УДК 681.5.004 DOI https://doi.org/10.35546/kntu2078-4481.2025.2.2.42

О. В. СИТНІКОВ
кандидат технічних наук,
доцент кафедри технічних та програмних засобів автоматизації
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
ORCID: 0000-0002-6806-1665

О. О. КВІТКА
кандидат хімічних наук, доцент,
доцент кафедри технічних та програмних засобів автоматизації
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
ORCID: 0000-0003-4034-7052

К. Ю. ЖЛОБІНСЬКА
магістрант кафедри технічних та програмних засобів автоматизації
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
ORCID: 0000-0001-6681-4451

Д. С. ОНИЩЕНКО
аспірант кафедри технічних та програмних засобів автоматизації
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
ORCID: 0009-0008-4276-4443

СТВОРЕННЯ АНКЛАВІВ БЕЗПЕКИ ДЛЯ ПРОМИСЛОВОЇ МЕРЕЖІ ПРОЦЕСУ ПАРО-ВОДНЕВОЇ КОНВЕРСІЇ МЕТАНУ

В статті, створення анклавів безпеки для промислової мережі процесу паро-водневої конверсії метан, авторів Ситнікова О. В., Квітки О. О., Жлобінської К. Ю. та Онищенко Д. С. наведено задача розробки структури мережі захисту периметрів анклавів у контексті зв'язку між ними та визначення критичності. Представлено структуру мережі, що складається з трьох основних рівнів, кожен з яких надає змогу виконувати конкретні задачі: корпоративний, операторський, виробничий.

Наведено загальний опис процесу паро-водневої конверсії метану. Вказано який саме контур буде розглядатися в дослідженнях – мережа компресора природного газу, оскільки саме з етапу подачі стиснутого в компресорі до необхідного тиску природного газу до наступного апарату підігрівача й починається сам процес виробництва.

Мережа розділена на функціональні групи, що базуватимуться на контурах, відповідних правилах підключень та згідно рівнів мережі. В дослідженнях керувалися принципом, що функціональні групи відповідають зазначеним рівням мережі, а отже пристрої належать до конкретної групи, якщо розташовані в спільній для них визначеній підмережі.

Наведено, що зі статистичної точку зору найчастіше виникають аварії на виробництві за рахунок відхилення технологічних параметрів від нормативних значень. Оскільки дані типи аварій призводять не тільки до виготовлення бракованої продукції, а й до аварій виробництва з наслідками для працівників, то вищий рівень критичності слід встановити для самих технологічних установок аналогічно до найвищого рівня.

Наведено принцип визначення периметрів, що відповідає рівню схеми – корпоративної, операторської, виробничої мережі, підсистеми керування компресором. В результаті проведених досліджень Представлено та запрограмовано схему захисту периметрів анклавів у контексті зв'язку між ними, із зазначенням відповідних засобів нагляду за потоками даних. За результатами проведених досліджень, створено запит на вибір технічних і програмних засобів кібербезпеки.

Ключові слова: *конверсія метану, кібербезпека, анклав безпеки програмування, моделювання складних систем.*

O. V. SYTNIKOV
Candidate of Technical Sciences,
Associate Professor at the Automation Hardware and Software Department
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
ORCID: 0000-0002-6806-1665

O. O. KVITKA
Candidate of Technical Sciences, Associate Professor,
Associate Professor at the Automation Hardware and Software Department
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
ORCID: 0000-0003-4034-7052

K. U. ZHLOBINSKA
Master's Degree Automation Hardware and Software Department
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
ORCID: 0000-0001-6681-4451

D. S. ONYSHCHENKO
Postgraduate Student at the Automation Hardware and Software Department
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
ORCID: 0009-0008-4276-4443

CREATION OF SAFETY ENCLAVES FOR THE INDUSTRIAL NETWORK OF THE STEAM-HYDROGEN METHANE CONVERSION PROCESS

In the article, creation of safety enclaves for the industrial network of the steam-hydrogen metan conversion process, authored by Sytnikov O. V., Kvitka O. O., Zhlobinska K. U. and Onyshchenko D. S., the task of developing a network structure for protecting enclave perimeters in the context of their connection and determining criticality is presented. The network structure is presented, consisting of three main levels, each of which allows performing specific tasks: corporate, operator, production.

