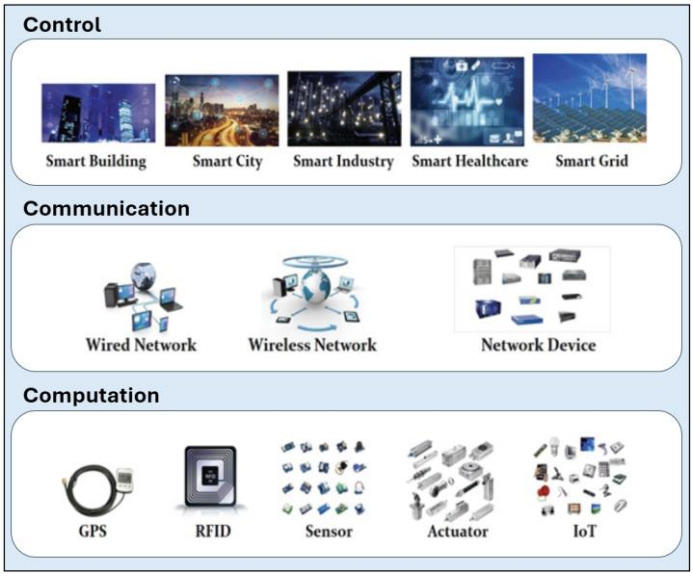
Қазақстанда электр энергетикасы, атом өнеркәсібі, газ және мұнай өндіру сияқты секторлардағы киберфизикалық жүйелерді қоса алғанда, аса маңызды инфрақұрылымдық объектілерді қорғауға ерекше назар аударылады. Бұл жүйелердің дұрыс жұмыс істемеуі Ұлттық қауіпсіздік пен экономиканың тұрақтылығы үшін ауыр зардаптарға әкелуі мүмкін болғандықтан, киберқорғаудың сенімді тетіктерін енгізу қажеттілігі одан да өзекті бола түсуде.

Киберфизикалық жүйелер – бұл кибернетикалық және физикалық компоненттердің өзара әрекеттесуіне негізделген интеллектуалды жүйелер. Бұл жүйелер физикалық әлемді, соның ішінде сенсорларды, датчиктерді, робототехниканы және интеграцияланған жүйелерді виртуалды деректер орталарымен байланыстырады. Киберфизикалық жүйелерді қолдану күнделікті өмірдің әртүрлі аспектілерінде жайлылықты, қауіпсіздікті және тиімділікті арттыру үшін маңызды (https://doi.org/10.6028/NIST.SP.1500-201).

Киберфизикалық жүйелер – есептеу, байланыс және басқару технологияларын біріктіретін күрделі жүйелер. Бұл жүйелер есептеу процестері мен коммуникациялар сияқты кибернетикалық мүмкіндіктерді сенсорлар мен жетектерді қамтитын физикалық компоненттермен біріктіреді (1-сурет). Киберфизикалық жүйелер медицина, автомобиль, энергетикалық желілер, қалалық инфрақұрылым, өнеркәсіптік өндіріс, авиация және ғимараттарды басқару жүйелерін қоса алғанда, көптеген салаларда қолданылады (Matthew N. O., Sadiku, 2017).

