НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

«До захисту допущено»
В.о. завідувача кафедри

_____ М.В.Грайворонський
(підпис)

“____”_____2019 р.

Дипломна робота

на здобуття ступеня бакалавра

з напряму підготовки 6.040301 «Прикладна математика» на тему:
Синтез структури системи захисту інформації на об`єктах критичної інфраструктури

Виконала: студентка _4___ курсу, групи ____ФІ-51_____
(шифр групи)

Сітко Дарина Павлівна _____ _____
(прізвище, ім’я, по батькові) (підпис)

Керівник_проректор з наук.-пед. роботи, д.т.н., проф. Новіков О.М. ___ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____ _____ _____
(назва розділу) (посада, вчене звання, науковий ступінь, прізвище, ініціали) (підпис)

Рецензент_____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ - 2019 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – перший (бакалаврський)

Напрям підготовки 6.040301 «Прикладна математика»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ М.В.Грайворонський
(підпис)
«___»_____2019 р.

ЗАВДАННЯ
на дипломну роботу студенту

Сітко Дарини Павлівни
(прізвище, ім'я, по батькові)

1. Тема роботи Синтез структури системи захисту інформації на об'єктах критичної інфраструктури _____
_____,
науковий керівник роботи Новіков Олексій Миколайович, д.т.н, професор
_____,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом по університету від «____ » 2019 р. № _____

2. Термін подання студентом роботи 10 червня 2019 р.

3. Вихідні дані до роботи _____
_____
_____

4. Зміст роботи _____
_____
_____
_____
_____

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо) _____
_____
_____
_____

6. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка

Студент _____ _____
(підпис) (ініціали, прізвище)

Керівник роботи _____ _____
(підпис) (ініціали, прізвище)

РЕФЕРАТ

Дипломна робота «СИНТЕЗ СТРУКТУРИ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ»: 47 с., 4 рис., 4 таблиці, 22 джерела посилання.

Об'єктом дослідження є розподілена система автоматичного керування (САК) критично важливими об'єктами інфраструктури (КВОІ), що складається із *c* компонентів, які приймають участь в обробці інформації й управлінні об'єктом та взаємодіють між собою.

Предметом дослідження є синтез системи захисту інформації на САК КВОІ.

Мета роботи полягає у розробці підходу до синтезу структури системи захисту інформації в системах автоматичного керування (САК) критично важливими об'єктами з використанням методів теорії ігор, а також забезпечення рівня захищеності, що є необхідним, використовуючи мінімальну кількість витрат на системи захисту інформації та умови якщо характер атак зловмисника буде комплексним.

Методи. Методика дипломної роботи носить комплексний характер та спирається на мету і завдання дослідження. Розроблено алгоритм реалізації підходу до вирішення питання побудови СЗІ на основі методів теорії ігор, експертної оцінки та математичного програмування у випадку обмеження кількості ресурсів.

Наукова новизна даної роботи полягає в застосуванні підходу до вирішення питання побудови СЗІ у випадку обмеження кількості ресурсів на системах автоматичного керування ГТС України.

Результати дипломної роботи рекомендується використовувати для розв'язання практичних проблем, пов'язаних з захистом критично-важливих об'єктів від атак зловмисників, в практичній діяльності студентів, які зіштовхуються з проблемами захисту інформації. Подальший розвиток підходу може бути спрямований на аналіз ситуацій із неповною інформацією,

за умови якщо одна або обидві сторони, що конфліктують не володіють інформацією про здійснені ходи суперника.

Ключові слова: критично важливі об’єкти інфраструктури, теорія ігор, системи захисту інформації, зловмисник, позиційна гра.

ABSTRACT

Graduate work «SYNTHESIS OF THE INFORMATION SECURITY SYSTEM STRUCTURE AT THE OBJECTS OF CRITICAL INFRASTRUCTURE»: 47 pages, 4 drawings, 4 tables, 22 sources.

The object of the study is a distributed automatic control system of critical infrastructure objects, which consists of C interacting components involved in the processing of information and control an object.

The subject of the study is the synthesis of the information security system (ISS) at the automatic control system of critical infrastructure objects.

The aim of the work is to develop the approach to the synthesis of the information security system structure at the automatic control system of critical infrastructure objects using the game theory and to provide the necessary protection level with minimum items used at ISS, provided complex character of the attacks.

Methods. The research methodology is determined by the purpose and tasks of the work and is of a complex nature. The algorithm of the approach implementation to the solution of the problem of information security system is developed under the condition of resource constraints on the basis of expert estimation methods, game theory and mathematical programming.

The scientific novelty of this work is to apply the approach with the aim of solving the problem of information security system development due to the limited resources which are used at automatic control system of the GTS of Ukraine.

The results of the graduate work are recommended to use for solving practical problems related with the protection of critical infrastructure objects from attacks, as well as in the practical work of students who encounter the problems of information security. The further development of the approach may be aimed at analyzing situations with incomplete information, for cases where one or both conflicting parties do not have information about the opponent's moves.

Keywords: critical infrastructure objects, game theory, information security systems, attacker, positional game.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

СЗІ – система захисту інформації.

САК – система автоматичного керування.

КВОІ – критично важливий об`єкт інфраструктури.

ДПКС - диспетчерський пункт компресорних станцій.

КС – коспресорна станція.

ВСТУП

У даний час спостерігається тенденція інтенсивного збільшення числа комп'ютерних інцидентів, пов'язаних з впливом комп'ютерних атак на критично важливі об'єкти інфраструктури (КВОІ) через глобальні інформаційні мережі, магістральне цифрове комунікаційне обладнання і несанкціоноване підключення зовнішніх електронних носіїв інформації.

Під КВОІ у всьому світі прийнято розуміти об'єкти, порушення (або припинення) функціонування яких призводить до втрати управління економікою або адміністративно-територіальними одиницями, їх невиправданої зміни (руйнування) або ж до істотного зниження безпечної життєдіяльності населення, яке проживає на цих територіях, на тривалий період часу.

Актуальність дослідження. Синтез структури системи захисту інформації (СЗІ) для забезпечення безвідмовної роботи об`єктів критичної інфраструктури має важливе значення в умовах зростаючої кількості атак на КВОІ та значущості самих КВОІ. Зокрема, актуальним вважаємо вирішення проблем науково-технічного характеру, які мають місце на об’єктах газотранспортної системи (ГТС) України через масштабність і стратегічне значенні газотранспортної галузі.

Мета роботи полягає у розробці підходу до синтезу структури системи захисту інформації в системах автоматичного керування САК критично важливими об’єктами з використанням методів теорії ігор, а також забезпечення рівня захищеності, що є необхідним, використовуючи мінімальну кількість витрат на системи захисту інформації та умови якщо характер атак зловмисника буде комплексним.

Реалізація поставленої мети передбачає розв’язання низки наступних **завдань**:

1) ретельно дослідити та проаналізувати вихідну інформацію з використанням методів експертної оцінки;

2) проаналізувати структуру САК, визначити кількість її компонентів та інформаційних потоків між ними, здійснити оцінку цінності компонентів для функціонування системи;

3) виявити та прооаналізувати вразливості, що характерні для систем із обраною архітектурою та технологіями;

4) проаналізувати та схарактеризувати загрози, що можуть бути реалізовані використовуючи наявні вразливості;

5) визначити релевантні механізми захисту;

6) здійснити синтез структури системи захисту інформації.

Об'єктом дослідження є розподілена САК КВОІ, що складається із *c* компонентів, які приймають участь в обробці інформації й управлінні об'єктом та взаємодіють між собою.

Предметом дослідження є синтез системи захисту інформації на САК КВОІ

Наукова новизна даної роботи полягає в застосуванні підходу до вирішення питання побудови СЗІ у випадку обмеження кількості ресурсів на системах автоматичного керування ГТС України.

Методи. Методика дипломної роботи носить комплексний характер та спирається на мету і завдання дослідження. Розроблено алгоритм реалізації підходу до вирішення питання побудови СЗІ на основі методів теорії ігор, експертної оцінки та математичного програмування у випадку обмеження кількості ресурсів.

