Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

на тему
Метод забезпечення кібербезпеки автоматизованих систем критичної інфраструктури газовидобувної компанії на основі оцінки ризиків

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

КРМКБ.180132.22.01.20 ПЗ

Виконав: студент 2 курсу, група КБм-22-1 Підпис Грох А.О.

Керівник доц., к.т.н, доцент Підпис Чешун В.М.

Нормоконтролер старший викладач Підпис Мостовий С.В.

До захисту допускаю:
Зав. кафедри кібербезпеки, к.т.н., доц Підпис Кльоц Ю.П.

14 грудня 2023 р.

Хмельницький, 2023

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Освітній рівень Магістр

Галузь знань 12 Інформаційних технологій

Спеціальність 125 Кібербезпека

Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ

Зав. кафедри Ю.П. Кльоц

"30" 08 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Гроху Антону Олександровичу

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Метод забезпечення кібербезпеки автоматизованих систем критичної інфраструктури газовидобувної компанії на основі оцінки ризиків

Керівник роботи Чешун Віктор Миколайович

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

кандидат технічних наук, доцент

Затверджена наказом № 30 ректора університету, додаток №25 від 15.08.2023

2. Строк подання студентом проекту (роботи) на кафедру 15.11.2023

3. Вихідні дані до проекту (роботи) Дослідження питання забезпечення кібербезпеки автоматизованих систем критичної інфраструктури газовидобувної компанії, визначення та моделювання її структури, ризиків та вразливостей. Формування методу забезпечення кібербезпеки таких систем на основі оцінки ризиків.

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити) Вступ. Визначити основні поняття, проаналізувати сучасні методи та засоби забезпечення інформаційної безпеки. Дослідити поняття інформаційної безпеки автоматизованих систем. Моделювання автоматизованих систем. Розробка методу оцінки ризиків кібербезпеки в автоматизованих системах. Висновки.

5. Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали і посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Мостовий С.В. Старший викладач кафедри кібербезпеки		

6. Дата видачі завдання «01» вересня 2023р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Вибір напряму дослідження і узгодження тематики КРМ з керівником	01.06.2023	
2	Ознайомлення з предметною областю; формулювання мети і задач дослідження; визначення об'єкта і предмета дослідження	04.09.2023	
3	Робота над розділом 1 – визначення основних понять, аналіз сучасних методів та засобів забезпечення інформаційної безпеки; постановка задачі	18.09.2023	
4	Робота над розділом 2 – Моделювання необхідних для виконання задачі структур, процесів та забезпечення.	02.10.2023	
5	Робота над розділом 3 – розробка моделей, алгоритмів та методів.	16.10.2023	
6	Робота над розділом 4 – застосування запропонованих рішень.	06.11.2023	
7	Робота над науковою публікацією	10.11.2023	
8	Узгодження отриманих результатів, оформлення пояснювальної записки згідно вимог	15.11.2023	
9	Попередній захист роботи	17.11.2023	
10	Захист роботи на засіданні ЕК	06.12.2023	

Студент _____ А.О. Грох
Підпис Ініціали, прізвище

Керівник проекту (роботи) _____ В.М. Чешун
Підпис Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: Метод забезпечення кібербезпеки автоматизованих систем критичної інфраструктури газовидобувної компанії на основі оцінки ризиків

Автор роботи: Грох Антон Олександрович.

Керівник роботи: к.т.н., доц. Чешун Віктор Миколайович

Загальний обсяг роботи: 92 сторінки, 29 рисунків, 21 таблиця, 2 додатки, 50 посилань.

Ключові слова: критична інфраструктура, забезпечення інформаційної безпеки автоматизованих систем, оцінка ризиків.

Критична інфраструктура займає важливу роль у функціонуванні держави та посідає надзвичайно важливо роль у суспільстві. Забезпечення інформаційної безпеки на таких підприємствах дозволяє мінімізувати потенціальні ризики, аварії та небезпечні наслідки. Оцінка ризиків – один з ключових параметрів забезпечення кібербезпеки на об'єктах критичної інфраструктури.

В роботі розглянуто сучасні підходи до забезпечення інформаційної безпеки автоматизованих систем об'єктів критичної інфраструктури. Визначено основні поняття, методи та засоби для побудови відповідних рішень, проаналізовано сучасні підходи до аналізу ризиків автоматизованих систем об'єктів критичної інфраструктури. Розроблено метод забезпечення кібербезпеки автоматизованих систем управління технологічними процесами, модель критичних процесів, технічного та програмного забезпечення критичної інфраструктури газовидобувної компанії.

05.12.23

ANNOTATION

Theme of qualification work: Method of ensuring cybersecurity of automated systems of critical infrastructure of a gas extraction company based on risk assessment.

Author of the work: Hrokh Anton Oleksandrovych

Mentor: Ph.D. Assoc. Cheshun Viktor Mykolayovych

Total volume of work: 92 pages, 29 figures, 21 tables, 2 appendices, 50 links.

Keywords: critical infrastructure, ensuring information security of automated systems, risk assessment.

Critical infrastructure plays an important role in the functioning of the state and occupies an extremely important role in society. Ensuring information security at such enterprises allows to minimize potential risks, accidents, and dangerous consequences. Risk assessment is one of the key parameters for ensuring cybersecurity at critical infrastructure facilities.

The work considers modern approaches to ensuring information security of automated systems for critical infrastructure facilities. The main concepts, methods, and tools for developing corresponding solutions are identified, and modern approaches to the risk analysis of automated systems for critical infrastructure facilities are analyzed. A method for ensuring cybersecurity of automated systems for managing technological processes has been developed, as well as a model of critical processes, technical and software support for the critical infrastructure of a gas production company.

05.12.23

ЗМІСТ

ВСТУП

Об’єкти критичної інфраструктури визначаються як поєднання незамінних функцій, які надаються державою. Зазвичай вони включають в себе життєво важливі напрямки діяльності держави, такі як енергетична, хімічна, продовольча, охорона здоров’я, транспортна, фінансова, інформаційно-комунікаційна, комунальна та інші важливі галузі. Призупинення їхньої діяльності або руйнування можуть становити катастрофічні наслідки для нормального функціонування держави в цілому або спричинити загрозу державній безпеці, фінансові збитки, чи навіть призвести до смертельних випадків серед громадян.

Стрімкий розвиток інформаційних технологій наразі є головною рисою сучасного світу, надаючи неймовірні можливості для людства та одночасно створюючи нові ризики. Також неможливо не погодитись, що глобальна розбудова цифрового суспільства та всеосяжне впровадження електронних технологій трансформували майже усі сфери людської діяльності, відповідно об’єкти критичної інфраструктури не залишились осторонь цифровізації. Наразі на таких об’єктах все частіше широко використовуються автоматизовані системи керування та інші технології, які дозволяють пришвидшити процеси управління. Тому під час побудови автоматичної системи керування об’єктом критичної інфраструктури та його життєдіяльності можуть виникати труднощі забезпечення кібербезпеки.

Сьогодні дуже розповсюджені дебати на міжнародному та національних рівнях в різних країнах світу, на яких обговорюється широкий спектр питань, пов’язаних з кібербезпекою в системах об’єктів критичної інфраструктури. Зокрема це зумовлено тим, що такі системи є завжди актуальними для здійснення кібератак, особливо в умовах кібервійн, так як зупинка роботи такого об’єкту може призвести до величезних збитків, також вони містять велику кількість конфіденційних даних, інформації державного значення тощо.

З урахуванням вищезазначеного, можемо зауважити, що захист важливих інфраструктур, таких як автоматизована система керування критичними об’єктами є надзвичайно важливим питанням та вимагає комплексного підходу до

інформаційної безпеки та поєднує у собі фізичні, цифрові та процедурні компоненти, які забезпечують рівень кібербезпеки, необхідний для захисту від різноманітних загроз. Отже, при проектуванні системи забезпечення інформаційної безпеки для автоматизованої системи керування об’єктами критичної інфраструктури важливо вміти правильно та всеохоплююче оцінювати можливі ризики.

Саме тому все частіше виникають різноманітні дискусії між науковцями, спеціалістами з ІТ технологій, політиками тощо, як в середині країни, так і на міжнародній арені, стосовно забезпечення кібербезпеки на об’єктах критичної інфраструктури.

Провівши аналіз наукових праць вітчизняних та зарубіжних науковців, різноманітних підходів та концепцій ми дійшли до висновку, що питання забезпечення кібербезпеки в системах об’єктів критичної інфраструктури є малодослідженим. Хоча ця тема неодноразово піднімалась в колах науковців та існують певні напрацювання стосовно кібербезпеки на об’єктах критичної інфраструктури, метод забезпечення кібербезпеки автоматизованих систем об’єктів критичної інфраструктури на основі оцінки ризиків є новою науковою категорією та потребує детального вивчення.

Мета дослідження. Підвищення ефективності інформаційної безпеки автоматизованих систем критичної інфраструктури газовидобувної компанії з-за допомогою ризик-орієнтованого підходу.

Об’єкт дослідження. Інформаційна безпека та захист автоматизованих систем автоматизованого об’єктів критичної інфраструктури.

Предмет дослідження. Метод та алгоритми оцінки інформаційних ризиків автоматизованих систем критичної інфраструктури газовидобувної компанії.

Досягнення мети дослідження пов’язане з наступними завданнями:

1. Визначити основні засади діяльності критичної інфраструктури та безпосередньо газовидобувної компанії.

2. Дослідити структурні елементи автоматизованої системи критичної інфраструктури газовидобувної компанії, порядок їхньої взаємодії.

3. Розробити модель автоматизованої системи критичної інфраструктури газовидобувної компанії з метою аналізу її активів, в тому числі їхніх вразливостей.

4. Розробити метод забезпечення кібербезпеки автоматизованих систем критичної інфраструктури газовидобувної компанії та відповідні алгоритми.

Методи дослідження. В дослідженні було використано такі методи дослідження, як аналіз, синтез, математичне моделювання. Також було використано за основу базові положення інформаційної безпеки, теорії множин.

Наукова новизна отриманих результатів:

1. Побудовано модель автоматизованої системи об’єктів критичної інфраструктури на основі взаємозв’язків між фізичними, логічними активами та критичними процесами

2. Розроблено метод, заснований на алгоритмах оцінки ризиків інформаційної безпеки автоматизованих систем об’єктів критичної інфраструктури, що дозволяє визначити актуальний рівень безпеки на відповідному об’єкті, засновуючись на основі аналізу та обробки ризиків.

Практична цінність одержаних результатів. Отримані результати дозволяють ефективно реалізувати метод управління ризиками інформаційної безпеки автоматизованої системи критичної інфраструктури газовидобувної компанії та ідентифікувати критичні процеси, можливі вразливості комп’ютерної безпеки, моделювати загрози, виходячи з них, а також керувати ризиками інформаційної безпеки критичної інфраструктури.

Перелік публікацій. За темою магістерської роботи опубліковано 3 тези доповідей на Всеукраїнській та міжнародних науково-практичних конференціях.

1 ВИЗНАЧЕННЯ ОСНОВНИХ ПОНЯТЬ, АНАЛІЗ СУЧАСНИХ МЕТОДІВ ТА ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

1.1 Визначення поняття критичної інфраструктури, її роль у функціонуванні держави та категоризація об'єктів критичної інфраструктури

Для розуміння сучасних викликів та загроз, які виникають під час діяльності об'єктів критичної інфраструктури необхідно визначити їх суть, організаційні засади створення та діяльності, а також їхню роль в державному управлінні та безпеці.

В першу чергу, важливо визначити поняття критичної інфраструктури. Відповідно до національного законодавства, критична інфраструктура визначається, як «сукупність об'єктів критичної інфраструктури. Об'єктами критичної інфраструктури визначаються об'єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам» [1]. На нашу думку, таке визначення не відкриває суть даного поняття та не дозволяє нам зрозуміти його роль.

Водночас науковці здійснюють більш широке визначення критичної інфраструктури, зокрема Д. С. Бірюков та С. І. Кондратов вважають, що терміном «критична інфраструктура», зазвичай, охоплюються ті об'єкти, системи, мережі або їх частини, порушення функціонування або руйнування яких призведе до найсерйозніших наслідків для соціальної та економічної сфери держави, негативно вплине на рівень її обороноздатності та національної безпеки. Крім того, функціонування критичної інфраструктури в мирний час пов'язується із підтримуванням життєво важливих функцій в суспільстві, захистом базових потреб його членів і формуванням у них відчуття безпеки і захищеності [2].

Вероглядс О. надає наступне визначення: критична інфраструктура – це

підприємства й установи (незалежно від форми власності) таких галузей, як енергетика, хімічна промисловість, транспорт, банки та фінанси, інформаційні технології, телекомунікації (електронні комунікації), продовольство, охорона здоров'я, комунальне господарство, що є стратегічно важливими для функціонування економіки та безпеки держави, суспільства, населення, виведення з ладу або руйнування яких може позначитися на національній безпеці й обороні, природному середовищі, призвести до значних матеріальних і фінансових збитків, людських жертв [3].

Критично важливі об'єкти інфраструктури діють як система життєзабезпечення повсякденного існування людей. Співтовариства людей підтримуються доволі комплексною і складною мережею інфраструктурних систем. Громадяни очікують і покладаються на функціонування в своїх країнах установ і служб для захисту свого здоров'я, фізичної безпеки, охорони й економічного благополуччя. Виведення з ладу, серйозні збої і навіть дрібні, але постійні недоліки в роботі та функціонуванні певної інфраструктури чи її елементів можуть створювати загрозливі, а іноді й критичні для нормальної життєдіяльності ситуації. Тому в більшості зарубіжних країн із метою систематизації потенційно небезпечних об'єктів введено до обігу термін «критична інфраструктура» [4].

Як правило, до критичної інфраструктури відносять енергетичні та транспортні магістральні мережі, нафто- та газопроводи, морські порти, канали швидкісного та урядового зв'язку, системи життєзабезпечення (водо- та теплопостачання) мегаполісів, утилізації відходів, служби екстреної допомоги населенню та служби реагування на надзвичайні ситуації, високотехнологічні підприємства та підприємства військово-промислового комплексу, а також центральні органи влади [5].

Можемо погодитись з думками кожного з авторів, адже, критична інфраструктура – це сукупність об'єктів, систем, установ, які належать до різних галузей та дійсно відіграють визначальну роль у забезпеченні життєдіяльності держави, забезпечуючи стабільний економічний розвиток, безпеку громадян, функціонування державних установ та підтримуючи обороноздатність.

Визначивши поняття критичної інфраструктури можемо сформулювати її роль у функціонуванні держави. На нашу думку, критична інфраструктура відіграє надзвичайно важливу роль у суспільстві та публічному управлінні, включаючи в себе такі основні аспекти, як національна безпека та оборона, економічна стійкість, доступ до життєво важливих послуг, таких як медицина, електроенергія, водопостачання, транспортна система тощо.

Законом України «Про критичну інфраструктуру» для організації ефективного забезпечення безпеки і стійкості критичної інфраструктури з урахуванням специфіки забезпечення окремих життєво важливих функцій та/або послуг визначаються сектори критичної інфраструктури. До життєво важливих функцій та/або послуг, порушення яких призводить до негативних наслідків для національної безпеки України, належать, зокрема [1]:

– урядування та надання найважливіших публічних (адміністративних) послуг;
– енергозабезпечення (у тому числі постачання теплової енергії);
– водопостачання та водовідведення;
– продовольче забезпечення;
– охорона здоров’я;
– фармацевтична промисловість;
– виготовлення вакцин, стале функціонування біолабораторій;
– інформаційні послуги;
– електронні комунікації;
– фінансові послуги;
– транспортне забезпечення;
– оборона, державна безпека;
– правопорядок, здійснення правосуддя, тримання під вартою;
– цивільний захист населення та територій, служби порятунку;
– космічна діяльність, космічні технології та послуги;
– хімічна промисловість;
– дослідницька діяльність.

Категоризацію критично важливих об'єктів слід проводити незалежно від належності відомства та типу об'єкта. Метою категоріювання є пред'явлення кількісних і якісних вимог до системи фізичного захисту. Ці вимоги пред'являються залежно від рівня втрат і присвоєної у відповідності з ним категорією об'єкта. Категорія об'єкта повинна визначатися на основі оцінки потенційної небезпеки об'єкта, при цьому повинна враховуватися ймовірність наступних видів та масштабів втрат [6].

У випадках категоріювання об'єктів критичної інфраструктури потрібно створити комісію з категоріювання, і першою дією комісії є складання переліку процесів організації [7]:

– управлінських;

– технологічних;

– виробничих;

– фінансово-економічних тощо, в яких використовуються об'єкти інфраструктури.

Формально правила категоріювання передбачають включення до переліку взагалі всіх процесів, але в реальності процеси, пов'язані виключно з ручною або механізованою працею потім все одно будуть виключені з розгляду.

Підсумовуючи все вище викладене варто підкреслити, що критична інфраструктура визначається як сукупність об’єктів, систем тощо, які є надзвичайно важливими для функціонування держави та суспільства в цілому. Роль критичної інфраструктури полягає в забезпеченні безпеки, стійкості розвитку держави, її обороноздатності та повсякденного життя громадян. Розподіл об’єктів критичної інфраструктури на категорії допомагає краще розуміти їхню роль та функціонування в загальній системі, захищати від загроз та вживати необхідні заходи для захисту відповідних об’єктів. Негативні фактори впливу або відмови в роботі критичної інфраструктури можуть призвести до катастрофічних наслідків, тому важливо приділяти окрему увагу її захисту, ретельно планувати заходи та порядок відновлення у разі кризових ситуацій.

1.2 Нормативне забезпечення кібербезпеки в об’єктах критичної інфраструктури

В умовах повномасштабної війни в Україні, всесвітньої геополітичної напруги та кризи все частіше така ворожнеча відбувається у кіберпросторі. Відповідно останнім часом збільшились та масштабувались кібервійни, ми можемо спостерігати як щодня у світі зазнають атак безліч структур та установ, в тому числі об’єкти критичної інфраструктури.

Передовий міжнародний досвід переконливо засвідчує, що за останні роки у світі в 57 разів збільшилася кількість кібератак, у зв’язку з чим провідні країни змушені посилювати захист стратегічно важливих підприємств та об’єктів критичної інфраструктури. Наразі найрозвиненіші держави світу витрачають на кібербезпеку у 5 разів більше, ніж на інші напрямки ІТ-галузі. За оцінками фахівців, вже у 2025 році ці витрати можуть сягнути 10,5 трильйонів доларів у світових масштабах. Одним із основних чинників, які утворюють значну небезпеку об’єктам критичної інфраструктури, є кіберзагрози та кібератаки. [8].

Останнім часом все більше й більше країн втягуються у «холодну війну» в кіберпросторі, накопичують «кіберможливості», шпигують і тестують комп'ютерні мережі, готуючись використовувати можливості Інтернету в кібервійнах. Деякі країни терміново підвищують свої кібернетичні можливості шляхом створення спеціальних підрозділів з питань протидії нападу в кіберпросторі (Ізраїль, КНР, Німеччина, Франція, Індія, Південна Корея, Естонія та ін.). Крім того, координація зусиль з даного питання на міжнародному рівні дуже активно розгортається в рамках НАТО та ЄС [9].

Термін «інформаційна безпека» чітко визначений в міжнародному стандарті «ISO/IEC 27000», опублікованому Міжнародною Організацією зі стандартизації (ISO) та Міжнародною електротехнічною Комісією (IEC), який зазначає, що це поняття окреслює збереження конфіденційності, цілісності та доступності інформації [10].

Відповідно до національного законодавства, кібербезпека - це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [11];

Вітчизняні науковці мають схожу думку, зокрема Мельник С.В., Тихомиров О.О., Лєнков О.С. визначають кібербезпеку у нормативному контексті як захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у сфері функціонування інформаційно-телекомунікаційних систем.

У технологічному контексті - це процесс захисту кіберпростору від реальних та потенційних кіберзагроз.

На філософсько-соціологічному рівні осмислення кібербезпеку можна інтерпретувати через сукупність умов функціонування суб'єкта у кіберпросторі, що забезпечують його оптимальний інформаційний розвиток [12].

Ми можемо погодитись з усім вищезазначеним, адже інформаційна безпека дійсно передбачає збереження конфіденційності, цілісності та доступності інформації та є загальним підходом до забезпечення безпеки даних.

Кібербезпека, визначена в національному законодавстві та вітчизняними науковцями включає в себе захищеність життєво важливих інтересів людини, громадянина, суспільства та держави в кіберпросторі.

Поняття захищеності інформації є важливим аспектом в сучасному світі, особливо в публічному та державному секторах.

1.3 Поняття автоматизовних систем управління технологічними процесами об’єктів критичної інфраструктури, їх структура та забезпечення

Автоматизація в сучасних системах використовується для вирішення різноманітних проблем та задач, які можуть виникати під час роботи підприємств, в тому числі об’єктів критичної інфраструктури. При цьому вирішуються задачі, пов’язані з кожним елементом технологічного об’єкту управління, таким чином зменшується кількість необхідних людських та енергетичних ресурсів. Відповідно під час впровадження автоматизованих систем повинна зберігатись якість продукту та необхідна його кількість за певну одиницю часу.

Автоматизована система повинна забезпечити три головних властивості технологічного процесу, який, до речі, схожий з властивостями інформаційної безпеки – конфіденційність, цілісність, доступність. У випадку з автоматизованою системою – це будуть ефективність, надійність та безпека.

Відповідно ефективність – це зниження затрат ресурсів та енергоресурсів для виробництва продукції. Надійність – це забезпечення незмінності якості продукту, в тому числі в умовах відказу технологічного обладнання. Безпека – це підвищення терміну служби технологічного обладнання шляхом вибору оптимальних режимів роботи, зменшення участі людини в технологічному процесі.

Ящук В.І. зазначає, що автоматизовані системи вносять в повсякденне життя об’єктів критичної інфраструктури певний порядок, регламентуючи роботу та заощаджуючи час. Разом із тим, надалі невирішеними залишаються питання розв’язання функціональних задач діяльності об’єктів критичної інфраструктури з метою підвищення їх безпеки; належна увага не приділяється проблемам ефективного використання інформаційних технологій об’єктів критичної інфраструктури. Загальними особливостями об’єктів критичної інфраструктури є автоматизація процесів планування, обліку і управління основних напрямків діяльності об’єктів критичної інфраструктури. Тому загалом їх можна розглядати як інтегровану сукупність таких основних підсистем: управління фінансами, управління матеріальними потоками, управління обслуговуванням, управління

якістю, управління персоналом, управління збутом, аналіз фінансів, собівартості, оборотних коштів, управління маркетингом тощо [13].

Також для забезпечення інформаційної безпеки автоматизованих систем об’єктів критичної інфраструктури важливо розуміти процес управління та контролю з-за допомогою таких систем. Пропонуємо розглянути це на прикладі автоматизованої системи управління технологічним процесом на газовидобувному підприємстві.

Нехай технологічна установка по видобуванню газу буде об’єктом управління, а система автоматичного управління – органом управління. Таким чином вона здійснює керування механізмами на свердловинах, які регулюють потоки газу, а технологічна установка формує зворотній зв’язок, надсилаючи сигнали з датчиків та відповідно здійснює функції контролю. На основі зворотного зв’язку система автоматичного управління може корегувати процеси керування. Таким чином така система є закритою та в ній відсутній людський вплив. Це дозволяє швидко обробляти інформацію під час формування сигналів керування та обробляти великі потоки даних. Відповідно людина не здатна настільки швидко приймати інформацію, обробляти її та приймати правильні рішення, тобто замінити систему автоматичного управління (рис. 1.1).

Рисунок 1.1 – Система автоматичного управління

Система, в якій приймає участь в прийнятті та реалізації рішень по керуванню технологічним процесом, відносяться до класу автоматизованих систем управління технологічним процесом.

Відповідно до ДСТУ автоматизована система керування технологічними процесами – це автоматизована система, яка призначена для вироблення та реалізації керувальної дії на технологічний об’єкт керування згідно з прийнятими критеріями керування [14].

А. О. Бобух слушно зазначає, що АСК ТП характеризується єдністю і взаємодією трьох основних складових [15]:

– об'єкт керування (ОК) - це технологічні процеси з агрегатами, апаратами, установками та ін. та трубопроводами матеріальних потоків, що з'єднують все устаткування;

– технічні засоби (ТЗ) - автоматичне обладнання обробки інформації, в тому числі (МПК);

– оперативний персонал (ОП)

– оператори-технологи, експлуатаційний персонал.

Відповідно, для управління в рамках АСУ на екранах технічних засобів демонструються показники приладів, де працівник може взаємодіяти з об’єктом управління. Проте, зазвичай така взаємодія не є прямою, тому оператору в деяких випадках необхідно перевіряти фактичний результат виконання певних дій на підприємстві (рис. 1.2).

Технічне забезпечення АСУ ТП включає в себе відповідне обладнання, до якого відносять (рис. 1.3):

– периферійне обладнання – безпосередньо взаємодіє з об’єктом управління;

– програмований логічний контролер або віддалений термінал управління;

– серверне обладнання, на якому встановлюється SCADA (Supervisory Control And Data Acquisition);

– програмне забезпечення, що дозволяє автоматизувати процес управління різними технологічними процесами в реальному часі. Програмний комплекс

забезпечує збір даних, обробку та передачу їх в диспетчерську, наочне відображення на моніторах комп'ютерів, управління пристроями і механізмами виконання, архівацію всієї необхідної інформації [16];

– автоматизоване робоче місце для диспетчера або оператора;
– мережеве обладнання;
– канали зв’язку між всіма видами обладнання.

Рисунок 1.2 – Автоматизована система управління технологічними процесами

Програмне забезпечення включає в себе програмну логіку, власне на якій побудована АСУ ТП та складається з системного програмного забезпечення, яке забезпечує середовище для виконання спеціалізованих програм та задач. На автоматизованих робочих місцях та серверах – це операційна система, на мережевому та периферійному обладнанні зазвичай використовується вбудоване програмне забезпечення, зазвичай – це прошивка.

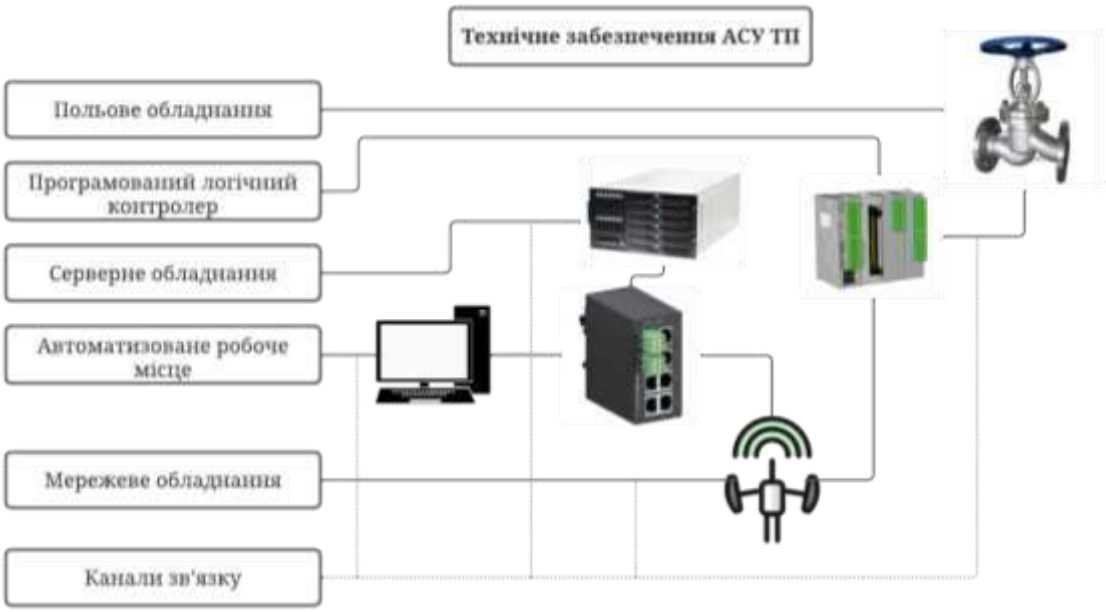


Рисунок 1.3 – Технічне забезпечення АСУ ТП

Спеціальне програмне забезпечення слід розподіляти на базове, до якого відноситься серійне програмне забезпечення від виробника та яке неможливо перепрограмувати під незадекларовані потреби (до прикладу SCADA системи, які виконують роль середовища, завчасно заданих розробником завдань) та відповідно, прикладне програмне забезпечення, до прикладу, проект SCADA, алгоритм програмованого логічного контролера, тощо. Тобто таке забезпечення є унікальним для окремої установки або класу технологічних установок.

Відповідно до вищезазначеного, варто зауважити, що базове програмне забезпечення є більш вразливим до несанкціонованого доступу та потеціально вразливішим. Прикладне програмне забезпечення, як правило, містить унікальний програмний код для кожного класу промислових об’єктів, що, безумовно, є перевагою, однак такі системи приваблюють зловмисників, тому що задають логіку роботи АСУ ТП. Прикладом такої атаки слугує кейс із поширенням вірусу «Stuxnet» на п’яти промислових об’єктах Ірану. З огляду на те, що згадані підприємства були не підключені до мережі Інтернет через питання безпеки, фахівці дійшли висновку, що зараження вірусом відбувалося через фізичне проникнення людей з носіями вірусу на підприємства. Хтось, свідомо чи ні,

приносив із собою заражений диск і вставляв його у внутрішню мережу, інфікуючи її у такий спосіб [18].

Взаємодія програмного забезпечення АСУ ТП з фізичними пристроями зазвичай здійснюється за допомогою методів: DDE, OLE, COM, DCOM, OPC[17].

– DDE (Dynamical Date Exchange) – динамічний обмін даними. З'явився в 1987 році разом з Windows 2.0.

– OLE (Object Linking and Embedding) – зв'язування та впровадження

– об'єктів.

– COM (Component Object Model) – модель багатокомпонентних об'єктів.

– DCOM (Distributed Component Object Model) – модель багатокомпонентних об'єктів для розподілених систем. Дозволяє взаємодіяти програмам, які виконуються на різних комп'ютерах локальної мережі. Вона стала універсальною технологією взаємодії SCADA-системи, як клієнта із сервером, який забезпечує зв'язок з апаратами і засобами. DCOM стало базою для створення OPC.

– OPC (OLE for Process Control) – найчастіше працюють за схемою «клієнтсервер».

Також важливою складовою забезпечення АСУ ТП є інформаційне забезпечення. Перевисокова Н. В. відносить до інформаційного забезпечення автоматизованих систем інформаційну базу та засоби її організації та реалізації. Інформаційне забезпеченням АСУ, на думку науковиці, визначається як сукупність єдиної системи класифікації та кодування техніко-економічної інформації, уніфікованих систем документації і масивів інформації, які використовуються в автоматизованих системах управління, в тому числі форми документів, відеограм, масивів і інтерфейси або протоколи обміну даними [19].