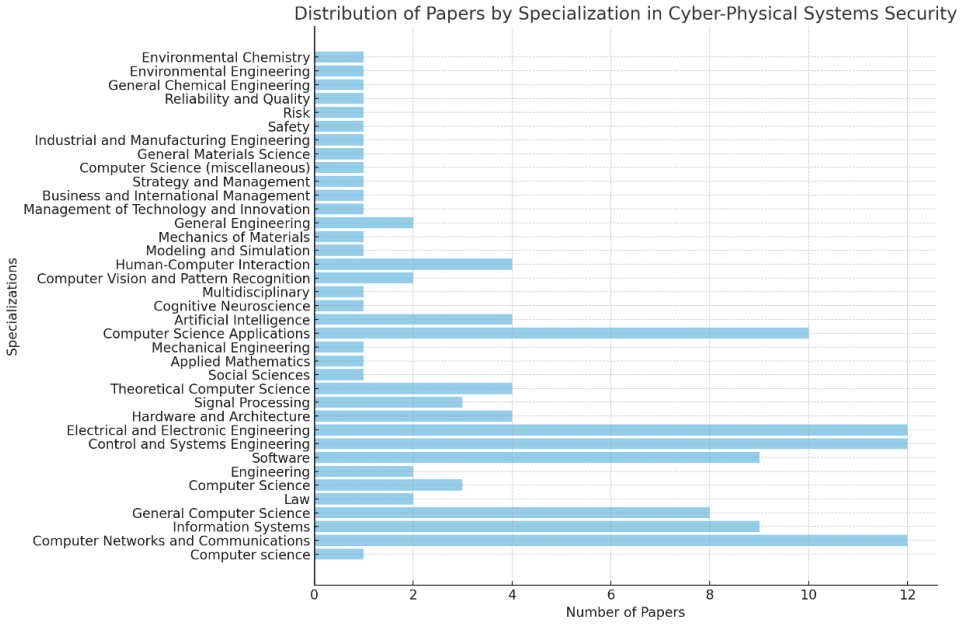
Киберфизикалық жүйелердің киберқауіпсіздік өзектілігі олардың әртүрлі салалар үшін маңыздылығына және қоғамның күнделікті өміріне ауқымды енгізілуіне байланысты. Бұл жүйелер физикалық нысандар мен процестерді цифрлық технологиялармен біріктіреді, бұл тиімділікті арттыруға, автоматтандыруға және басқаруға жаңа мүмкіндіктер ашады, сонымен қатар жаңа шабуыл векторлары мен осалдықтарын тудырады.

Материалдар және зерттеу әдістері. Зерттеу барысында киберфизикалық жүйелерге жасалған кибершабуылдарға шолу жасалды. Іздеу ғылым саласындағы ең ірі библиографиялық және рефераттық деректер қоры Scopus платформасында «Cyber-Physical Systems», «IoT», «CPS Security», «CPS Cyber Attack» кілт сөздері бойынша жүргізілді. Зерттеуде 50-ге жуық ғылыми басылымдар зерттелді.



1-сурет. Киберфизикалық жүйелердің компоненттері
Ескерту – (2) Matthew N. O. Sadiku and others. (2017). Cyber-Physical Systems: A Literature Review мақаласынаан алынды

Киберфизикалық жүйелер бойынша зерттеулер негізінен Control and Systems Engineering, Electrical and Electronic Engineering, Computer Networks and Communications бағыттарында жүргізілген. Бұл зерттеудің негізгі бағыттары киберфизикалық жүйелердің күрделілігі мен пәнаралық сипатын көрсететін жүйелерді басқару, желілік технологиялар және компьютерлік қосымшалардың қиылысына бағытталғанын көрестеді (2-сурет).



2-сурет. Киберфизикалық жүйелер бойынша зерттеу бағыттары
Ескерту – автормен құрастырылған

3-сурет. Киберфизикалық жүйелер бойынша зерттеу бағыттары
Ескерту – автормен құрастырылған

Зерттеу барысында сұрыпталған 50 жуық ғылыми жұмыстар негізінде киберфизикалық жүйелердің қазіргі таңда өзекті зерттеу бағыттары анықталды (3-сурет):

– Киберфизикалық жүйелердің осалдықтары мен қауіпсіздігі – 30 %.
– Өнеркәсіптегі киберфизикалық жүйелерді қорғау – 25 %.
– Киберфизикалық жүйелерде машиналық оқыту және жасанды интеллект қолдану – 20 %.
– IoT қауіпсіздігі – 15 %.
– Киберфизикалық жүйелердің қауіпсіздігі және сенімділігі – 10 %.

Талдау нәтижесінде киберфизикалық жүйелерге жасалған ірі 10 кибершабуыл сұрыпталды (Abdulmalik Humayed, Jingqiang Lin, Fengjun Li & Bo Luo., 2017; Hakan Kayan, 2022; Case D. & Wilhoit K., 2017; Cardenas A., Amin S. & Sastry S., 2008; Knapp E. & Langill J., 2014; Fisher D. 2015; Cheung S., 2007; Ten C.W., Liu, C.C. & Manimaran G., 2008; Lee R. M., Assante, M. J. & Conway T., 2016; Langner R., 2011).