1 ТЕОРЕТИКО-МЕОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

1.1 Побудова системи захисту інформації для протидії протиправним діям зловмисника

Захисту від можливих атак зловмисників потребують сучасні системи автоматичного керування (САК). Через побудову системи захисту інформації (СЗІ), яка є комплексом технічних і технологічних засобів, організаційних заходів, що перешкоджають несанкціонованому доступу до інформації може бути забезпечена безпека інформації. Надзвичайно важливо зважати на дії зловмисника під час побудови СЗІ через організацію простих (одноетапних) або комплексних атак, які містять набір взаємозв'язаних етапів. який реалізує загрози для САК. Як стверджують В.В. Глушак та О.М. Новіков етапами комплексної атаки є розвідка, проникнення (власне атака) та зачищення слідів атаки [3].

На нинішньому етапі запропоновано низку емпіричних та формальних методів, які спрямовано на вирішення завдання синтезу СЗІ. Мета такого завдання полягає в забезпеченні ефективного захисту від зловмисника. Тому важливим та складним завданням, яке може базуватися як на формальному так і неформальному підходах вважається побудова СЗІ задля супротиву протиправним діям зловмисника.

Широке застосування отримав логіко-ймовірнісний підхід, що забезпечує захист структурно-складних систем. Означений метод отримав свою розробку та поширення в працях аких вчених як Є.Д. Солженцева, І.А. Рябініна, О.С. Можаєва, Г.М. Черкасова, та інших [3]. Подальший розвиток та результати застосування такого підходу для завдань інформаційної безпеки подають в своїх роботах такі вчені як В.В. Глушак, О.М. Новіков, А.М. Родіонов та інші [1; 2].

Створення сукупності механізмів захисту, у відповідності до заданих вимог щодо ефективності протидії зловмиснику становить мету процесу побудови системи захисту інформації, який включає в себе етапи: 1) аналізу системи; 2) вибір механізмів захисту; 3) оцінка ефективності системи.

У випадку виявлення недостатньої ефективності СЗІ на етапі її оцінки, процес вибору механізмів буде повторюватися аж доки не вирішиться поставлене завдання.

Власне від кваліфікованості розробника залежить якість синтезу структури СЗІ. Підходи, що грунтуються на формальних методах синтезу, зокрема, математичному програмуванні та дослідженні операцій застосовуються задля зменшення впливу розробника, як стверджують О.М. Новіков та М.В. Грайворонський [2].

Побудова системи захисту інформації здійснюється з використанням математичного апарату теорії ігор, а саме передбачає прийняття рішень в умовах невизначеності з урахуванням конфліктних взаємовідносин суб'єктів системи, володіючи інформацією про стани системи, можливі рішення та «виграші» від обраних рішень. Будемо застосовувати позиційну гру. Позиційна гра це гра з класу ігор, що описують конфліктні ситуації, розвиток яких здійснює вплив на поведінку гравців. В процесі гри ми переходимо від одного стану гри до іншого, вибираючи при цьому дії із множини доступних альтернатив. На етапі сьогодення для зазначених вище завдань, теорія ігор широко застосовується в різних сферах народного господарства, а також в інформаційних технологіях, економіці, промисловості й військовій справі [7].

З огляду на означене, уважаємо, що мінімізація витрат на формування СЗІ та важливість забезпечення необхідного рівня захищеності є на нинішній момент актуальною задачею. Таким чином, такий критерій можливо вивести із моделі, розробленої в термінах теорії ігор.

1.2 Критично важливі об`єкти інфраструктури в умовах комп'ютерних атак

У даний час спостерігається тенденція інтенсивного збільшення числа комп'ютерних інцидентів, пов'язаних з впливом комп'ютерних атак на критично важливі об'єкти інфраструктури (КВОІ) через глобальні інформаційні мережі, магістральне цифрове комунікаційне обладнання і несанкціоноване підключення зовнішніх електронних носіїв інформації.

Під КВОІ прийнято розуміти об'єкти, порушення (або зупинка) функціонування яких призведе до втрати управління економікою або адміністративно-територіальними одиницями, їх невиправданої зміни (руйнування) або ж до істотного зниження безпечної життєдіяльності населення, яке проживає на цих територіях, на тривалий період часу.

До критично важливих інформаційних об'єктів належать сучасні комп'ютеризовані елементи та інформаційні ресурси систем управління енергетики, транспорту, зв'язку, міської інфраструктури, промислових підприємств.

Часто обговорювана останнім часом [10] проблема КВОІ полягає в наступному: майже у всіх найважливіших секторах економіки існують системи, елементи яких настільки далеко рознесені в просторі, що економічними методами практично неможливо повністю захистити всі об'єкти навіть одного з секторів, не кажучи вже про систему цілком. Головною проблемою особи, що приймає рішення в галузі забезпечення безпеки функціонування подібних систем, (далі - ОПР) є питання оцінки наявних загроз і ризиків, які є значущими як для системи в цілому, так і для її елементів, і визначення пріоритетності захисту елементів і об'єктів КВОІ з урахуванням наявних в розпорядженні ресурсів.

Крім величезних розмірів багато секторів економіки настільки складні, що технологічно і економічно неможливо передбачити і прорахувати всі

наслідки будь якого інциденту, незалежно від того, чи викликаний він зловмисними діями людей або природними катаклізмами. Як правило, вкрай важко передбачити наслідки малих збурень в одній частині КВОІ для інших її ділянок.

Наприклад, всі комунікації в мережі інтернет в Південній Африці були повністю припинені внаслідок падіння веж-близнюків у результаті терористичної атаки на США 9 вересня 2001 р. відносно незначні несправності в електричних мережах компанії First Energy Corp. в Огайо (США) прискорили в серпні 2003 р блекаут, що торкнулася 50 млн чол. за тисячі кілометрів від джерела проблеми. По суті, існуюча інфраструктура уразлива просто тому, що вона містить настільки багато взаємопов'язаних компонентів, що аналіз їх взаємодій перетворюється в нездійсненне завдання для більшості технічних консультантів, аналітиків і ОПР, що визначають політику безпеки системи.

До факторів що створюють ризик доцільно віднести [11; 43]: терористична небезпека території, терористична загрози для розміщених на розглядаємій території об'єктів, вразливість (або захищеність) об'єктів по відношенню до терористичних дій, наслідки руйнування (припинення функціонування) об'єкта для розглянутого суб'єкта і сприйняття терористичного ризику населенням на розглянутій території. Показники, що враховують ці чинники, є умовними, а комплексний показник, який можна інтерпретувати як імовірність складної події, визначається добутком показників по окремим подіям.

Реалізація загроз несанкціонованого впливу на системи автоматизації та їх компоненти може привести до порушення режиму функціонування або збою в технологічному процесі. Виходячи з цього до КВОІ в Україні можна віднести:

- електроенергетику та атомну енергетику;
- газотранспортну систему (ГТС);
- хімічну промисловість;
- автомобільні магістралі;

- систему телекомунікацій тощо.

З метою забезпечення необхідного рівня інформаційної безпеки КВОІ доцільно завчасно оцінити їх реальний рівень захищеності і стійкості функціонування в умовах комп'ютерних атак.

1.3 Газотранспортна система України як критично важливий об`єкт інфраструктури

У роботі буде розглядатися КВОІ ГТС України. Газотранспортна система (ГТС) України – це єдиний технологічний комплекс, що виконує дві основні функції: транспортування і розподіл природного газу споживачам України та транзит природного газу територією України до країн Центральної та Західної Європи. Основними елементами системи є магістральні трубопроводи, газорозподільні, газовимірювальні станції та зв’язані з ними підземні сховища газу і компресорні станції. (рис. 1.1)