На нашу думку, до інформаційного забезпечення АСУ ТП необхідно відносити інформаційні активи, вхідні/вихідні сигнали, протокольовані події, які в свою чергу дозволяють отримати дані про те, як відбувається технологічний процес. Детальна інформація дозволяє відновити виробництво після аварійних

ситуацій, проаналізувати дані та знайти причину збою. На даному етапі важливим критерієм є саме цілісність такої інформації.

Дані, які отримує оператор в ході роботи, пропонуємо розділити на вихідні документи та екранні форми. До перших відноситься документація, яка необхідна для звітності роботи, а екранні форми – це інформація, яка надається працівнику під час роботи на екрані автоматизованого робочого місця (рис. 1.4).

Рисунок 1.4 – Інформаційне забезпечення АСУ ТП

1.4 Інтегровані системи керування, механізми сполучення, типова структура автоматизованої системи управління технологічними процесами

З метою комплексного забезпечення інформаційної безпеки на об’єктах критичної інфраструктури, а саме автоматизованих систем газовидобуваної компанії, надзвичайно важливо дослідити поняття інтегрованих систем керування, адже саме вони стають об'єктом збільшеного інтересу для кіберзлочинців та кібершпигунів.

Інтегрована АСУ підприємством (об’єднанням) – це багаторівнева автоматизована система управління, яка призначена для комплексної автоматизації функцій управління інженерно-технічною, адміністративно-господарською, виробничо-технологічною і соціальною діяльністю промислових підприємств і забезпечує ефективніше розв’язання задач з планування, випуску, розробки,

освоєння, виробництва і реалізації продукції. Наприклад, до складу інтегрованої АСУ науково-виробничим об’єднанням належать локальні АСУ: автоматизовані системи управління об’єднанням (АСУО), підприємствами (АСУП), цехами, дільницями, АСУ технологічними процесами (АСУ ТП), системи автоматизованого проектування конструкторського (САПР-К) і технологічного (САПР-Т) призначення, автоматизовані системи наукових досліджень (АСНД) та інші види АСУ. [19].

Під час проектування сучасних АСУ ТП також розробляються інтегровані системи управління (рис. 1.5). Першим видом інтегрованих систем є суміжні. Вони використовуються для обліку ресурсів, що видобуваються, моніторингу стану виробництва та передачі інформації з діагностики. Наступним видом є автоматизована система диспетчерського управління (АСДУ), вона необхідна для управління технологічними процесами диспетчерами в режимі реального часу.

Якщо на об’єкті використовується розподілений технологічний комплекс, застосовується система лінійної телемеханіки (СЛТМ) для керування ним.

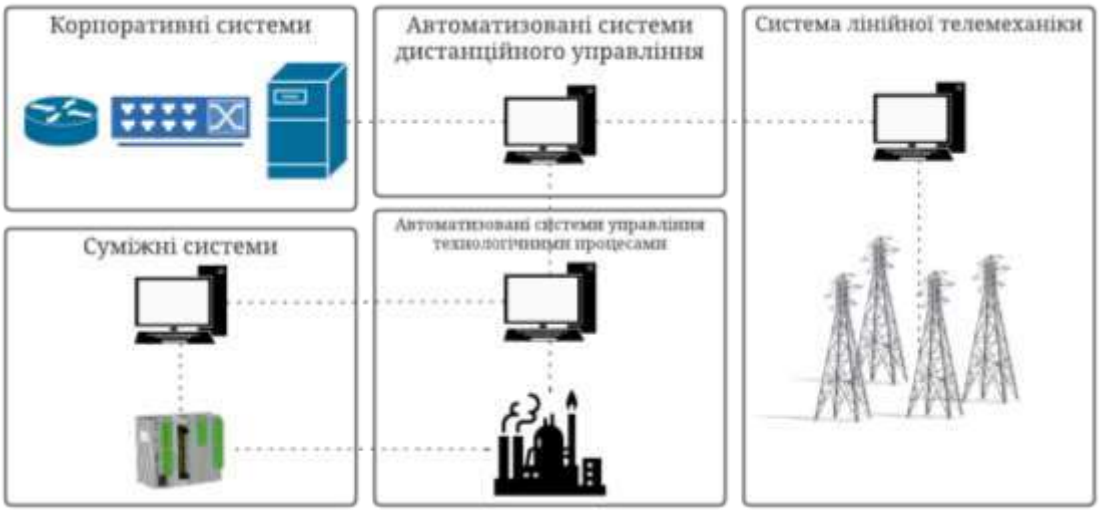


Рисунок 1.5 – Інтегровані системи управління АСУ ТП

Наступним важливим критерієм розуміння роботи АСУ ТП об’єкту критичної інфраструктури є механізми його сполучення. Вони включають в себе компоненти та технології для передачі і обміну даними між різними складовими

системи. Зазвичай механізми сполучення АСУ ТП розподіляються на нижній, середній та верхній рівні.

На нижньому рівні знаходяться технологічний об’єкт та периферійне обладнання у вигляді механізмів та датчиків. Для отримання інформації іншою системою на цьому рівні іншою системою необхідно встановлювати додаткові датчики, які будуть пов’язані з окремим програмованим логічним контролером. На нижньому рівні з точки зору інформаційної безпеки сполучення між системами відсутнє, тому що використовується логічний зв’язок через об’єкт управління, тобто датчики будуть збирати однакову інформацію для різних систем.

На середньому рівні для розуміння того, як відбувається сполучення необхідно розглянути принип роботи одного з модульних пристроїв. На нашу думку, варто розглянути програмований логічний контролер (ПЛК).

ПЛК може складатися з [20]:

– модуля центрального процесора (CPU);
– модуля аналогових виходів;
– модуля аналогових входів;
– модуля комунікацій;
– модуля дискретних виходів;
– модуля дискретних входів;
– модуля керування осями;
– модуля лічильників;
– спеціальних модулів;
– блоків пам'яті ROM, PROM, EPROM, EEPROM.

Два ПЛК, між якими відбувається сполучення взаємодіють на основі модулей вводу/виводу (рис. 1.6). Таким чином з точки зору роботи ПЛК вони є один для одного датчиками або виконуваними механізмами, тобто можна або отримати інформацію, або надіслати її, на основі чого ПЛК по заданих алгоритмах буде виконувати певні дії.

З точки зору інформаційної безпеки такий метод сполучення є менш безпечним за нижній рівень, проте через середній рівень впливати на сервери, чи

робочі станції складно, так як багато залежить від технологій, які застосовуються безпосередньо на пристроях. До прикладу, на таких системах можна використовувати протокол HART. Протокол HART (Highway Addressable Remote Transducer) де-факто став стандартом протоколу обміну інформацією з інтелектуальними промисловими засобами вимірювання. Інформаційна магістраль фізично реалізується за допомогою двопровідної лінії, якою організовується аналоговий канал передачі інформації, наприклад, сигналом струму в стандартному діапазоні 4-20 мА. Адресація і обмін службовою інформацією здійснюється за допомогою цифрових сигналів, які пересилаються тим самим каналом поруч з аналоговим сигналом. Специфікація HART-протоколу визначає фізичну форму передачі, процедури обміну, структуру повідомлення, формати даних і набір команд. Спочатку HART-протокол був розроблений фірмою Rosemount Inc. Але потім, з метою підтримки просування на ринок інтелектуальних промислових приладів з цифровим обміном інформацією, ця фірма передала всі права на протокол так званому Фонду HART-комунікацій (HART Communication Foundation). Зараз використання HART-протоколу є вільним [21].

Відповідно, якщо на такому рівні використовується протокол HART та аналоговий канал, перепрограмувати інші пристрої важче, ніж при використанні протоколу Ethernet. Також на деяких ПЛК може використовуватись неспеціалізоване або вразливе програмне забезпечення, до прикладу «Windows XP». Такі пристрої є найбільш вразливими до зовнішнього впливу.

Наступний рівень сполучення АСУ ТП – це вищий рівень (рис. 1.7.), на якому зазвичай використовуються засоби обчислювальної техніки, серверів та робочих станцій. Вони присутні як в основній, так і в суміжній системах. На вищевказаному рівні інтеграція суміжних систем здійснюється на основі виділених комунікаційних серверів або OPC-серверів, які в свою чергу, взаємодіють на основі протоколу OPC (Open Platform Communications) . Більшість з таких серверів, як правило, побудовані на основі операційної системи Windows Server. Основним недоліком такого сполучення, з точки зору інформаційної безпеки – це використання Windows-систем та вразливого протоколу RPC (Remote procedure call).

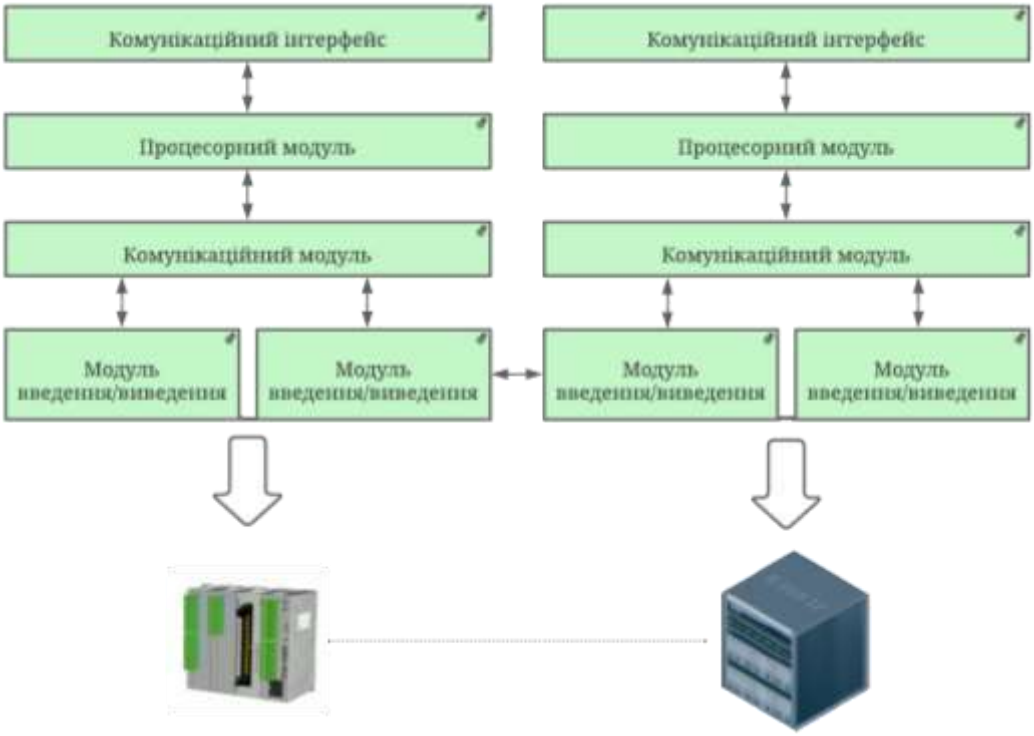


Рисунок 1.6 – Механізми сполучення АСУ ТП на середньому рівні

Важливим аспектом дослідження інформаційної безпеки автоматизованих систем управління технологічним процесом об’єктів критичної інфраструктури є розуміння їхньої типової структури. Пропонуємо розглянути її аналогічно механізмам сполучення, розподіливши на рівні управління.

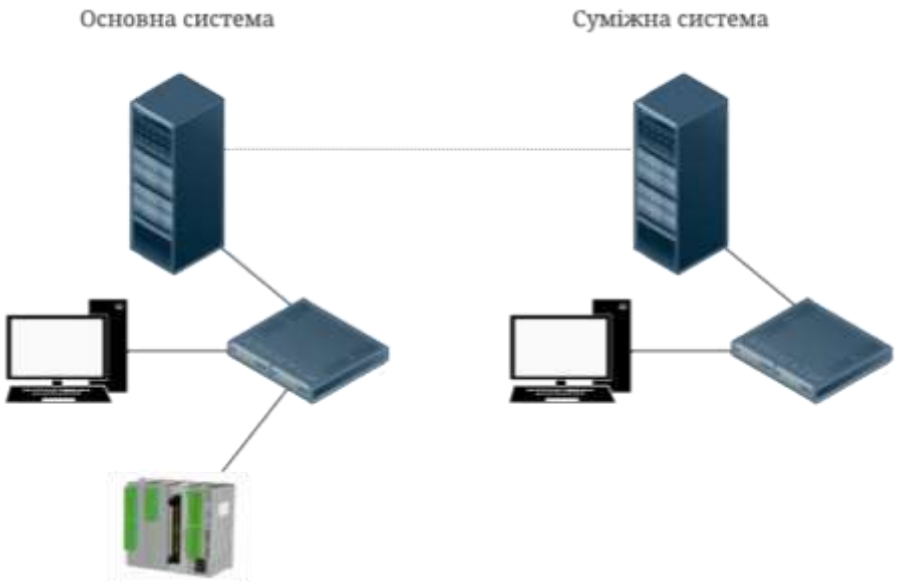


Рисунок 1.7 – Механізми сполучення АСУ ТП на верхньому рівні

Островерхов М.Я. вважає, що найчастіше використовується трирівнева структура АСУ ТП (рис. 1.8) [17].

Ми погоджуємося з думкою науковця та відповідно розглядаємо типову структуру АСУ ТП на трьох рівнях: нижньому, середньому та верхньому (рис. 1.9).

Нижній рівень АСУ ТП складається з польового обладнання, яке включає датчики, пристрої виконання та пристрої регулювання, які відносяться до об’єктів управління. Польове обладнання за допомогою електричних кабелів підключається до одного з модулів вводу/виводу. Підсистема введення/виведення складається з апаратних модулів, які в свою чергу, відрізняються по типу електричного сигналу.

Рисунок 1.8 – Структура АСУ ТП

Якщо до модуля підключається датчик, то модуль здійснює введення сигналу в систему і називається модулем введення; якщо підключається пристрій виконання, то модуль виводить керуючий вплив з системи та називається модулем виведення. По типам сигналів модулі розподіляються на аналогові, дискретні та цифрові.

Електричний сигнал, який надходить з датчика, в підсистемі введення/виведення інтерпретується як вимірювання певної фізичної величини, до прикладу тиску газу, після цього аналоговий сигнал перетворюється в цифрову форму та передається по спеціальній шині в контролер.

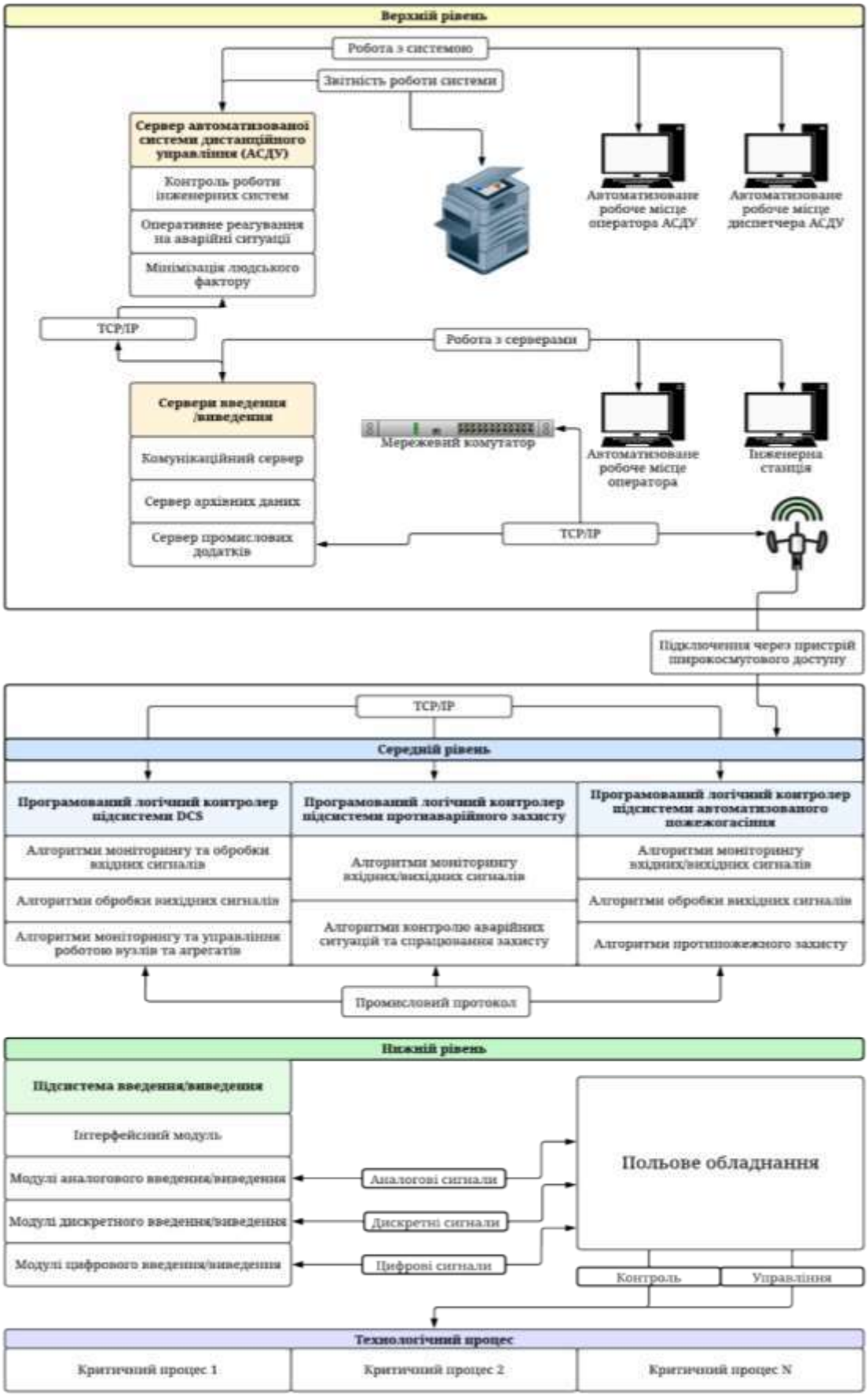


Рисунок 1.9 – Схема типового АСУ ТП на промисловому об’єкті критичної інфраструктури

Середній рівень АСУ ТП складається з програмованого логічного контролера, віддаленого терміналу та необхідних вторинних приборів. Основною задачею програмованого логічного контролера та віддаленого терміналу є обробка інформації, яка надходить з системи введення/виведення та зворотній вплив. Ця обробка виконується з-за допомогою завчасно заданих алгоритмів керування та є циклічною. Зв'язок між нижнім та середнім рівнем забезпечується за допомогою інтерфейсного модуля.

Технічний рівень реалізується на мікропроцесорних пристроях [17]:

– контролери на базі ПК, в тому числі для промислового застосування випускають відомі фірми: Octagon, Advantech, Analog Devices;

– локальні ПЛК;

– мережевий комплект контролерів;

– повномасштабні серії контролерів.

Локальні ПЛК можуть бути вбудовані в обладнання або у вигляді автономних пристроїв. Вони мають порти для з'єднання з датчиками по системі «точка-точка» та інтерфейси для підключення в комп'ютерну мережу. Випускаються також локальні ПЛК спеціального типу (наприклад, для аварійного захисту). Найчастіше вони мають близько 10 входів/виходів;

Мережевий комплект контролерів – найбільш широкий клас, який впроваджується в АСУТП. Контролери мають декілька локальних пультів операторів, набір інтерфейсів для різних стандартів комп'ютерних мереж та дозволяють реалізувати різні топологічні схеми мереж;

Повномасштабні серії контролерів дозволяють автоматизувати виробничу діяльність великого підприємства.

Верхній рівень системи складається з серверів введення/виведення, сервера автоматизованої системи дистанційного управління та автоматизованого робочого місця.

1.5 Постановка задачі

Вимоги вирішення науково-технічної задачі створення методу забезпечення кібербезпеки автоматизованої системи критичної інфраструктури газовидобувної компанії, а саме автоматизованої системи управління технологічними процесами, який поєднує оцінку збитків та можливості реалізації загроз в умовах складної, ієрархічної структури, вимагає оцінити можливі ризики.

Проведений в цьому розділі аналіз дозволяє визначити наступні задачі магістерської роботи:

1. Створення моделі автоматизованої системи управління технологічними процесами з метою визначення активів ієрархічної структури та їхньої взаємодії при вирішення задачі керування ризиками.

2. Методу, заснованого на алгоритмах оцінки ризиків інформаційної безпеки з урахуванням збитків від реалізації загроз, які експлуатують вразливості системи та безпосередньо впливають на активи.

Цим питанням присвячені наступні розділи магістерської роботи.

2 ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ АСУ ТП, МОДЕЛЮВАННЯ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ ТЕХНОЛОГІЧНИМИ ПРОЦЕСАМИ

2.1 Інформаційна безпека автоматизованої системи, управління технологічними процесами, основні типи загроз

Відповідно до вищезазначеного, а саме: видів, функцій структури АСУ ТП, механізмів її сполучення, неможливо не погодитись, що аспект інформаційної безпеки є вкрай складним та важливим питанням.

Велика кількість промислових об’єктів, які потенційно можуть бути ідентифіковані, як об’єкти критичної інфраструктури використовують технологічні системи, що дозволяє підвищити ефективність виробництва, оптимізувати використання ресурсів, зменшити вплив людського фактору на виробництво, якісно виконувати складні завдання, контролювати роботу систем завдяки обробці та архівації даних. Більшої актуальності набирає процес автоматизації та «інтелектуалізації» таких систем. При цьому розробка нормативно-правових актів та стандартів із забезпечення кібербезпеки, їх функціонування, дещо відстає від розвитку та поширення таких систем, а відповідно з цим, затримується розробка суто технічних методів із кіберзахисту та їх практична реалізація, не сформовані підходи до управління ризиками при впровадженні та подальшій експлуатації АСУ ТП [22].

Через необхідність безперервної роботи базові компоненти АСУ ТП (індустріальні протоколи, операційні системи, системи управління базами даних) не мають можливості регулярного оновлення. До джерел вразливостей можна віднести використання широко розповсюджених технологій (операційні системи - Windows, WinCE, Linux тощо, застосунки — системи управління базами даних, вебсервери та відповідні широко вживані мережеві протоколи — HTTP, RPC, FTP, DCOM, SNMP тошо) для підвищення ефективності управління організацією з

використанням віддаленого доступу. При цьому трапляються випадки підключення АСУ ТП до корпоративних мереж. Усе зазначене призводить до появи вразливостей у системі, з використанням яких реалізуються нові загрози [23].

Саме тому необхідно визначити основні типи загроз та порушень інформаційної безпеки, які можуть виникати під час роботи АСУ ТП.

Типи загроз інформаційної безпеки дуже широке поняття та містить багато різновидів та класифікацій. Зокрема Верескун М.В. зазначає, що загрози інформаційній безпеці - це можливі дії або події, які можуть вести до порушень ІБ. Вони також є кінцевими цілями (або результатами) діяльності її порушників. Види загроз інформаційної безпеки дуже різноманітні і мають безліч класифікацій. Та пропонує власну класифікацію, яка, на його думку, є найбільш актуальною по відношенню саме до промислових підприємств (рис. 2.1) [24].

Рисунок 2.1 – загрози інформаційній безпеці промислових підприємств

Ми погоджуємось з думками вітчизняних науковців та, в свою чергу, пропонуємо під час класифікації загроз враховувати специфіку АСУ ТП. Таким чином нам вдалось акцентувати увагу на трьох основних типах порушень інформаційної безпеки на вищезгаданому об’єкті:

– нехтування правилами та халатність працівників об’єкта критичної інфраструктури як інциденти можуть виникати, якщо співробітники використовують інфраструктуру підприємства не за цільовим призначенням. До

прикладу, несанкціоноване підключення зовнішніх пристроїв (модемів, носіїв інформації тощо), установка стороннього програмного забезпечення, підключення сторонніх пристроїв до корпоративної мережі тощо;

– розкрадання, на відміну від попереднього типу порушення, цей тип виконується навмисно, з ціллю використання АСУ ТП для того, щоб розкрадати продукт, що виробляється;

– цільова кібератака (Advanced Persistent Treat (APT)) може мати безліч причин та наслідків. В основному здійснюються з метою принесення шкоди критичному об’єкту інфраструктури, спричинення аварій або зупинення виробництва, якщо мова йде про кібервійни та кібертероризм, або з метою промислового шпигунства (отримати конфіденційні дані).

Пропонуємо далі розглянути детально кожен з вищезазначених типах порушень інформаційної безпеки з урахуванням архітектури АСУ ТП об’єкта критичної інфраструктури, яку ми розглядали у попередніх підрозділах (рис. 2.2).

Нехтування правилами та халатність працівників об’єкта критичної інфраструктури. Типовим сценарієм такого порушення є підключення працівником інфікованого знімного носія шкідливим програмним забезпеченням (ШПЗ). Якщо на пристрої відсутній антивірус або застаріле програмне забезпечення, ШПЗ проникає на клієнтську машину оператора, порушує її роботу та може розповсюджуватись по корпоративній мережі. Як наслідок, може припинитись робота клієнтської машини або декількох робочих станцій через брак системних ресурсів. У випадку, якщо ШПЗ – це вірус-вимагач, може бути заблокований доступ до операційної системи з вимогою викупу для відновлення попереднього стану системи.

Другий сценарій – підключення несанкціонованого модему до автоматизованого робочого місця з доступом до SCADA-системи. Таким чином цей пристрій опиняється у Всесвітній мережі та потенційно є вразливим до безлічі загроз. До прикладу, це дозволяє здійснити DoS-атаку (Denial of Service) на пристрої всередині корпоративної мережі.

Рисунок 2.2 – Клас атак – халатність працівників

Варто зазначити, що специфіка роботи АСУ ТП не дозволяє нехтувати правилами інформаційної безпеки, адже навіть короткочасні зловмисні впливи на об'єкт критичної інфраструктури може призвести до незворотніх наслідків.

Щодо розкрадання, інформація під час роботи АСУ ТП розподіляється по ієрархії, відповідно до структури від нижчого до верхнього рівня. Для реалізації такого порушення інформаційної безпеки зловмиснику необхідно вплинути на показання системи, тобто зробити так, щоб в систему потрапляли хибні показання. Такого можна досягнути шляхом перепрограмування ПЛК, використати ШПЗ, з-за допомогою якого змінити дані, які передаються на автоматизоване робоче місце тощо (рис. 2.3).

Цільові кібератаки, на нашу думку, в умовах сьогодення є найпоширенішими з усіх вищевказаних типів. В свою чергу, їх слід поділяти на два типи:

– атаки з метою несанкціонованого доступу до інформації (рис. 2.4);

– атаки з метою диверсії на виробництві та порушення технологічного процесу (рис. 2.5).

Рисунок 2.3 – Клас атаки – розкрадання

Атаки з метою отримання конфіденційної інформації зазвичай направлені на отримання даних обмеженого доступу для нанесення збитків підприємству або державі. До такої інформації зазвичай відносять конфігурації ПЛК, дані з пульта керування оператора, архівні відомості SCADA-систем тощо.

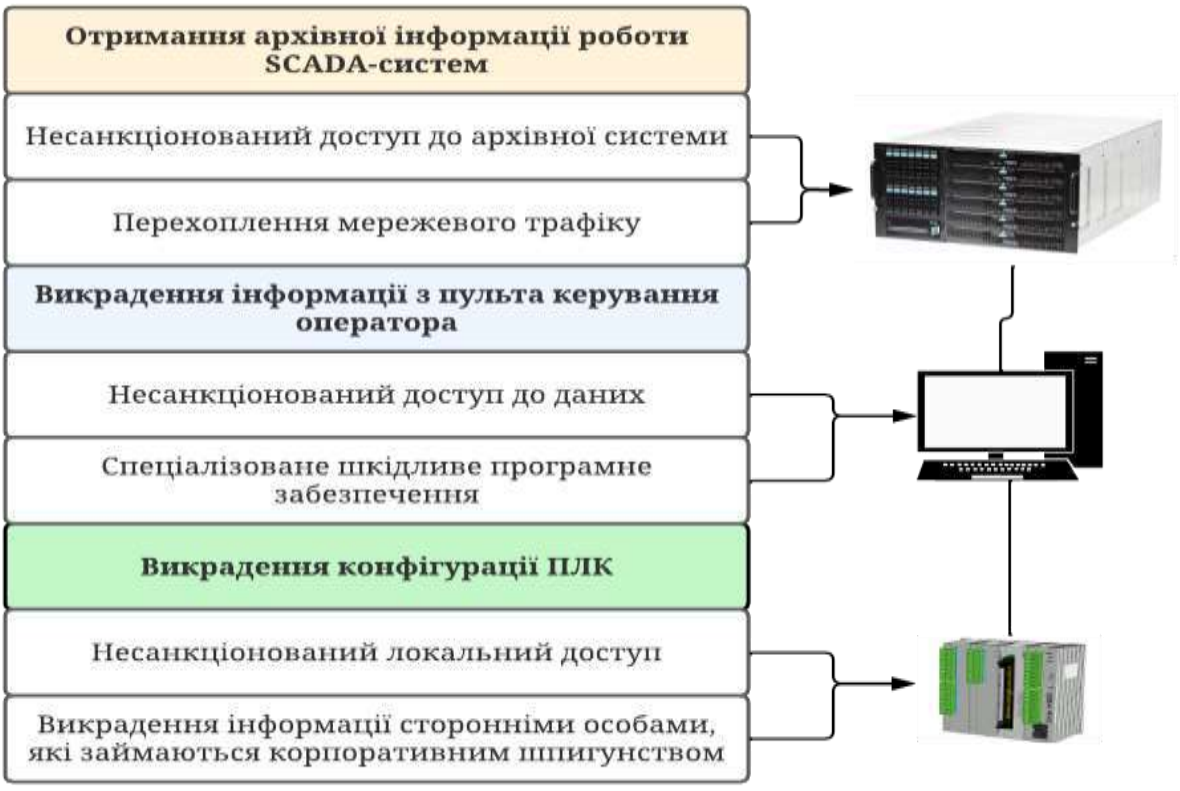


Рисунок 2.4 – цільова атака з метою отримання інформації

Атаки з метою порушення технологічного процесу зазвичай призводять до аварійного стану на виробництві та досягаються шляхом перепрограмування ПЛК або автоматизованого робочого місця, яке відповідає за контроль датчиків об’єкта. Як правило, на критично важливих підприємствах передбачені системи захисту від таких випадків, тому в разі виходу з ладу показників певних пристроїв, система повинна автоматично їх вимкнути (рис. 2.5).

Менш передбачуваними є атаки, які здійснюються з метою впливу на кінцевий продукт. Ідея такої атаки полягає в зміні принципів роботи механізмів, які відповідають, до прикладу, за відділення газу від конденсату. Таки чином, якщо зловмиснику вдалось досягнути мети, продукт, що видобувається буде мати іншу консистенцію та якість. Це може вплинути на репутацію компанії та завдати значних збитків.