Киберфизикалық жүйелерге жасалған кибершабуылды іріктеу кезінде келесі критерийлер қолданылды: келтірілген залалдың ауқымы, шабуыл кезінде қолданған әдістер және киберқылмыскерлерді ынталандыру факторы.

1-кесте. Киберфизикалық жүйелерге жасалған ірі 10 кибершабуыл

Жыл	Шабуыл атауы	Мотивация	Шабуыл
2014	Неміс өнеркәсіп жүйесіне шабуыл	Диверсия және осалдықты көрсету	Германиядағы болат зауытында өнеркәсіптік басқару жүйесін бұзу. Хакерлер SCADA жүйелері арқылы өндіріс желісіне физикалық зақым келтірді
2015	Украина энергетика жүйесіне шабуыл	Саяси мотивация	BlackEnergy зиянды программасы арқылы SCADA жүйелерін бұзу және электр желілерін өшірді
2016	Лос-Анджелестегі ауруханаға абуыл	Қаржылық мотивация	Ауруханадағы медициналық жабдықтар мен басқару жүйелерін бұзған зиянды программа
2017	Triton	Маңызды инфрақұрылымды диверсиялау	Мұнай-химия зауытындағы қауіпсіздік жүйелерін бұзуға арналған TRITON зиянды программасы

1-кестенің соңы

Жыл	Шабуыл атауы	Мотивация	Шабуыл
2018	Сауд Арабия мұнай нысандарына шабуыл	Экономикалық мотивация	SCADA жүйесі арқылы мұнай-химия объектілеріндегі операциялардың бұзылуына және өндірістің тоқтауына себеп болған зиянды программа
2019	Оңтүстік Африка гидро энергетика нысанына шабуыл	Диверсия	Тазарту қондырғыларындағы судың химиялық параметрлерін өзгертуге арналған SCADA жүйелерін бұзу, бұл судың ластануына әкелді
2020	Израиль гидро энергетика нысанына шабуыл	Геосаяси мотивация	Судағы химиялық заттардың деңгейін өзгерту әрекеті арқылы сорғыны басқару және суды бақылау жүйелерін бұзу
2021	Oldsmar Water Treatment Plant	Диверсия	Судағы тазарту деңгейін қауіпті деңгейге дейін өзгертуге тырысу үшін су тазарту станциясының SCADA жүйесін бұзу
2022	Үндістан электр жүйесіне шабуыл	Кибершпионаж	Желілік қауіпсіздіктің осалдығы арқылы энергетикалық компаниялардың SCADA жүйелерін бұзу
2023	АҚШ аэроғарыш өнеркәсібіне шабуыл	Қаржылық және тыңшылық мотивация	Зиянды программалар арқылы өндірісті басқару жүйелеріне шабуыл жасау және авиацияға арналған компоненттердің сызбаларын ұрлау

Ескерту – автормен құрастырылған

Соңғы 10 жылда киберфизикалық жүйелерге жасалған кибершабуылдарды талдау негізінде бірнеше негізгі қорытындылар жасалды.

Маңызды инфрақұрылымға жасалатын кибершабуылдар санының өсуі. 2014 жылдан бастап электр энергетика, гидро энергетика және денсаулық сақтау жүйелері сияқты нысандарға кибершабуылдар санының айтарлықтай өсуі байқалды. Бұл үрдіс маңызды әлеуметтік процестердің жұмыс істеуі тәуелді болатын киберфизикалық жүйелердің осалдығының жоғары деңгейін көрсетеді. Аталған факт инфрақұрылымның аса маңызды объектілерін қорғауға бағытталған қауіпсіздік шараларын күшейту қажеттігін айғақтайды.