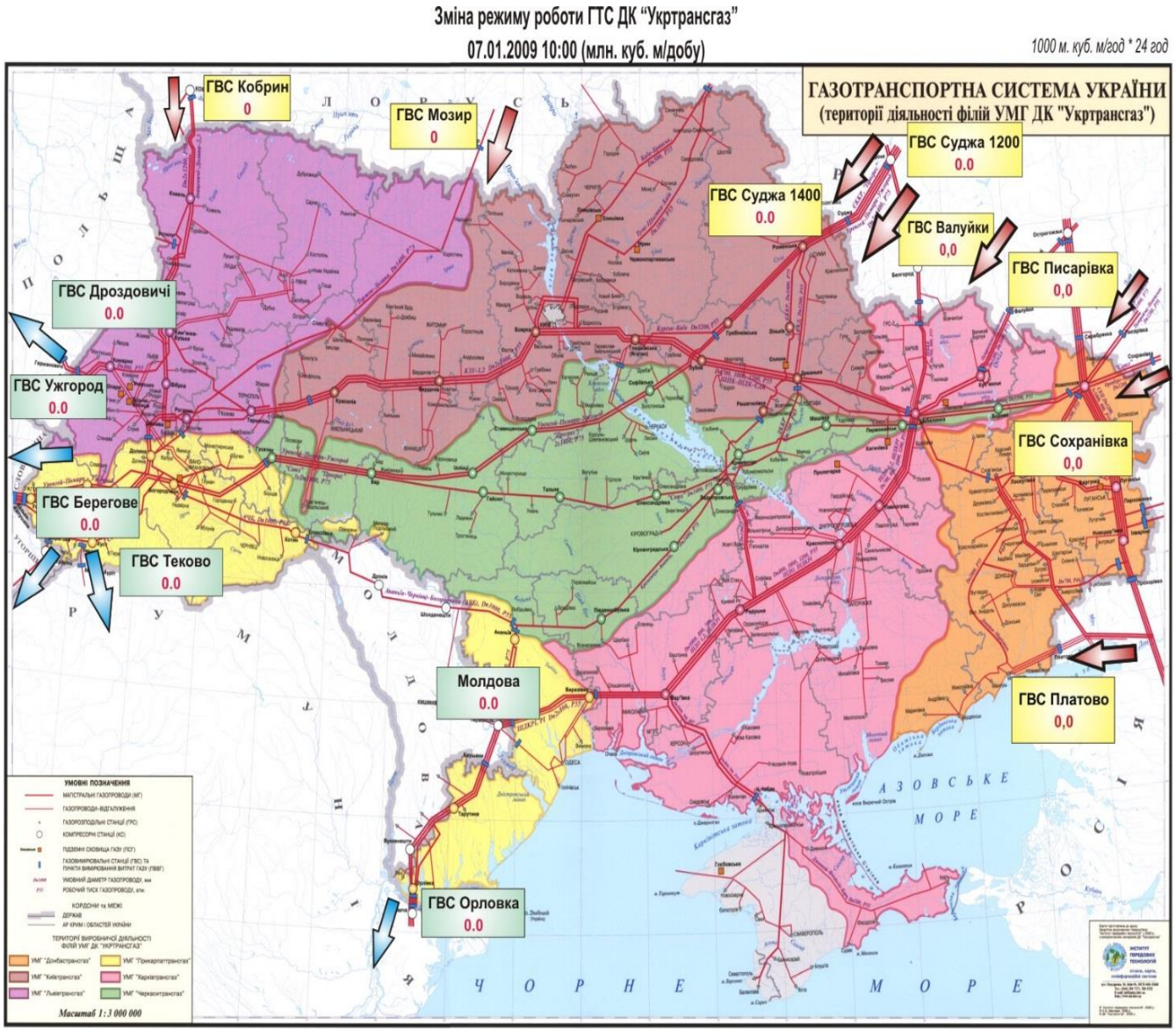

Рисунок 1.1 – Газотранспортна система України

На нинішньому етапі розвитку енергетичної галузі України відбувається широке зростання у сферах її діяльності інтегральних інтелектуальних технологій. Це дозволяє на сьогоднішній день досягти більш нового рівня комп'ютеризації функцій управління технологічними процесами, в тому числі і в сфері зберігання й транспортування природного газу. Впровадження сучасних інформаційних технологій задля покращення процесів накопичення, оброблення та передачі інформації експлуатаційних та режимних параметрів роботи головних її об'єктів є важливою та актуальною на сьогодні, з огляду на важливість ГТС України як стратегічного об'єкту держави [11].

В результаті швидкого вдосконалення інформаційних технологій, впровадження промислових мікроконтролерів нового покоління, доступності високоякісних сенсорів разом зі розширенням обсягу інформації, що обробляється в інформаційних системах диспетчерських пунктів ГТС з`явилась зацікавленність до розробки складних програмних алгоритмів управління значною кількістю об'єктів в реальному часі.

Однією з найважливіших задач для народного господарства є забезпечення відмовостійкості та надійності роботи систем трубопровідного транспорту. Одним із основних шляхів вирішення цієї задачі є розроблення і покращення моделей та методів прийняття рішень в умовах невизначеності при створенні та впровадженні САК. З цього можна зробити висновок про необхідність покращення наявних методів накопичення та оброблення інформації, в яких створюються та вдосконалюються дієві підходи до розробки апаратно-програмних комплексів й програмного забезпечення систем управління об'єктами ГТС.

Нині в світі вартість програмного забезпечення (ПЗ) технологічного обладнання не менша ніж вартість самого обладнання. Саме тому на підприємствах ГТС основних держав-гравців на міжнародній арені пострадянського простору, які займаються транспортуванням газу з`явилася

тенденція до розроблення вітчизняного ПЗ для цифрової обробки даних дистанційного керування системами телемеханіки, систем телеметрії, тощо.

Насамперед, перед фахівцями в області інформаційних технологій постає важливе завдання створення доступного та зручного для диспетчера людино-машинного інтерфейсу (HCI), що дозволяє дієво керувати технологічним процесом транспортування газу та характерними параметрами технологічного обладнання. Ця функція побудована по такому принципу, що в разі появи певного відхилення у технологічному процесі виникає повідомлення про це та рекомендовані дії, що повинен здійснювати диспетчер в цій ситуації. Саме так має працювати система підтримки прийняття рішень (СППР) диспетчерського персоналу.

Технологічні процеси газотранспортної системи відбуваються під прямим «наглядом» задіяних ефективних САК. Однак, це зовсім не зменшує степінь відповідальності диспетчерського персоналу (операторів), робота яких полягає в своєчасному прийнятті єдиновірного рішення. Перш за все це відноситься до аварійних ситуацій, коли від дій оператора та злагодженої роботи всього колективу залежить правильність та швидкість ліквідації значних аварій та недопущення їх виникнення.

В зв`язку з окресленими питаннями (проблемами) одним з найважливіших інструментів покращення промислової безпеки об'єктів ГТС та зменшення витрат на їх функціонування є ретельна підготовка спеціалістів по трубопровідному транспорту навичкам безаварійної експлуатації трубопровідних систем. Застосування комп'ютерних комплексів підтримки диспетчерських рішень (КПДР), інтерфейс яких наближений до реальних систем управління пришвидшить і зробить більш ефективним процес такої підготовки. Шляхом впровадження комплексів підтримки диспетчерських рішень на підприємствах, керівництво значно покращує професійний рівень операторів, які приймають рішення в результаті отримання, передачі й оброблення інформації САК.

Щоб виконати різні експерименти, спрямовані на покращення ефективності режиму роботи газотранспортної системи (ГТС) та економії природного газу при його транспортуванні, на основі нових інформаційних технологій відтворити методики обробки різного роду ситуацій, які виникають при роботі об’єктів ГТС, доцільно прободити розробку КПДР з використанням сучасних програмних засобів [11].

Значний внесок в розробку методів побудови і використання КПДР для транспорту підготовки фахівців трубопровідного внесли такі вчені: С.О.Сарданашвілі, Л.І.Григор'єв, В.А.Дятлов, В.В.Альошин, В.Є.Селезньов, С.М.Прялов, М.Г.Сухарев, О.М.Карасевич, В.С.Панкратов та ін.

Зарубіжні вчені J.Marko, M.Tirpak, J.Henderson, A.Heringh, G.Johannsen внесли значний внесок в створення та покращення сучасних автоматизованих методів проектування інформаційних систем комплексів підтримки диспетчерських рішень, що базуються на введенні сучасних розробок в галузі теорії і практики управління.

Зокрема, актуальним вважаємо вирішення проблем науково-технічного характеру, які мають місце на об’єктах газотранспортної системи (ГТС) України через масштабність і стратегічне значенні газотранспортної галузі.

Відомо, що загальна протяжність газопроводів в ГТС складає 38.55 тис. км з пропускною здатністю 287.7 і 178.5 млрд. м3/рік на вході і на виході відповідно. Газотранспортної система України містить 72 компресорні станції (КС) із 110 компресорними цехами, а також 702 газоперекачувальними агрегатами загальною потужністю 5443 МВт, 12 підземних сховищ газу активною місткістю 31 млрд. м3, 1455 газорозподільних станцій (ГРС), при цьому кількість працюючих на ГТС становить близько 28 тис. чол. Дані об’єкти входять в технологічний комплекс ПАТ «Укртрансгаз», який працює в безперервному режимі [12].