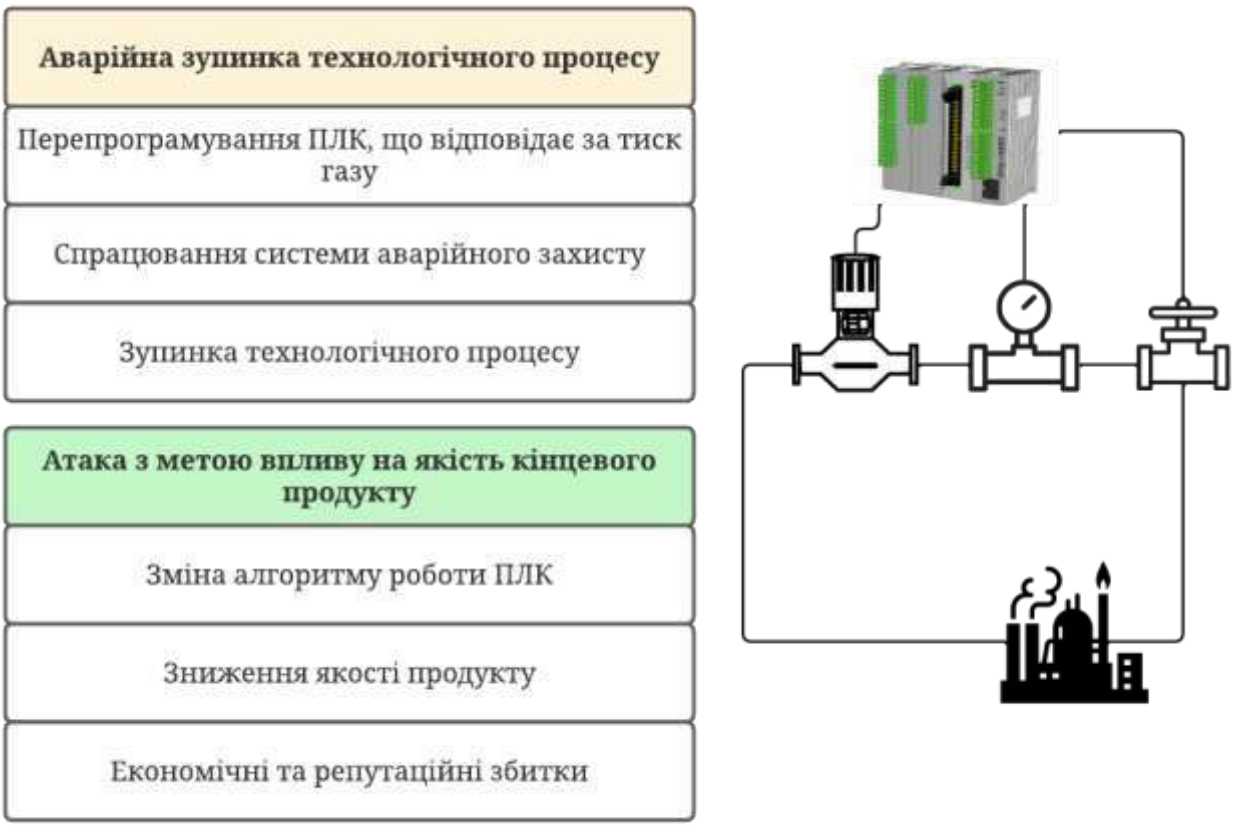


Рисунок 2.5 – Сценарії цільових атак з диверсійними цілями

Окрему увагу слід приділити стадіям атаки на АСУ ТП (рис. 2.6), так як це дозволить ретельніше ідентифікувати потенційні загрози та в подальшому розробити методи реагування на кіберінциденти. Пропонуємо розглянути стадії атаки на АСУ ТП відповідно до її структури та стадій технологічного процесу, які починаються на верхньому рівні та закінчуються на нижньому.

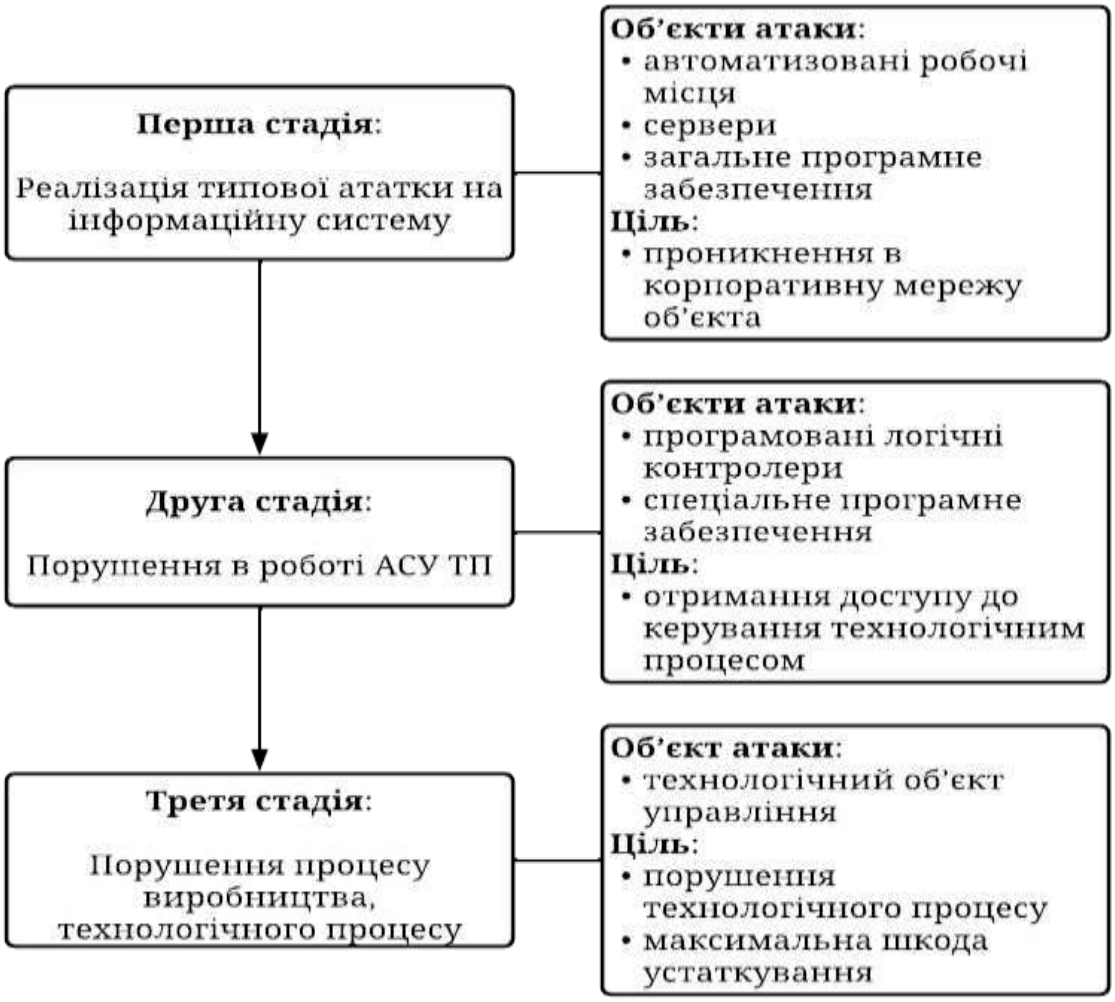


Рисунок 2.6 – стадії атаки на АСУ ТП

Перша стадія – це атака через людино-машинний інтерфейс АСУ ТП або через підключення до суміжних систем. Як ми вже згадували раніше, ці системи використовують популярні IT-рішення, які містять загальновідомі вразливості, тому вони вразливі до звичайних атак, в ході яких зловмисник проникає до захищеного периметру АСУ ТП.

Друга стадія – це наступний етап атаки, на якому вразливими об’єктами є технологічні елементи системи, до прикладу, SCADA-системи або алгоритми ПЛК. При цьому основна ціль – порушення технологічного процесу, збої в роботі АСУ ТП тощо.

Третя стадія – атака на технологічні об’єкти управління, які керуються ПЛК або віддаленим терміналом. Ця стадія характеризується завданням максимальної шкоди підприємству.

В цьому розділі пропонуємо змоделювати АСУ ТП з точки зору інформаційної безпеки з метою подальшої оцінки ризиків. Під час моделювання основна увага буде приділена взаємодії елементів системи відповідно до структури АСУ ТП. Модель інфраструктури буде складатись з множини активів на різних рівнях ієрархії АСУ ТП.

2.2 Вибір підходу до моделювання

В попередньому розділі нами було проаналізовано типову структуру АСУ ТП, механізми сполучення, інтегровані системи керування та протоколи, які використовуються для передачі інформації, після чого ми дійшли до висновку, що такі системи є складними у взаємодії компонентів між собою. Відповідно це наштовхує на думку, що в системах АСУ ТП є високий потенціал виникнення вразливих елементів у її структурі і з цим неможливо не погодитись.

Існують різні підходи до моделювання систем захисту інформації (СЗІ), що відбивають різні аспекти систем захисту [25]:

− моделі, що використовують підходи теорії ймовірності та нейронних мереж;

− моделі, побудовані з використанням теорії мереж Петра-Маркова;

− моделі, що ґрунтуються на теорії кінцевих автоматів;

− моделі, збудовані з використанням теорії графів;

− моделі, що використовують теорію нечітких множин;

− моделі, збудовані з використанням ентропійного підходу;

− теоретико-множинні моделі.

Зазвичай щоб вибрати підхід для моделювання потрібно звертати увагу на вхідні дані та результати розрахунків, які отримуються на виході. Вхідна інформація повинна базуватись на статистиці для існуючих інформаційних систем або даних відповідних експертів. Модель повинна містити формальний опис об’єкта моделювання, при цьому необхідно враховувати ієрархічну структуру АСУ ТП. Тому на першому етапі пропонуємо використати теоретико-множинну модель.

2.3 Модель автоматизованої системи технологічних процесів критичних інфраструктур газовидобувної компанії

З попереднього розділу ми дійшли до висновку, що автоматизація відіграє ключову роль у забезпеченні безперебійного функціонування критичної інфраструктури. Модель, запропонована у цьому розділі містить комплексний підхід до автоматизації, де кожен рівень системи відповідає своїй ролі з метою підвищення ефективності, надійності та безпеки виробничих процесів.

Для моделювання автоматизованої системи управління технологічними процесами та її елементів пропонуємо використати теоретико-множинний підхід. Першочергово необхідно визначити всі множини елементів загальної структури сучасної автоматизованої системи управління технологічними процесами, які можуть певним чином вплинути на оцінку ризиків та співвідношення між ними, що розглядались в минулому розділі (рис. 2.7).

Таким чином в модель було включено всі можливі активи автоматизованої системи управління технологічними процесами, відтворено їхній взаємозв’язок з урахуванням складності та ієрархічного розподілу складових цієї системи.

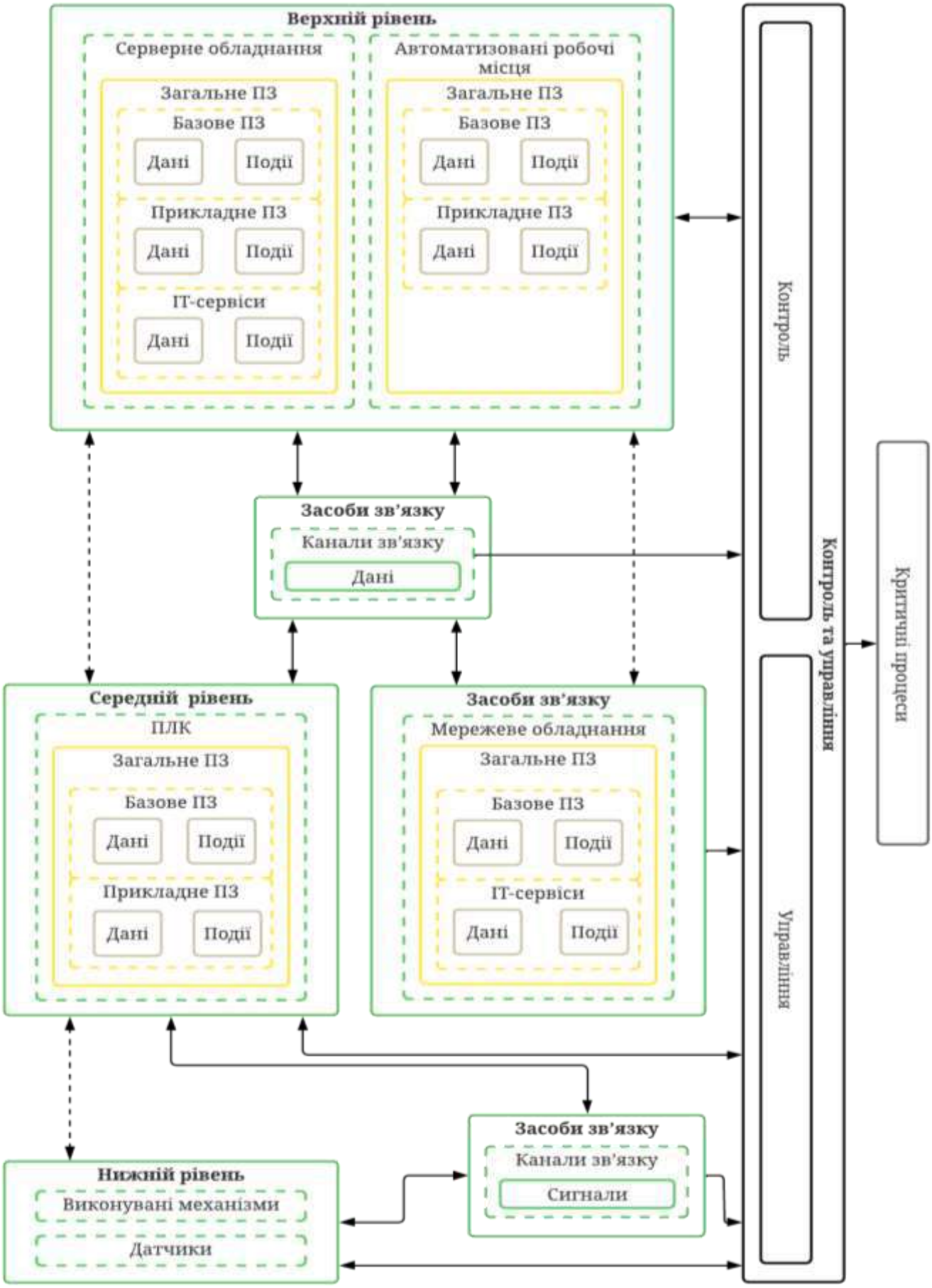


Рисунок 2.7 – Взаємозв’язок елементів АСУ ТП

2.3.1 Модель критичних процесів

Взаємозв’язок критичних процесів та польового обладнання пропонуємо змоделювати у вигляді наступної схеми (рис. 2.8).

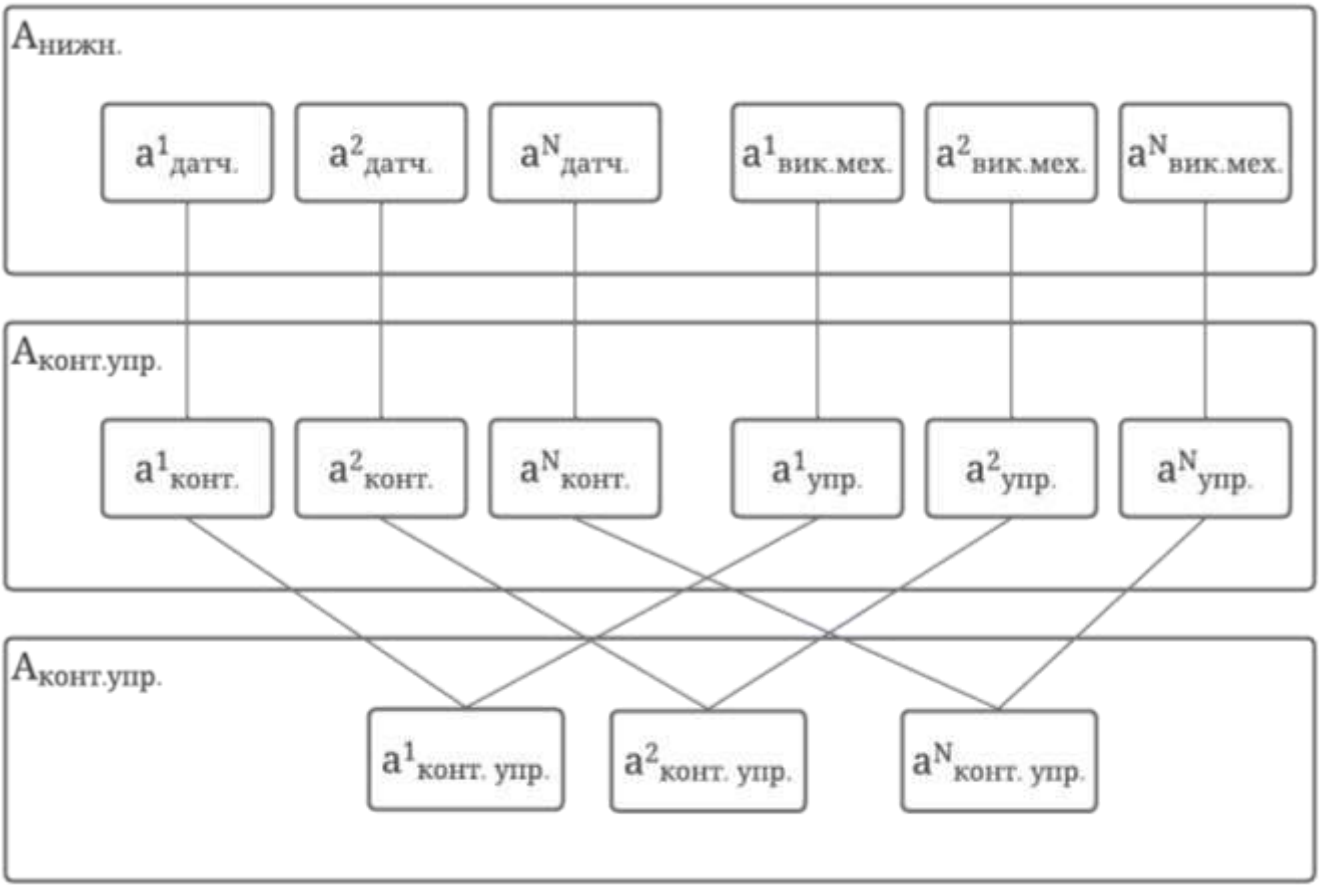


Рисунок 2.8 – Модель критичних процесів АСУ ТП

Модель критичних процесів АСУ ТП визначається сукупністю елементів:

$$M_{\text{кр.пр.}} = (A_{\text{тех.пр.}}, A_{\text{конт.упр.}}, G_{\text{кр.пр.}}), \quad (2.1)$$

де $A_{\text{тех.пр.}} = A_{\text{кр.пр.}} \cup A_{\text{нижн.}}$ – множина елементів технологічного процесу. $A_{\text{нижн.}}$ – множина елементів нижнього рівня АСУ ТП; $A_{\text{конт.упр.}} = A_{\text{конт.}} \cup A_{\text{упр.}}$ – множина процесів по контролю та управлінню критичних процесів; $G_{\text{кр.пр.}} = (A_{\text{тех.пр.}}, A_{\text{конт.упр.}})$ – формалізація структури взаємодії критичних процесів з нижнім рівнем АСУ ТП.

2.3.2 Модель технічного забезпечення

У попередньому розділі ми визначили типову структуру АСУ ТП та зазначили, що вона будується за ієрархічним принципом та поділяється на три рівні: нижній, середні та верхній.

На нижньому рівні використовуються датчики та виконувані механізми. В прикладі нашого об’єкту критичної інфраструктури, газовидобувного підприємства на цьому рівні знаходяться датчики температури, тиску, розходу тощо. На середньому рівні – контролери, які передають дані з датчиків на верхній рівень та керують виконуваними механізмами. На верхньому рівні розміщуються: централізоване дистанційне управління (зазвичай SCADA-системи), сервера введення/виведення, робочі місця диспетчерів та операторів підприємства, бази даних, програмне забезпечення для збору даних, візуалізації та моніторингу технологічного процесу. Технічне забезпечення включає засоби забезпечення, засоби зв’язку, відповідні канали зв’язку та інші елементи, представлені у схемі (рис. 2.9).

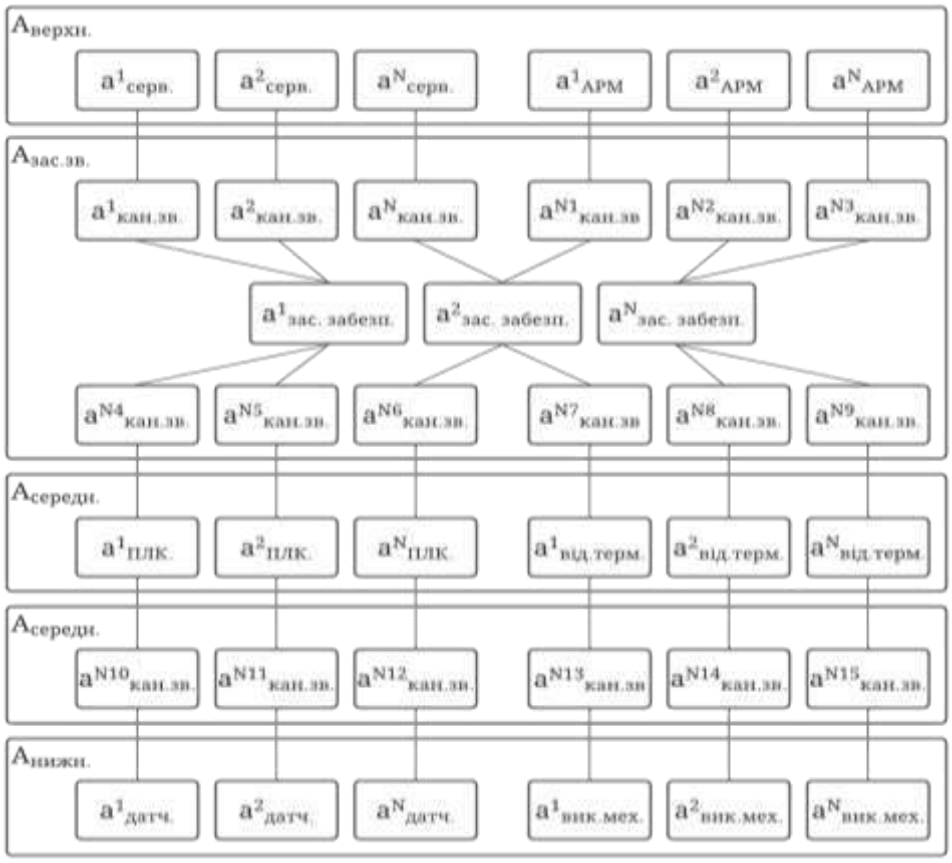


Рисунок 2.9 – Модель технічного забезпечення АСУ ТП

Модель технічного забезпечення АСУ ТП визначається сукупністю елементів:

$$M_{\text{тех.заб.}} = (A_{\text{тех.заб.}},\ G_{\text{фіз.струк.}}), \quad (2.2)$$

де $A_{\text{тех.заб.}} = A_{\text{нижн.}} \cup A_{\text{середн.}} \cup A_{\text{верхн.}} \cup A_{\text{зас.зв.}}$ – множина елементів технічного забезпечення АСУ ТП. $A_{\text{нижн.}} = A_{\text{датч.}} \cup A_{\text{вик.мех.}}$ – множина елементів нижнього рівня АСУ ТП; $A_{\text{датч.}}$ – множина датчиків; $A_{\text{вик.мех.}}$ – множина виконуваних механізмів; $A_{\text{середн.}} = A_{\text{ПЛК}} \cup A_{\text{від.терм.}}$- множина елементів середнього рівня, $A_{\text{ПЛК}}$ – множина програмованих логічних контролерів, $A_{\text{віддал.терм.}}$ – множина віддалених терміналів; $A_{\text{верхн.}} = A_{\text{серв.}} \cup A_{\text{АРМ}}$ – множина елементів верхнього рівня, $A_{\text{серв.}}$ – множина серверів, $A_{\text{АРМ}}$ - множина автоматизованих робочих місць; $A_{\text{зас.зв.}} = A_{\text{зас.забезп.}} \cup A_{\text{кан.зв.}}$ – множина елементів засобів зв'язку, $A_{\text{зас.забезп.}}$ – множина засобів забезпечення зв'язку, $A_{\text{кан.зв.}}$ – множина каналів зв'язку; $G_{\text{фіз.струк=}}(A_{\text{тех.заб.}},\ A_{\text{кан.зв.}})$ – формалізація фізичної структури АСУ ТП.

2.3.3 Модель програмного забезпечення

Для здійснення потрібних функцій елементів верхнього та середнього рівнів систем автоматичного керування технологічними процесами (АСУ ТП), систем управління та забезпечення необхідно виконувати логічні операції. За логічне виконання таких функцій відповідає встановлене заздалегідь програмне забезпечення. Схема взаємодії програмного забезпечення (рис. 2.10).

Модель програмного забезпечення АСУ ТП визначається сукупністю елементів:

$$M_{\text{прог.заб.}} = (A_{\text{прог.заб.}}, A_{\text{тех.зас}},\ K^{\text{тех.зас.}}_{\text{заг.прог.заб}}, G_{\text{лог.струк.}}), \quad (2.3)$$

де $A_{\text{прог.заб.}} = A_{\text{заг.прог.заб.}} \cup A_{\text{баз.прог.заб.}} \cup A_{\text{прик.прог.заб.}} \cup A_{\text{IT серв.}}$ – множина елементів програмного забезпечення АСУ ТП, $A_{\text{заг.прог.заб.}}$ – множина загального програмного забезпечення, $A_{\text{баз.прог.заб.}}$ – множина базового програмного забезпечення, $A_{\text{прик.прог.заб.}}$ – множина прикладного програмного забезпечення,

$A_{\text{IT}-\text{серв.}}$ – множина IT-сервісів; $A_{\text{тех.зас.}} \subseteq A_{\text{тех.заб.}}$ – підмножина технічних засобів з встановленим програмним забезпеченням; $K^{\text{тех.зас.}}_{\text{заг.прог.заб}}: A_{\text{тех.зас}} \times A_{\text{заг.прог.заб.}} \to \{0,1\}$ – співвідношення, що визначає встановлення загального програмного забезпечення на конкретний технічний засіб; $G_{\text{лог.струк.}} = (A_{\text{прог.заб.}}, A_{\text{інф.заб.}})$ – формалізація логічної структури АСУ ТП. $A_{\text{нижн.}} = A_{\text{датч.}} \cup A_{\text{вик.мех.}}$ – множина елементів нижнього рівня АСУ ТП; $A_{\text{датч.}}$ – множина датчиків; $A_{\text{вик.мех.}}$ – множина виконуваних механізмів; $A_{\text{середн.}} = A_{\text{ПЛК}} \cup A_{\text{від.терм.}}$- множина елементів середнього рівня, $A_{\text{ПЛК}}$ – множина програмованих логічних контролерів, $A_{\text{віддал.терм.}}$ – множина віддалених терміналів; $A_{\text{верхн.}} = A_{\text{серв.}} \cup A_{\text{АРМ}}$ – множина елементів верхнього рівня, $A_{\text{серв.}}$ – множина серверів, $A_{\text{АРМ}}$ - множина автоматизованих робочих місць; $A_{\text{зас.зв.}} = A_{\text{зас.забезп.}} \cup A_{\text{кан.зв.}}$ – множина елементів засобів зв'язку, $A_{\text{зас.забезп.}}$ – множина засобів забезпечення зв'язку, $A_{\text{кан.зв.}}$ – множина каналів зв'язку; $G_{\text{фіз.струк=}}(A_{\text{тех.заб.}}, A_{\text{кан.зв.}})$ – формалізація фізичної структури АСУ ТП.

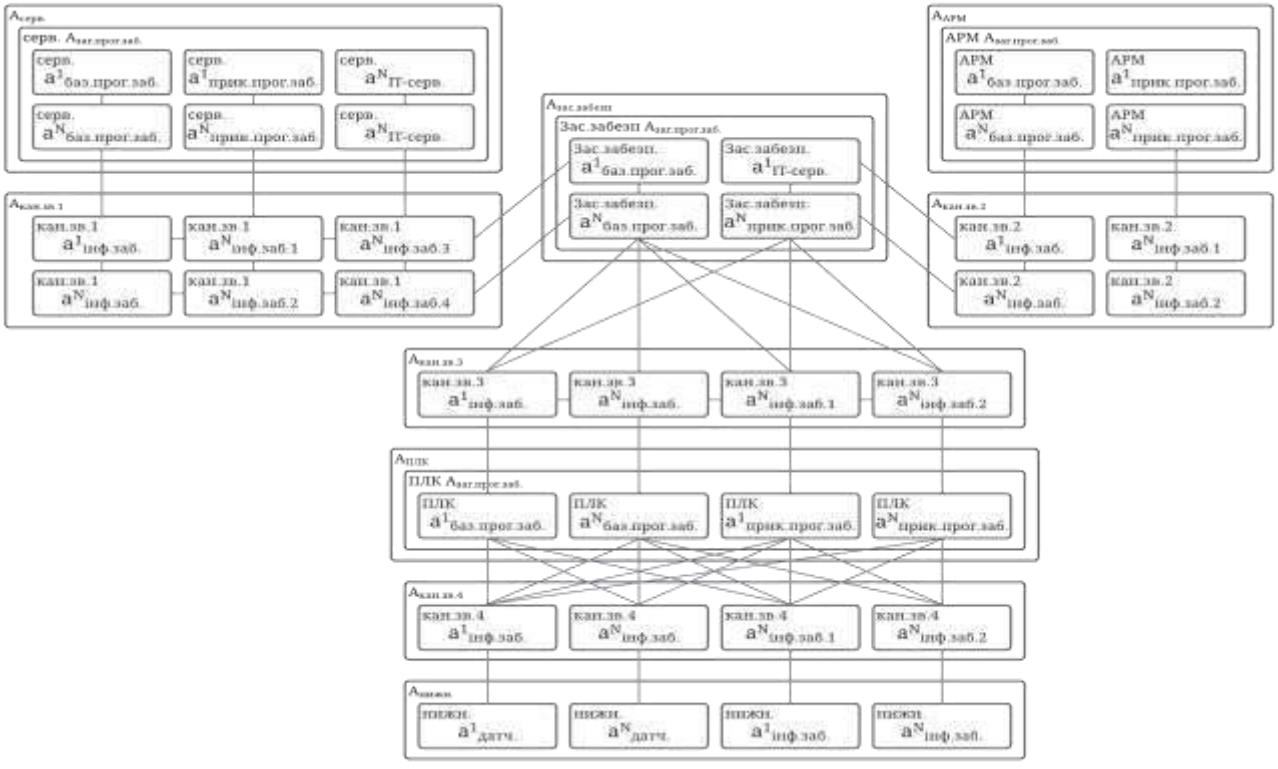


Рисунок 2.10 – Логічна структура взаємодії програмного забезпечення

2.4 Висновки

В цьому розділі було визначено поняття інформаційної безпеки та основні загрози автоматизованої системи управління технологічними процесами газовидобувної системи. Досліджено основні типи порушень управління безпекою, розглянути можливі сценарії кіберінцидентів.