Кибершабуыл әдістерінің эволюциясы. Киберфизикалық жүйелердегі заманауи кибершабуылдар барған сайын күрделі және мақсатты болып келеді. Атап айтқанда, SCADA жүйелеріне және өнеркәсіптік басқару жүйелерінің басқа компоненттеріне нұқсан келтіруге арналған арнайы зиянды программалар жиі қолданылады. Сонымен қатар, өндірістік процестерді басқару жүйелерін бұзуға бағытталған ransomware типіндегі зиянды программалар және кибершпиондау технологияларын қолданатын шабуылдар санының өсуі байқалады.

Киберфизикалық жүйелердің киберқауіпсіздігінің маңыздылығының артуы. Зерттеу барысында жасалған шолу киберфизикалық жүйелердің киберқауіпсіздігін күшейту қажеттілігін көрсетеді, әсіресе энергетика, су, көлік және денсаулық сақтау сияқты маңызды секторларда. Желілерді сегменттеу, бағдарламалық жасақтаманы уақтылы жаңарту және қызметкерлердің ықтимал қауіптер туралы хабардарлығын арттыру сияқты қатаң қауіпсіздік шаралары болған кезде көптеген шабуылдардың алдын алуға болады.

SCADA жүйесіне жасалған шабуылдың артуы. Зерттеу барысында шабуылдардың басым бөлігі SCADA жүйесі арқылы жасалғанын көріп отырмыз. SCADA киберфизикалық жүйелерді бақылау және басқару үшін пайдаланылатындықтан кибершабуылдың негізгі нысанына айналғанын байқадық. Себебі, бұл бизнесті бұзуға, экономикалық және әлеуметтік хаос тудыруға немесе стратегиялық артықшылықтарға қол жеткізуге мүмкіндік береді. SCADA жүйелері көбінесе әлсіз қорғанысқа ие, бұл оларды диверсия, тыңшылық,

бопсалау немесе кибер қаруды сынау үшін оңай нысанаға айналдырады. Соңғы жылдары мемлекеттік нысандарға бағытталған шабуылдар жиілеп бара жатқанын атап өту өте маңызды, бұл киберкеңістіктегі геосаяси тәуекелдердің артып келе жатқанын көрсетеді.

Киберфизикалық жүйелердің қоғамның қауіпсіздігі мен тұрақтылығы үшін маңызды екенін ескерсек, оларды қорғау бүкіл әлем деңгейінде басымдыққа айналуы керек.

Киберфизикалық жүйелердің осалдығы кибер және физикалық компоненттердің интеграциясына байланысты, бұл шабуыл кезінде физикалық зақымдану қаупін арттырады. Ескірген жабдықты пайдалану және жалпы қабылданған қауіпсіздік стандарттарының болмауы мәселені күшейтеді. Сонымен қатар, жүйелердің күрделі архитектурасы, бағдарламалық жасақтама менеджеріндегі осалдықтар және персоналдың жеткіліксіз дайындығы қосымша тәуекелдер тудырады. IoT құрылғыларының көбеюі және желілердің нашар сегменттелуі де осалдыққа ықпал етеді. Біріктірілген бұл факторлар маңызды инфрақұрылымды қорғау үшін киберфизикалық жүйелердің киберқауіпсіздігін жақсарту қажеттілігін көрсетеді.

Зерттеу тақырыбы бойынша жүргізілген ғылыми жарияланымдарға шолу және талдау барысында киберфизикалық жүйелерге жасалатын кибершабуылдардың кең таралған техникалары мен оларды қорғау әдістері анықталды.

2-кесте. Киберфизикалық жүйелерге жасалатын кибершабуылдардың кең таралған техникалары мен оларды қорғау әдістері