Задачі збільшення безпеки експлуатації об’єктів ГТС та їх модернізації є найбільш актуальними на даний час. З досвіду та практики (й аналізу) можна зробити висновок про необхідність вирішення наведених задач разом з

науково-технічними задачами із створення САК на базі процедур управління і апаратно-програмних засобів. Ці процедури в свою чергу потребують розробки методів оптимального управління, проектування та їх технічної реалізації і впровадження, а також дослідження саме об'єктів управління.

Нині в газотранспортній системі України склалася ситуація, коли на технологічних об'єктах ГТС встановлено значну кількість САК, що розроблені різними виробниками і організаціями. Чимала частина наведених систем не відповідає сучасним вимогам до функціональності, відкритості та надійності, фізично зношена та морально застаріла.

Згдно того, що компресорні станції відповідають за основні режими функціонування об'єктів газотранспортної системи та є найбільш складними в плані автоматизації, зробимо висновок, що задачі з створення нових САК КС на основі уніфікованих технологій та їх модернізації можна поставити в першочергові в структурі ГТС України. Проте методи і засоби вирішення наведених задач повинні мати наукове обґрунтування [12].

В роботах вчених Герасименко В.П, Грудза В.Я., Горбійчука М.І., Заміховського Л.М., Єршова В.Н., Семенцова Г.Н., Ковалко М.П., , Бойко Л.Г., Козакевича В.В., Дьоміна А.Є., Ольштейна Е.А., Тітенського В.І., Краснова Д.С., Комісарова Г.А. і ін., а також закордонних вчених H.Pearson, W. Jansen, J. Fabri, W.C. Moffat, F.K. Moore, E.M. Greitzer, I.R.Baher відображено вирішення проблем автоматизації процесів керування.

1.4 Оцінка вразливості критично важливих об`єктів інфраструктури

У даній роботі ми розглянемо методи виявлення вразливостей в критично важливих об`єктах інфраструктури і план захисних заходів. Щоб

запропонувати ряд заходів щодо зниження вразливості КВОІ необхідно проаналізувати вразливості таких систем.

Методи аналізу надійності систем були запропоновані для оцінки вразливості в роботах Garcia, M. L [8].

Наприклад, оцінка надійності в режимі реального часу електричної мережі може дати результат, що система надійна, якщо немає єдиної точки відмови [9].

Метод аналізу дерева помилок(відмов) який використовується в транспортних системах, електростанціях та інших критичних системах [13], зазвичай ідентифікує мінімальні набори подій, або «набори», які найбільш ймовірно зруйнують систему, і оголошує систему стійкою, якщо сумарна ймовірність події досить низька.

Проте інфраструктура, яка протистоїть одиничним точковим випадковим збоям (відмовам) з низькою ймовірністю виникнення, може не захистити себе від напрямленої атаки зловмисника.

Аналіз вразливостей повинен враховувати можливість збирати інформацію про нашу інфраструктуру і використовувати цю інформацію для виявлення слабких точок.

Так як кількість компонентів САК критичною інфраструктурою у відкритому доступі зростає з кожним роком, вважаємо що громадські джерела часто забезпечують 100 відсотків інформації, необхідної для планування руйнівної атаки на КВОІ.

Зокрема в результаті досліджень було виявлено 175 632 компоненти САК [18], що доступні в мережі Інтернет на 2018 рік. (рис. 1.2)

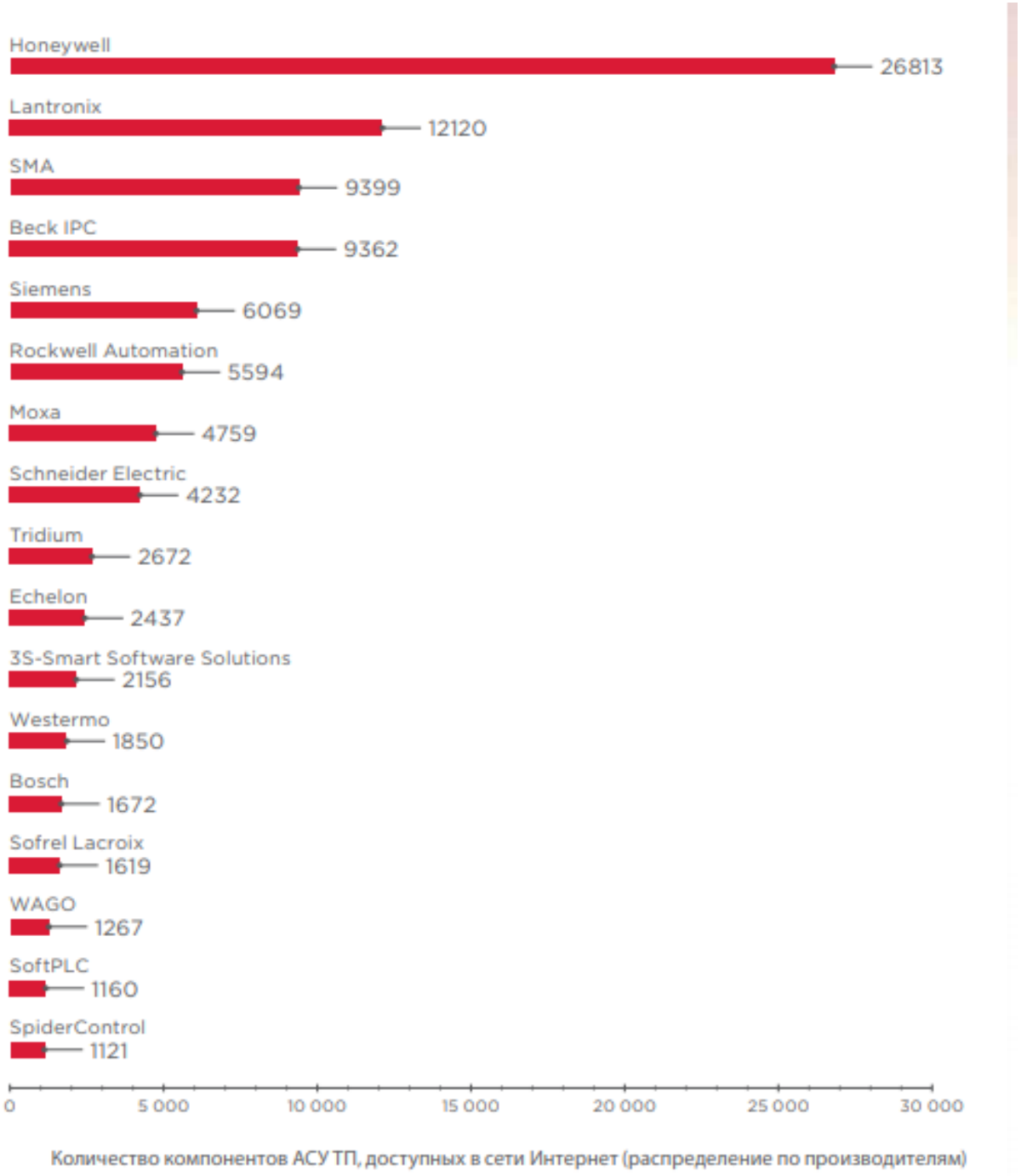

Рисунок 1.2 – Кількість компонентів САК, що доступні в мережі Інтернет за виробниками

Ми припускаємо, що якась терористична організація буде використовувати свої обмежені наступальні ресурси, щоб максимізувати збиток критичній інфраструктурі, яку вона вирішить атакувати; і що терористична організація володіє всією необхідною інформацією щоб виконати свою місію.

Припустимо, що наша КВОІ буде атакована і будемо застосовувати заходи для її захисту. Бюджет для цього завжди буде обмеженим.

Будемо оцінювати і розставляти пріоритети для наших критичних об’єктів:

-критичність (наскільки це важливий актив),

-вразливість (наскільки схильний актив для спостереження або нападу),

-відновлюємість (наскільки важко він буде відновлюватися після нанесеного збитку)

- загроза (наскільки ймовірна атака на цей актив).