Після обрання підходу до моделювання було побудовано математичну модель, яка дозволяє використати конкретну технологію моделювання захисту від кібервпливів автоматизованої системи управління технологічними процесами критичної інфраструктури газовидобувної компанії.

Таким чином, запропонована модель автоматизованої системи управління технологічними процесами містить наступні елементи:

$$M_{\text{авт.сис}} = (M_{\text{кр.пр.}}, M_{\text{тех.заб.}}, M_{\text{прог.заб.}}), \tag{2.4}$$

де $M_{\text{кр.пр.}}$ – модель критичних процесів, $M_{\text{тех.заб.}}$ – модель технічного забезпечення, $M_{\text{прог.заб.}}$ – модель програмного забезпечення.

Наукова новизна моделі автоматизованої системи управління технологічними процесами полягає в деталізації особливостей багаторівневої ієрархічної структури, вона відрізняється наявністю співвідношень між активами і критичними процесами, що відповідають за технологічний процес, що дозволяє на основі вищевказаної ієрархії активів визначати та оцінювати ризик від впливу потенційних загроз.

3 МЕТОДИ ОЦІНКИ РИЗИКІВ КІБЕРБЕЗПЕКИ В АВТОМАТИЗОВАНИХ СИСТЕМАХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

3.1 Методи оцінювання ризиків інформаційної безпеки

Як ми зазначали раніше, ризики, що виникають в контексті інформаційної безпеки на об'єктах критичної інфраструктури, можуть мати серйозні наслідки не лише для окремих компаній чи організацій, а й для цілого суспільства. Тому оцінка ризиків кібербезпеки в автоматизованих системах є надзвичайно важливим питанням, яке дозволяє ідентифікувати потенційні загрози, оцінити їх вплив та розробити ефективні стратегії реагування та запобігання виникненню таких ситуацій в подальшому.

В цьому розділі пропонується вирішення задачі розробки методу оцінки інформаційних ризиків автоматизованих систем управління технологічними процесами об'єктів критичної інфраструктури та розробка власного методу оцінки ризиків автоматизованої системи управління технологічними процесами, заснованого на оцінці вразливостей таких систем та потенційних збитків. Також буде проаналізовано існуючі методи для оцінки інформаційних ризиків та розглянуто актуальні джерела, які містять дані про вразливості.

Зазвичай для автоматизації технологічних процесів використовується автоматизована система управління технологічними процесами, побудована на базі програмованих логічних контролерів. Їхня коректна робота повинна забезпечувати правильність, якість та безпеку всього технологічного процесу. Також, як ми вже згадували раніше, ПЛК розміщуються на середньому рівні, на якому використовується закрите програмне забезпечення.

С. Ф. Гончар зауважує, що загальний пріоритет цілей інформаційної безпеки відрізняється від класичного. Безпека в цих системах, перш за все, стосується підтримки доступності компонентів усіх систем. Забезпечення цілісності для АСУ

ТП являється, як правило, другою по пріоритетності задачею. Забезпечення конфіденційності для АСУ ТП має найменше значення, оскільки та технологічна інформація, що циркулює в АСУ ТП не відноситься до інформації з обмеженим доступом [26].

В АСУ ТП в основному використовується пропрієтарне програмне забезпечення та закриті мережі, на перший погляд це ускладнює можливості зловмисника проникнути до системи, проте неодноразові випадки, пов’язані з зараженням АСУ ТП свідчать про зворотне. Відповідно, можна припустити, що вразливими до атак є системи всіх рівнів. Це заставляє розглянути інформаційну безпеку АСУ ТП об’єктів критичної інфраструктури під іншим кутом.

Наявність мережевого з’єднання між елементами АСУ ТП та поява віддалених інтерфейсів їх обслуговування створюють умови для виникнення потенційних вразливостей всієї системи. Враховуючи, що такі системи зазвичай використовуються на об’єктах критичної інфраструктури, до них відповідно, застосовуються підвищені вимоги забезпечення стабільності та надійності процесів виробництва. Такі вимоги потребують особливого та цілісного підходу до оцінки ризиків.

Проаналізувавши стан вищезазначеного питання в сучасному науковому середовищі, ми виділили що підходів та алгоритмів оцінки ризиків є безліч. Ми виділили найпоширеніші та взяли їх за основу нашого дослідження. Зокрема варто розглянути наступні методи: «SANS Institute», «CRAMM» та «OCTAVE».

Метод «Sans Institute» використовує якісне ранжування, яке засновано на використанні декількох якісних категорій вразливостей (наприклад, «низький», «середній» або «високий») [27]. Відповідно, таким чином здійснюється розподілення за рівнем критичності атаки. Критичність атаки визначається величиною ризику, який виникає внаслідок її реалізації (Severity). Величина ризику, в свою чергу визначається вірогідністю успішного виконання атаки та величиною можливих збитків. Величина можливих збитків визначається значимістю ресурсів на які направлена атака (Criticality). Вірогідність успішного виконання атаки (Lethality) визначається ефективністю методів та величини

вразливості системи захисту. Величина вразливості системи захисту визначається ефективністю контрзаходів системного (System Countermeasures) та мережевого рівнів (Network Countermeasures).

Формула для визначення серйозності загрози: Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures) [28]. Ця формула дозволяє визначати величину ризиків, які можуть бути виявлені з-за допомогою IDS (Intrusion Detection System) при аналізі результатів моніторингу мережевого трафіку.

Головним недоліком такого методу оцінювання ризиків інформаційної безпеки є прив'язка до завчасно визначеної шкали відповідності, що в разі нестандартного сценарію атаки може призвести до неточності її оцінки.

Метод CRAMM (методика аналізу та управління ризиками ССТА) - це широко визнана та всеосяжна методологія, що використовується для оцінки ризиків інформаційної безпеки в організаціях. Вона була розроблена британською урядовою організацією ССТА. CRAMM відома своїм систематичним підходом до ідентифікації, оцінки та управління ризиками для критичних активів інформаційних технологій [29, 30].

Методологія включає три основних етапи [31]:

– ідентифікація та оцінка активів – ідентифікуються та оцінюються активи, які потребують захисту;

– оцінка загроз та вразливостей – оцінюються потенційні загрози та вразливості, які можуть вплинути на визначені активи;

– вибір та рекомендація контрзаходів – на основі оцінки вибираються та рекомендуються відповідні контрзаходи для мінімізації виявлених ризиків. Ці етапи виконуються у двох фазах: фазі аналізу та фазі управління.

В методиці CRAMM в якості оцінки рівня загрози мається на увазі частота її виникнення, а під оцінкою рівня вразливості – вірогідність успіху під час реалізації загрози. Тому така оцінка не дозволяє точно класифікувати загрози за рівнем небезпеки, так як найбільш небезпечні та відповідно рідкісні загрози, будуть мати найменшу оцінку.

Метод OCTAVE Метод OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) - це підхід, який використовується для оцінки інформаційних ризиків та визначає стратегію оцінки й планування дій для забезпечення безпеки інформації на основі оцінки ризиків. Метод зосереджений на організаційних ризиках і розглядає стратегічні проблеми інформаційної безпеки, пов'язані з практичною діяльністю організації [32].

Цей метод складається з трьох фаз оцінки:

– розробка профілю загроз;
– ідентифікація вразливостей інфраструктури;
– розробка стратегії та плану безпеки.

Недолік такого методу в тому, що при оцінці ризику здійснюється оцінка лише очікуваних збитків, без оцінки вірогідності. Це означає, що малоймовірні ризики з високими збитками можуть бути більш пріоритетними, ніж більш ймовірні ризики.

Таким чином, проаналізувавши вищезазначені методи оцінювання ризиків інформаційної безпеки, ми вирішили розробити власний метод, при цьому врахувавши їхні переваги та недоліки.

3.2 Модель загроз автоматизованої системи управління технологічними процесами об’єкта критичної інфраструктури

Модель загроз АСУ ТП (рис. 3.1) об’єкта критичної інфраструктури визначається сукупністю елементів:

$$M_{\text{загр.}} = (M, B, E, K_{\text{загр.}}, L_{\text{пониж.}}, D_K^B, D_K^E), \tag{3.1}$$

де A – множина активів АСУ ТП; В – множина вразливостей; C – множина загроз; K - $A \times B \times E$ – формалізація моделі загроз; $L_{\text{пониж.}}$ – множина заходів обробки

ризиків пониженням; $D_K^B: L_{\text{пониж.}} \times B \rightarrow \{0,1\}$ - співвідношення для визначення впливу заходів обробки ризиків пониженням на вразливості; $D_K^E: L_{\text{пониж.}} \times E \rightarrow \{0,1\}$ – співвідношення для визначення впливу заходів обробки ризиків пониження ризиків на загрози.

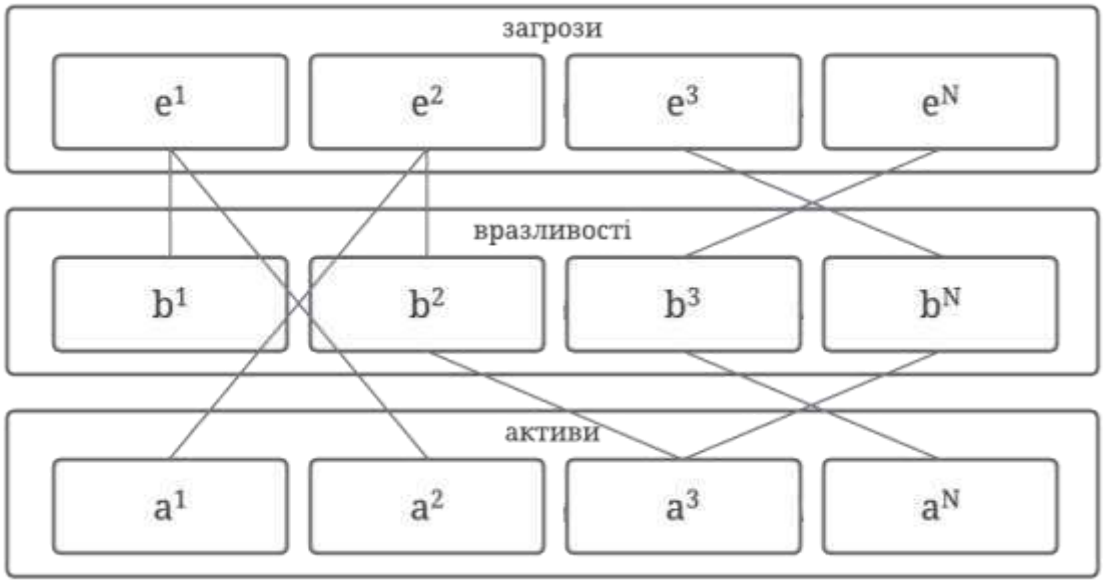


Рисунок 3.1 – Модель загроз АСУ ТП

У процесі управління ризиками кібербезпеки ключовим є призначення відповідальної особи або групи осіб для прийняття рішень. Ця роль може включати в себе визначення, аналіз, оцінку та адресацію загроз кібербезпеки організації. Управління ризиками кібербезпеки не є виключно завданням служби безпеки; кожен в організації має відігравати свою роль. Це включає в себе співробітників, керівників бізнес-підрозділів та інших осіб та експертних груп, кожна з яких має свої завдання та відповідальності в контексті управління ризиками [38].

Тому також під час управління ризиками на об’єкті критичної інфраструктури необхідно створити експертну групу, яка в межах нашого дослідження представлена у вигляді множини J та експерта в ній j^k.

3.3 Алгоритми оцінки критичних процесів, активів, розподілення заходів обробки ризиків, розрахунку збитків від реалізації загрози автоматизованої системи управління технологічними процесами об'єкта критичної інфраструктури

В першу чергу для розробки алгоритмів необхідно визначити допустимий рівень ризику для автоматизованої системи. Відповідно до стандарту NIST, допустимий ризик визначається як рівень залишкового ризику, який вважається прийнятним для певної IT-системи [39]. Це означає, що після впровадження всіх необхідних заходів безпеки, деякий рівень ризику все ще може існувати, але він визнається прийнятним з точки зору на потенційні втрати або перебої в роботі системи.

В контексті автоматизованих систем управління технологічними процесами, це означає, що організація повинна визначити свій «поріг терпимості» до ризику Це включає в себе аналіз потенційних загроз, вразливостей та можливих наслідків порушень безпеки. Важливо враховувати не тільки безпосередній вплив на IT-системи, але й загальний вплив на технологічні процеси. Визначення допустимого рівня ризику дозволяє організації приймати обгрунтовані рішення щодо інвестицій в заходи безпеки та менеджменту ризиків, виходячи з їхньої ефективності та вартості.

В межах нашого дослідження пропонуємо побудувати графік залежності між рівнями допустимих збитків, де R_{min} – незначні збитки, якими можна знехтувати, R_{max} – максимально допустимі збитки. Дана функція повинна будуватись на основі рішень експертів j^k експертної групи J.

Ідентифікація моделі здійснюється у вигляді:

$$O = f(\beta, I), \tag{3.2}$$

де O – оцінка вірогідності реалізації загрози; β – вектор коефіцієнтів функції; I – нормована оцінка збитків при реалізації загрози.

Ідентифікація повинна відбуватись послідовно, в два етапи. На першому необхідно здійснити структурну ідентифікацію, тобто визначити вид функції. На

другому – вирахувати коефіцієнти, за яких дані будуть найбільш наближені до експериментальних. Це можна досягти методом найменших квадратів:

$$\sum_{n=1}^{N_E}((f(\beta, i^n) - j_E^n)^2 \to min, \quad (3.3)$$

де n – номер загрози; N_E – кількість загроз; j_E^n – оцінка експерта j^k.

Після встановлення контексту для оцінки ризиків необхідно здійснити аналіз ризиків.

Раніше в роботі нам вдалось з'ясувати, що основне завдання будь-якої АСУ ТП – це забезпечення критичних процесів та дієздатності виробництва в цілому. Відповідно, для оцінки збитків, в першу чергу необхідно визначити економічні збитки, які можуть виникати у разі припинення чи порушення кожного критичного процесу. Для цього пропонуємо використати наступний алгоритм:

1. З-за допомогою графу $G_{\text{кр.пр.}}$ визначити множину критичних процесів $A_{\text{кр.пр.}}$ АСУ ТП.

2. Для кожного критичного процесу $a_{\text{кр.пр.}}^n \in A_{\text{кр.пр.}}$ визначити витрати, викликані припиненням або порушенням його роботи:

$$L_{\text{вит.}}^n = K_{\text{лік.}}^n + K_{\text{шкод.}}^n + K_{\text{лок.}}^n + K_{\text{тр.ос.}}^n + K_{\text{вир.}}^n + K_{\text{недост.}}^n + K_{\text{прац.}}^n \quad (3.2)$$

де, $K_{\text{лік.}}^n$- витрати на лікування постраждалих; $K_{\text{шкод.}}^n$ – витрати на відшкодування збитків постраждалим; $K_{\text{лок.}}^n$ – витрати, пов'язані з локалізацією та ліквідацією наслідків аварії; $K_{\text{тр.ос.}}^n$ – витрати на відшкодування збитків третім особам; $K_{\text{вир.}}^n$ – витрати на відновлення виробництва; $K_{\text{недост.}}^n$- витрати, пов'язані з компенсацією недостачі продукції; $K_{\text{прац.}}^n$- витрати на виплати працівникам, яких залучили для ліквідації наслідків.

3. Для кожного критичного процесу $a_{\text{кр.пр.}}^n \in A_{\text{кр.пр.}}$ визначити втрати, які виникли внаслідок припинення, чи порушення роботи:

$$L^n_{\text{втр.}} = Q^n_{\text{штр.}} + Q^n_{\text{репут.}} + Q^n_{\text{дог.}} + Q^n_{\text{контр.}} + Q^n_{\text{цін.}} + Q^n_{\text{викр.}} \quad (3.3)$$

де, $Q^n_{\text{штр.}}$ – втрати, викликані штрафами, неустойками тощо; $Q^n_{\text{репут.}}$ – репутаційні втрати (зниження потенційних контрактів); $Q^n_{\text{дог.}}$- втрати, пов'язані з втратою попередніх договорів та контрактів; $Q^n_{\text{контр.}}$- втрати внаслідок відмови контрагентів виконувати поточні договори; $Q^n_{\text{цін.}}$- втрати, викликані пошкодженням або знищенням виробничих матеріальних цінностей; $Q^n_{\text{викр.}}$- прямі фінансові втрати, викликані викраденням або іншою втратою.

4. Для кожного критичного процесу $a^n_{\text{кр.пр.}} \in A_{\text{кр.пр.}}$визначити втрати та витрати за час припинення або порушення цього процесу, за одну хвилину:

$$L^n_{\text{ч.}} = M^n_{\text{зрп.}} + M^n_{\text{обл.}} + M^n_{\text{приб.}} \quad (3.4)$$

де, $M^n_{\text{зрп.}}$ – витрати на заробітну платню працівникам за одну годину припинення або порушення роботи критичного процесу; $M^n_{\text{обл.}}$ – витрати на обладнання процесу, робота якого порушена; $M^n_{\text{приб.}}$ – втрати від недоотриманого прибутку за одну годину простою.

5. На основі показників (3.2), (3.3), (3.4) здійснюється оцінка важливості кожного елемента множини $a^n_{\text{кр.пр.}} \in A_{\text{кр.пр.}}$:

$$L^n_{\text{кр.пр.}} = (L^n_{\text{вит.}}, L^n_{\text{втр.}}, L^n_{\text{ч.}}) \quad (3.5)$$

6. Визначити сумарні збитки при припиненні роботи всіх критичних процесів об'єкту критичної інфраструктури I_Σ.

Для цього пропонуємо побудувати наступну блок-схему (рис. 3.2):

Рисунок 3.2 – Блок-схема виконання алгоритму оцінки важливості критичних процесів

Після проведення оцінки важливості критичних процесів АСУ ТП об’єкта критичної інфраструктури необхідно визначити важливість активів АСУ ТП, які забезпечують його життєздатність та процес роботи.

Наступний алгоритм буде виглядати таким чином:

1. Виконати алгоритм оцінки важливості критичних процесів АСУ ТП.

2. Використовуючи формалізації структур $G_{\text{кр.пр.}}$, $G_{\text{фіз.струк.}}$, $G_{\text{лог.струк.}}$ та $A_{\text{заг.прог.заб.}}$, $A_{\text{вик.мех.}}$ для всіх активів АСУ ТП скласти ієрархію між ними від рівня критичних процесів до рівня виконуваних механізмів (рис. 3.3).

3. Для побудови оцінки активів технічного забезпечення слід припустити, що витрати і втрати для кожного критичного процесу незалежні один від одного. При цьому використовуються максимальні значення часових затрат для кожного

елемента технічного забезпечення, пов’язаних критичних процесів. Таким чином, оцінка важливості активів АСУ ТП буде виглядати наступним чином (3.6):

$$L^n_{\text{тех.заб.}} = \left(\sum_{n=1}^{E^n_{\text{тех.заб.}}} L^n_{\text{вит.}},\ \sum_{n=1}^{E^n_{\text{тех.заб.}}} L^n_{\text{втр.}},\ n_{max}\ L^n_{\text{ч.}} \right) \quad (3.6)$$

4. Для раніше побудованої ієрархії (крок 2) розподілити кожний параметр між залежними елементами нижчого рівня.

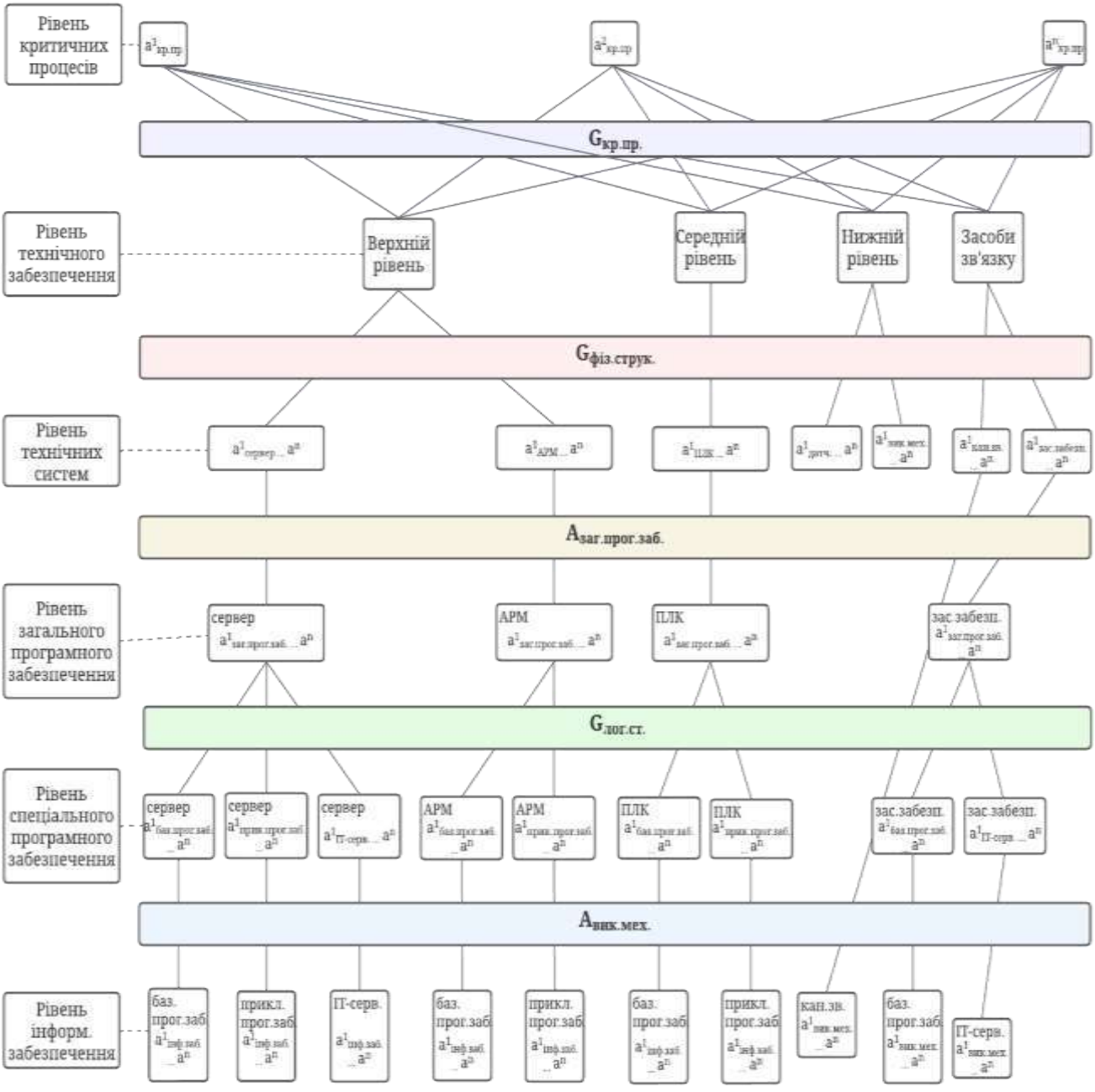


Рисунок 3.3 – Ієрархія активів АСУ ТП

З метою упорядкування виконання вищезгаданого алгоритму пропонуємо блок-схему (рис. 3.4).

Рисунок 3.4 – Порядок виконання алгоритму оцінки важливості активів АСУ ТП

Зазвичай в автоматизованих системах управління технологічними процесами використовуються заходи, які призначені для попередження та зниження можливих збитків або реалізацій загроз. Ми раніше згадували про них та позначали множиною $L_{\text{пониж.}}$, тобто використовується мінімізація та превенція можливих ризиків, в основному на основі концепції «захисту в глибину».

У контексті критичної інфраструктури, особливо для промислових систем управління, охоплює комплексну стратегію забезпечення безпеки, яка використовує багаторівневий підхід для захисту від різноманітних загроз, включно з хакерами та вандалами. Ця стратегія забезпечує фізичний доступ до інфраструктури, використовуючи систему контролю доступу в мережі (NAC) і традиційні заходи безпеки, а також реалізує політики та процедури, які включають навчання та програми підвищення обізнаності з питань кібербезпеки, оцінку ризиків та план безпеки. Філософія захисту в глубину також використовує IT-

технології для забезпечення розділення та сегментації мереж на VLAN, демілітаризовані зони, VPN, використовуючи міжмережеві екрани, комутатори та маршрутизатори [33].

Відповідно кожний захід забезпечення зниження ризиків можна віднести до окремого рівня захисту (рис. 3.5).

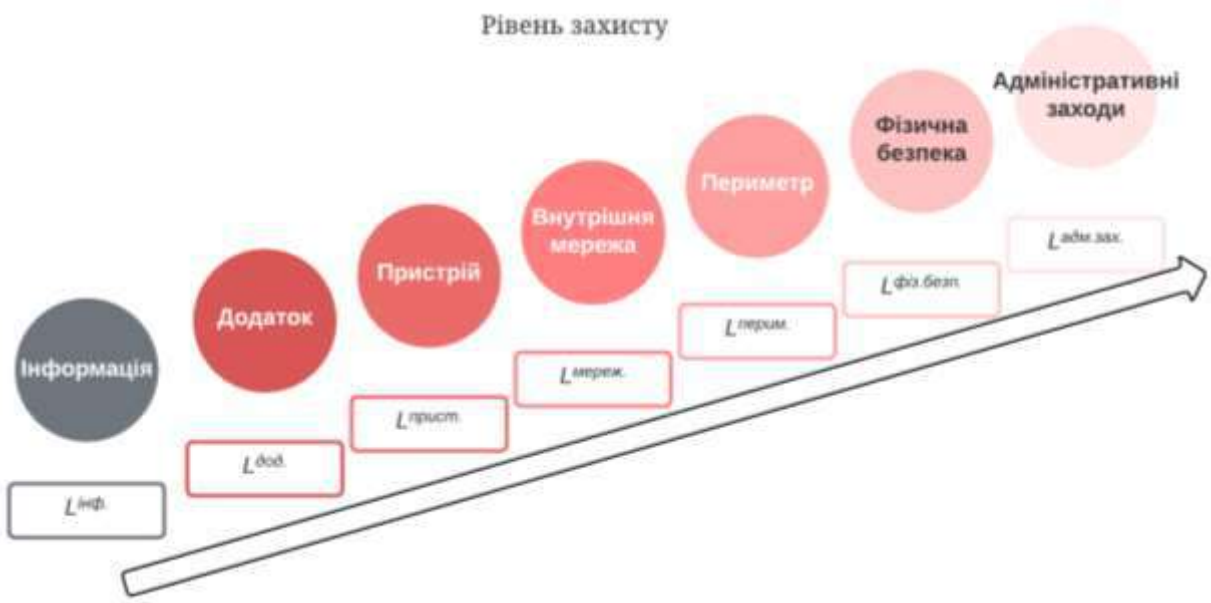


Рисунок 3.5. – Рівень захисту АСУ ТП «в глибину»

З метою використання вищезгаданого принципу захисту пропонуємо наступний алгоритм розподілу по рівням захисту для захисту від певної загрози e^u:

1. Використовуючи модель загроз $M_{\text{загр.}}$ визначити множину вразливостей $B^e \subseteq B$, які можуть експлуатуватись при реалізації загрози e^u.

2. Для загроз e^u та кожної вразливості $b^u \in B^u$ визначити множину заходів обробки ризиків пониженням $L^e_{\text{поніж.}} \subseteq L_{\text{поніж.}}$, для яких виконуються умови $D^B_K(b^u, l^o) = 1; D^E_K(e^u, l^o) = 1; l^o \in L^e_{\text{поніж.}}$.

3. Призначити відповідно до рівня захисту «в глибину» кожний елемент множини $l^o \in L^e_{\text{поніж.}}$ кожній можливій множині: $L^{\text{інф.}}, L^{\text{дод.}}, L^{\text{прист.}}, L^{\text{мереж.}}, L^{\text{перим.}} L^{\text{фіз.безп.}}, L^{\text{адм.зах.}}$.

Покрокове виконання цього алгоритму пропонуємо у наступній блок-схемі (рис. 3.6).

Рисунок 3.6. – Блок-схема алгоритму розподілу по рівням захисту

Важливим параметром оцінки ризиків є визначення збитків від потенційної реалізації загрози. Для цього пропонуємо алгоритм оцінки збитків при реалізації загрози e^u. З метою реалізації цього алгоритму слід використати метод Дельфі, основа якого полягає в оцінці ризиків вразливостей інформаційних систем шляхом систематичного збору інформації від експертів. Основні кроки включають формування групи експертів, які не спілкуються між собою безпосередньо, анонімне висловлення думок щодо проблеми, підготовку загального звіту з усіх пропозицій та повторне висловлення думок на основі цього звіту. Цей процес повторюється, поки не буде досягнуто консенсусу [34].

1. На формалізації загроз $K_{\text{загр.}}$ визначити множину потенційно вразливих активів A^u та загроза e^u.

2. З-за допомогою алгоритму розподілу по рівням захисту для захисту від певної загрози e^u, визначити множину $L^e_{\text{пониж.}}$.

3. З-за допомогою використання методу Дельфі визначити експертну групу, яка визначає показники впливу загрози e^u на множину активів A^u та відповідні витрати K_E^n та показники впливу загрози e^u на втрати множини активів A^u у вигляді Q_E^n, що вимірюються у відсотках. Також потрібно визначити час припинення або порушення роботи активів A^u під час впливу загрози e^u у вигляді $ч_E^n$, що вимірюється в хвилинах.

4. Збитки реалізації загрози e^u визначаються наступним значенням (3.7):

$$L_E^n = K_E^n \times \sum_{n=1}^{N_E^n} L_{\text{витр.}}^n + Q_E^n \times \sum_{n=1}^{N_E^n} L_{\text{втр.}}^n + ч_E^n \times \sum_{n=1}^{N_E^n} L_{\text{ч.}}^n \qquad (3.7)$$

5. Виконати нормалізацію збитків відносно сумарних збитків I_Σ, що визначались у попередніх алгоритмах: $i_E^n = \frac{L_E^n}{I_\Sigma}$.

Покрокове виконання цього алгоритму пропонуємо у блок-схемі (рис. 3.7).

Рисунок 3.7 – Блок-схема алгоритму оцінки збитків при реалізації загрози e^u

За основу наступного алгоритму, а саме оцінки збитків при експлуатації загрози e^u нами було використано стандарт CVSS. CVSS (Common Vulnerability Scoring System) є відкритим промисловим стандартом для оцінки серйозності вразливостей безпеки. Він генерує оцінку від 0 до 10 на основі серйозності вразливості, розраховану за допомогою трьох груп метрик: базових, тимчасових та навколишніх. Базові метрики виробляють оцінку від 0 до 10, яка потім може бути змінена за допомогою оцінки тимчасових та навколишніх метрик [35].