Шабуыл түрі	Қорғаныс шаралары	Әдебиет
Зиянды программа	• Антивирустық программаны қолдану және программалық жасақтаманы үнемі жаңарту; • Зиянды программаны таратуды шектеу үшін желіні сегментациялау; • Процестерді бақылау және талдау; • Деректердің тұрақты сақтық көшірмесін жасау.	(Zhenhua Yu, Hongxia Gao. (2023)), (Gunes V., Peter S., Givargis T. & Vahid F. (2014))
SQL инъекция	• Параметрленген сұранысарды пайдалану; • Қолданушы деректерін тексеру және фильтрлеу; • Деректер базасына кіру құқығын шектеу; • Web Application Firewall технологиясын қолдану.	(Cheung S. (2007)), (Mo Y. (2012))
MITM	• Деректерді шифрлауды қолдану(TLS / SSL); • Деректер арналарын қорғау үшін VPN технологиясын енгізу; • Сертификат деңгейіндегі аутентификация процессі; • Аномалияны анықтау және алдын алу механизмдерін қолдану (IDS/IPS).	(Cardinas A. (2008)), (Ten C. W. (2010))
Спуффинг шабуылы	• Көп факторлы аутентификацияны қолдану; • Дереккөздің түпнұсқалығын тексеру үшін цифрлық қолтаңбалар мен сертификаттарды енгізу; • Желілік деректерді шифрлау.	(He H. & Yan J. (2016)), (Amin S. (2013))
DDoS шабуылы	• Жүктемені өңдеу үшін таратылған жүйелерді пайдалану; • DDoS қорғау жүйелерін енгізу; • Трафикті шектеу және күдікті сұрауыстарды фильтрлеу; • Жүктеме теңгергіштерін пайдалану.	(Dhal R. & Kumar S. (2018)), (Xu L. (2014))
Ескерту – автормен құрастырылған		

Киберфизикалық жүйелерге жасалған шабуылдарды талдау қауіпсіздікті қамтамасыз

етудің әртүрлі тәсілдерін қажет ететінін көрсетеді. Зиянды программалар, SQL инъекция, MITM шабуылы, спуффинг және DDoS шабуылдары сияқты киберфизикалық жүйелерге жаслатны заманауи шабуылдар маңызды инфрақұрылымға үлкен қауіп төндіреді. Аталған шабуылдардың әрқайсысы үшін жүйелердің осалдығын азайтуға және шабуылдаушылардың оларды пайдалануына жол бермеуге бағытталған арнайы қорғаныс шаралары бар.

Зиянды программалар киберфизикалық жүйелер үшін ең көп таралған қауіптердің бірі болып қала береді. Зиянды программадан қорғаудың негізгі шаралары антивирустық программаны пайдалану және программалық жасақтаманы үнемі жаңарту болып табылады, бұл белгілі осалдықтардың жұмыс істеуіне жол бермейді. Желіні сегменттеу зиянды программалардың жүйеге енген жағдайда зиянды кодтың таралуын шектейді, ал процестерді бақылау және талдау аномалияларды анықтауға көмектеседі. Деректердің үнемі сақтық көшірмесін жасау сонымен қатар оқиғаларды қалпына келтіруді және деректердің жоғалуын азайтуды қамтамасыз ететін маңызды қорғаныс әдісі ретінде қызмет етеді.

SQL инъекция шабуылы киберфизикалық жүйелерге интеграцияланған деректер базасына қауіп төндіреді. Негізгі қорғаныс шарасы зиянды кодтың SQL сұраныстарының енуіне жол бермейтін параметрленген сұраныстарды пайдалану болып табылады. Қолданушы деректерін тексеру және фильтрлеу рұқсат етілмеген сұраныстарды енгізу мүмкіндігін азайтады және деректер базасына кіру құқығын шектеу маңызды ресурстарды қорғайды. Web Application Firewall (WAF) технологиясын енгізу күдікті сұраныстарды фильтрлеу және веб-қосымшалардың қауіпсіздігін қамтамасыз ету арқылы қосымша қорғаныс қабатын жасайды.

MITM типті шабуылдар киберфизикалық жүйелердің компоненттері арасында берілетін деректердің тұтастығы мен құпиялылығын бұзуы мүмкін. Бұл шабуылды алдын алу үшін деректерді шифрлауды (TLS/SSL) пайдалану және қауіпсіз деректер арналарын құру үшін VPN технологиясын енгізу қажет. Сертификат деңгейіндегі аутентификациялау процессі қолданушылар мен құрылғылардың түпнұсқалығын тексеруді қамтамасыз етеді, ал жүйеге кіруді анықтау және алдын алу механизмдері (IDS/IPS) рұқсатсыз кіру әрекеттерін анықтауға мүмкіндік береді.