A general description of the process of steam-hydrogen conversion of methane is given. It is indicated which circuit will be considered in the studies – the natural gas compressor network, since it is from the stage of supplying natural gas compressed in the compressor to the required pressure to the next heater device that the production process itself begins.

The network is divided into functional groups, which will be based on circuits, corresponding connection rules and according to network levels. The studies were guided by the principle that functional groups correspond to the specified network levels, and therefore devices belong to a specific group if they are located in a common subnet defined for them.

It is stated that from a statistical point of view, accidents in production most often occur due to deviations of technological parameters from standard values. Since these types of accidents lead not only to the production of defective products, but also to production accidents with consequences for employees, a higher level of criticality should be set for the technological installations themselves, similar to the highest level.

The principle of determining perimeters is presented, which corresponds to the level of the scheme – corporate, operator, production network, compressor control subsystem. As a result of the research, a scheme for protecting the perimeters of enclaves in the context of communication between them is presented and programmed, indicating the appropriate means of monitoring data flows. Based on the results of the research, a request for the selection of technical and software cybersecurity tools is created.

Key words: *conversion of methane, cybersecurity, security enclave, programming, modeling of complex systems.*

Постановка проблеми

Паро-воднева конверсія метану – сукупність технологічних процесів розроблена для отримання водню шляхом реакції з насиченою водяною парою в якості теплоносія. Економічний ефект виробництва значною мірою залежить від організації безпекових режимів роботи промислової мережі. Процес відбувається в декілька стадій [1–2]. Створення анклавів безпеки для промислової мережі підприємства, що складається з трьох основних рівнів, є запорукою безпечного перебігу технологічного процесу [3].

Також необхідним виступає задача по створено запит на вибір технічних і програмних засобів кібербезпеки мережі підприємства.

Аналіз останніх досліджень і публікацій

Аналіз технологічного процесу паро-водневої конверсії метану, розглянуто в роботах [2–6], максимальна увага приділяється тепло-енергетичним процесам, що відбуваються в реакторі. Розглянуті питання моделювання об'єкту керування та моделювання та синтез системи керування як складної системи [3, 6]. Запрограмовано регулятор, що представляє собою програмований логічний контролер (ПЛК), для автоматизованого керування виробничими процесами [4, 5].

Однак, в приведених дослідженнях відсутні принципи моделювання, програмування та створення системи кібербезпеки мережі.

Формулювання мети дослідження

Метою роботи виступає створення та дослідження структури мережі захисту периметрів анклавів у контексті зв'язку між ними та алгоритму визначення критичності активу.

Викладення основного матеріалу дослідження

Структура мережі складається з трьох основних рівнів, кожен з яких надає змогу виконувати специфічні функції: корпоративний (є основною точкою входу мережі, відповідає за керування підприємством, включаючи адміністрування раду процесів, управління ресурсами, комунікацію), операторський (призначений для моніторингу в реальному часі процесів та систем операторами, дає змогу операторам відслідковувати та реагувати на певні події, збої, збирати та аналізувати дані), виробничий (призначений для безпосереднього керування технологічним процесом, включає в себе пристрої та системи задіяні в процесі).

Мережа складається з зазначених вище рівнів. В межах мережі є один маршрутизатор, підключений до всіх рівнів. Кожен рівень має специфічну структуру. Процес дослідження, моделювання та програмування системи відноситься до моделювання складних систем керування.