Кожна з цих груп включає в себе ряд окремих метрик, які визначають різні аспекти вразливості. Для кожної метрики встановлені відповідні літерні позначення для побудови вектора CVSS, значення яких представлені в таблицях 3.1, 3.2, 3.3.

Таблиця 3.1 – Базові метрики CVSS.

Базові Метрики (Base Metrics)			
Літера	Метрика	Опис	Параметри
AV	Attack Vector	Місце розташування атакувальника	Network (N), Adjacent (A), Local (L), Physical (P)
AC	Attack Complexity	Складність атаки	Low (L), High (H)
PR	Privileges Required	Вимоги до привілеїв для атаки	None (N), Low (L), High (H)
UI	User Interaction	Необхідність взаємодії з користувачем	None (N), Required (R)
S	Scope	Зміна області дії вразливості	Unchanged (U), Changed (C)
C	Confidentiality	Вплив на конфіденційність	None (N), Low (L), High (H)
I	Integrity	Вплив на цілісність	None (N), Low (L), High (H)
A	Availability	Вплив на доступність	None (N), Low (L), High (H)

Таблиця 3.2 – Тимчасові метрики CVSS

Тимчасові Метрики (Temporal Metrics)			
Літера	Метрика	Опис	Параметри
E	Exploit Code Maturity	Зрілість коду експлуатації	Not Defined (X), High (H), Functional (F), Proof-of-Concept (P), Unproven (U)
RL	Remediation Level	Рівень усунення вразливості	Not Defined (X), Unavailable (U), Workaround (W), Temporary Fix (T), Official Fix (O)
RC	Report Confidence	Впевненість у звіті	Not Defined (X), Confirmed (C), Reasonable (R), Unknown (U)

Таблиця 3.3 – Навколишні метрики CVSS

Навколишні Метрики (Environmental Metrics)			
Літера	Метрика	Опис	Параметри
1	2	3	4
CR	Confidentiality Requirement	Вимоги до конфіденційності	Not Defined (X), Low (L), Medium (M), High (H)
IR	Integrity Requirement	Вимоги до цілісності	Not Defined (X), Low (L), Medium (M), High (H)
AR	Availability Requirement	Вимоги до доступності	Not Defined (X), Low (L), Medium (M), High (H)
MAV	Modified Attack Vector	Модифіковане місце атаки	Not Defined (X), Network (N), Adjacent (A), Local (L), Physical (P)
MAC	Modified Attack Complexity	Модифікована складність атаки	Not Defined (X), Low (L), High (H)

Кінець таблиці 3.2

1	2	3	4
MPR	Modified Privileges Required	Модифіковані вимоги до привілеїв	Not Defined (X), None (N), Low (L), High (H)
MUI	Modified User Interaction	Модифікована необхідність взаємодії з користувачем	Not Defined (X), None (N), Required (R)
MS	Modified Scope	Модифікована область дії	Not Defined (X), Unchanged (U), Changed (C)
MC	Modified Confidentiality	Модифікований вплив на конфіденційність	Not Defined (X), None (N), Low (L), High (H)
MI	Modified Integrity	Модифікований вплив на цілісність	Not Defined (X), None (N), Low (L), High (H)
MA	Modified Availability	Модифікований вплив на доступність	Not Defined (X), None (N), Low (L), High (H)

Відповідно до цього стандарту, значення вектору вразливості b^u та його оцінка виглядатимуть наступним чином:

$$CVSS(b^u) = CVSS/AV{:}\ X/AC{:}\ X/PR{:}\ X/UI{:}\ X/S{:}\ X/C{:}\ X/I{:}\ X/A{:}\ X, \quad (3.8)$$

де, X – певне значення таблиць 3.1, 3.2, 3.3. $CVSS(b^u) \in \{0, \dots, 10\}$ – оцінка вразливості b^u.

Таким чином, у разі експлуатації вразливостей при реалізації загрози e^u пропонуємо наступний алгоритм, з використанням стандарту CVSS:

1. Використовуючи модель загроз $M_{\text{загр.}}$ визначити множину активів A^u, які можуть зазнати впливу реалізації загрози e^u.

2. З використанням алгоритму оцінки збитків при реалізації загрози e^u визначити множину $L^e_{\text{пониж.}}$, яка може вплинути на загрозу e^u.

3. Для загрози e^u з-за допомогою використання методу Дельфі визначити експертну групу, яка визначає показники впливу загрози e^u на множину активів A^u та відповідні витрати K^n_E та показники впливу загрози e^u на втрати множини активів A^u у вигляді Q^n_E, що вимірюються у відсотках. Також потрібно визначити час припинення або порушення роботи активів A^u під час впливу загрози e^u у вигляді ч^n_E, що вимірюється в хвилинах.

4. Для множини активів A^u на моделі загроз $M_{\text{загр.}}$ визначити множину вразливостей B^u, які можуть використовуватись під час реалізації загрози e^u.

5. Для кожної вразливості множини $b^u \in B^u$ з використанням стандарту CVSS визначаються відповідні метрики. Якщо в системі присутні декілька вразливостей в множині B^u вектор $CVSS^u$ отримує максимальні метрики з кожної вразливості та нормалізується (3.7).

6. Порівняти показники впливу на втрати, витрати та вектору $CVSS^u$ та вибрати максимальний показник. Відповідно $K^n_b = \max(K^n_e, CVSS^u)$ та $Q^u_b = \max(Q^n_e, CVSS^u)$.

7. Збитки при реалізації загрози e^u з використанням вразливості b^u визначаються наступним значенням:

$$L^n_B = K^n_B \times \sum_{n=1}^{N^n_E} L^n_{\text{витр.}} + Q^n_B \times \sum_{n=1}^{N^n_E} L^n_{\text{втр.}} + \text{ч}^n_E \times \sum_{n=1}^{N^n_E} L^n_{\text{ч.}} \qquad (3.12)$$

8. Нормалізувати оцінки збитків відносно сумарних збитків, що визначались у алгоритмі важливості елементів сумарних збитків: $i^n_E = \frac{L^n_B}{I_\Sigma}$.

Покрокове виконання цього алгоритму пропонуємо у наступній блок-схемі (рис. 3.8).

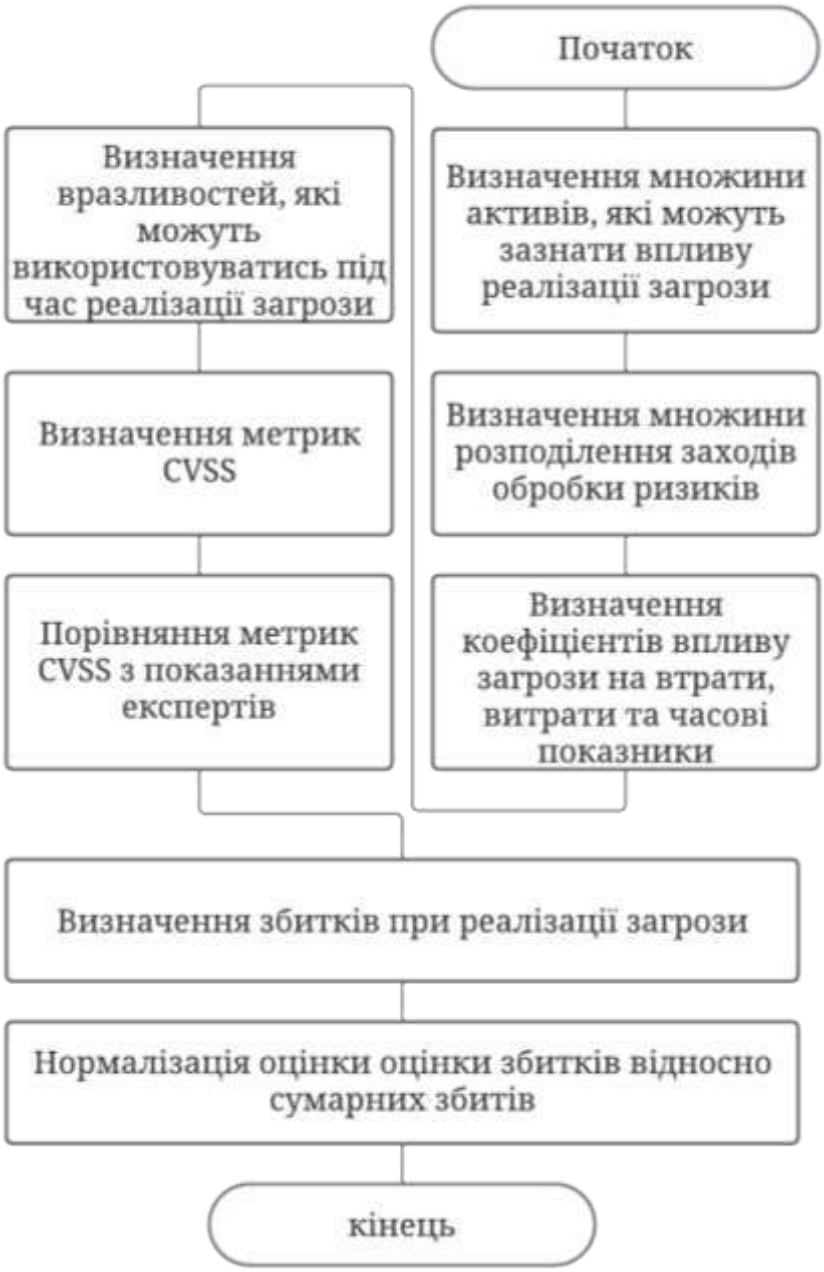


Рисунок 3.8 – Блок схема порядку виконання алгоритму оцінки збитків при експлуатації загрози.

Після того, як нами було розроблено алгоритми оцінки збитків при реалізації загрози e^u потрібно здійснити оцінку вірогідності реалізації цієї загрози. Для цього ми вирішили використати метод аналізу дерева подій Метод аналізу дерева подій (Event Tree Analysis, ETA) використовується для аналізу реалізації загроз в інформаційних системах і є потужним інструментом для визначення всіх наслідків системи, які можуть мати місце після певної ініціюючої події. Ця техніка може бути застосована до широкого спектру систем, включаючи об’єкти критичної

інфраструктури, в тому числі газовидобувні підприємства. Вона допомагає виявити потенційні проблеми на ранніх етапах проектування, що позитивно впливає на превентивному запобіганню наслідків виникнення певної події [37].

Таким чином було розроблено наступний алгоритм оцінки вірогідності реалізації загрози e^u:

1. За допомогою алгоритму розподілення заходів обробки ризиків визначити множину $L^e_{\text{пониж.}}$, що впливає на загрозу e^u та групувати її відповідно до рівнів захисту «в глибину».

2. Відповідно до рівнів захисту «в глибину» побудувати дерево подій (рис. 3.9).

3. За допомогою аналізу дерева подій виконати оцінку вірогідності нейтралізації загрози e^u на кожному рівні захисту:

$$j^n = (1 - j_1^n) \times (1 - j_2^n) \times (1 - j_3^n) \times (1 - j_4^n) \times \\ \times (1 - j_5^n) \times (1 - j_6^n) \times (1 - - j_7^n), \qquad (3.13)$$

де j_n^n – це оцінка експерта з експертної групи.

Оцінка експерта проводиться шляхом вербального обговорення, яке далі переводиться за допомогою шкали Харрінгтона у числове значення [47]

Порядок виконання алгоритму оцінки вірогідності реалізації загрози e^u запропоновано у відповідній блок-схемі (рис. 3.10)

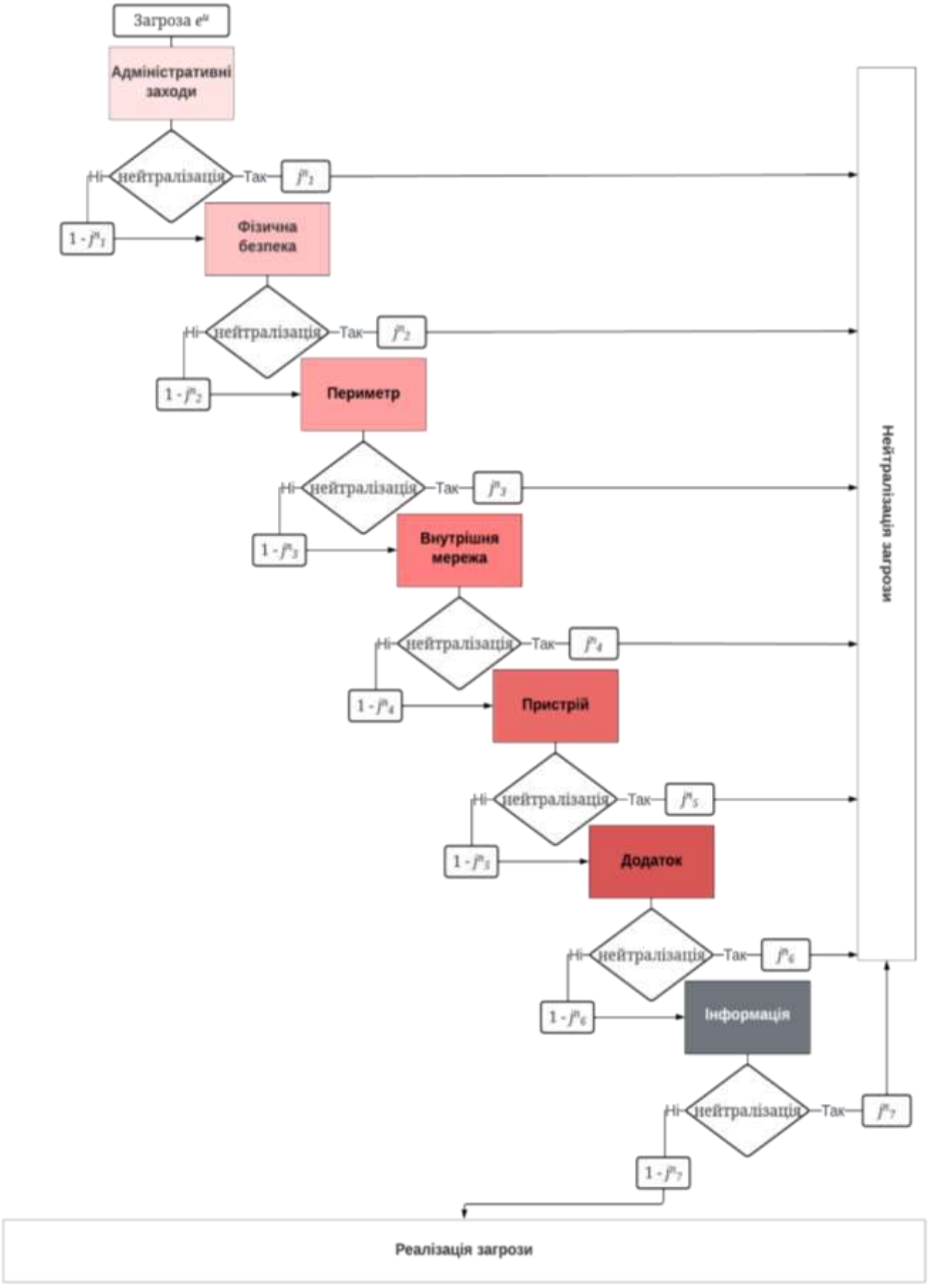


Рисунок 3.9 – Аналіз дерева подій

Рисунок 3.10 – Блок-схема виконання алгоритму оцінки вірогідності реалізації загрози

3.4 Висновки

В цьому розділі розроблені алгоритми, які дозволяють виконати оцінку ризиків інформаційної безпеки автоматизованої системи управління технологічними процесами газовидобувної компанії.

Наукова новизна запропонованого методу та алгоритмів полягає в наступному:

– обчислюється оцінка важливості критичних процесів, в тому числі продукції за певну одиницю часу та в подальшому виконується розподіл збитків по всій ієрархічній структурі автоматизованої системи управління технологічними процесами, що відрізняються урахуванням експлуатації вразливостей системи, що дозволяє врахувати важливість кожного активу в системі.

– кожний актив групується по рівню та оцінці можливості нейтралізації загрози відповідно до принципу захисту «в глубину», поєднуючи це з деревом подій, що дозволяє ефективно використовувати засоби нейтралізації та знижувати можливість реалізації загроз.

– поєднується теоретико-множинна модель автоматизованої системи управління технологічними процесами, алгоритми для оцінки збитків та можливості реалізації загрози, що дозволяє виконати послідовну та рівномірну оцінку ризиків та визначити які з них є недопустимими.

4 РОЗРОБКА ТА ПРАКТИЧНЕ ЗАСТОСУВАННЯ МЕТОДУ ОЦІНКИ РИЗИКІВ КІБЕРБЕЗПЕКИ В АВТОМАТИЗОВАНИХ СИСТЕМАХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

4.1 Формування моделі загальної характеристики підприємства

Для практичного застосування методу забезпечення кібербезпеки автоматизованих систем критичної інфраструктури газовидобувної компанії на основі оцінки ризиків необхідно в першу чергу виразити всі її складові у формі таблиць, де вказати перелік компонентів та їхнє місце у відповідній моделі.

Для наглядної демонстрації розробленого методу пропонуємо умовно розподілити процес видобування природнього газу на технологічні процеси (табл. 4.1).

Таблиця 4.1 – Технологічні процеси видобування природнього газу

№	Опис технологічного процесу	$A_{\text{кр.пр.}}$
1	Видобування природного газу з свердловини	$a^1_{\text{кр.пр.}}$
2	Пониження тиску газу	$a^2_{\text{кр.пр.}}$
3	Транспортування газу до цеху початкової обробки	$a^3_{\text{кр.пр.}}$
4	Видалення кислотних газів	$a^4_{\text{кр.пр.}}$
5	Транспортування газу до цеху очищення та охолодження	$a^5_{\text{кр.пр.}}$
6	Охолодження газу, видалення водяної пари	$a^6_{\text{кр.пр.}}$
7	Транспортування рідини до резервуарів	$a^7_{\text{кр.пр.}}$
8	Відділення рідких вуглеводнів шляхом очищення	$a^8_{\text{кр.пр.}}$
9	Транспортування газу до цеху осушування	$a^9_{\text{кр.пр.}}$
10	Осушування газу	$a^{10}_{\text{кр.пр.}}$
11	Відділення домішок	$a^{11}_{\text{кр.пр.}}$
12	Транспортування газу до газотранспортної системи	$a^{12}_{\text{кр.пр.}}$

Відповідно кожен технологічний процес відбувається на певному рівні ієрархії АСУ ТП та взаємодіє з технічним забезпеченням нижнього рівня, такими як датчики контролю певних технологічних процесів, а механізми виконання в свою чергу, здійснюють безпосереднє керування (табл. 4.2).

Таблиця 4.2 – Взаємодія критичних процесів та технічного забезпечення

№	Взаємодія критичних процесів та технічного забезпечення	$A_{\text{кр.пр.}}$	$A_{\text{датч.}}$
1	Датчики температури, тиску	$a^1_{\text{кр.пр.}}$	$a^1_{\text{датч.}}, a^2_{\text{датч.}}$
2	Датчики температури, тиску	$a^2_{\text{кр.пр.}}$	$a^3_{\text{датч.}} \dots a^5_{\text{датч.}}$
3	Датчики температури, тиску, об’єму	$a^3_{\text{кр.пр.}}$	$a^6_{\text{датч.}} \dots a^8_{\text{датч.}}$
4	Датчики температури, тиску	$a^4_{\text{кр.пр.}}$	$a^9_{\text{датч.}} \dots a^{11}_{\text{датч.}}$
5	Датчики температури, тиску, об’єму	$a^5_{\text{кр.пр.}}$	$a^{12}_{\text{датч.}} \dots a^{15}_{\text{датч.}}$
6	Датчики температури, тиску	$a^6_{\text{кр.пр.}}$	$a^{16}_{\text{датч.}}, a^{17}_{\text{датч.}}$
7	Датчики температури, тиску	$a^7_{\text{кр.пр.}}$	$a^{18}_{\text{датч.}} \dots a^{21}_{\text{датч.}}$
8	Датчики температури, тиску	$a^8_{\text{кр.пр.}}$	$a^{22}_{\text{датч.}} \dots a^{24}_{\text{датч.}}$
9	Датчики температури, тиску	$a^9_{\text{кр.пр.}}$	$a^{25}_{\text{датч.}}, a^{26}_{\text{датч.}}$
10	Датчики температури, тиску	$a^{10}_{\text{кр.пр.}}$	$a^{27}_{\text{датч.}} \dots a^{30}_{\text{датч.}}$
11	Датчики температури, тиску	$a^{11}_{\text{кр.пр.}}$	$a^{31}_{\text{датч.}} \dots a^{33}_{\text{датч.}}$
12	Датчики температури, тиску, виміру розходу	$a^{12}_{\text{кр.пр.}}$	$a^{34}_{\text{датч.}} \dots a^{39}_{\text{датч.}}$

Також необхідно представити управління критичними процесами та механізмами виконання (табл. 4.3).

Далі визначаємо технічне забезпечення та базове програмне забезпечення на відповідному обладнанні (табл. 4.4).

Таблиця 4.3 – Управління критичними процесами та механізмами виконання

№	$A_{\text{кр.пр.}}$	$A_{\text{вик.мех.}}$
1	$a^{1}_{\text{кр.пр.}}$	$a^{1}_{\text{вик.мех.}},\ldots a^{5}_{\text{датч.}}$
2	$a^{2}_{\text{кр.пр.}}$	$a^{6}_{\text{вик.мех.}},\ldots a^{9}_{\text{датч.}}$
3	$a^{3}_{\text{кр.пр.}}$	$a^{10}_{\text{датч.}} \ldots a^{15}_{\text{датч.}}$
4	$a^{4}_{\text{кр.пр.}}$	$a^{16}_{\text{датч.}} \ldots a^{19}_{\text{датч.}}$
5	$a^{5}_{\text{кр.пр.}}$	$a^{20}_{\text{датч.}} \ldots a^{25}_{\text{датч.}}$
6	$a^{6}_{\text{кр.пр.}}$	$a^{26}_{\text{датч.}}, a^{27}_{\text{датч.}}$
7	$a^{7}_{\text{кр.пр.}}$	$a^{28}_{\text{датч.}} \ldots a^{34}_{\text{датч.}}$
8	$a^{8}_{\text{кр.пр.}}$	$a^{35}_{\text{датч.}} \ldots a^{41}_{\text{датч.}}$
9	$a^{9}_{\text{кр.пр.}}$	$a^{42}_{\text{датч.}}, a^{48}_{\text{датч.}}$
10	$a^{10}_{\text{кр.пр.}}$	$a^{49}_{\text{датч.}} \ldots a^{57}_{\text{датч.}}$
11	$a^{11}_{\text{кр.пр.}}$	$a^{58}_{\text{датч.}} \ldots a^{60}_{\text{датч.}}$
12	$a^{12}_{\text{кр.пр.}}$	$a^{61}_{\text{датч.}} \ldots a^{64}_{\text{датч.}}$

Таблиця 4.4 – Технологічне забезпечення та загальне програмне забезпечення

$A_{\text{тех.заб.}}$	Опис технічного забезпечення	$A_{\text{заг.прог.заб.}}$
$a^{1}_{\text{ПЛК}}$, … $a^{12}_{\text{ПЛК}}$	Програмовані логічні контролери для збору інформації з датчиків та управління механізмами виконання	$a^{\text{ПЛК1}}_{\text{заг.прог.заб.}}$, … $a^{\text{ПЛК12}}_{\text{заг.прог.заб.}}$
$a^{1}_{\text{зас.забезп.}}$, … $a^{12}_{\text{зас.забезп.}}$	Включають мережеві екрани, комутатори, точки доступу тощо.	$a^{\text{зас.забезп.1}}_{\text{заг.прог.забезп.}}$, … $a^{\text{зас.забезп.12}}_{\text{заг.прог.забезп.}}$
$a^{1}_{\text{серв.}}$, … $a^{5}_{\text{серв.}}$	Сервери, які відповідають за роботу ПЛК, збирання та передачу даних.	$a^{\text{серв.1}}_{\text{заг.прог.забезп.}}$, … $a^{\text{серв.5}}_{\text{заг.прог.забезп.}}$
$a^{1}_{\text{АРМ}}$, … $a^{5}_{\text{АРМ}}$	Автоматизовані робочі місця, які включають інженерні та операторські станції.	$a^{\text{АРМ1}}_{\text{заг.прог.забезп.}}$, … $a^{\text{АРМ5}}_{\text{заг.прог.забезп.}}$

Відповідно датчики та механізми виконання отримують та передають сигнали програмованих логічних контролерів на середньому рівні автоматизованої системи управління технологічними процесами тому необхідно визначити порядок взаємодії підключення множини ПЛК $A_{\text{ПЛК}}$ з елементами множини нижнього рівня $A_{\text{нижн.}}$ у вигляді таблиці (табл. 4.5), де $A_{\text{кан.зв.}}$ – канал зв'язку між ними.

Таблиця 4.5 – Фізичний зв'язок програмованих логічних контролерів та елементів нижнього рівня

$\text{A}_{\text{ПЛК}}$	$\text{A}_{\text{кан.зв.}}$	$A_{\text{датч.}}$	$A_{\text{вик.мех.}}$	$A_{\text{кр.пр.}}$
$a^{1}_{\text{ПЛК}}$	$a^{1}_{\text{кан.зв}}, \dots a^{5}_{\text{кан.зв.}}$	$a^{1}_{\text{датч.}},\dots a^{5}_{\text{датч.}}$	$a^{1}_{\text{вик.мех.}},\dots a^{5}_{\text{вик.ме}}$	$a^{1}_{\text{кр.пр.}}$
$a^{2}_{\text{ПЛК}}$	$a^{6}_{\text{кан.зв}}, \dots a^{8}_{\text{кан.зв.}}$	$a^{6}_{\text{датч.}},\dots a^{9}_{\text{датч.}}$	$a^{6}_{\text{вик.мех.}},\dots a^{9}_{\text{вик.ме}}$	$a^{2}_{\text{кр.пр.}}$
$a^{3}_{\text{ПЛК}}$	$a^{9}_{\text{кан.зв}}, \dots a^{12}_{\text{кан.зв.}}$	$a^{10}_{\text{датч.}} \dots a^{15}_{\text{датч.}}$	$a^{10}_{\text{вик.мех.}} \dots a^{15}_{\text{вик.м}}$	$a^{3}_{\text{кр.пр.}}$
$a^{4}_{\text{ПЛК}}$	$a^{13}_{\text{кан.зв}}, \dots a^{20}_{\text{кан.зв.}}$	$a^{16}_{\text{датч.}} \dots a^{19}_{\text{датч.}}$	$a^{16}_{\text{вик.мех.}} \dots a^{19}_{\text{вик.м}}$	$a^{4}_{\text{кр.пр.}}$
$a^{5}_{\text{ПЛК}}$	$a^{21}_{\text{кан.зв}}, \dots a^{25}_{\text{кан.зв.}}$	$a^{20}_{\text{датч.}} \dots a^{25}_{\text{датч.}}$	$a^{20}_{\text{вик.мех.}} \dots a^{25}_{\text{вик.м}}$	$a^{5}_{\text{кр.пр.}}$
$a^{6}_{\text{ПЛК}}$	$a^{26}_{\text{кан.зв}}, \dots a^{33}_{\text{кан.зв.}}$	$a^{26}_{\text{датч.}}, a^{27}_{\text{датч.}}$	$a^{26}_{\text{вик.мех.}}, a^{27}_{\text{вик.мех}}$	$a^{6}_{\text{кр.пр.}}$
$a^{7}_{\text{ПЛК}}$	$a^{34}_{\text{кан.зв}}, \dots a^{37}_{\text{кан.зв.}}$	$a^{28}_{\text{датч.}} \dots a^{34}_{\text{датч.}}$	$a^{28}_{\text{вик.мех.}} \dots a^{34}_{\text{вик.м}}$	$a^{7}_{\text{кр.пр.}}$
$a^{8}_{\text{ПЛК}}$	$a^{38}_{\text{кан.зв}}, \dots a^{40}_{\text{кан.зв.}}$	$a^{35}_{\text{датч.}} \dots a^{41}_{\text{датч.}}$	$a^{35}_{\text{вик.мех.}} \dots a^{41}_{\text{вик.м}}$	$a^{8}_{\text{кр.пр.}}$
$a^{9}_{\text{ПЛК}}$	$a^{41}_{\text{кан.зв}}, \dots a^{45}_{\text{кан.зв.}}$	$a^{42}_{\text{датч.}}, a^{48}_{\text{датч.}}$	$a^{42}_{\text{вик.мех.}}, a^{48}_{\text{вик.мех}}$	$a^{9}_{\text{кр.пр.}}$
$a^{10}_{\text{ПЛК}}$	$a^{46}_{\text{кан.зв}}, \dots a^{50}_{\text{кан.зв.}}$	$a^{49}_{\text{датч.}} \dots a^{57}_{\text{датч.}}$	$a^{49}_{\text{вик.мех.}} \dots a^{57}_{\text{вик.м}}$	$a^{10}_{\text{кр.пр.}}$
$a^{11}_{\text{ПЛК}}$	$a^{51}_{\text{кан.зв}}, \dots a^{55}_{\text{кан.зв.}}$	$a^{58}_{\text{датч.}} \dots a^{60}_{\text{датч.}}$	$a^{58}_{\text{вик.мех.}} \dots a^{60}_{\text{вик.м}}$	$a^{11}_{\text{кр.пр.}}$
$a^{12}_{\text{ПЛК}}$	$a^{56}_{\text{кан.зв}}, \dots a^{60}_{\text{кан.зв.}}$	$a^{61}_{\text{датч.}} \dots a^{64}_{\text{датч.}}$	$a^{61}_{\text{вик.мех.}} \dots a^{64}_{\text{вик.м}}$	$a^{12}_{\text{кр.пр.}}$

Також варто визначити зв'язок між технічним забезпеченням та засобами забезпечення, де $\text{A}_{\text{кан.зв.}}$ – канал зв'язку між ними (табл. 4.6).

Таблиця 4.6 – Взаємозв’язок між технічним забезпеченням та засобами зв’язку

$A_{\text{тех.заб.}}$	$A_{\text{кан.зв.}}$	$A_{\text{зас.забезп.}}$
$a^{1}_{\text{ПЛК}}, \dots a^{12}_{\text{ПЛК}}$	$a^{61}_{\text{кан.зв.}}, \dots a^{81}_{\text{кан.зв.}},$	$a^{1}_{\text{зас.забезп.}}, \dots a^{12}_{\text{зас.забезп.}}$
$a^{1}_{\text{серв.}}, \dots a^{5}_{\text{серв.}}$	$a^{82}_{\text{кан.зв.}}, \dots a^{91}_{\text{кан.зв.}}$	$a^{5}_{\text{зас.забезп.}}, a^{6}_{\text{зас.забезп.}}$
$a^{1}_{\text{АРМ}}, \dots a^{5}_{\text{АРМ}}$	$a^{92}_{\text{кан.зв.}}, \dots a^{98}_{\text{кан.зв.}}$	$a^{7}_{\text{зас.забезп.}}, a^{8}_{\text{зас.забезп.}}$

Відповідно до попередніх розділів, ми дослідили, що на деякому устаткуванні разом із загальним програмним забезпеченням встановлюється спеціальне програмне забезпечення (табл. 4.7).