Вирішення проблем аналізу вразливостей та оцінки надійності КВОІ відображені в теоретичних і прикладних роботах вчених G. Brown, M. Carlyle, J. Salmerón, K. Wood., M. L Garcia, N. Roberts, W. Vesely, D. Haasl, F. Goldberg та ін. [7; 8].

Висновки до розділу 1

В розділі розглянуто загальні теоретичні відомості про системи захисту інформації та доведено важливість їх використання в сучасних системи автоматичного керування (САК). Також поставлена актуальна задача, що буде вирішена в наступних розділах. З огляду на означене, уважаємо, що мінімізація витрат на формування СЗІ та важливість забезпечення необхідного рівня захищеності є на нинішній момент актуальною задачею. Таким чином, такий критерій можливо вивести із моделі, розробленої в термінах теорії ігор.

Також розглянуто критично важливі об`єкти інфраструктури в умовах зростаючої кількості комп'ютерних атак, описана газотранспортна система (ГТС) України як критично важливий об`єкт.

Здійснено аналіз вразливості критично важливих об`єктів інфраструктури та представлено кількість компонентів САК, що доступні в мережі Інтернет за виробниками, що, в свою чергу, підвищує ймовірність успішної атаки на САК зловмисником.

2 АНАЛІЗ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ ЛОКАЛЬНИХ ДИСПЕТЧЕРСЬКИХ ПУНКТІВ КОМПРЕСОРНИХ СТАНЦІЙ «КИЇВТРАНСГАЗ»

2.1 Опис системи диспетчеризації «Київтрансгаз»

Об’єктом дослідження є розподілена САК КВОІ, що складається із c компонентів, які приймають участь в обробці інформації й управлінні об'єктом та взаємодіють між собою.

Кожен компонент САК КВОІ описується переліком характеристик, серед яких операційне середовище, технологія обробки інформації тощо. Вказані параметри компонентів становлять їх цінність для системи. Цінність будемо позначатися через q_c.

Кожен із компонентів має вразливість в залежності від певних загроз із A визначених загроз. Припускатимемо, що інформація про архітектуру САК є відкритою та знайомою сторонам конфлікту. Окрім цього, задається ймовірність успішного здійснення загрози a проти компоненту системи c, а також ймовірність нейтралізації загрози, шляхом встановлення механізмів захисту p. Отже, при моделюванні варто враховувати, що на дієвість рішень, які приймаються зловмисником чи захисником впливають випадкові фактори.

У роботі буде розглядатися САК КВОІ ГТС України. Газотранспортна система (ГТС) України – це єдиний технологічний комплекс, що виконує дві основні функції: транспортування і розподіл природного газу споживачам України та транзит природного газу територією України до країн Центральної та Західної Європи. Основними елементами системи є магістральні трубопроводи, газорозподільні, газовимірювальні станції та зв’язані з ними підземні сховища газу і компресорні станції.

Зокрема будемо розглядати як КВОІ систему диспетчеризації «Київтрансгаз». Система диспетчеризації «Київтрансгаз» складається з локальних диспетчерських пунктів компресорних станцій (ДПКС). На цих об`єктах застосовуються сучасні засоби інформаційних технологій та

обчислювальної техніки зв’язку. За допомогою системи здійснюється управління та контроль технологічними процесами. Вона також здійснює контроль транспортування і розподілу газу всіх компресорних станцій (КС) та газорозподільних станцій [5].

Основну функцію ДПКС визначають як організацію централізованого отримання, обробки та своєчасного доступу до бази технологічної інформації, яка поступає від різноманітних джерел. ДПКС обладнані засобами контролю параметрів та самодіагностики, що виконуються при залученні відповідного програмного забезпечення. Окрім цього, ДПКС здійснює безперервне функціонування із резервуванням серверів збору й обробки інформації [5].

Основними вимогами до комплексу системи диспетчеризації «Київтрансгаз» є:

1) безпечне зберігання та доступ до інформації;

2) робота в неперервному режимі;

3) здійснення автоматичного завантаження у випадку збоїв апаратного та програмного забезпечення за кількість часу, яка є не більше 5 хвилин;

4) здійснення підключення та актуалізація параметрів всяких програмно-технічних засобів, які використовують стандартні протоколи для обміну інформацією;

5) здійснення поповнення теперішньої технологічної інформації з періодом, що не більше ніж 1 хвилина;

6) здійснення архівації технологічних параметрів в системах керування базами даних (СУБД), терміном до одного року;

7) надання доступу до теперішніх та минулих параметрів шляхом використання робочого місця оператора або web-сторінки на всякому комп’ютері локальної мережі «Київтрансгаз» або Інтернет у виді звітів, трендів, мнемосхем та таблиць;

8) надання стандартних засобів для формування звітів, використовуючи дані архівів;

9) здійснення віддаленого адміністрування;

10) здійснення самодіагностики [5].

Склад системи:

-ДПКС «Яготин», м. Яготин Київської області (КС «Глушківська», контрольні пункти телемеханіки, газорозподільчі станції);

-ДПКС «Бердичів», с. Садки Житомирської області (КС «Бердичів», контрольні пункти телемеханіки, газорозподільчі станції);

-ДПКС «Гребенківська», м. Лохвиця Полтавської області (КС «Гребенківська»);

- ДПКС «Диканька», смт Диканька Полтавської області (КС «Диканька», контрольні пункти телемеханіки, газорозподільчі станції);

- ДПКС «Ромненська» (КС «Ромненська», контрольні пункти телемеханіки);

- КС «Боярка» (м. Боярка Київської області);

- КС «Зіньків» (м. Зіньків Полтавської області);

-КС «Решетилівка» (смт Решетилівка Полтавської області);

-КС «Красилів» (м. Красилів Хмельницької області);

- КС «Лубни» (м. Лубни Полтавської області);

-Центральний ДПКС «Київ».

Інформація з локальних ДПКС нагромаджується у центральному ДПКС «Київ». Під час цього процесу на центральний архівний сервер локальними серверами архівної інформації передаються дані за допомогою функції копіювання даних. Така функція забезпечує додаткову надійність зберігання інформації.

Регіональні ДПКС накопичують дані у реальному часі, переносять їх на локальні сервери архівної інформації та передають їх на центральний ДПКС «Київ» у реальному часі, а потім за допомогою локальних автоматизованих

робочих місць (АРМ) оператора відтворюють дані, що були отримані про хід технологічного процесу [5].

Центральний ДПКС «Київ» та кожна регіональна ДПКС та складаються з наступних елементів (рис. 2.1):

1. Application Server (AS)– головний сервер накопичення та оброблення інформації;

2. Historian Server (HS) – сервер зберігання архівної інформації;

3. Information Server (IS) – резервний сервер накопичення та оброблення інформації з наявністю додаткової функції надання інформації у реальному часі та архівних даних із застосуванням web-інтерфейсу;

4. А також декількох автоматизованих робочих місць операторів задля контролю й управління технологічним процесом.