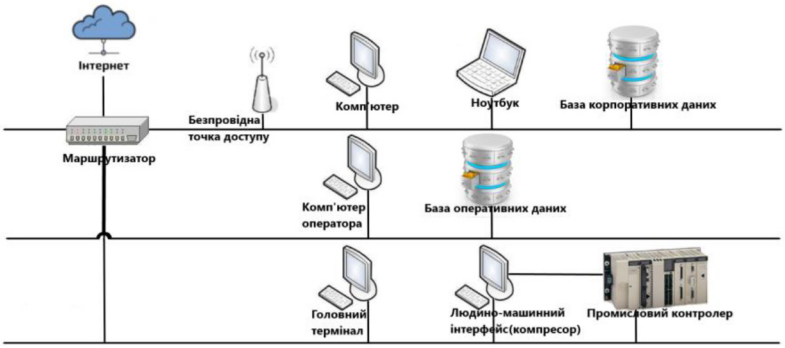

Рис. 1. Структура мережі підприємства

Корпоративний рівень складається з: 1) безпровідної точки доступу Wi-Fi (для бездротового доступу до мережі інших пристроїв); 2) корпоративних комп'ютера та ноутбука (для співробітників і виконання ними корпоративних функцій); 3) корпоративної бази даних (для централізованого зберігання даних корпоративного рівня).

Операторський рівень складається з: 1) комп'ютера оператора (робоча станція оператора); 2) бази даних з оперативними даними (для централізованого зберігання даних про стан та деталі перебігу виробничого процесу).

Виробничий рівень складається з: 1) головного терміналу (центральна та основна робоча станція для управління всіма процесами виробництва); 2) людино-машинного інтерфейсу (ЛМІ) (інтерфейс для зручності керування та роботи з відповідними даними про перебіг процесу виробництва в реальному часі); 3) промислового контролера (програмований логічний контролер – ПЛК – для автоматизованого керування виробничими процесами).

Розглянемо загальний опис процесу паро-водневої конверсії метану [2–3]. Природний газ, стиснений в компресорі до тиску 4 МПа, проходить підігрівач, обігрівається димовими газами конвертора метану, і надходить в систему очищення газу від сірчистих сполук. Система складається з реактора каталітичного гідрування і адсорбера сірководню. Очищений від сполук сірки природний газ надходить в сатуратор (пароносійну вежу), в якій змішується з водяною парою в співвідношенні H_2O: газ = 4:1. Новоутворена парогазова суміш підігрівається до 380 °С в теплообміннику і подається в трубчастий конвертер парової конверсії метану (I ступінь). Трубки конвертера обігріваються за рахунок спалювання в ньому метану, забезпечуючи температуру 800 °С. Після першого ступеня конверсії газ, що містить до 10 % об. залишкового метану і водяну пару в відношенні 0,8:1, направляється в шахтний конвертер повітряної конверсії метану (II ступінь), в який вводиться підігріте повітря. При цьому в конвертері за рахунок екзотермічності реакції (г) підтримується автотермічний режим роботи. З реактора конвертований газ при температурі 900–1000 °С надходить в котел-утилізатор *8*, в якому виробляється пар високих параметрів (10 МПа, 480 °С). Потім охолоджений до 380 °С газ послідовно проходить конвертер оксиду вуглецю (II) I ступеня, котел-утилізатор, в якому додатково охолоджується до 25 °С, і конвертер оксиду вуглецю (II) II ступеня. Вихідний з конвертера газ містить всього 0,5 % обсягу оксиду вуглецю (II). Для видалення з газу утвореного в результаті конверсії оксиду вуглецю (IV) газ проходить через зрошуваний водою скрубер, в якому охолоджується до 30 °С і направляється на етаноламінне очищення в скрубер і регенератор.

Через складну будову виробництва в роботі розглянуто (змодельовано складну систему) лише частину виробничої мережі з метою створення системи кібербезпеки – мережа компресора природного газу, оскільки саме з етапу подачі стиснутого в компресорі до необхідного тиску природного газу до наступного апарату підігрівача й починається сам процес виробництва. В межах даної мережі наведено один ПЛК, що відповідає за автоматизовану роботу та управління роботою компресора. Контур в межах досліджуваної мережі забезпечує контроль витрати природного газу, що надходить до компресору та керування роботою компресора природного газу.

Мережа розділена на функціональні групи, що базуватимуться на контурах, відповідних правилах підключень та згідно рівнів мережі. В дослідженнях керувалися принципом, що функціональні групи відповідають

зазначеним рівням мережі, а отже пристрої належать до конкретної групи, якщо розташовані в спільній для них визначеній підмережі.