Таблиця 4.7 – Список встановленого спеціального програмного забезпечення

$A_{\text{спец.прог.заб.}}$	$A_{\text{заг.прог.заб.}}$	Опис програмного забезпечення
1	2	3
$a^{1}_{\text{баз.прог.заб.}}, \dots a^{10}_{\text{баз.прог.заб.}}$	$a^{\text{серв.1}}_{\text{заг.прог.забезп.}}, \dots a^{\text{серв.5}}_{\text{заг.прог.забезп.}}$ $a^{\text{АРМ1}}_{\text{заг.прог.забезп.}}, \dots a^{\text{АРМ5}}_{\text{заг.прог.забезп.}}$	Включає драйвери пристроїв та додатки керування
$a^{11}_{\text{баз.прог.заб.}}, \dots a^{16}_{\text{баз.прог.заб.}}$	$a^{\text{серв.1}}_{\text{заг.прог.забезп.}}, \dots a^{\text{серв.5}}_{\text{заг.прог.забезп.}}$	Програми для керування мережею та системою
$a^{17}_{\text{баз.прог.заб.}}, \dots a^{18}_{\text{баз.прог.заб.}}$	$a^{\text{серв.3}}_{\text{заг.прог.забезп.}}, \dots a^{\text{серв.4}}_{\text{заг.прог.забезп.}}$	Програми збору подій та інформації про стан системи
$a^{19}_{\text{баз.прог.заб.}}$	$a^{\text{серв.1}}_{\text{заг.прог.забезп.}}$	Центр управління мережею
$a^{20}_{\text{баз.прог.заб.}}, \dots a^{23}_{\text{баз.прог.заб.}}$	$a^{\text{АРМ2}}_{\text{заг.прог.забезп.}}, \dots a^{\text{АРМ5}}_{\text{заг.прог.забезп.}}$	Програми для управління процесами виробництва
$a^{24}_{\text{баз.прог.заб.}}, \dots a^{34}_{\text{баз.прог.заб.}}$	$a^{\text{серв.1}}_{\text{заг.прог.забезп.}}, \dots a^{\text{серв.5}}_{\text{заг.прог.забезп.}}$ $a^{\text{АРМ1}}_{\text{заг.прог.забезп.}}, \dots a^{\text{АРМ5}}_{\text{заг.прог.забезп.}}$	Microsoft .NET Framework
$a^{35}_{\text{баз.прог.заб.}}, \dots a^{45}_{\text{баз.прог.заб.}}$	$a^{\text{серв.1}}_{\text{заг.прог.забезп.}}, \dots a^{\text{серв.5}}_{\text{заг.прог.забезп.}}$ $a^{\text{АРМ1}}_{\text{заг.прог.забезп.}}, \dots a^{\text{АРМ5}}_{\text{заг.прог.забезп.}}$	Microsoft .NET Client Profile

Продовження таблиці 4.7

1	2	3
$a^{46}_{\text{баз.прог.заб.}}$, … $a^{51}_{\text{баз.прог.заб.}}$	$a^{\text{серв.1}}_{\text{заг.прог.забезп.}}$,… $a^{\text{серв.5}}_{\text{заг.прог.забезп.}}$	Microsoft SQL Server
$a^{52}_{\text{баз.прог.заб.}}$, … $a^{57}_{\text{баз.прог.заб.}}$	$a^{\text{АРМ1}}_{\text{заг.прог.забезп.}}$,… $a^{\text{АРМ5}}_{\text{заг.прог.забезп.}}$	Microsoft Office
$a^{58}_{\text{баз.прог.заб.}}$, … $a^{63}_{\text{баз.прог.заб.}}$	$a^{\text{АРМ1}}_{\text{заг.прог.забезп.}}$,… $a^{\text{АРМ5}}_{\text{заг.прог.забезп.}}$	Microsoft Report Viewer
$a^{64}_{\text{баз.прог.заб.}}$, … $a^{69}_{\text{баз.прог.заб.}}$	$a^{\text{АРМ1}}_{\text{заг.прог.забезп.}}$,… $a^{\text{АРМ5}}_{\text{заг.прог.забезп.}}$	Microsoft XML Parser
$a^{70}_{\text{баз.прог.заб.}}$, … $a^{75}_{\text{баз.прог.заб.}}$	$a^{\text{АРМ1}}_{\text{заг.прог.забезп.}}$,… $a^{\text{АРМ5}}_{\text{заг.прог.забезп.}}$	Програмний засіб для створення звітів
$a^{76}_{\text{баз.прог.заб.}}$, … $a^{88}_{\text{баз.прог.заб.}}$	$a^{\text{ПЛК1}}_{\text{заг.прог.забезп.}}$, … $a^{\text{ПЛК12}}_{\text{заг.прог.забезп.}}$	Програмне забезпечення для відправки даних на сервер
$a^{1}_{\text{прикл.прог.заб.}}$, … $a^{12}_{\text{прикл.прог.заб.}}$	$a^{\text{ПЛК1}}_{\text{заг.прог.забезп.}}$, … $a^{\text{ПЛК12}}_{\text{заг.прог.забезп.}}$	Програмне забезпечення для збору інформації з датчиків
$a^{13}_{\text{прикл.прог.заб.}}$, … $a^{25}_{\text{прикл.прог.заб.}}$	$a^{1}_{\text{ПЛК}}$, … $a^{12}_{\text{ПЛК}}$	Програми керування механізмами виконання
$a^{24}_{\text{баз.прог.заб.}}$, … $a^{25}_{\text{баз.прог.заб.}}$	$a^{\text{серв.1}}_{\text{заг.прог.забезп.}}$, $a^{\text{АРМ1}}_{\text{заг.прог.забезп.}}$	Програмний засіб для керування механізмами виконання з АРМ
$a^{26}_{\text{баз.прог.заб.}}$	$a^{\text{серв.3}}_{\text{заг.прог.забезп.}}$	Програмне рішення для керування SCADA системами
$a^{1}_{\text{ІТ}-\text{серв.}}$	$a^{\text{серв.1}}_{\text{заг.прог.забезп.}}$	Microsoft Active Directory для керування сервером
$a^{2}_{\text{ІТ}-\text{серв.}}$, … $a^{3}_{\text{ІТ}-\text{серв.}}$	$a^{\text{зас.забезп.1}}_{\text{заг.прог.забезп.}}$, $a^{\text{зас.забезп.2}}_{\text{заг.прог.забезп.}}$	Правила доступу до системи

Кінець таблиці 4.7

1	2	3
$a^{4}_{\text{IT}-\text{серв.}}$, … $a^{5}_{\text{IT}-\text{серв.}}$	$a^{\text{зас.забезп.1}}_{\text{заг.прог.забезп.}}$, $a^{\text{зас.забезп.2}}_{\text{заг.прог.забезп.}}$	DHCP – сервер для мережевого обладнання
$a^{6}_{\text{IT}-\text{серв.}}$	$a^{\text{серв.1}}_{\text{заг.прог.забезп.}}$	DNS-сервер
$a^{7}_{\text{IT}-\text{серв.}}$	$a^{\text{серв.3}}_{\text{заг.прог.забезп.}}$	NTP-сервер
$a^{8}_{\text{IT}-\text{серв.}}$, … $a^{15}_{\text{IT}-\text{серв.}}$	$a^{\text{зас.забезп.3}}_{\text{заг.прог.забезп.}}$,… $a^{\text{зас.забезп.8}}_{\text{заг.прог.забезп.}}$	Пересилання трафіку

Для передачі інформації всередині системи та пристроїв використовується логічна взаємодія. Потрібно виразити $G_{\text{фіз.струк.}}$ у вигляді таблиці (табл. 4.8).

Таблиця 4.8 – Логічний зв’язок програмного забезпечення

$A_{\text{спец.прог.заб.}}$	$A_{\text{інф.заб.}}$	$A_{\text{прог.заб.}}$	Опис
1	2	3	4
$a^{17}_{\text{баз.прог.заб.}}$	$a^{1}_{\text{інф.заб.}}$, … $a^{12}_{\text{інф.заб.}}$	$a^{1}_{\text{ПЛК}}$, … $a^{12}_{\text{ПЛК}}$	Логування подій програмованих логічних контролерів
$a^{17}_{\text{баз.прог.заб.}}$	$a^{13}_{\text{інф.заб.}}$, $a^{14}_{\text{інф.заб.}}$	$a^{\text{зас.забезп.1}}_{\text{заг.прог.забезп.}}$, $a^{\text{зас.забезп.2}}_{\text{заг.прог.забезп.}}$	Логування подій мережевого екрану
$a^{17}_{\text{баз.прог.заб.}}$	$a^{15}_{\text{інф.заб..}}$, $a^{16}_{\text{інф.заб..}}$	$a^{\text{зас.забезп.3}}_{\text{заг.прог.забезп.}}$, $a^{\text{зас.забезп.4}}_{\text{заг.прог.забезп.}}$	Логування подій комутаторів
$a^{17}_{\text{баз.прог.заб.}}$	$a^{17}_{\text{інф.заб..}}$,… $a^{20}_{\text{інф.заб..}}$	$a^{\text{серв.1}}_{\text{заг.прог.забезп.}}$, …$a^{\text{серв.4}}_{\text{заг.прог.забезп.}}$	Логування подій серверів
$a^{17}_{\text{баз.прог.заб.}}$	$a^{21}_{\text{інф.заб..}}$	$a^{\text{серв.5}}_{\text{заг.прог.забезп.}}$	Логування подій NTP-сервера

Продовження таблиці 4.8

1	2	3	4
$a^{17}_{\text{баз.прог.заб.}}$	$a^{22}_{\text{інф.заб..}}$, … $a^{27}_{\text{інф.заб.}}$	$a^{\text{АРМ1}}_{\text{заг.прог.забезп.}}$, …$a^{\text{АРМ5}}_{\text{заг.прог.забезп.}}$	Логування подій автоматизованих робочих місць
$a^{17}_{\text{баз.прог.заб.}}$	$a^{28}_{\text{інф.заб.}}$	$a^{46}_{\text{баз.прог.заб.}}$	Зберігання інформації в базах даних
1	2	3	4
$a^{16}_{\text{баз.прог.заб.}}$	$a^{29}_{\text{інф.заб.}}$, … $a^{41}_{\text{інф.заб.}}$	$a^{\text{ПЛК1}}_{\text{заг.прог.забезп.}}$, …$a^{\text{ПЛК12}}_{\text{заг.прог.забезп.}}$,	Логування інформації з датчиків, що передаються до програмованих логічних контролерів
$a^{18}_{\text{баз.прог.заб.}}$	$a^{42}_{\text{інф.заб.}}$	$a^{47}_{\text{баз.прог.заб.}}$	Зберігання інформації в базах даних
$a^{25}_{\text{прик.прог.заб.}}$	$a^{43}_{\text{інф.заб.}}$	$a^{47}_{\text{баз.прог.заб.}}$	Зберігання інформації в базах даних
$a^{25}_{\text{прик.прог.заб.}}$	$a^{44}_{\text{інф.заб.}}$, … $a^{49}_{\text{інф.заб.}}$	$a^{76}_{\text{баз.прог.заб.}}$, … $a^{81}_{\text{баз.прог.заб.}}$	Обмін інформацією між сервером та програмованим логічним контролером
$a^{25}_{\text{прик.прог.заб.}}$	$a^{50}_{\text{інф.заб.}}$, … $a^{54}_{\text{інф.заб.}}$	$a^{13}_{\text{прикл.прог.заб.}}$, … $a^{25}_{\text{прикл.прог.заб.}}$	Обмін інформацією між сервером та програмованим логічним контролером
$a^{25}_{\text{прик.прог.заб.}}$	$a^{55}_{\text{інф.заб.}}$, … $a^{65}_{\text{інф.заб.}}$	$a^{20}_{\text{баз.прог.заб.}}$, … $a^{23}_{\text{баз.прог.заб.}}$	Вивід інформації на екрани робочих місць операторів
$a^{26}_{\text{прик.прог.заб.}}$	$a^{66}_{\text{інф.заб.}}$	$a^{46}_{\text{баз.прог.заб.}}$	Зберігання інформації в базах даних
$a^{27}_{\text{прик.прог.заб.}}$	$a^{67}_{\text{інф.заб.}}$	$a^{51}_{\text{баз.прог.заб.}}$	Зберігання інформації в базах даних

Кінець таблиці 4.8

1	2	3	4
$a^{1}_{\text{IT}-\text{серв.}}$	$a^{68}_{\text{інф.заб.}}$, … $a^{71}_{\text{інф.заб.}}$	$a^{\text{серв.1}}_{\text{заг.прог.забезп.}}$, … $a^{\text{серв.5}}_{\text{заг.прог.забезп.}}$	Звернення до служби каталогів серверами
$a^{1}_{\text{IT}-\text{серв.}}$	$a^{72}_{\text{інф.заб.}}$, … $a^{77}_{\text{інф.заб.}}$	$a^{\text{АРМ1}}_{\text{заг.прог.забезп.}}$, … $a^{\text{АРМ5}}_{\text{заг.прог.забезп.}}$	Звернення до служби каталогів автоматизованих робочих місць
$a^{4}_{\text{IT}-\text{серв.}}$	$a^{78}_{\text{інф.заб.}}$, … $a^{80}_{\text{інф.заб.}}$	$a^{\text{зас.забезп.3}}_{\text{заг.прог.забезп.}}$, $a^{\text{зас.забезп.4}}_{\text{заг.прог.забезп.}}$	Надання мережевих адрес комутаторам
$a^{4}_{\text{IT}-\text{серв.}}$	$a^{81}_{\text{інф.заб.}}$,	$a^{\text{серв.3}}_{\text{заг.прог.забезп.}}$	Надання мережевої адреси NTP-серверу
$a^{5}_{\text{IT}-\text{серв.}}$	$a^{82}_{\text{інф.заб.}}$, $a^{83}_{\text{інф.заб.}}$	$a^{\text{зас.забезп.3}}_{\text{заг.прог.забезп.}}$, $a^{\text{зас.забезп.4}}_{\text{заг.прог.забезп.}}$	Надання резервних мережевих адрес комутаторам
$a^{5}_{\text{IT}-\text{серв.}}$	$a^{84}_{\text{інф.заб.}}$	$a^{\text{зас.забезп.5}}_{\text{заг.прог.забезп.}}$	Надання резервної мережевої адреси точці доступу
$a^{5}_{\text{IT}-\text{серв.}}$	$a^{85}_{\text{інф.заб.}}$	$a^{5}_{\text{серв.}}$	Надання резервної мережевої адреси NTP-серверу
$a^{6}_{\text{IT}-\text{серв.}}$	$a^{85}_{\text{інф.заб.}}$, … $a^{88}_{\text{інф.заб.}}$	$a^{\text{серв.1}}_{\text{заг.прог.забезп.}}$, … $a^{\text{серв.5}}_{\text{заг.прог.забезп.}}$	Система доменних імен для звернень серверів
$a^{6}_{\text{IT}-\text{серв.}}$	$a^{85}_{\text{інф.заб.}}$, … $a^{88}_{\text{інф.заб.}}$	$a^{\text{АРМ1}}_{\text{заг.прог.забезп.}}$, … $a^{\text{АРМ5}}_{\text{заг.прог.забезп.}}$	Система доменних імен для звернень автоматизованих робочих місць

4.2 Формування моделі загроз автоматизованої системи управління технологічними процесами газовидобувного підприємства

Після завершення формування моделі АСУ ТП необхідно сформувати модель загроз АСУ ТП. В першу чергу необхідно сформувати множину вразливостей B для множини $A_{\text{прог.заб.}}$(табл. 4.9) [40, 41,42, 43,44].

Таблиця 4.9 – Вразливості програмного забезпечення автоматизованої системи управління технологічними процесами газовидобувного підприємства

B	Опис вразливості	$\text{A}_{\text{прог.заб.}}$
1	2	3
b^1	Вразливість служби віддаленого доступу (RAS) операційної системи Windows	$a^{\text{серв.1}}_{\text{заг.прог.забезп.}},\ldots a^{\text{серв.5}}_{\text{заг.прог.забезп.}}$ $a^{\text{АРМ1}}_{\text{заг.прог.забезп.}},\ldots a^{\text{АРМ5}}_{\text{заг.прог.забезп.}}$
b^2	Вразливість ядра операційної системи Windows	$a^{\text{серв.1}}_{\text{заг.прог.забезп.}},\ldots a^{\text{серв.5}}_{\text{заг.прог.забезп.}}$ $a^{\text{АРМ1}}_{\text{заг.прог.забезп.}},\ldots a^{\text{АРМ5}}_{\text{заг.прог.забезп.}}$
b^3	Вразливість операційної системи Windows	$a^{\text{серв.1}}_{\text{заг.прог.забезп.}},\ldots a^{\text{серв.5}}_{\text{заг.прог.забезп.}}$ $a^{\text{АРМ1}}_{\text{заг.прог.забезп.}},\ldots a^{\text{АРМ5}}_{\text{заг.прог.забезп.}}$
b^4	Вразливість клієнта віддаленого робочого столу Windows (MS15-067)	$a^{\text{серв.1}}_{\text{заг.прог.забезп.}},\ldots a^{\text{серв.5}}_{\text{заг.прог.забезп.}}$ $a^{\text{АРМ1}}_{\text{заг.прог.забезп.}},\ldots a^{\text{АРМ5}}_{\text{заг.прог.забезп.}}$
b^5	Вразливість служби Security Service операційної системи Windows	$a^{\text{серв.1}}_{\text{заг.прог.забезп.}},\ldots a^{\text{серв.5}}_{\text{заг.прог.забезп.}}$ $a^{\text{АРМ1}}_{\text{заг.прог.забезп.}},\ldots a^{\text{АРМ5}}_{\text{заг.прог.забезп.}}$
b^6	Віддалене виконання коду через неправильну перевірку введення при обробці URL в Microsoft Windows Support Diagnostic Tool	$a^{\text{серв.1}}_{\text{заг.прог.забезп.}},\ldots a^{\text{серв.5}}_{\text{заг.прог.забезп.}}$ $a^{\text{АРМ1}}_{\text{заг.прог.забезп.}},\ldots a^{\text{АРМ5}}_{\text{заг.прог.забезп.}}$
b^7	Вразливість планувальника завдань Windows до підвищення привілеїв	$a^{\text{серв.1}}_{\text{заг.прог.забезп.}},\ldots a^{\text{серв.5}}_{\text{заг.прог.забезп.}}$ $a^{\text{АРМ1}}_{\text{заг.прог.забезп.}},\ldots a^{\text{АРМ5}}_{\text{заг.прог.забезп.}}$

Кінець таблиці 4.9

1	2	3
b^8	Вразливість реалізації RDP протоколу операційної системи Windows	$a^{\text{серв.1}}_{\text{заг.прог.забезп.}},\dots a^{\text{серв.5}}_{\text{заг.прог.забезп.}}$ $a^{\text{АРМ1}}_{\text{заг.прог.забезп.}},\dots a^{\text{АРМ5}}_{\text{заг.прог.забезп.}}$
b^9	NET Core вразливість щодо відмови в обслуговуванні	$a^{\text{серв.1}}_{\text{заг.прог.забезп.}},\dots a^{\text{серв.5}}_{\text{заг.прог.забезп.}}$ $a^{\text{АРМ1}}_{\text{заг.прог.забезп.}},\dots a^{\text{АРМ5}}_{\text{заг.прог.забезп.}}$
b^{10}	Невиправлений драйвер HTTP.sys операційної системи Windows	$a^{\text{серв.1}}_{\text{заг.прог.забезп.}},\dots a^{\text{серв.5}}_{\text{заг.прог.забезп.}}$ $a^{\text{АРМ1}}_{\text{заг.прог.забезп.}},\dots a^{\text{АРМ5}}_{\text{заг.прог.забезп.}}$
b^{11}	Windows Print Spooler Підвищення рівня привілеїв (LPE)	$a^{\text{серв.1}}_{\text{заг.прог.забезп.}},\dots a^{\text{серв.5}}_{\text{заг.прог.забезп.}}$ $a^{\text{АРМ1}}_{\text{заг.прог.забезп.}},\dots a^{\text{АРМ5}}_{\text{заг.прог.забезп.}}$
b^{12}	Вразливості powershell операційної системи Windows	$a^{\text{серв.1}}_{\text{заг.прог.забезп.}},\dots a^{\text{серв.5}}_{\text{заг.прог.забезп.}}$ $a^{\text{АРМ1}}_{\text{заг.прог.забезп.}},\dots a^{\text{АРМ5}}_{\text{заг.прог.забезп.}}$
b^{13}	Вразливість SCADA системи (до прикладу CWE-732: неправильне призначення дозволу для критичного ресурсу)	$a^{26}_{\text{баз.прог.заб.}}$
b^{14}	Вразливість робочої станції, яка дозволяє переповнити буфер обміну	$a^{17}_{\text{баз.прог.заб.}}, \dots a^{23}_{\text{баз.прог.заб.}}$
b^{15}	.NET Framework вразливість віддаленого виконання коду	$a^{24}_{\text{баз.прог.заб.}}, \dots a^{34}_{\text{баз.прог.заб.}}$
b^{16}	.NET Framework підвищення вразливості прав	$a^{24}_{\text{баз.прог.заб.}}, \dots a^{34}_{\text{баз.прог.заб.}}$
b^{17}	.NET Framework вразливість щодо відмови в обслуговуванні	$a^{24}_{\text{баз.прог.заб.}}, \dots a^{34}_{\text{баз.прог.заб.}}$
b^{18}	Вразливість пакету програм Microsoft Office	$a^{52}_{\text{баз.прог.заб.}}, \dots a^{57}_{\text{баз.прог.заб.}}$

Далі після того як ми ідентифікували вразливості в системі, необхідно визначити модель загроз $K_{\text{загр.}}$, що включатиме перелік загроз, які будуть

експлуатовані з використанням вразливостей з попередньої таблиці та при цьому важливе врахування вектору $CVSS^1$ (табл. 4.10) [46].

У результаті реалізації загроз інформаційній безпеці критичної інфраструктури можливе порушення приватності інформації (через витоки, перехоплення, несанкціоноване копіювання або розповсюдження), її цілісності (через втрату, знищення або зміну даних) та доступності (через блокування доступу до інформації). Такі порушення можуть вплинути на достовірність та своєчасність функціонування системи, можливо навіть призвести до її повної відмови в роботі [45].

Таблиця 4.10 – Визначення загроз АСУ ТП

E	Опис загрози	B	A
1	2	3	4
e^1	Загроза імплементації коду чи стороннього програмного забезпечення	b^1, … b^6, b^{15},	$a^1_{\text{інф.заб.}}$, … $a^{12}_{\text{інф.заб.}}$
e^2	Загроза впливу на програмні засоби з високими привілеями	b^1, b^3, b^4, b^5, b^6, b^7, b^{14}	$a^{\text{серв.1}}_{\text{заг.прог.забезп.}}$,… $a^{\text{серв.4}}_{\text{заг.прог.забезп.}}$ $a^{\text{АРМ1}}_{\text{заг.прог.забезп.}}$,… $a^{\text{АРМ5}}_{\text{заг.прог.забезп.}}$
e^3	Загроза відновлення або повторного використання інформації щодо аутентифікації	b^{13}	$a^{26}_{\text{баз.прог.заб.}}$
e^4	Загроза зараження DNS-кешу		$a^6_{\text{ІТ}-\text{серв.}}$

Кінець таблиці 4.10

1	2	3	4
e^5	Загроза використання стандартної інформації аутентифікації	b^{16}, b^{17}	$a^{24}_{\text{баз.прог.заб.}}$, … $a^{34}_{\text{баз.прог.заб.}}$
e^6	Загроза підвищення привілеїв користувача	b^7, b^{11}	$a^{26}_{\text{баз.прог.заб.}}$
e^7	Загроза використання PowerShell для виконання шкідливих скриптів	b^{12}	$a^{\text{серв.1}}_{\text{заг.прог.забезп.}}$,… $a^{\text{серв.5}}_{\text{заг.прог.забезп.}}$ $a^{\text{АРМ1}}_{\text{заг.прог.забезп.}}$,… $a^{\text{АРМ5}}_{\text{заг.прог.забезп.}}$
e^8	Загроза використання вразливостей мережевих протоколів	b^1, b^8 …,b^{10}, b^{15}, … b^{18}	$a^{24}_{\text{баз.прог.заб.}}$, … $a^{34}_{\text{баз.прог.заб.}}$, $a^{52}_{\text{баз.прог.заб.}}$, … $a^{57}_{\text{баз.прог.заб.}}$
e^9	Загроза неправомірних дій в каналах зв’язку		$a^{1}_{\text{кан.зв}}$, … $a^{98}_{\text{кан.зв.}}$
e^{10}	Загроза перехоплення керування автоматизованою системою управління ТП	b^{13}	$a^{26}_{\text{баз.прог.заб.}}$, $a^{17}_{\text{баз.прог.заб.}}$, … $a^{23}_{\text{баз.прог.заб.}}$
e^{11}	Загроза зміни параметрів програмованих логічних контролерів внаслідок несанкціонованого доступу	b^{13}	$a^{17}_{\text{баз.прог.заб.}}$, … $a^{23}_{\text{баз.прог.заб.}}$

4.3 Аналіз ризиків інформаційної безпеки автоматизованої системи управління технологічними процесами об’єкту критичної інфраструктури

Після вираження фізичної та логічної структуру АСУ ТП газовидобувного підприємства, дані отримані в результаті необхідно використати для роботи з алгоритмами, що були представлені в розділі 3 та виконати аналіз ризиків, що і було виконано в цьому підрозділі.

Використовуючи алгоритм оцінки важливості елементів в множині критичних процесів АСУ ТП ми провели відповідний розрахунок та отримали наступні результати (табл. 4.11):

1. Множина критичних процесів визначена у таблиці 4.1.

2. Визначили витрати для кожного критичного процесу $a^{n}_{\text{кр.пр.}} \in A_{\text{кр.пр.}}$, викликані припиненням або порушенням його роботи $L^{n}_{\text{вит.}}$.

3. Визначили втрати, які виникли внаслідок припинення, чи порушення роботи $L^{n}_{\text{втр.}}$.

4. Для кожного критичного процесу $a^{n}_{\text{кр.пр.}} \in A_{\text{кр.пр.}}$визначили втрати та витрати за час припинення або порушення цього процесу, за одну хвилину $L^{n}_{\text{ч.}}$.

5. На основі попередніх показників визначили важливість кожного критичного процесу $L^{n}_{\text{кр.пр.}}$.

6. Визначили сумарні збитки при припиненні чи порушенні роботи всіх критичних процесів.

Таким чином сумарні збитки при припиненні роботи всіх критичних процесів I_{Σ} буде дорівнювати 772 600 грн.

Далі з використанням алгоритму оцінки важливості активів АСУ ТП ми:

1. Виконали алгоритм оцінки важливості критичних процесів АСУ ТП (табл. 4.12).

2. Склали ієрархію активів АСУ ТП (рис. 3.3)

3. Виконали розрахунок важливості активів АСУ ТП (табл. 4.13).

4. Розподілили кожний параметр між залежними елементами нижчого рівня відповідно ієрархії (табл. 4.14).

Далі з-за допомогою алгоритму розподілу по рівням захисту була виконана ідентифікація та розподіл множини $L^{e}_{\text{пониж.}}$(табл. 4.15).

Таблиця 4.11 – Оцінка важливості критичних процесів

$A_{\text{кр.пр.}}$	$L^{n}_{\text{вит.}}$	$L^{n}_{\text{втр.}}$	$L^{n}_{\text{ч.}}$	$L^{n}_{\text{кр.пр.}}$
$a^{1}_{\text{кр.пр.}}$	29800	24100	5800	(29800, 24100, 5800)
$a^{2}_{\text{кр.пр.}}$	29500	28000	5500	(29500, 28000, 5500)
$a^{3}_{\text{кр.пр.}}$	30000	29300	7000	(30000, 29300, 7000)
$a^{4}_{\text{кр.пр.}}$	30500	29800	7500	(30500, 29800, 7500)
$a^{5}_{\text{кр.пр.}}$	29800	24100	5800	(29800, 24100, 5800)
$a^{6}_{\text{кр.пр.}}$	35000	29100	9500	(35000, 29100, 9500)
$a^{7}_{\text{кр.пр.}}$	28300	26300	5500	(28300, 26300, 5500)
$a^{8}_{\text{кр.пр.}}$	29800	24100	5800	(29800, 24100, 5800)
$a^{9}_{\text{кр.пр.}}$	33500	31000	9800	(33500, 31000, 9800)
$a^{10}_{\text{кр.пр.}}$	34200	31500	9700	(34200, 31500, 9700)
$a^{11}_{\text{кр.пр.}}$	29800	24100	5800	(29800, 24100, 5800)
$a^{12}_{\text{кр.пр.}}$	23800	24000	5500	(23800, 24000, 5500)

Таблиця 4.13 – Оцінка важливості множин технічного забезпечення

$A_{\text{тех.заб.}}$	$L^{n}_{\text{вит.}}{}^{\text{тех.заб.}}$	$L^{n}_{\text{втр.}}{}^{\text{тех.заб.}}$	$L^{n}_{\text{ч.}}{}^{\text{тех.заб.}}$	$L^{n}_{\text{тех.заб.}}$
$A_{\text{верхн.}}$	45520	34866	17480	(45520, 34866, 17480)
$A_{\text{середн.}}$	22760	17432	17480	(22760, 17432, 17480)
$A_{\text{нижн.}}$	22760	34866	43700	(22760, 34866, 43700)
$A_{\text{зас.зв.}}$	22760	17432	8740	(22760, 17432, 8740)

Таблиця 4.14 – Оцінка важливості множин технічних засобів

$A_{\text{тех.зас}}$	$L^{n\ \text{тех.зас.}}_{\text{вит.}}$	$L^{n\ \text{тех.зас.}}_{\text{втр.}}$	$L^{n\ \text{тех.зас.}}_{\text{ч.}}$	$L^{n}_{\text{тех.зас.}}$
$a^{1}_{\text{серв.}}$	15172	11622	5826	(15172, 11622, 5826)
$a^{2}_{\text{серв.}}$	4138	3168	1588	(4138, 3168, 1588)
$a^{3}_{\text{серв.}}$	5516	4223	2118	(5516, 4223, 2118)
$a^{4}_{\text{серв.}}$	2758	2112	1058	(2758, 2112, 1058)
$a^{5}_{\text{серв.}}$	2758	2112	1058	(2758, 2112, 1058)
$a^{1}_{\text{АРМ}}, \dots a^{5}_{\text{АРМ}}$	9654	7394	3706	(9654, 7394, 3706)
$a^{1}_{\text{ПЛК}}, \dots a^{12}_{\text{ПЛК}}$	1516	1162	1164	(1516, 1162, 1164)
$a^{1}_{\text{датч.}}, \dots a^{64}_{\text{датч.}}$	76	116	146	(76, 116, 146)
$a^{1}_{\text{вик.мех.}}, \dots a^{64}_{\text{вик.мех.}}$	152	232	292	(152, 232, 292)
$a^{1}_{\text{зас.забезп.}}, \dots a^{12}_{\text{зас.забезп.}}$	3416	2666	1600	(3416, 2666, 1600)
$a^{1}_{\text{кан.зв}}, \dots a^{98}_{\text{кан.зв.}}$	74	36	28	(74, 36, 28)

Таблиця 4.15 – Розподіл множини $L^{e}_{\text{пониж.}}$ на підмножини

$L^{e}_{\text{пониж.}}$	Опис
1	2
$L^{1}_{\text{адм.зах}}$	Політика безпеки
$L^{2}_{\text{адм.зах}}$	Посадові інструкції працівників
$L^{1}_{\text{фіз.безп.}}$	Огородження периметру підприємства парканом
$L^{2}_{\text{фіз.безп.}}$	Розміщення обладнання в закритих приміщеннях
$L^{3}_{\text{фіз.безп.}}$	Пост охорони на вході до підприємства
$L^{4}_{\text{фіз.безп.}}$	Закриття приміщень на ключ.
$L^{5}_{\text{фіз.безп.}}$	Зберігання ключів у відповідальної особи.
$L^{6}_{\text{фіз.безп.}}$	Зовнішнє відеоспостереження території об'єкта.