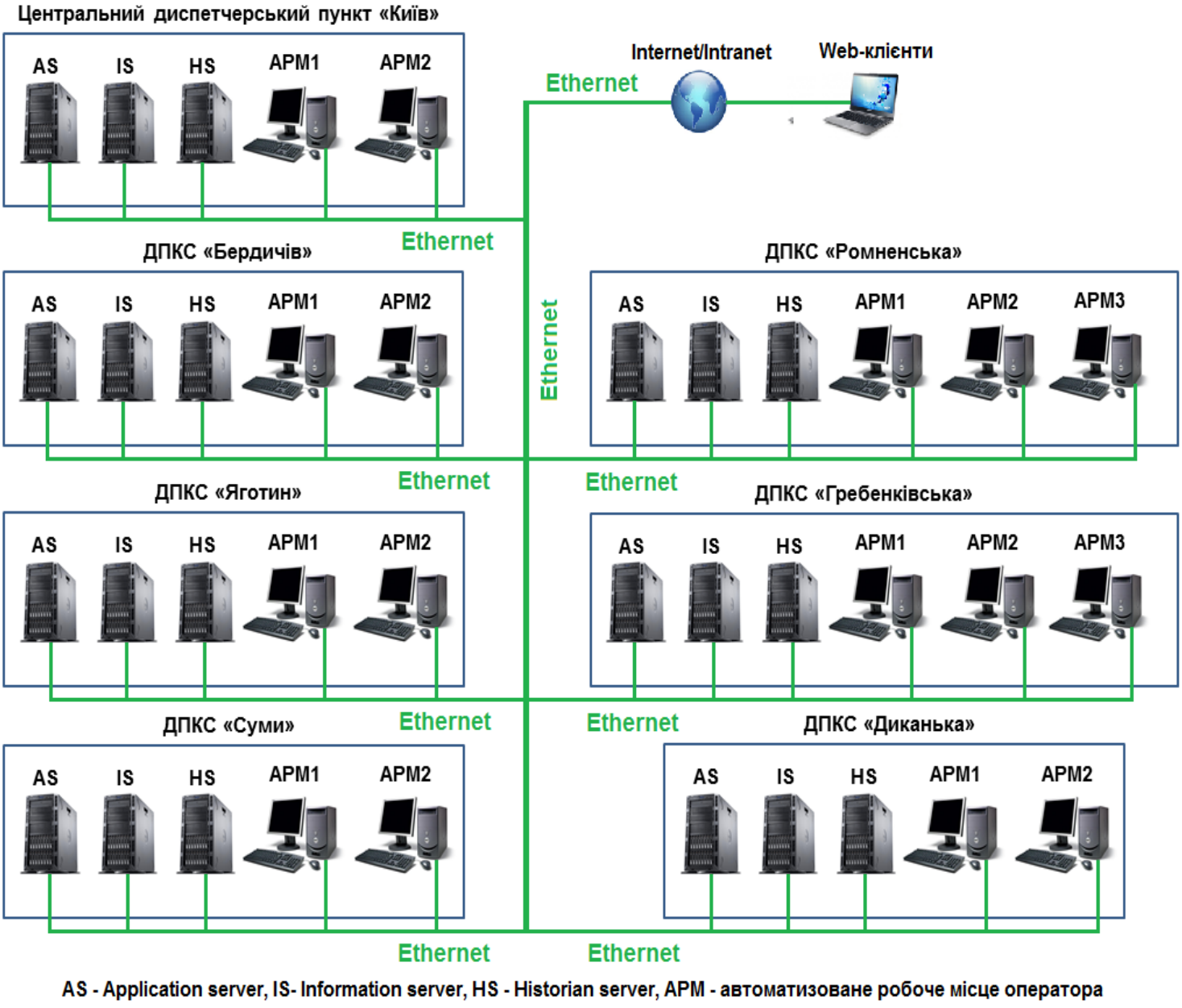

Рисунок 2.1 - Структура основних елементів (вузлів) системи

Система диспетчеризації «Київтрансгаз» створена на основі пакету програмного забезпечення (ПЗ) Wonderware System Platform 4.0, за допомогою якої можливо виконати наведені вище функції для розподілених систем керування.

На автоматизованому робочому місці оператора встановлено програмне забезпечення In Touch for System Platform, що гарантує забезпечення людино-машинного інтерфейсу, працюючий в реальному часі.

Центральний ДПКС «Київ» а також кожна регіональна ДПКС поєднані в локальну обчислювальну мережу «Київтрансгаз».

2.2 Вразливості систем автоматичного керування в УМГ «Київтрансгаз»

В даний час на об'єктах промисловості в основному використовуються типові SCADA-системи та промислові АСУ ТП зі стандартними протоколами обміну даними. З одного боку використання типових систем управління і передачі інформації мережею дозволяє здійснити більш легкий обмін даними між різними рівнями системи, що підвищує її ефективність, а з іншого це призводить до збільшення ймовірності здійснення мережевих загроз. І ця проблема потребує вирішення в найкоротші терміни, але на створення і поширення нових захищених SCADA-систем потрібно досить багато часу, що призводить до необхідності шукати і усувати вразливі місця в безпеці інформаційних систем на даному етапі їх розвитку.

Назараз промислові системи освоїли такі мережеві технології, як Ethernet і TCP / IP. Ці технології широко використовуються в промислових АСУ та SCADA-системах, створюючи умови для більш ефективної роботи

підприємств і роблячи системи контролю більш доступними для користувачів. Але поряд з перевагами вони перенесли і проблему: об'єднання інформаційних мереж на різних рівнях підприємства в єдиний інформаційний простір значно підвищує вразливість системи з боку зовнішніх атак, мережевих «черв'яків», вірусів та хакерів.

Проаналізувавши поточний стан систем автоматичного керування газоперекачувальних агрегатів в УМГ «Київтрансгаз» І.В. Назаренко стверджує, що ресурс експлуатації перевищено для 67% систем, протягом 1-3 років свій ресурс вичерпають ще 17%. Відповідно за системами САК компресорної станції (КС) ресурс експлуатації перевищено для 59% та вичерпають свій ресурс 18%. Унеможливлюють безвідмовну роботи систем автоматики відсутність запчастин, що не випускаються, відсутність деяких виробників САК та розробників ПЗ САК [17].

Окрім того на 2017 рік доля вразливостей за виробником компонетів САК для УМГ «Київтрансгаз», а саме Schneider Electric склала – 47 [18].

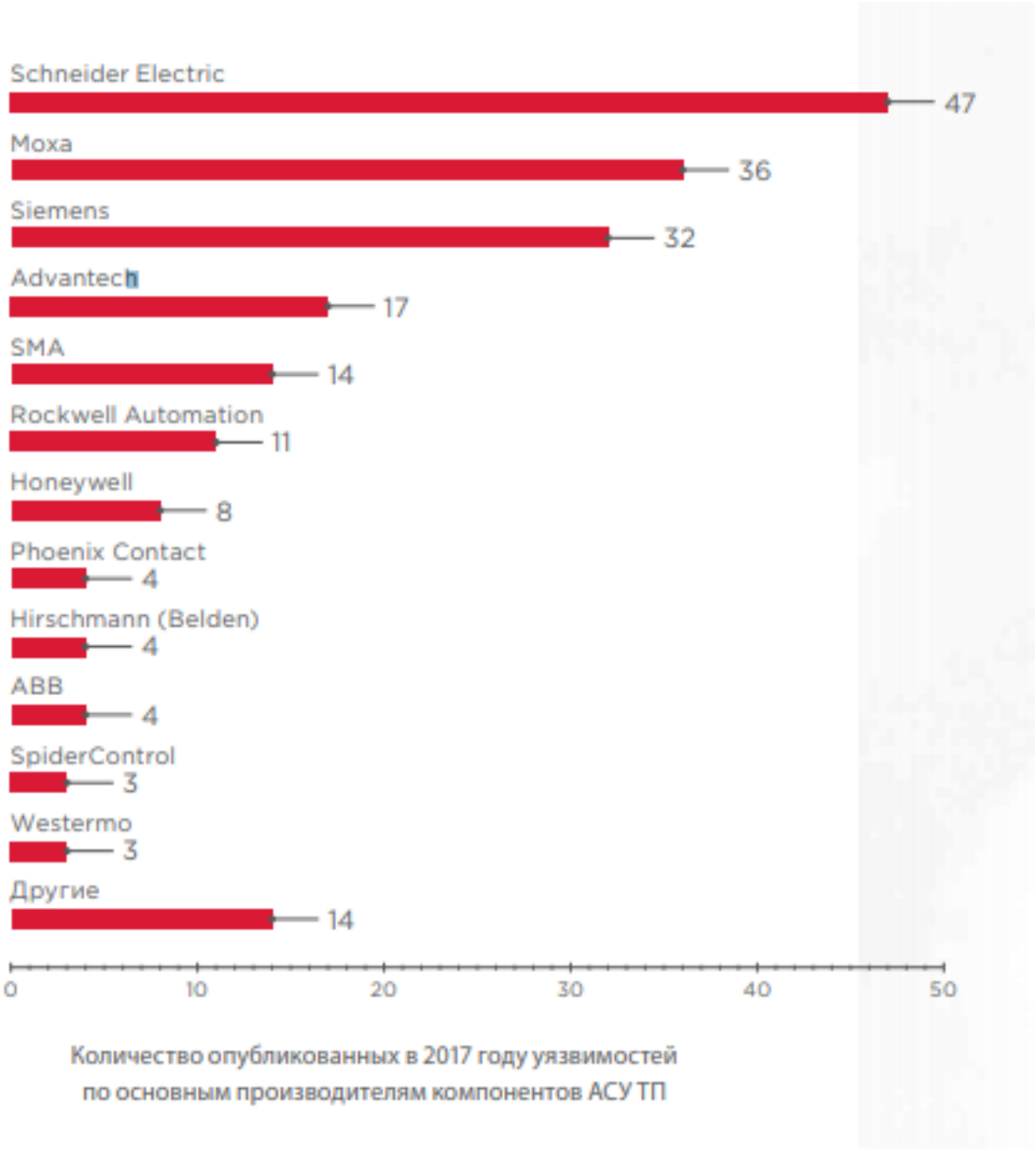

Рисунок 2.2 – Кількість вразливостей за основними виробниками компонентів САК

В системі на базі Wonderware System Platform 4.0 були виявлені вразливості, наслідком виконання атак на які буде можлива «Відмова в обслуговуванні» нашій системі, тобто зупинка постачання газу користувачам.