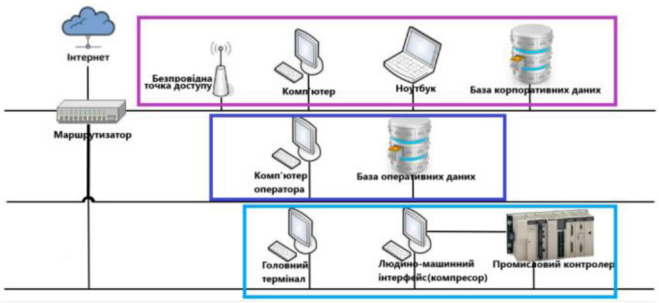

Рис. 2. Функціональні групи за підключенням до мережі

Розбиття на основі контурів керування. Керувалися тим, що якщо контури керування підключені до одного польового керівного пристрою, то слід вважати однією функціональною групою. Відповідну групу підключено до шини *RS*-485 (рис. 3).

Рис. 3. Функціональна група за належністю до контурів керування

Розбиття на основі диспетчерського керування, або підключення до ЛМІ диспетчерів. Керувалися правилом, що до однієї функціональна групи мають належати головний термінал, ЛМІ компресора та ПЛК (рис. 4).

Рис. 4. Функціональна група за підключенням до ЛМІ диспетчерів

Розбиття на основі процесів керування. В даному випадку за процес керування відповідають комп'ютер оператора, головний термінал та ЛМІ (рис. 5).

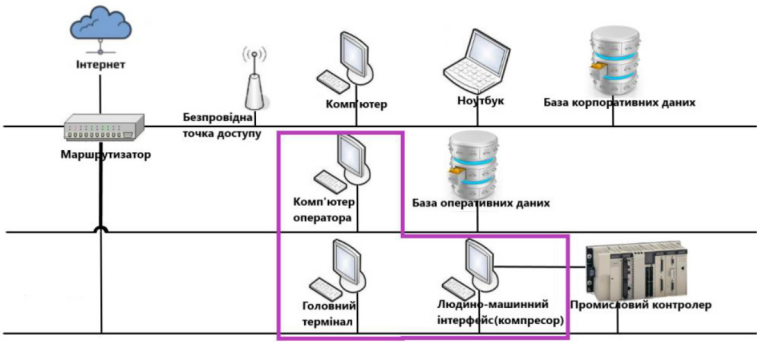

Рис. 5. Функціональна група за процесами керування

Розбиття на основі доступу до даних процесів керування. Проаналізовано кому і на якому рівні надано доступ до якого типу даних. В межах дослідженої мережі доступ до даних виробничого рівня та операторського рівня мають всі, єдина ланка корпоративного рівня, що не має доступу до означених даних, це сама база даних корпоративного рівня, оскільки це не має сенсу. Користувачі корпоративного рівня отримують дані з інших рівнів посилаючи запити на отримання.

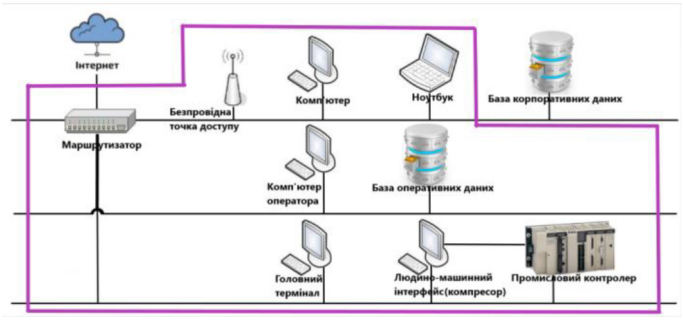

Рис. 6. Функціональна група за доступом до даних процесів керування

Розбиття на основі користувачів і їхніх ролей. Означено які користувачі мають доступ до яких ланок якого рівня. В нашому випадку кожен працівник/користувач має доступ до відповідних ланок мережі виключно на рівні цієї ж мережі, окрім оператора, оскільки для постановки задач на виробництво і виконання конкретних клієнтських замовлень йому треба доступ до корпоративної бази даних.