Кінець таблиці 4.15

1	2
$L^1_{\text{перим.}}$	Шифрування трафіку між корпоративною та АСУ ТП мережами
$L^2_{\text{перим.}}$	Наявність фільтрації трафіку між мережами інформаційних систем
$L^1_{\text{мереж.}}$	Наявність мережевих екранів
$L^2_{\text{мереж.}}$	Наявність резервних каналів зв’язку
$L^3_{\text{мереж.}}$	Наявність резервних комутаторів
$L^4_{\text{мереж.}}$	Системи аутентифікації та авторизації
$L^1_{\text{прист.}}$	Чітка система паролів робочих машин та пристроїв
$L^2_{\text{прист.}}$	Розмежування прав доступу на основі привілеїв для кожної окремої ролі
$L^3_{\text{прист.}}$	Наявність резервних копій системи та зокрема операційних систем після першого налаштування
$L^1_{\text{дод.}}$	Авторизація в додатках через обліковий запис Active Directory
$L^2_{\text{дод.}}$	Наявність логування подій в додатках
$L^1_{\text{інф.}}$	Розмежування прав доступу до інформації на основі привілеїв

4.4 Оцінка ризиків інформаційної безпеки автоматизованої системи управління технологічними процесами об’єкту критичної інфраструктури.

Після проведеного аналізу ризиків відповідно далі необхідно провести їхню оцінку. Першочергово нами було здійснено оцінку ризиків, що не використовують вразливості системи. Для цього ми використали алгоритм оцінки збитків при реалізації загрози e^u(табл. 4.16).

Таблиця 4.16 – Оцінка збитків при реалізації загроз

E	$L_A^{e^n}$	$L_{\text{вит.}}^n$	$L_{\text{втр.}}^n$	$L_{\text{ч.}}^n$	L_E^n
e^4	(910, 696, 348)	1	1	362	64594
e^9	(17760, 13440, 6720)	1	1	22	105120

Оцінка збитків для загроз, які при реалізації використовують вразливості виконувалась з-за допомогою алгоритму оцінки збитків при експлуатації загрози (табл. 4.16).

Таблиця 4.17 – Оцінка збитків при експлуатації вразливостей

E	$L_A^{e^n}$	$L_{\text{вит.}}^n$	$L_{\text{втр.}}^n$	$L_{\text{ч.}}^n$	CVSS	L_B^n
e^1	(1390, 1064, 794)	0,8	0,9	216	0,95	87878
e^2	(39712, 30414, 15232)	1	0,9	22	0,95	234636
e^3	(974, 746, 374)	0,9	0,9	362	0,98	69414
e^5	(4524, 3413, 1734)	0,9	0,8	104	1	97988
e^6	(974, 746, 374)	0,9	0,9	294	0,98	56788
e^7	(5138, 3926, 1968)	0,9	0,9	124	1	130898
e^8	(39712, 30414, 15232)	1	1	20	0,86	216886
e^{10}	(10448, 7994, 3998)	0,9	0,9	54	0,88	124544
e^{11}	(11422, 8740,4372)	1	1	22	0,84	142578

Далі нами було з-за допомогою наступного алгоритму було оцінено вірогідність реалізації кожної загрози (табл. 4.18).

Таблиця 4.18 – Результати виконання алгоритму оцінки вірогідності реалізації загрози

E	j^n
e^1	0,69
e^2	0,31
e^3	0,85
e^4	0,76
e^5	0,67
e^6	0,79
e^7	0,54
e^8	0,39
e^9	0,70
e^{10}	0,75
e^{11}	0,59

4.5 Висновки

В цьому розділі було виконано практичне впровадження методу забезпечення кібербезпеки автоматизованих систем критичної інфраструктури газовидобувної компанії, а саме її автоматизованої системи управління технологічними процесами.

Зокрема було використано алгоритми вищезазначеного методу, які дозволили визначити:

– критичні процеси відповідно до ієрархічної структури автоматизованої системи.

– порядок взаємодії критичних процесів та технічного забезпечення.

– структуру управління критичними процесами та механізмами виконання.

– порядок технічного та загального програмного забезпечення

– структуру фізичного зв’язку між програмованими логічними контролерами та елементами нижнього рівня ієрархічної структури автоматизованої системи управління технологічними процесами.

– взаємозв’язок між технічним забезпеченням та засобами зв’язку.

– список встановленого спеціального програмного забезпечення.

– структуру логічного зв’язку програмного забезпечення.

– вразливості програмного забезпечення автоматизованої системи управління технологічними процесами газовидобувної компанії.

– визначити конкретний перелік загроз автоматизованої системи управління технологічними процесами.

Також в ході роботи було виконано оцінку важливості множин технічного забезпечення, технічних засобів, розподіл заходів захисту та відповідні оцінки ризиків.

ВИСНОВКИ

В магістерській роботі розглядається важлива галузь інформаційної безпеки – управління кіберризиками автоматизованих систем критичної інфраструктури газовидобувної компанії на основі оцінки ризиків, а саме автоматизованої системи управління технологічними процесами. Необхідність проведення оцінки ризиків в умовах багаторівневої, складної ієрархічної структури вимагала розробки відповідного методу, який складається з алгоритмів. У роботі було отримані наступні результати, які відрізняються науковою та технічною новизною:

1. Визначено основні поняття критичної інфраструктури та її роль у сучасному світі. Зокрема ми дійшли до висновку, що критична інфраструктура є ключовою для функціонування держави та суспільства, оскільки включає в себе набір об'єктів та систем, від яких залежить національна безпека, стабільність та обороноздатність країни, а також повсякденне життя громадян. Вона відіграє вирішальну роль у підтриманні безпеки та стійкості країни. Класифікація об'єктів критичної інфраструктури на категорії дозволяє краще зрозуміти їхню роль у системі, забезпечувати ефективний захист від потенційних загроз та планувати адекватні заходи захисту та відновлення в кризових ситуаціях. Важливість її захисту та відновлення після можливих збоїв в роботі не може бути недооцінена, оскільки негативні наслідки від її порушення можуть мати катастрофічний вплив.

2. Розглянуто нормативне забезпечення кібербезпеки на об’єктах критичної інфраструктури та зазначено, що визначення поняття кібербезпеки в національному та міжнародному законодавстві, охоплює захист життєво необхідних інтересів людини, громадянина, суспільства та держави в кіберпросторі. Захист інформації є надзвичайно важливим у сучасному світі, особливо у сфері публічного та державного управління.

3. Визначено поняття автоматизованих систем та систем управління технологічними процесами об’єктів критичної інфраструктури.

4. Розроблено теоретико-множинну модель автоматизованої системи управління технологічними процесами газовидобувної компанії, яка відрізняється наявністю опису взаємодії активів різних рівнів відповідно до ієрархічної структури автоматизованої системи управління технологічними процесами. Модель відображає логічну та фізичну структури взаємодії між активами, а також вплив на критичні процеси автоматизованої системи управління технологічними процесами газовидобувного підприємств, що дозволяє здійснити аналіз характеристик технічних та програмних засобів, технологічних процесів та в подальшому ефективно використовувати отримані результати для оцінки ризиків інформаційної безпеки.

5. Розроблено метод оцінки ризиків інформаційної безпеки автоматизованої системи управління технологічними процесами газовидобувної компанії на основі відповідних алгоритмів.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Про критичну інфраструктуру : Закон України від 16.11.2021 р. № 1882-IX : станом на 5 груд. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 07.09.2023).

2. Зелена книга з питань захисту критичної інфраструктури в Україні: зб. матеріалів міжнар. експерт. нарад / упоряд.: Д. С. Бірюков, С. І. Кондратов; за заг. ред. О. М. Суходолі. Київ : НІСД, 2015. 176 с.

3. Верголяс О. Реформування системи захисту та підвищення стійкості критичної інфраструктури України в розрізі актуальних загроз. URL: https://coolyanews.info/reformuvannyasistemi-zahistu-ta-piidvischennya-stiijkostii-kritichnoyi-iinfrastrukturi-ukrayinii-vrozriiziiaktual.html (дата звернення: 07.09.2023).

4. Гора І. В., Батюк О. В. Окремі питання захисту об’єктів критичної інфраструктури: зарубіжний досвід. Соціально-правові студії. 2021. №1 (11). С. 132-139.

5. Бірюков Д. С., Кондратов С. І. Захист критичної інфраструктури: проблеми та перспективи впровадження в Україні: аналітична доповідь. Київ : НІСД, 2012. 57 с.

6. Domaratskyy M. B. The methodology of state classification of critical objects. States and Regions. Series: Public Administration. 2019. No. 4. P. 278–281. URL: https://doi.org/10.32840/1813-3401-2019-4-44 (дата звернення: 08.09.2023).

7. Домарацький М. Б. Особливості категоріювання об’єктів критичної інформаційної інфраструктури // Фінансова система та економічна безпека: збірник тез наукових робіт учасників міжнародної НПК для студентів, аспірантів та молодих учених. Київ : Аналітичний центр «Нова Економіка». 2019. Ч. 2. С. 91–92.

8. Мануїлов Я. С. Забезпечення кібербезпеки об’єктів критичної інфраструктури в умовах кібервійни. Інформація і право. 2023. № 1 (44). С. 154–167.

9. Войціховський А. В. Питання захисту критичної інфраструктури від кіберзагроз. м. Харків, 23 листоп. 2023 р. Харків, 2018. С. 363–367.

10. ISO/IEC 27000. Серія стандартів. ООО «ІНТЕРСЕРТ-УКРАЇНА». URL: https://intercert.com.ua/articles/regulatory-documents/210-iso-27000 (дата звернення: 11.09.2023).

11. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII : станом на 17 серп. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 12.09.2023).

12. Мельник С. В., Тихомиров О. О., Лєнков О. С. До проблеми формування понятійно-термінологічного апарату кібербезпеки. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. 2011. № 30. С. 165–171.

13. Ящук В. І. Принципи проектування автоматизованих інформаційних систем управління об’єктами критичної інфраструктури. Львів, 2021.

14. ДСТУ 2709-94. Автоматизовані системи керування технологічними процесами. Метрологічне забезпечення. Чинний від 1994-07-29. Вид. офіц. Київ : Держстандарт України, 1994. 10 с.

15. Бобрух А. О. Автоматизовані системи керування технологічними процесами / ред. М. З. Аляб’єв. Харків : ХНАМГ, 2006. 185 с.

16. SCADA система. OPEKS energysystems. opeks.ua. URL: https://opeks.ua/ua/scada-sistema/ (дата звернення: 12.09.2023).

17. Островерхов М. Я. Комп’ютерні засоби автоматизації електротехнологічних установок. Конспект лекцій. Київ : КПІ ім. Ігоря Сікорського, 2022. 222 с.

18. Stuxnet - перша цифрова зброя-вірус? - BBC News Україна. BBC News Україна. URL: https://www.bbc.com/ukrainian/news/2011/02/110215_stuxnet_virus_oh (дата звернення: 13.09.2023).

19. Перевисокова Н. В. Інтегровані системи управління. Конспект лекцій. Івано-Франківськ : ДВНЗ Прикарпат. нац. ун-т ім. Василя Стефаника, 2013. 41 с.

20. Програмований логічний контролер – Вікіпедія. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Програмований_логічний_контролер (дата звернення: 13.09.2023).

21. Промислові комп’ютерні мережі. семінари. : навч. посіб. / уклад.: Д. М. Складанний, Є. О. Тюріна. Київ : КПІ ім. Ігоря Сікорського, 2023. 54 с.

22. Сапожнік Т. М., Пахольченко Д. В., Бакалинський О. О. Проблеми забезпечення кіберзахисту АСУ ТП.

23. Науково-практичний аналіз рекомендацій з кібербезпеки автоматизованих систем управління технологічними процесами / В. Ю. Зубок та ін. Електрон. моделювання. 2022. Т. 44, № 2. С. 68–81.

24. Верескун М. В. Методичне забезпечення системи інформаційної безпеки промислових підприємств. Економіка і організація управління. 2014. № 1 (17) - 2 (18). С. 54–60.

25. Захист інформації в автоматизованих системах управління: навчальний посібник : навч. посіб. / уклад.: І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. Житомир : ЖДУ ім. І. Франка, 2018. 226 с.

26. Гончар С. Ф. Особливості забезпечення кібербезпеки об’єктів критичної інфраструктури. Моделювання та інформаційні технології. 2071. № 80. С. 27–32.

27. Методика проведення незалежного аудиту інформаційної безпеки установи щодо ефективності забезпечення захисту інформації / М. В. Артемчук та ін. Вісник ВІТІ. комунікаційні та інформаційні системи. 2021. № 2. С. 4–17.

28. Alert level information. CIS. URL: https://www.cisecurity.org/cybersecurity-threats/alert-level (дата звернення: 20.09.2023).

29. Cramm risk assessment. Risk Publishing. URL: https://riskpublishing.com/cramm-risk-assessment/#google_vignette (дата звернення: 21.09.2023).

30. Cramm. ENISA. URL: https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html (дата звернення: 22.09.2023).

31. Mullerova J., Nemec V. Risk assessment RM/RA cramm–quantitative method for environmental, technology and social threats. 19th international multidisciplinary scientific geoconference SGEM 2019 : Proceedings Paper. 2019. P. 279–285.

32. Метод аналізу ризиків OCTAVE. Wiki TNEU. URL: http://surl.li/obvrn (дата звернення: 25.09.2023).

33. Abdelghani T. Implementation of defense in depth strategy to secure industrial control system in critical infrastructures. American journal of artificial intelligence. 2019. Т. 3, № 2. С. 17. URL: https://doi.org/10.11648/j.ajai.20190302.11 (дата звернення: 09.10.2023).

34. Метод Дельфі як метод кількісної оцінки думки експертів. Його переваги і недоліки. Studies. URL: https://studies.in.ua/soc-ekzam/3314-metod-delf-yak-metod-klksnoyi-ocnki-dumki-ekspertv-yogo-perevagi-nedolki.html (дата звернення: 13.10.2023).

35. What is common vulnerability scoring system (CVSS) | centraleyes. Centraleyes. URL: https://www.centraleyes.com/glossary/common-vulnerability-scoring-system/ (дата звернення: 20.10.2023).

36. Vulnerability metrics. NVD. URL: https://nvd.nist.gov/vuln-metrics/cvss (дата зверення: 27.10.2023)

37. Event tree analysis. Wikipedia. URL: https://en.wikipedia.org/wiki/Event_tree_analysis (дата звернення: 01.11.2023).

38. Cybersecurity risk management: frameworks, plans, & best practices. Hyperproof. URL: https://hyperproof.io/resource/cybersecurity-risk-management-process/ (дата звернення: 02.11.2023).

39. Information technology security training requirements: a role- and performance-based model / D. E. de Zafra et al. ; ed. by M. Wilson. Washington : U.S. GOVERNMENT PRINTING OFFICE, 1998. 232 p.

40. CVE TOP 12 in 2022 for penetration testing. CQR. URL: https://cqr.company/ua/blog/cve-top-12-in-2022-for-penetration-testing/ (дата звернення: 03.11.2023).

41. National vulnerability database. NVD. URL: https://nvd.nist.gov/ (дата звернення: 10.11.2023).

42. Common weakness enumeration. CWE. URL: https://cwe.mitre.org/ (дата звернення: 13.11.2023).

43. 13 червня 2023 р. – оновлення лише системи безпеки для .NET framework 3.5, 4.6.2, 4.7, 4.7.1, 4.7.2, 4.8 для windows embedded 8.1 і windows server 2012 R2 (KB5027533) - підтримка від microsoft. Microsoft Support. URL: https://support.microsoft.com/uk-ua/topic/13-червня-2023-р-оновлення-лише-системи-безпеки-для-net-framework-3-5-4-6-2-4-7-4-7-1-4-7-2-4-8-для-windows-embedded-8-1-і-windows-server-2012-r2-kb5027533-9fc06d3d-91aa-43a6-9071-3b26f36ea0be (дата звернення: 17.11.2023).

44. Бюлетень з безпеки (Майкрософт) MS17-022. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/ru-ru/security-updates/securitybulletins/2017/ms17-022 (дата звернення: 21.11.2023).

45. Класифікація та аналіз загроз інформаційній безпеці в ключових системах інформаційної інфраструктури. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2015. № 1 (29). С. 56–61.

46. Mitre att&ck®. URL: https://attack.mitre.org/ (дата звернення: 01.12.2023).

47. Шкала харрінгтона. ni.biz.ua. URL: http://ni.biz.ua/17/17_9/17_94234_shkala-harringtona.html (дата звернення: 04.12.2023).

48. Грох А. О., Орленко В. С., Чешун В. М. Стеганоалгоритм з форматними перетвореннями. Інформаційно-комп’ютерні технології - 2023 : XIII Міжнародно науково-техн. конф., м. Житомир, 30–31 берез. 2023 р. Житомир, 2023. С. 216.

49. Грох А. О., Чешун В. М. Оцінка ризиків кібербезпеки автоматизованих систем об’єктів критичної інфраструктури. «Військова освіта і наука: сьогодення та майбутнє» : XIX Міжнародно наукова-практ. конф., м. Київ, 10 листоп. 2023 р. Київ, 2023. С. 406.

50. Грох А., Чешун В. М., Орленко В. С. Загрози і ризики кібербезпеки систем електронного урядування. “Молодіжна військова наука у Київському національному університеті імені Тараса Шевченка” : Всеукр. науково-практ. конф. молодих вчен., ад’юнктів, слухачів, курсантів і студентів, м. Київ, 27 квіт. 2023 р. Київ, 2023. С. 430.

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Інститут цифровізації освіти НАПН України
Національний технічний університет України «Київський політехнічний інститут» ім. І. Сікорського
Вінницький національний технічний університет
Житомирський військовий інститут імені С.П. Корольова
Тернопільський національний технічний університет імені Івана Пулюя
Харківський національний університет радіоелектроніки
Уманський державний педагогічний університет імені Павла Тичини
Національний університет біоресурсів і природокористування України
Інститут геохімії навколишнього середовища НАН України
Черкаський державний технологічний університет
Національний авіаційний університет
Luleå university of technology (Королівство Швеція)
Politechnika Opolska (Poland)
Warsaw University of Technology (Poland)
Технічний університет (Чеська Республіка)
Університет країни Басків (Іспанія)
ADA University (Азербайджан)
Silesian University of Technology (Poland)

ТЕЗИ ДОПОВІДЕЙ

XIII Міжнародної науково-технічної конференції

Інформаційно-комп'ютерні технології - 2023

м. Житомир, 30-31 березня 2023 р.

Житомир
2023

УДК 004
Т11

Рекомендовано до друку Вченою радою Державного університету «Житомирська політехніка» (протокол № 28 від 28.04.2023р.)

Т11 **Тези** XIII Міжнародної науково-технічної конференції «Інформаційно-комп'ютерні технології», м. Житомир, 30–31 березня 2023 р. – Житомир: Житомирська політехніка, 2023. – 216 с.

Представлено доповіді учасників XIII Міжнародної науково-технічної конференції. Наведено аналіз та результати досліджень сучасних проблем інформаційних технологій, математичного моделювання та розробки програмного забезпечення, інформаційних систем, комп'ютерної інженерії та кібербезпеки, цифрової обробки сигналів та зображень, комп'ютерно-інтегрованих технологій, робототехніки та приладобудування, інформаційних технологій в телекомунікаціях та біомедицині, інформаційно-комунікаційних технологій в освіті.

УДК 004

Наукове видання

Тези XIII Міжнародної науково-технічної конференції «Інформаційно-комп'ютерні технології» Житомир, 30–31 березня 2023 р.

Відповідальний за випуск Т.М. Нікітчук

Свідоцтво про внесення до Державного реєстру субєктів видавничої справи ДК № 7177 ВІД 04.11.2021 р.

Адреса редакції: Державний університет «Житомирська політехніка», вул. Чудновська, 103, м.Житомир, 10005

$$d_i = \sqrt{\omega_1 (x_1 - y_{1i})^2 + \omega_2 (x_2 - y_{2i})^2 + ... + \omega_n (x_n - y_{ni})^2},$$

де d_i – це відстань між оцінкою поведінки користувача, що аналізується, і збереженою оцінкою поведінки i-го користувача,

$x_1, x_2, ..., x_n$ –значення параметрів, що перевіряються,

$y_{1i}, y_{2i}, ..., y_{ni}$ –значення збережених параметрів i-го користувача,

$\omega_1, \omega_2, ..., \omega_n$ –вагові коефіцієнти.

Для розрахунку $y_1, y_2, ..., y_n$ можуть бути використані значення, отримані зі збору даних користувачів на підставі цих параметрів. Наприклад, якщо для користувача 1 були зібрані наступні значення:

– кількість натискань на клавішу за 5 секунд: 15;
– кількість помилок при наборі тексту на 10 символів: 2;
– кількість переглядів каталогів за хвилину: 3;
– кількість кліків миші за 10 секунд: 5.

Тоді значення у для кожного параметра можуть бути обчислені наступним чином:

– y_{11}= 15;
– y_{21} = 2;
– y_{31} = 3;
– y_{41} = 5.

Важливо зазначити, що вибір та обчислення поведінкових параметрів залежить від конкретної задачі, а також від технічних можливостей збору та аналізу поведінкових даних.

Висновки

Методи аналізу поведінкових ознак користувачів дозволяють визначити унікальний шаблон поведінки кожного користувача і використовувати його для аутентифікації. Це знижує ризик роботи з системою викрадача паролю, оскільки змінити поведінкові параметри важко.

Проте, важливо враховувати ризики та обмеження методів поведінкової біометрії. Користувач може змінити свій шаблон поведінки, наприклад, змінити стиль набору тексту або швидкість набору, що може спричинити помилки в аутентифікації. Для досягнення максимальної ефективності, методи поведінкової аутентифікації можуть бути поєднані з іншими методами аутентифікації, такими як двофакторна аутентифікація або використання сильних паролів. Комбінування декількох методів аутентифікації може допомогти зменшити ризики та підвищити безпеку користувача.

Застосування методів поведінкової біометрії в бізнес-середовищах може бути складним, оскільки вони вимагають спеціального програмного забезпечення та обладнання, що може збільшити витрати на забезпечення безпеки.

УДК 004.056:621.397.3:004.942

Грох А.О., студент,
Орленко В.С., к.т.н., доцент,
Чешун В.М., к.т.н., доцент
Хмельницький національний університет

СТЕГАНОАЛГОРИТМ З ФОРМАТНИМИ ПЕРЕТВОРЕННЯМИ

Під час роботи стеганографічних алгоритмів виникають проблеми пов'язані з міжформатними перетвореннями [1]. JPEG є форматом стискування з втратами, тому втрати , як правило, не дають відновити вбудовувану інформацію. Це пов'язано з тим, що відновлення робиться після міжформатних перетворень JPEG-RGB_BMP-JPEG. У реалізованій стеганосистемі названа проблема розв'язана із залученням ряду превентивних заходів при вбудовуванні інформації. Вбудовування інформації відбувається за алгоритмом, представленим на рисунку 1.

Рисунок 1 – Стеганографічний алгоритм вбудовування інформації

За алгоритмом спочатку відбувається перетворення файлу JPEG у файл BMP (потік даних). В результаті відбувається збільшення розміру потоку даних через зміни кодування інформації про колір різних

ВІЙСЬКОВИЙ ІНСТИТУТ
КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

ЗБІРНИК
ТЕЗ ДОПОВІДЕЙ

XIX Міжнародної науково-практичної конференції

«Військова освіта і наука: сьогодення та майбутнє»

10 листопада 2023 року

Київ – 2023

Військова освіта і наука: сьогодення та майбутнє : зб. тез доповідей XIX Міжнародної науково-практичної конференції, м. Київ, 10 листопада 2023 р. Київ : Військовий інститут Київського національного університету імені Тараса Шевченка, 2023. 406 с.

Рекомендовано до друку Вченою радою Військового інституту Київського національного університету імені Тараса Шевченка
(протокол від 16.11.2023 № 3).

У збірнику тез доповідей друкуються матеріали виступів наукових і науково-педагогічних працівників, курсантів (студентів) Військового інституту Київського національного університету імені Тараса Шевченка та інших вищих військових та закладів вищої освіти України.

У публікаціях розглядаються: технічні проблеми озброєння і військової техніки та технології подвійного призначення; актуальні проблеми лінгвістичного забезпечення Збройних Сил України; актуальні питання військової психології та соціальної роботи; інформаційно-психологічна боротьба у воєнній сфері; інформаційно-медійне забезпечення МОУ та ЗСУ в умовах правового режиму воєнного стану; фінанси; актуальні проблеми військового права в умовах воєнного стану; актуальні проблеми геопросторової підтримки військ в умовах ведення російсько-української війни; наукові проблеми військової політології та морально-психологічного впливу

ЗМІСТ

коефіцієнтів готовності всіх рівнів побудови та інтервалів наступного технічного обслуговування для об'єктів РЕТ та міжповірочних інтервалів для ЗВТ.

Висновок. Запропоновані рішення мають в своїй основі використання статистичної інформації про відмови шаф, блоків, субблоків та інформації про надлишковий ресурс зазначених рівнів ієрархії з урахуванням технічного стану ТЕЗ як їх складових. Це дозволить розрахувати значення коефіцієнту готовності об'єктів як функцію коефіцієнтів готовності складових частин з урахуванням результатів фізичного діагностування.

Грох А.О. (ХмНУ)
к.т.н., доц. Чешун В.М. (ХмНУ)

ОЦІНКА РИЗИКІВ КІБЕРБЕЗПЕКИ АВТОМАТИЗОВАНИХ СИСТЕМ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Сьогодні на міжнародному та національних рівнях популярні дебати з широкого спектру питань, пов'язаних з кібербезпекою в системах об'єктів критичної інфраструктури. Це зумовлено актуальністю таких систем як об'єктів для здійснення кібератак, особливо в умовах кібервійн. Зупинка роботи такого об'єкту може призвести до величезних збитків, несанкціонованого доступу до великихобсягів конфіденційних даних, інформації державного значення тощо. У випадку реалізації кіберзагроз в автоматизованих системах управління технологічними процесами, які працюють на об'єктах критичної інфраструктури, можуть бути різноманітні негативні наслідки : порушення національної безпеки; сприяння актам тероризму; втрата або скорочення виробництва; травми або смерть людей; екологічні збитки; втрата приватної або конфіденційної інформації; тощо.

Існує низка стандартів та нормативних документів щодо управління та оцінки ризиків. Зокрема до них відносять ISO 31000, NIST SP 800-30, NIST 800-37, ISO/IEC 27005. Вищевказані стандарти дозволяють здійснити загальну оцінку, структуризацію та керування ризиками для швидкого реагування на інциденти та правильного розподілу ресурсів. У промисловості використовується ряд загальних методологій оцінки IT-ризиків: критична операційна оцінка загроз і вразливостей OCTAVE; метод аналізу та управління ризиками центрального комп'ютерного та телекомунікаційного агентства CRAMM; консультативний, об'єктивний і бифункціональний аналіз ризиків COBRA; заснована на моделях методологія оцінки ризиків для критично важливих для безпеки систем CORAS. Також існує широкий спектр академічних пропозицій: метод аналізу ризиків інформаційної безпеки ISRAM; оцінка витрат, порівняльний аналіз та оцінка ризиків COBRA; спрощена практична методологія аналізу ризиків SPRINT; методологія бізнес-процесів управління інформаційними ризиками BPIRM, тощо.

Специфіка автоматизованих систем об'єктів критичної інфраструктури зумовлює виникнення ризиків, які зазвичай не враховуються у звичайних IT-системах. Відповідно системи об'єктів критичної інфраструктури вимагають комплексного та індивідуального підходу. Під час оцінки ризиків важливо враховувати особливість кожного об'єкту, визначати активи інфраструктури, які потребують захисту, ідентифікувати загрози, ранжувати їх за критеріями та отримати актуальну стратегію захисту.

ВІЙСЬКОВИЙ ІНСТИТУТ
КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

ТЕЗИ ДОПОВІДЕЙ

Всеукраїнської науково-практичної конференції молодих вчених, ад'юнктів, слухачів, курсантів і студентів

"Молодіжна військова наука у Київському національному університеті імені Тараса Шевченка"

27 квітня 2023 року

За загальною редакцією начальника Військового інституту Київського національного університету імені Тараса Шевченка бригадного генерала Анатолія Шевченка

Київ – 2023

УДК 355(477)37
ББК 32.26.8-68.49

Збірник тез доповідей Всеукраїнської науково-практичної конференції молодих вчених, ад'юнктів, слухачів, курсантів і студентів "Молодіжна військова наука у Київському національному університеті імені Тараса Шевченка", м. Київ, 27 квітня 2023 р. Київ: Військовий інститут Київського національного університету імені Тараса Шевченка. Київ: ВІКНУ 2023. 430 с.

Рекомендовано до друку Вченою радою Військового інституту Київського національного університету імені Тараса Шевченка
(протокол від 20.04.2023 № 9).

Опубліковано тези доповідей молодих вчених, ад'юнктів, слухачів, курсантів і студентів Військового інституту Київського національного університету імені Тараса Шевченка, інших вищих військових та вищих навчальних закладів України, вітчизняних фахівців із: Актуальних питань гуманітарного розвитку Збройних Сил України; Технічних проблем озброєння і військової техніки та технологій подвійного призначення; Актуальних проблем військового права в умовах воєнного стану; Фінансів; Інформаційно-психологічної боротьби у воєнній сфері; Актуальних проблем лінгвістичного забезпечення Збройних Сил України; Актуальних проблем геопросторової підтримки військ в умовах ведення російсько-української війни; Медіакомунікацій Міністерства оборони України і Збройних Сил України в умовах правового режиму воєнного стану.