Спуффинг шабуылдары киберфизикалық жүйелердегі сәйкестендіру мен аутентификация процесстеріне қауіп төндіреді. Көп факторлы аутентификация дәстүрлі аутентификация әдістерін толықтыра отырып, осы шабуылдардың алдын алудың ең тиімді әдістерінің бірі болып табылады. Цифрлы қолтаңбалар мен сертификаттарды пайдалану хабарлама көздерінің түпнұсқалығын тексеру үшін де маңызды, ал желілердегі деректерді шифрлау олардың жалған болу мүмкіндігін азайтады.

DDoS шабуылдары жүйенің ресурстарын шамадан тыс жүктеуге бағытталған және қызмет көрсетуден бас тартуы мүмкін. Мұндай шабуылдардан қорғау үшін жүктемені өңдеу үшін таратылған жүйелер қолданылады, бұл сұраныстарды қайта бөлуге және белгілі бір түйіндерге жүктемені азайтуға мүмкіндік береді. DDoS қорғаныс жүйелерін енгізу күдікті трафикті уақтылы фильтрлеуге мүмкіндік береді, ал жүктеме теңгергіштері серверлер арасында сұраныстардың біркелкі таралуын қамтамасыз етеді, бұл шамадан тыс жүктемені болдырмайды.

Қорғаныс шараларын талдау киберфизикалық жүйелердің кешенді қауіпсіздігі техникалық шешімдерді (шифрлау, желіні сегментациялау, IDS/IPS) және ұйымдастырушылық шараларды (программалық жасақтаманы жаңарту, көп факторлы аутентификация) қамтитын көп деңгейлі тәсілді қажет ететінін көрсетеді. Киберфизикалық жүйелерге жасалған шабуылдардың әрқайсысының жеке қорғаныс әдістерін қажет ететін өзіндік ерекшеліктері бар. Бұл шараларды тиімді қолдану киберфизикалық жүйелердің шабуылдарға төзімділігін

арттыруға және олардың сенімді жұмыс істеуін қамтамасыз етуге көмектеседі.

Қорытынды. Киберфизикалық жүйелер заманауи инфрақұрылымның негізгі элементі бола отырып, кибершабуылдардың кең спектріне ұшырайды, бұл кешенді қорғаныс шараларын әзірлеуді және енгізуді талап етеді. Зиянды программалар, SQL инъекция, MITM, спуфинг және DDoS сияқты жалпы шабуылдарды талдау олардың әрқайсысының бірегей сипаттамалары бар екенін және киберфизикалық жүйелердің қауіпсіздігіне қауіп төндіретінін көрсетеді. Мұндай жүйелерді тиімді қорғау компьютерлік желіні сегментациялау, шифрлауды пайдалану, көп факторлы аутентификация, IDS/IPS және программалық жасақтаманы үнемі жаңартуды қоса алғанда, көп деңгейлі техникалық және ұйымдастырушылық шараларды біріктіруді талап етеді. Бұл шараларды енгізу киберфизикалық жүйелердің шабуылдарға төзімділігін арттырады, олардың сенімді жұмысын қамтамасыз етеді және маңызды инфрақұрылым үшін тәуекелдерді азайтады.

Кибершабуылдардың күрделілігі мен жиілігін ескере отырып, киберфизикалық жүйелердің қауіпсіздігін қамтамасыз ету оларды пайдалану мен дамытуға жауапты мемлекеттік және коммерциялық ұйымдар үшін басымдық болып қала береді.

Мүдделер қақтығысы. Авторлар мүдделер қақтығысының жоқтығын мәлімдеді.

Әдебиеттер тізімі

June 2017. Framework for Cyber-Physical Systems: Volume 1, Overview. National Institute of Standards and Technology (NIST) Special Publication 1500-201. https://doi.org/10.6028/NIST.SP.1500-201.