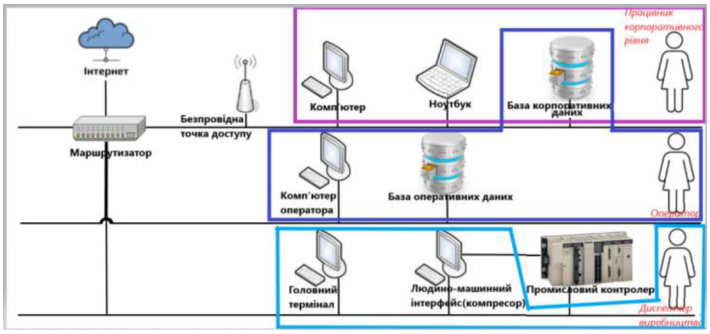

Рис. 7. Функціональні групи за користувачами та ролями

Розбиття на основі протоколів та межі застосування протоколів *Ethernet, Http, Ethernet* промисловий та *Modbus*.

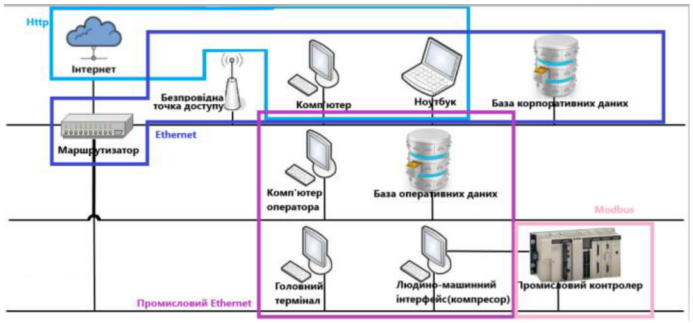

Рис. 8. Функціональні групи на основі протоколів

Визначення критичності кожного пристрою мережі, що зроблено за алгоритмом.

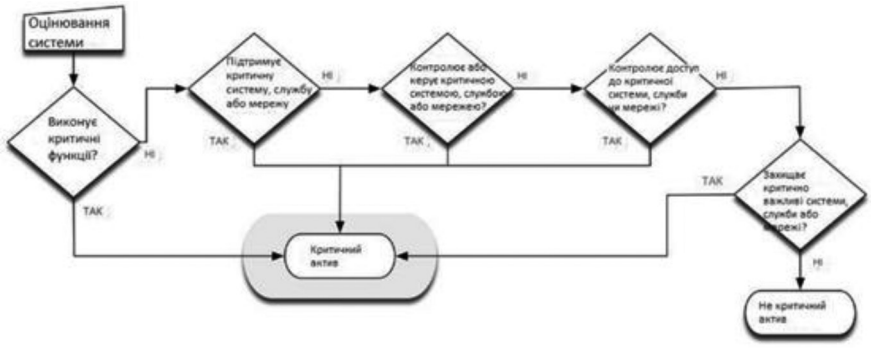

Рис. 9. Схема алгоритму визначення критичності активу

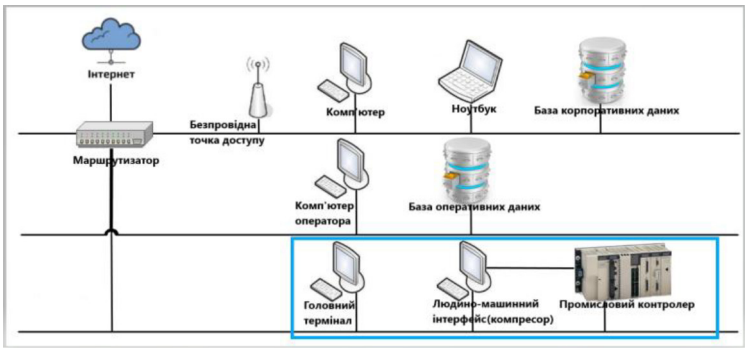

Рис. 10. Функціональна група за критичністю

Зі статистичної точку зору найчастіше виникають аварії на виробництві за рахунок відхилення технологічних параметрів від нормативних значень. Оскільки дані типи аварій призводять не тільки до виготовлення бракованої продукції, а й до аварій виробництва з наслідками для працівників, то вищий рівень критичності слід встановити для самих технологічних установок аналогічно до рівня критичності устаткування – 5-ого (найвищого). Інші активи не можна визначити як критичні, оскільки вони не беруть участь в роботі контурів керування та контролю.