УДК 355(477)37
ББК 32.26.8-68.49

Грох А.О (ХмНУ)
канд.техн.наук, доц. Чешун В.М. (ХмНУ)
канд.техн.наук, доц. Орленко В.С. (ХмНУ)

ЗАГРОЗИ І РИЗИКИ КІБЕРБЕЗПЕКИ СИСТЕМ ЕЛЕКТРОННОГО УРЯДУВАННЯ

Електронне урядування стало сучасним та ефективним інструментом управління великою кількістю процесів в інформаційному просторі для підвищення якості життя громадян. Цей підхід широко використовується для забезпечення зв'язку між органами влади та громадою через застосування сучасних технологій та електронних засобів. Завдяки системам електронного урядування (СЕУ), громадяни мають можливість звернутися до органів влади через електронні портали, висловити свої пропозиції та ідеї, дізнатися про актуальні події та проєкти, скористатися електронними документами та послугами. Електронне урядування дозволяє забезпечити ефективну взаємодію між різними рівнями влади, у тому числі місцевими та державними органами влади.

Запровадження електронного урядування є необхідною умовою для успішної інтеграції України до ЄС і слід відзначити значні успіхи нашої держави у розвитку цього напрямку, прикладом чого є інноваційний проєкт Єдиного порталу державних послуг Дія.

Як і функціонування будь-яких інформаційних систем, робота СЕУ пов'язана з кіберзагрозами, що включають в себе атаки з використанням вірусів, троянських програм, шпигунського програмного забезпечення та інших зловмисних програм, хакерські атаки тощо [1]. Особливістю СЕУ є надзвичайно великі обсяги конфіденційної, а, подеколи, і секретної інформації, що приваблюють зловмисників і агентів держави-ворога в умовах повномасштабної війни (в кіберпросторі тощо).

Атаки можуть бути спрямовані на крадіжку конфіденційних даних, знищення інформації або системи, переривання роботи систем, на злам системи для різних злочинних цілей. Це пов'язано з традиційними ризиками втрати конфіденційності, цілісності або доступності інформації, але, через специфіку СЕУ можуть мати критичні наслідки. В [2] кіберзагрози СЕУ прирівнюються до загроз національній безпеці держави.

Через неоднорідність і складність СЕУ, оцінка загроз і ризиків у них потребує застосування технологій реверсінжинірингу систем у багаторівневу ієрархічну структуру програмних та технічних засобів і організаційних заходів з подальшим переходом до багаторівневої моделі загроз, ризиків і контрзаходів.

Список використаних джерел:

1. Хмелевський Р. М., Хмелевський Ю. М., Козачок В. А., Семко В. В., Ільїн О. О. Проблеми інформаційної безпеки та розвитку Системи електронного урядування в Україні. Сучасний захист інформації. 2018. №3(35).С. 71-78.

2. Чукут С.А. Тенденції та проблеми впровадження електронного урядування в Україні. URL: t.ly/ASJu (дата звернення: 05.04.2023).

ДОДАТОК Б

Презентація кваліфікаційної роботи

Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

Грох Антон Олександрович

Метод забезпечення кібербезпеки автоматизованих систем критичної інфраструктури газовидобувної компанії на основі оцінки ризиків

спеціальність 125 – Кібербезпека

Науковий керівник: к.т.н., доцент **Чешун Віктор Миколайович**

ЗАГАЛЬНА ХАРАКТЕРИСТИКА КВАЛІФІКАЦІЙНОЇ РОБОТИ МАГІСТРА

Мета кваліфікаційної роботи полягає у підвищенні ефективності інформаційної безпеки автоматизованих систем критичної інфраструктури газовидобувної компанії з-за допомогою ризик-орієнтованого підходу.

Об'єктом дослідження є інформаційна безпека та захист автоматизованих систем об'єктів критичної інфраструктури.

Предметом дослідження є метод та алгоритми оцінки інформаційних ризиків автоматизованих систем критичної інфраструктури газовидобувної компанії.

Наукова новизна отриманих результатів:

1. Побудовано модель автоматизованої системи об'єктів критичної інфраструктури на основі взаємозв'язків між фізичними, логічними активами та критичними процесами.

2. Розроблено метод, заснований на алгоритмах оцінки ризиків інформаційної безпеки автоматизованих систем об'єктів критичної інфраструктури, що дозволяє визначити актуальний рівень безпеки на відповідному об'єкті, засновуючись на основі аналізу та обробки ризиків.

Практична значимість отриманих результаті полягає в ефективній реалізації методу управління ризиками інформаційної безпеки автоматизованої системи критичної інфраструктури газовидобувної компанії та ідентифікувати критичні процеси, можливі вразливості комп'ютерної безпеки, моделювати загрози, виходячи з них, а також керувати ризиками інформаційної безпеки критичної інфраструктури.

Задачі досліджень у роботі формулюються наступним чином:

- визначити основні поняття та роль критичної інфраструктури у функціонуванні держави;
- проаналізувати сучасні методи та засоби забезпечення інформаційної безпеки об'єктів критичної інфраструктури;
- розробити математичну модель ієрархічної структури автоматизованої системи управління технологічними процесами газовидобувної компанії;
- розробити метод оцінки ризиків кібербезпеки в автоматизованих системах;
- виконати апробацію запропонованих теоретичних і алгоритмічних рішень.

В основі методів дослідження лежать базові положення інформаційної безпеки, теорії множин. В роботі було використано такі методи дослідження, як аналіз, синтез, математичне моделювання.

Апробація роботи. Наукові результати і основні положення магістерської роботи доповідались і обговорювались на Всеукраїнській і 2-х міжнародних науково-практичних конференціях.

Публікації. За темою магістерської роботи опубліковано тези доповідей на Всеукраїнській та 2-х міжнародних науково-практичних конференціях.

ІЄРАРХІЧНА СТРУКТУРА АВТОМАТИЗОВАНОЇ СИСТЕМИ УПРАВЛІННЯ ТЕХНОЛОГІЧНИМИ ПРОЦЕСАМИ ГАЗОВИДОБУВНОЇ КОМПАНІЇ

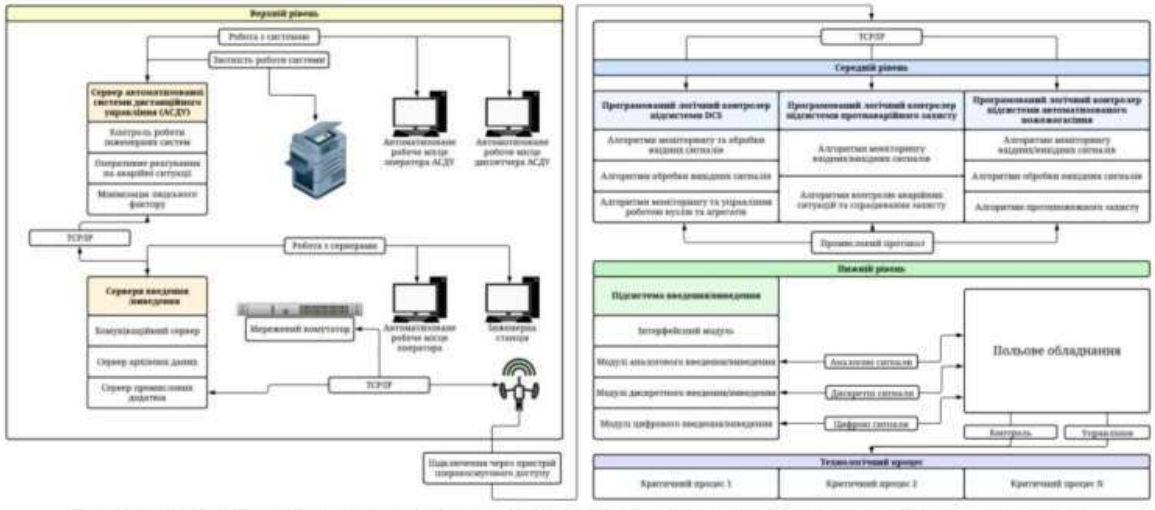


Схема ієрархічної структури типової автоматизованої системи управління технологічними процесами

Висновок 1 : Автоматизована система управління технологічними процесами має складну, ієрархічну структуру, що зумовлює необхідність особливого підходу до забезпечення кібербезпеки.

Завдання 1 : Створити математичну модель автоматизованої системи управління технологічними процесами.

Завдання 2 : Розробка методу, заснованого на алгоритмах оцінки ризиків інформаційної безпеки з урахуванням збитків від реалізації загроз, які експлуатують вразливості системи та мають безпосередній вплив на активи.

МАТЕМАТИЧНА МОДЕЛЬ АСУ ТП

Модель критичних процесів

$$M_{\text{кр.пр.}} = (A_{\text{тех.пр.}}, A_{\text{конт.упр.}}, G_{\text{кр.пр.}})$$

$A_{\text{тех.пр.}} = A_{\text{кр.пр.}} \cup A_{\text{нижн.}}$ – **множина елементів технологічного процесу;**

$A_{\text{конт.упр.}} = A_{\text{конт.}} \cup A_{\text{упр.}}$ **- множина процесів по контролю та управлінню критичних процесів;**

$G_{\text{кр.пр.}} = (A_{\text{тех.пр.}}, A_{\text{конт.упр.}})$ – **формалізація структури взаємодії критичних процесів;**

$M_{\text{кр.пр.}} = (A_{\text{тех.пр.}}, A_{\text{конт.упр.}}, G_{\text{кр.пр.}})$

Модель технічного забезпечення

$$M_{\text{тех.заб.}} = (A_{\text{тех.заб.}}, \quad G_{\text{фіз.струк.}})$$

$A_{\text{тех.заб.}} = A_{\text{нижн.}} \cup A_{\text{середн.}} \cup A_{\text{верхн.}} \cup A_{\text{зас.зв.}}$ – **множина елементів технічного забезпечення;**

$G_{\text{фіз.струк=}}(A_{\text{тех.заб.}}, A_{\text{кан.зв.}})$ – **формалізація фізичної структури.**

Модель програмного забезпечення

$$M_{\text{прог.заб.}} = (A_{\text{прог.заб.}}, A_{\text{тех.зас}}, K^{\text{тех.зас.}}_{\text{заг.прог.заб}}, G_{\text{лог.струк.}})$$

$A_{\text{прог.заб.}} = A_{\text{заг.прог.заб.}} \cup A_{\text{баз.прог.заб.}} \cup A_{\text{прик.прог.заб.}} \cup A_{\text{IT серв.}}$ – **множина елементів ПЗ;**

$A_{\text{тех.зас.}} \subseteq A_{\text{тех.заб.}}$ – **підмножина технічних засобів з встановленим програмним забезпеченням;**

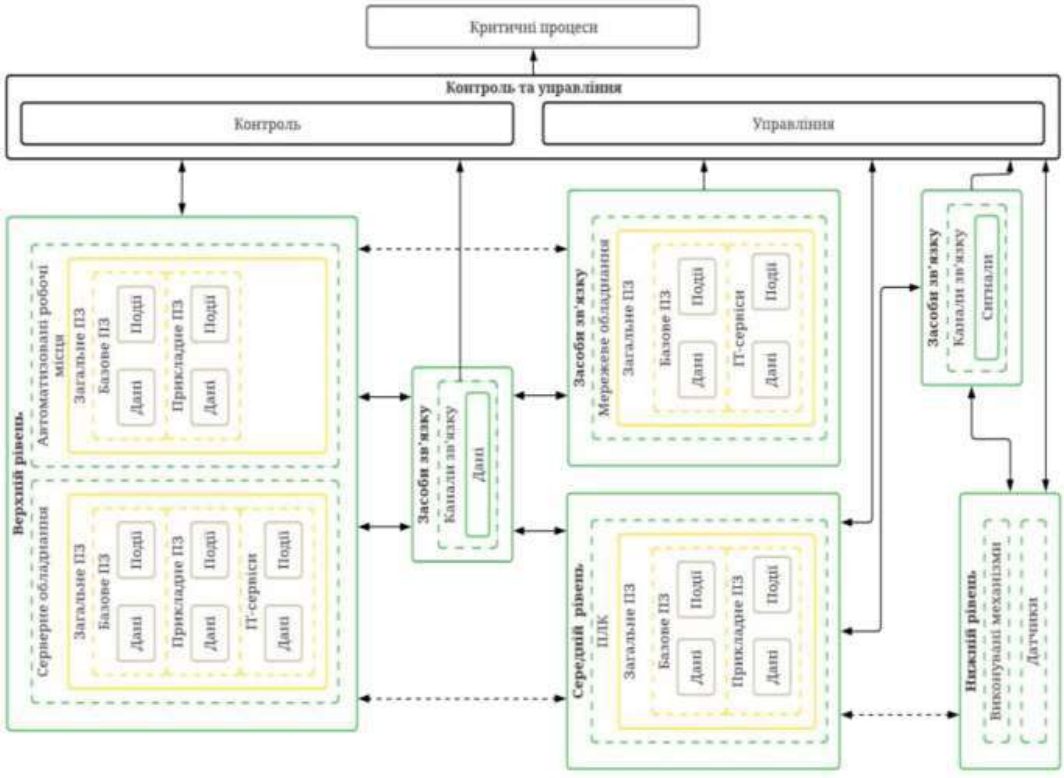
$K^{\text{тех.зас.}}_{\text{заг.прог.заб}}: A_{\text{тех.зас}} \times A_{\text{заг.прог.заб.}} \to \{0,1\}$ – **співвідношення, що визначає встановлення загального програмного забезпечення на конкретний технічний засіб;**

$G_{\text{лог.струк.}} = (A_{\text{прог.заб.}}, A_{\text{інф.заб.}})$ – **формалізація логічної структури.**

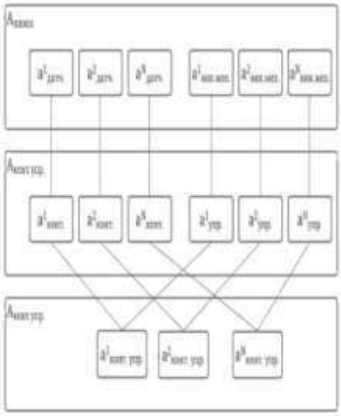
Модель автоматизованої системи управління технологічними процесами

$$M_{\text{авт.сис}} = (M_{\text{кр.пр.}}, M_{\text{тех.заб.}}, M_{\text{прог.заб.}})$$

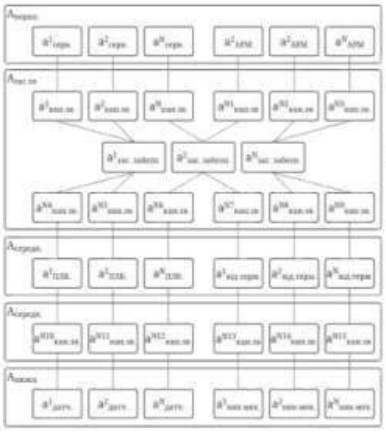
СТРУКТУРНО-ЛОГІЧНА СХЕМА ВЗАЄМОЗВ'ЯЗКУ ЕЛЕМЕНТІВ АСУ ТП



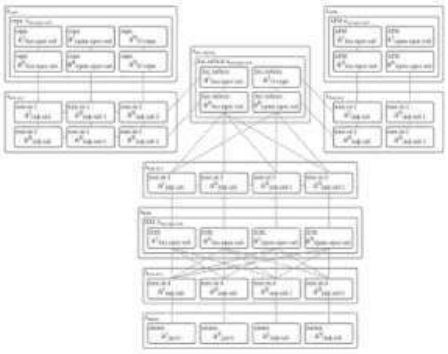
СХЕМАТИЧНЕ ЗОБРАЖЕННЯ МОДЕЛЕЙ КРИТИЧНИХ ПРОЦЕСІВ, ТЕХНІЧНОГО ЗАБЕЗПЕЧЕННЯ, ВЗАЄМОДІЇ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ



Модель критичних процесів АСУ ТП



Модель технічного забезпечення



Модель логічної взаємодії програмного забезпечення

Основні положення методу

- Основна мета методу – управління кіберризиками автоматизованих систем критичної інфраструктури газовидобувної компанії на основі оцінки ризиків.
- Математичною основою методу є структурно-логічна модель ієрархії активів АСУ ТП, моделі критичних процесів, технічного забезпечення, логічної взаємодії програмного забезпечення та модель загроз.
- Метод побудований на основі алгоритмів оцінки критичних процесів, активів, розподілення заходів оброки ризиків, розрахунку збитків від реалізації загрози автоматизованої системи управління технологічними процесами газовидобувної компанії.

СХЕМИ ВИКОНАННЯ АЛГОРИТМІВ ОЦІНКИ ВАЖЛИВОСТІ КРИТИЧНИХ ПРОЦЕСІВ ТА АКТИВІВ

Блок-схема виконання алгоритму оцінки важливості критичних процесів

Блок-схема виконання алгоритму оцінки важливості активів

СХЕМИ ВИКОНАННЯ АЛГОРИТМІВ РОЗПОДІЛУ ПО РІВНЯМ ЗАХИСТУ, ОЦІНКИ ЗБИТКІВ ПРИ РЕАЛІЗАЦІЇ, ЕКСПЛУАТАЦІЇ ТА ОЦІНКИ ВІРОГІДНОСТІ РЕАЛІЗАЦІЇ ЗАГРОЗИ

Алгоритм розподілу по рівням захисту

Алгоритм оцінки збитків при реалізації загрози

Алгоритм оцінки збитків при експлуатації загрози

Алгоритм оцінки вірогідності реалізації загрози

АПРОБАЦІЯ МЕТОДУ

Таблиця 4.11 – Оцінка важливості критичних процесів

$A_{\text{кр.пр.}}$	$L^n_{\text{вит.}}$	$L^n_{\text{втр.}}$	$L^n_{\text{ч.}}$	$L^n_{\text{кр.пр.}}$
$a^1_{\text{кр.пр.}}$	29800	24100	5800	(29800, 24100, 5800)
$a^2_{\text{кр.пр.}}$	29500	28000	5500	(29500, 28000, 5500)
$a^3_{\text{кр.пр.}}$	30000	29300	7000	(30000, 29300, 7000)
$a^4_{\text{кр.пр.}}$	30500	29800	7500	(30500, 29800, 7500)
$a^5_{\text{кр.пр.}}$	29800	24100	5800	(29800, 24100, 5800)
$a^6_{\text{кр.пр.}}$	35000	29100	9500	(35000, 29100, 9500)
$a^7_{\text{кр.пр.}}$	28300	26300	5500	(28300, 26300, 5500)
$a^8_{\text{кр.пр.}}$	29800	24100	5800	(29800, 24100, 5800)
$a^9_{\text{кр.пр.}}$	33500	31000	9800	(33500, 31000, 9800)
$a^{10}_{\text{кр.пр.}}$	34200	31500	9700	(34200, 31500, 9700)
$a^{11}_{\text{кр.пр.}}$	29800	24100	5800	(29800, 24100, 5800)
$a^{12}_{\text{кр.пр.}}$	23800	24000	5500	(23800, 24000, 5500)

Таблиця 4.13 – Оцінка важливості множини технічного забезпечення

$A_{\text{тех.заб.}}$	$L^{n\ \text{тех.заб.}}_{\text{вит.}}$	$L^{n\ \text{тех.заб.}}_{\text{втр.}}$	$L^{n\ \text{тех.заб.}}_{\text{ч.}}$	$L^n_{\text{тех.заб.}}$
$A_{\text{верхн.}}$	45520	34866	17480	(45520, 34866, 17480)
$A_{\text{середн.}}$	22760	17432	17480	(22760, 17432, 17480)
$A_{\text{нижн.}}$	22760	34866	43700	(22760, 34866, 43700)
$A_{\text{заг.зн.}}$	22760	17432	8740	(22760, 17432, 8740)

Таблиця 4.14 – Оцінка важливості множини технічних засобів

$A_{\text{тех.зас.}}$	$L^{n\ \text{тех.зас.}}_{\text{вит.}}$	$L^{n\ \text{тех.зас.}}_{\text{втр.}}$	$L^{n\ \text{тех.зас.}}_{\text{ч.}}$	$L^n_{\text{тех.зас.}}$
$a^1_{\text{серв.}}$	15172	11622	5826	(15172, 11622, 5826)
$a^2_{\text{серв.}}$	4138	3168	1588	(4138, 3168, 1588)
$a^3_{\text{серв.}}$	5516	4223	2118	(5516, 4223, 2118)
$a^4_{\text{серв.}}$	2758	2112	1058	(2758, 2112, 1058)
$a^5_{\text{серв.}}$	2758	2112	1058	(2758, 2112, 1058)
$a^1_{\text{АРМ}}, \dots a^5_{\text{АРМ}}$	9654	7394	3706	(9654, 7394, 3706)
$a^1_{\text{ПЛК}}, \dots a^{12}_{\text{ПЛК}}$	1516	1162	1164	(1516, 1162, 1164)
$a^1_{\text{датч.}}, \dots a^{64}_{\text{датч.}}$	76	116	146	(76, 116, 146)
$a^1_{\text{вик.мех.}}, \dots a^{64}_{\text{вик.мех.}}$	152	232	292	(152, 232, 292)
$a^1_{\text{зас.забезп.}}, \dots a^{12}_{\text{зас.забезп.}}$	3416	2666	1600	(3416, 2666, 1600)
$a^1_{\text{канл.зв}}, \dots a^{90}_{\text{канл.зв.}}$	74	36	28	(74, 36, 28)

Таблиця 4.16 – Оцінка збитків при реалізації загроз

E	$L^{e^n}_A$	$L^n_{\text{вит.}}$	$L^n_{\text{втр.}}$	$L^n_{\text{ч.}}$	L^n_E
e^4	(910, 696, 348)	1	1	362	64594
e^9	(17760, 13440, 6720)	1	1	22	105120

Таблиця 4.17 – Оцінка збитків при експлуатації вразливостей

E	$L^{e^n}_A$	$L^n_{\text{вит.}}$	$L^n_{\text{втр.}}$	$L^n_{\text{ч.}}$	CVSS	L^n_B
e^1	(1390, 1064, 794)	0,8	0,9	216	0,95	87878
e^2	(39712, 30414, 15232)	1	0,9	22	0,95	234636
e^3	(974, 746, 374)	0,9	0,9	362	0,98	69414
e^5	(4524, 3413, 1734)	0,9	0,8	104	1	97988
e^6	(974, 746, 374)	0,9	0,9	294	0,98	56788
e^7	(5138, 3926, 1968)	0,9	0,9	124	1	130898
e^8	(39712, 30414, 15232)	1	1	20	0,86	216886
e^{10}	(10448, 7994, 3998)	0,9	0,9	54	0,88	124544
e^{11}	(11422, 8740,4372)	1	1	22	0,84	142578

Таблиця 4.18 – Результати виконання алгоритму оцінки вірогідності реалізації загрози

E	j^n
e^1	0,69
e^2	0,31
e^3	0,85
e^4	0,76
e^5	0,67
e^6	0,79
e^7	0,54
e^8	0,39
e^9	0,70
e^{10}	0,75
e^{11}	0,59

ВИСНОВКИ

В магістерській роботі розглядається важлива галузь інформаційної безпеки – управління кіберризиками автоматизованих систем критичної інфраструктури газовидобувної компанії на основі оцінки ризиків.

– Визначено основні поняття критичної інфраструктури та її роль у сучасному світі. Зокрема ми дійшли до висновку, що критична інфраструктура є ключовою для функціонування держави та суспільства, охоплює захист життєво необхідних інтересів людини, громадянина, суспільства та держави в кіберпросторі.

– Розглянуто нормативне забезпечення кібербезпеки на об'єктах критичної інфраструктури та зазначено, що визначення поняття кібербезпеки в національному та міжнародному законодавстві.

– Визначено поняття автоматизованих систем та систем управління технологічними процесами об'єктів критичної інфраструктури.

– Розроблено теоретико-множинну модель автоматизованої системи управління технологічними процесами газовидобувної компанії, яка відрізняється наявністю опису взаємодії активів різних рівнів відповідно до ієрархічної структури автоматизованої системи управління технологічними процесами. Модель відображає логічну та фізичну структури взаємодії між активами, а також вплив на критичні процеси автоматизованої системи управління технологічними процесами газовидобувного підприємств, що дозволяє здійснити аналіз характеристик технічних та програмних засобів, технологічних процесів та в подальшому ефективно використовувати отримані результати для оцінки ризиків інформаційної безпеки.

– Розроблено метод оцінки ризиків інформаційної безпеки автоматизованої системи управління технологічними процесами газовидобувної компанії на основі відповідних алгоритмів.

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Гроха Антона Олександровича
ПІБ здобувача вищої освіти

Студента ФІТ, 2 курсу, групи КБм-22-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у хмельницькому національному університеті» від 31.08.2023, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

05.12.23
дата

підпис

UNICHECK
by Turnitin

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1015996473

Дата перевірки:
12.12.2023 10:36:03 EET

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
12.12.2023 10:44:56 EET

ID користувача:
100008300

Назва документа: **Грох на плагіат**

Кількість сторінок: 88 **Кількість слів:** 14984 **Кількість символів:** 114877 **Розмір файлу:** 1.84 MB **ID файлу:** 1015679365

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

12.5%
Схожість

Найбільша схожість: 1.29% з Інтернет-джерелом (http://www.lute.lviv.ua/fileadmin/www.lac.lviv.ua/data/kafedry/Kome.

12.2% Джерела з Інтернету	647	Сторінка 90
0.81% Джерела з Бібліотеки	41	Сторінка 93

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи	850
Підозріле форматування	24 сторінки

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 0.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 10%**

	Документ		Сумарний збіг по Базі Даних	
ID: 122668 Назва: Метод забезпечення кібербезпеки автоматизованих систем критичної інфраструктури газовидобувної компанії на основі оцінки ризків Додано в БД: 2023-12-12 Автора: Грох А.О. Керівники: Чешун В.М. Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	82500	1214	1232 (1%)	16 (1%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:
Назва: Метод забезпечення кібербезпеки автоматизованих систем критичної інфраструктури газовидобувної компанії на основі оцінки ризиків

Автор: Грох Антон Олександрович

Спеціальність: 125 – Кібербезпека

Освітня програма: освітньо-професійна

Науковий керівник: Чешун Віктор Миколайович, к.т.н, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Згідно з правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 31.08.2023 р. для кваліфікаційних робіт освітньо-професійних програм підготовки здобувачів другого (магістерського) рівня вищої освіти встановлюється мінімально допустимий рівень унікальності тексту робіт, що допускаються до захисту, на рівні 75%.

Оригінальність тексту представленої на розгляд роботи за результатами перевірки системою Unichek складає 87,5%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 100%, що відповідає вимогам Положення.

Запозичення, виявлені у роботі, є законними і не є плагіатом, оскільки:

1) виявлені системою Unicheck збіги сукупно адресуються до 647 джерел інтернету і 41 джерела з бібліотеки ХНУ;

2) запозичення, виявлені в тексті роботи, є фрагментарними або мають належним чином оформленні посилання;

3) максимальний збіг з одним джерелом не перевищує 1.29% і оформлений посиланнями;

4) у тексті кваліфікаційної роботи системою перевірки на плагіат Unicheck виявлено схожість з деякими документами у частині загальновживаних обов'язкових словосполучень у стандартних бланках (титулка), у структурі змісту, у назвах розділів/підрозділів тощо;

5) виявлені модифікації тексту відносяться суто до математичних формул та не є модифікаціями тексту і не впливають на відсоток схожості.

Керівник роботи _____ В.М. Чешун

Гарант ОП _____ В.Ю. Тітова

Завідувач кафедри кібербезпеки _____ Ю.П. Кльоц

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «магістр»

Студент Грох Антон Олександрович

Тема Метод забезпечення кібербезпеки автоматизованих систем критичної інфраструктури газовидобувної компанії на основі оцінки ризиків

Спеціальність 125 – Кібербезпека

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «магістр»:

кількість листів креслень - ; кількість сторінок записки 92

1. Короткий зміст роботи та прийнятих рішень В роботі розглянуто сучасні підходи до забезпечення інформаційної безпеки автоматизованих систем об'єктів критичної інфраструктури. Визначено основні поняття, методи та засоби для побудови відповідних рішень, проаналізовано сучасні підходи до аналізу ризиків автоматизованих систем об'єктів критичної інфраструктури. Розроблено метод забезпечення кібербезпеки автоматизованих систем управління технологічними процесами, модель критичних процесів, технічного та програмного забезпечення критичної інфраструктури газовидобувної компанії.

2. Висновок про відповідність кваліфікаційної роботи завданню Кваліфікаційна робота відповідає поставленому завданню як в теоретичній, так і в практичній частині

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі подана загальна характеристика поставленої задачі, чітко визначено об'єкт, предмет та методи дослідження, сформульована актуальність; визначені задачі, які необхідно вирішити для досягнення поставленої мети, практична цінність отриманих результатів, їхня новизна та наведені відомості про публікації. В першому розділі изначено основні поняття критичної інфраструктури та її роль у сучасному світі. Зокрема ми дійшли до висновку, що критична інфраструктура є ключовою для функціонування держави та суспільства, оскільки включає в себе набір об'єктів та систем, від яких залежить національна безпека, стабільність та обороноздатність країни, а також повсякденне життя громадян. В другому розділі розроблено теоретико-множинну модель автоматизованої системи управління технологічними процесами газовидобувної компанії, яка відрізняється наявністю опису взаємодії активів різних рівнів відповідно до ієрархічної структури автоматизованої системи управління технологічними процесами. В третьому розділі розроблено метод оцінки ризиків інформаційної безпеки автоматизованої системи управління технологічними процесами газовидобувної компанії на основі відповідних алгоритмів. Четвертий розділ присвячений апробації методу.

4. Позитивні сторони роботи Кваліфікаційна робота містить актуальні рішення і пропозиції, орієнтовані на вдосконалення і розширення можливостей управління ризиками інформаційної безпеки автоматизованої системи критичної інфраструктури газовидобувної компанії та ідентифікувати критичні процеси, можливі вразливості комп'ютерної безпеки, моделювати загрози, виходячи з них, а також керувати ризиками інформаційної безпеки критичної інфраструктури.

5. Негативні сторони роботи В роботі не здійснено аналіз особливостей застосування методу на конкретному прикладі діючої газовидобувної компанії України

6. Оцінка графічного оформлення та пояснювальної записки роботи Оформлення всіх матеріалів кваліфікаційної роботи є якісним, здійснене з дотриманням актуальних стандартів та інституційних положень ХНУ. Пояснювальна записка відповідає нормам щодо її оформлення як за структурою, так і за представленням і форматуванням матеріалу.

7. Відгук про роботу в цілому Кваліфікаційна робота заслуговує позитивної оцінки. Весь матеріал кваліфікаційної роботи структурований, чіткий та наскрізно пов'язаний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. Презентаційний та ілюстративний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої мети.

8. Інші зауваження -

9. Оцінка кваліфікаційної роботи Враховуючи всі позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що вона заслуговує оцінку «добре».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)
Підченко Сергій Костянтинович
Завідувач кафедри ТМІТ, доктор технічних наук, професор

« 14 » 12 2023. (підпис)