Зокрема вразливість CVE-2011-2962 викликає переповнення буфера віддаленним зловмисникам викликати збої в обслуговуванні. Маємо повне розкриття інформації, в результаті чого виявляються всі системні файли. Вразливість має високий рівень загрози системі (9,3 по шкалі CVSS) [19].

Зловмисник може викликати переповнення буфера в стеку, запросивши неіснуючий файл, який може дозволити виконання довільного коду.

Використовуючи стек протоколів TCP / IP можна здійснити безліч атак на серверні служби АС, в тому числі і стандартну атаку «Відмова в обслуговуванні», яка може виявитися однією з найбільш критичних загроз для функціонування промислових мереж. Дана атака багатогранна: вона може реалізовуватися як по відношенню до систем шару інформаційного супроводу і управління, так і безпосередньо не стосуються програмного комплексу контролерів. Для реалізації подібної атаки потрібно використовувати уразливості системи. Одна з них робить можливим використання XML-коду файлів не тільки для підтримки процесу функціонування системи, а й для його порушення.

Зокрема фахівці дослідницького центру Positive Research компанії Positive Technologies виявили уразливість CVE-2013-0686, пов'язану з некоректною перевіркою даних в Wonderware Information Server.

Уразливість в WIS дозволяє зловмисникам отримати доступ до локальних ресурсів (файлів і внутрішніх ресурсів), використовуючи небезпечну обробку зовнішніх сутностей XML. Використовуючи спеціально сформовані XML-файли, зловмисник може відправити вміст локальних або віддалених ресурсів на свій сервер або викликати відмову про обслуговуванні системи (DoS) [20].

Також вразливість CVE-2014-2380, а саме – ненадійне шифрування даних облікових записів в Wonderware Information Server.

Шифрування в WIS не відповідає вимогам. Розшифрувавши дані облікових записів, зловмисник зможе підвищити свої привілеї. Для проведення даної атаки необхідна компрометація системи [21].

2.3 Побудова системи захисту інформації як позиційна гра

Будемо розглядати побудову системи захисту інформації як антагоністичну гру двох гравців з повною інформацією, за умови що сторони діють в умовах ризику. В такій грі ходи можуть мати детермінований та стохастичний характер. Детерміновані ходи це свідомий вибір стратегії дій гравців серед наявних альтернатив.

Вибір стратегії зловмисником визначає, яку загрозу чи розвідку a йому застосовувати проти якого із компонентів c. Сукупність рішень (альтернатив) представимо у вигляді матриці $Y = \{y_{ac}\}$, яка складається із булевих елементів, де $y_{ac} = 1$ означає рішення, про реалізацію загрози a проти компонента системи (в нашому випадку компресорна станція) c.

Вибір стратегії (рішення) захисника напрямлений на встановлення механізму захисту $p = 1,2,...,P$ в компоненті системи (КС) c. Так само набір його рішень опишемо матрицею булевих елементів $X = \{x_{cp}\}$, де $x_{cp} = 1$ означає рішення, про встановлення механізму захисту p в компоненті (КС) c.

Стохастичний хід являє собою вибір, який виконується не певним гравцем, а під впливом випадкових факторів. У теорії ігор сукупність таких факторів називають «природою» — додатковим гравцем, який робить свої ходи випадково (стохастично). Для прикладу, у процесі перебирання паролів існує не нульова ймовірність підбирання правильного пароля або інакше, під час встановлення системи виявлення вторгнень існує ненульова ймовірність викриття протиправних розвідувальних дій зловмисника. Одночасно для кожного випадкового ходу задається розподіл ймовірностей на множині всіх рішень «природи».

Нехай, «природа» впливає на рішення, що прийняв як захисник так і зловмисник. Тоді позначимо через змінну h_{ac} ймовірність успіху зловмисника під час реалізації загрози a проти компоненту САК (компресорної станції) c. А через d_{ap} позначимо ймовірність викриття чи нейтралізації загрози a, одночасно з встановленням механізму захисту p.

Позиція це ситуація, в якій опиняються гравці після того як здійснили свої ходи (рішення).

Множину всіх наявних позицій розіб`ємо на такі підмножини:

- позиції, які стосуються зловмисника, в кожній із яких він робить вибір одного із рішень, доступних йому (з $\{y_{ac}\}$);
- позиції, які стосуються захисника, в кожній із яких він робить вибір одного із рішень, доступних йому (з $\{x_{cp}\}$).

Можна виділяти окремо позиції з випадковими ходами, проте в нашій моделі стохастичні ходи «природи» прямо пов’язані з невипадковими ходами обох гравців та будуть розглядатися разом.

Отже, практикуючи кожну із стратегій чи то захисником чи зловмисником існує ненульова ймовірність успіху (чи невдачі) стратегії в певному обчислювальному середовищі, за встановленої апріорної ймовірності успіху обраної події.

2.4 Побудова цільової функції для моделі системи захисту інформації «захисник-зловмисник»

Існує 3 моделі побудови системи захисту інформації : AD («зловмисник-захисник»), DA («захисник- зловмисник») та DAD («захисник- зловмисник-захисник»), які застосовуються для вирішення проблем захисту конкретних об’єктів критичної інфраструктури [6].

Для нашої системи ми будемо застосовувати модель «захисник-зловмисник». Для побудови цільової функції маємо визначити змінні.

Позначимо множину загроз, які можуть бути реалізовані в системі ДПКС та нанести їй збиток через $a \in A$, $A=\{a_1,..., a_n\}$. Список можливих загроз складається, базуючись на вже існуючих вразливостях, що можуть бути застосовані зловмисниками різних типів (як внутрішніми, так і зовнішніми), із різним рівнем кваліфікації в сфері захисту інформації, різними правами доступу (від користувачів до адміністраторів), різними теоретичними та практичними знаннями.

Завданий збиток Q_c, який виражається у виді витрат та втраченої вигоди є кількісною величиною для оцінки ризиків. Як наслідок, значення збитку Q_c, що було спричинене певній КС c тотожне цінності даного компонента q_c для роботи системи загалом. Далі будемо вважати ці величини еквівалентними.

Завдання захисника цієї системи зводиться до вибору функціональних профілів захищеності $p \in P$, $P = \{p,..., p_m\}$ для кожної КС, які сприятимуть мінімізації збитків від можливих дій зловмисника за існуючих загроз та обмежень на впровадження системи захисту.

Подолання потенційних атак буде здійснюватися з використанням функціональних профілів захищеності p. Кожен із профілів захищенності може нейтралізувати одну чи більше загроз a із множини A. Введемо матрицю захищеності D $=\{d_{ap}\}$, що відповідає за здатність певного профілю p протидіяти потенційній атаці a. Визначимо d_{ap} так:

d_{ap} = 1, якщо механізм захисту p здатний протидіяти атаці a на КС (ймовірність виявлення або нейтралізацію загрози а) d_{ap} = 0, інакше.

В системі наявна певна статистична невизначеність, тобто відомо деякі ймовірності вибору стратегій захисником. Визначимо ймовірність впровадження загрози a на компресорній станції c як h_{ac} так що: h_{ac} = 1; якщо атака a на компресорну станцію c успішна; h_{ac} = 0, інакше.

Треба відобразити вплив стратегій захисника на ризик в системі. Для цього введемо додаткову змінну, що буде характеризувати здатність системи захисту протистояти атаці a на КС c - V_{ac}. Таким чином, $(1 - V_{ac})$ можна

інтерпретувати як існування незахищеної вразливості, яка може бути використана зловмисником.