Розбиття мережі на анклави безпеки [7–8].

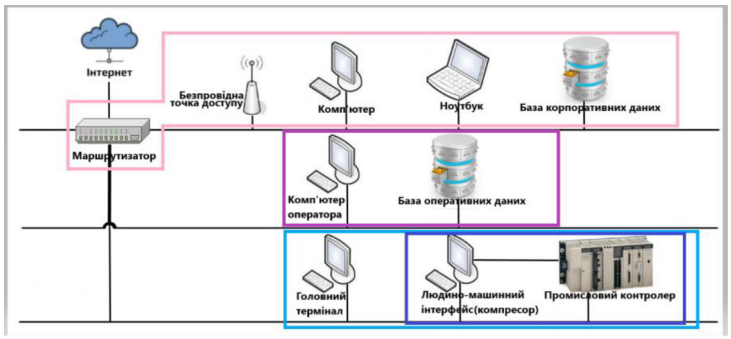

Рис. 11. Анклави безпеки пристроїв мережі

До мережі операторського рівня пізніше підібрано архітектуру її захисту.

Рис. 12. Анклави безпеки та зв'язки між ними

Розроблено та запрограмовано схему двоспрямованих зв'язків між наведеними вище базпековими анклавами [7–8].

Периметри визначатимуться згідно рівнів попередньої схеми: 1) периметр корпоративної мережі (має вихід в інтернет, має безпровідну точку доступу, з'єднана з операторською мережею по протоколу *Ethernet*); 2) периметр операторської мережі (з'єднана з корпоративною мережею по протоколу *Ethernet*, з виробничою – промисловий *Ethernet*); 3) периметр виробничої мережі (з'єднана з операторською мережею через промисловий *Ethernet*, з підсистемою керування компресором – промисловий *Ethernet*); 4) периметр підсистеми керування компресором (вона всередині мережі виробничого рівня, з нею з'єднана через промисловий Ethernet).

Схему захисту периметрів анклавів у контексті зв'язку між ними зображено на рис. 13. Біля анклавів зазначено відповідні засоби нагляду за потоками даних: системи виявлення загроз (IDS), системи запобігання загрозам (IPS), білі списки застосунків (AWL), моніторинг прикладного рівня (МПР), антивірус (Antivirus), віртуальна приватна мережа (VPN), багатофакторна аутентифікація (MFA).

Промислові *Firewall*-и треба налаштовувати так: дозволяти виключно передачі лише з відомих конкретних *IP*-адрес на відомі адреси та з безпечних портів на визначені порти. Встановлення підключення *Windows* пристрою адміністратора, знаючи порт, що використовується на виробництві.

Рис. 13. Захист периметрів анклавів у контексті зв'язку між ними

За результатами проведених досліджень, створено запит на вибір технічних і програмних засобів кібербезпеки:

IPS для ПК (*McAfee*) – комплексне рішення для запобігання вторгненням, що включає виявлення мережевих атак і блокування шкідливого трафіку.

Firewall для різних мереж (*Fortinet*) – високопродуктивний міжмережевий екран з підтримкою *VPN*, захистом від *DDoS* атак та гнучким управлінням безпековими правилами.

Firewall для критично важливих мереж (*Check Point*) – високоефективний міжмережевий екран з функціями сегментації мережі, глибокого аналізу трафіку та захисту від новітніх загроз.

IDS (*Suricata*) – сучасна система виявлення вторгнень з високою продуктивністю та можливостями аналізу мережевого трафіку для виявлення загроз.

Антивірус для серверу (*Bitdefender*) – антивірус для серверів з функціями реального часу, автоматичними оновленнями та широким спектром інструментів управління безпекою.

Висновки

В результаті проведених досліджень було виведено та досліджено структури мережі захисту периметрів анклавів, алгоритму визначення критичності активу та представлено вибір технічних і програмних засобів кібербезпеки.

Список використаної літератури

1. Woolf P. та ін. 6.4: ODE and Excel CSTR model with heat exchange [Електронний ресурс] // Engineering LibreTexts. 11.03.2023. URL: https://eng.libretexts.org/…/6.04%3A_ODE_and_Excel_CSTR_model_with_heat_exchange (дата звернення: 11.05.2025).