Matthew N. O. Sadiku and others. (2017). Cyber-Physical Systems: A Literature Review. European Scientific Journal December 2017 edition Vol.13, No.36 ISSN: 1857 – 7881 (Print) e - ISSN 1857- 7431. URL: http://dx.doi.org/10.19044/esj.2017.v13n36p52.

Abdulmalik Humayed, Jingqiang Lin, Fengjun Li, and Bo Luo. (2017). Cyber-Physical Systems Security – A Survey. Survey of Academic Paper. rXiv:1701.04525v1 [cs.CR].

Hakan Kayan and others. (2022). Cybersecurity of industrial cyber-physical systems: a review. ACM Computing Surveys (CSUR), Volume 54, Issue 11s. Article No.: 229.

Case, D., & Wilhoit, K. (2017). Triton: The First ICS Malware Designed to Attack Safety Instrumented Systems. FireEye Special Report.

Cardenas, A., Amin, S., & Sastry, S. (2008). Research Challenges for the Security of Control Systems. Proceedings of the 3rd conference on Hot Topics in Security.

Knapp, E., & Langill, J. (2014). Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. Elsevier.

Fisher, D. (2015). Black Energy Malware Used in Ukraine Power Grid Attacks. Kaspersky Lab Report.

Cheung, S., et al. (2007). Intrusion Detection Systems for SCADA Networks: A Survey and Taxonomy. Proceedings of the 2007 IEEE International Conference on Emerging Security Information.

Ten, C. W., Liu, C.-C., & Manimaran, G. (2008). Vulnerability Assessment of Cybersecurity for SCADA Systems. IEEE Transactions on Power Systems.

Lee, R. M., Assante, M. J., & Conway, T. (2016). Analysis of the Cyber Attack on the Ukrainian Power Grid. SANS Institute.

Langner, R. (2011). Stuxnet: A Case Study of Cyber Attacks on Industrial Control Systems. IEEE Security & Privacy.

A Survey on Cyber-Physical Systems Security. Zhenhua Yu, Hongxia Gao. (2023). IEEE Internet of Things Journal PP(99). DOI:10.1109/JIOT.2023.3289625.

Gunes, V., Peter, S., Givargis, T., & Vahid, F. (2014). Security and Privacy in Cyber-Physical Systems: A Survey. IEEE Internet of Things Journal.

Cheung, S., et al. (2007). Intrusion Detection Systems for SCADA Networks: A Survey and Taxonomy. Proceedings of the 2007 IEEE International Conference on Emerging Security Information.

Mo, Y., et al. (2012). Design of Secure Cyber-Physical Systems: A Review. IEEE Transactions on Automation Science and Engineering.

Cardinas, A., et al. (2008). Defending Against Cyber Attacks on Industrial Control Systems: Strategies and Countermeasures. IEEE Transactions on Control of Network Systems.

Ten, C. W., et al. (2010). Challenges for Securing Industrial Control Systems. IEEE Transactions on Power Delivery.

He, H., & Yan, J. (2016). Cyber-Physical Attacks and Defenses in the Smart Grid: A Survey. IEEE Communications Surveys & Tutorials.

Amin, S., et al. (2013). Security of Cyber-Physical Systems: Resilience Against Attacks. IEEE Transactions on

Automatic Control.
Dhal, R., & Kumar, S. (2018). Mitigation Strategies for Distributed Denial of Service (DDoS) Attacks in Cyber-Physical Systems. Journal of Network and Computer Applications.
Xu, L., et al. (2014). Securing the Internet of Things: A Case Study in Embedded Systems and Cyber-Physical Systems. IEEE Internet of Things Journal.

Information about authors

Kanzhekeyev Aidyn – Master, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, E-mail: aidyn-94-10@mail.ru, ORCID:0009-0005-0399-2409, +7 702 846 26 36

Konyrkhanova Asem – PhD, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan, E-mail: konyrkhanova_aa@enu.kz, ORCID:0000-0002-4901-8901, +7 771 437 70 79

Tolganbajuly Talant – PhD, «QazCloud» LLP, Astana, Kazakhstan, E-mail: talant.kz@mail.ru, ORCID: 0009-0000-5035-3232, +7 702 524 08 03