2. Blevins M. Control and Field Instrumentation Documentation (Chapter 7) [Електронний ресурс] / International Society of Automation. URL: https://www.isa.org/getmedia/e122051e-8c8c-48be-97ef-5d344c585771/Chapter7_Control (дата звернення: 14.05.2025).

3. Kimray. How to Read an Oil & Gas P&ID: Reference Guide [Електронний ресурс]. URL: https://kimray.com/sites/default/files/uploads/training-demos/Kimray%20 How%20to%20Read%20an%20Oil%20%26%20Gas%20P%26ID%20Reference%20Guide.pdf (дата звернення: 16.05.2025).

4. European Industrial Gases Association. DOC 172/24 – Combustion Safety for Steam Reformer Operation [Електронний ресурс]. 2024. URL: https://www.eiga.eu/uploads/documents/DOC172.pdf (дата звернення: 17.05.2025).

5. Steam boiler drum level measurement technology comparison: DP vs. GWR [Електронний ресурс] // VEGA Blog. 2020. URL: https://www.vega.com/en-us/company/blog/2020/steam-boiler-drum-level-measurement-technology-comparison (дата звернення: 18.05.2025).

6. Cahill J.; Petrishchev L. Hydrogen Production with Steam Methane Reforming and CCUS [Електронний ресурс]. Emerson Automation Experts, 07.04.2023. URL: https://www.emersonautomationexperts.com/2023/sustainability/hydrogen-production-steam-methane-reforming-ccus/ (дата звернення: 19.05.2025).

7. G. Belani, The Use of Artificial Intelligence in Cybersecurity: A Review. URL: https://www.computer.org/publications/tech-news/trends/the-use-ofartificial-intelligence-in-cybersecurity (дата звернення: 20.05.2025)

8. Лісовська Ю. П. Кібербезпека: ризики та заходи: навч. посібник. Київ : Видавничий дім «Кондор», 2019. 272 с.

References

1. Woolf P. та ін. 6.4: ODE and Excel CSTR model with heat exchange // Engineering LibreTexts. 11.03.2023. URL: https://eng.libretexts.org/…/6.04%3A_ODE_and _Excel_CSTR_model_with_heat_exchange (date of application: 11.05.2025). [in English]

2. Blevins M. Control and Field Instrumentation Documentation (Chapter 7) / International Society of Automation. URL: https://www.isa.org/getmedia/e122051e-8c8c-48be-97ef-5d344c585771/ Chapter7_Control (date of application: 14.05.2025). [in English]

3. Kimray. How to Read an Oil & Gas P&ID: Reference Guide. URL: https://kimray.com/sites/default/files/uploads/training-demos/Kimray%20How%20to%20Read%20an%20Oil%20%26%20Gas%20P%26ID%20Reference%20Guide.pdf (date of application: 16.05.2025). [in English].

4. European Industrial Gases Association. DOC 172/24 – Combustion Safety for Steam Reformer Operation. 2024. URL: https://www.eiga.eu/uploads/ documents/DOC172.pdf (date of application: 17.05.2025). [in English].

5. Steam boiler drum level measurement technology comparison: DP vs. GWR // VEGA Blog. 2020. URL: https://www.vega.com/en-us/company/blog/2020/steam-boiler-drum-level-measurement-technology-comparison (date of application: 18.02.2025). [in English].

6. Cahill J.; Petrishchev L. Hydrogen Production with Steam Methane Reforming and CCUS – Emerson Automation Experts, 07.04.2023. URL: https://www.emersonautomationexperts.com/2023/sustainability/hydrogen-production-steam-methane-reforming-ccus/ (date of application: 19.05.2025). [in English].

7. G. Belani, The Use of Artificial Intelligence in Cybersecurity: A Review. URL: https://www.computer.org/publications/tech-news/trends/the-use-ofartificial-intelligence-in-cybersecurity (date of application: 20.02.2025). [in English].

8. Lisovska Yu. P. (2019) Kiberbezpeka: ryzyky ta zakhody: navch. posibnyk. [Cybersecurity: risks and measures: textbook. manual] K. : Vydavnychyi dim “Kondor” 272 s. [in Ukrainian].