Загалом для функції ризику інформаційної безпеки R_{ac} запишемо співвідношення у вигляді добутку ймовірності P_{ac} реалізації загрози *a* та завданого збитку при реалізації цієї загрози Q_c із урахуванням ймовірності нейтралізації загрози з використанням встановлених додаткових механізмів захисту V_{ac}:

$$R_{ac} = P_{ac} \cdot Q_c \cdot (1 - V_{ac}) \quad (2.1)$$

Будемо вважати, що атака зловмисника складається із K етапів, при цьому збиток буде завданий, за умови, якщо всі етапи завершено успішно. Тоді, ймовірність реалізації загрози представимо в виді добутка ймовірностей успішної реалізації кожного з етапів k. Тоді, відповідно, співвідношення ризику:

$$R_{ac} = \prod_{k=1}^{K} P_{ac}^{k} \cdot Qc \cdot (1 - Vac) \quad (2.2)$$

В співвідношенні (2.2) висвітлено динамічний характер поведінки системи, за умови зміни стану під дією кожної з сторін. З огляду на поетапність здійснення атаки, опишемо відносини захисника та зловмисника, використовуючи позиційну гру, в якій учасники роблять ходи по черзі з намаганням досягти для себе максимальної користі. Можемо виокремити такі етапи позиційної гри відповідно до етапів комплексної атаки:

- На першому етапі, метою якого є вивчення, аналіз та пошук вразливостей в системі захисту для здійснення атаки, зловмисник здійснює розвідку.

-Завданням захисника на даному етапі є попередження можливої атаки, через нейтралізацію вразливостей, а також викриття зловмисника [15].

-На другому етапі, використовуючи знайдену вразливість, зловмисник знешкоджує систему захисту та здійснює атаку. Таким чином, одна чи кілька фундаментальних властивостей інформації (конфіденційність, цілісність, доступність) зазнає порушень на цьому етапі [15].

-З метою нейтралізації небажаних дій захисник застосовує визначені заходи та засоби захисту.

-На завершальному етапі атаки зловмисник знищує сліди, які можуть його викрити.

У випадку, якщо захисник зможе виявити та знешкодити зловмисника, може відбутися завершення гри на одному із ранніх етапів. Проте, якщо атака проведена успішно гра може бути завершена на останньому етапі.

Отже, апріорні ймовірності, відповідно до реалізації загроз h_{ac}^{k} та їх знешкодження d_{ap}^{k} можуть змінюватися з часом, і тому повинні задаватися для кожного з етапів k.

Виразимо цільову функцію через ризик інформаційної безпеки, яку захисник намагається зменшити, а зловмисник збільшити. Зловмисник обираючи стратегію дій оперує ймовірністю реалізації загроз:

$P_{\text{ac}}^{k} = \text{h}_{\text{ac}}^{k} \cdot \text{y}_{\text{ac}}^{k}$ та потенційним збитком с Q_{c}= q.

Захисник може зменшити ризик завдяки встановленню додаткових механізмів захисту:

$Vac = \left(\sum_{p=1}^{P} d_{ap}^{k} \cdot x_{cp}^{k} \right)$

Якщо Vac = 1, то К c є повністю захищеною від загрози a . У цьому випадку з метою недопущення встановлення надмірних засобів та заходів захисту застосовується обмеження $Vac \leq 1$.

Після підстановки визначених змінних в (2.2) та врахування мети захисника та зловмисника цільову функцію можна записати в такому вигляді:

$$\text{R} = \min_{x} \max_{y} \prod_{k=1}^{K} \sum_{a=1}^{A} \sum_{c=1}^{c} h_{ac}^{k} \cdot y_{ac}^{k} \cdot q_{c} \cdot \left(1 - \sum_{p=1}^{P} d_{ap}^{k} \cdot x_{cp}^{k}\right) \qquad (2.3)$$

За наступних обмежень:

$\sum_{a,c,k} y_{ac}^{k} \leq L$, де L - обмеження на кількість одночасно реалізованих загроз,

$\sum_{c,p,k} w_{p} \cdot x_{cp}^{k} \leq W$, де W - обмежені ресурси захисника,

$\sum_{p=1}^{P} d_{ap}^{k} \cdot x_{cp}^{k} \leq 1,$

$x_{cp}^{k} = \{0,1\}$, $y_{ac}^{k} = \{0,1\}$.

Для розв'язання нелінійної задачі (2.3) спершу перейдемо до двоїстої, через введення змінної θ та фіксацію значень стратегій захисника x :

$$R = \min_{\theta} \prod_{k} \sum_{a,c} \theta_{ac}^{k} \quad (2.4)$$

За обмежень:

$\theta_{ac}^{k} \leq h_{ac}^{k} \cdot q_{c} \cdot \left(1 - \sum_{p=1}^{P} d_{ap}^{k} \cdot x_{cp}^{k}\right),$

$\sum_{c,p,k} w_{p} \cdot x_{cp}^{k} \leq W,$

$\sum_{p=1}^{P} d_{ap}^{k} \cdot x_{cp}^{k} \leq 1,$

$\theta_{ac}^{k} \geq 0.$

Подальший розв'язок задачі (2.4) відбувається з використанням методу гілок та границь [14].У результаті розв'язання отримуємо оптимальний набір рішень захисника x_{cp}^{k} та зловмисника y_{ac}^{k}.

Висновки до розділу 2

У розділі було описано систему диспетчеризації «Київтрансгаз» як об'єкт дослідження. Було схарактеризовано та проілюстровано склад системи, визначено її основні функції.

Також було проведено аналіз вразливостей систем автоматичного керування в УМГ «Київтрансгаз» за допомогою даних по кількості вразливостей за основними виробниками компонентів САК.

У розділі було розглянуто принцип побудови системи захисту інформації з боку застосування механізму теорії ігор, а саме позиційної гри.

Існує 3 моделі побудови системи захисту інформації : AD («зловмисник-захисник»), DA («захисник- зловмисник») та DAD («захисник- зловмисник-захисник»), які застосовуються для вирішення проблем захисту конкретних об’єктів критичної інфраструктури.

Для нашої системи ми будемо застосовувати модель «захисник-зловмисник». Для побудови цільової функції визначаються змінні.

В розділі була здійснена побудова цільової функції для моделі системи захисту інформації «захисник-зловмисник»

А саме – визначено множина загроз, множина профілів захищенності в якості змінних. Було приведено і описано етапи проведення атаки зловмисником як кроки позиційної гри:

- Зловмисник проводить розвідку.
- Зловмисник проводить атаку.
-Зловмисник приховує сліди.

І, нарешті, отримано кінцеву цільову функцію для заданих обмежень (обмеження на кількість одночасно реалізованих загроз, обмеження на ресурси захисника).

3 ПОБУДОВА СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ЛОКАЛЬНИХ ДИСПЕТЧЕРСЬКИХ ПУНКТІВ КОМПРЕСОРНИХ СТАНЦІЙ НА ПРИКЛАДІ УМГ «КИЇВТРАНСГАЗ»

3.1 Визначення цінностей компонентів системи диспетчеризації «Київтрансгаз»

Відомо, що ДПКС системи диспетчеризації «Київтрансгаз» розподілені територіями Київської, Полтавської, Чернігівської, Хмельницької, Житомирської та Сумської областей і мають представництва C у певних населених пунктах. Центральне відділення, яке контролює роботу всієї системи диспетчеризації розташовано у Києві. Отже, система складається із с = 1,2,...,11 компонентів, які взаємодіють між собою.

Завдання полягає в побудові системи захисту інформації для описаної КВОІ, яка забезпечить здійснення функцій інформації: цілісність, конфіденційність та доступність даних. Припускаємо, що інформація щодо обчислювального середовища та технологій обробки інформації є доступною і можливо потрапить до зловмисника.

Проведемо аналіз системи та виділимо її компоненти c на початковому етапі побудови СЗІ. Потрібно визначити цінність q_c компонентів системи (КС) c, яка в подальшому буде використовуватися для оцінки можливих збитків. Успішне здійснення загрози проти якогось з компонентів системи спричинить зупинку постачання газу користувачам (відмова в обслуговуванні), що еквівалентна цінності цього компонента для функціонування системи в цілому. За відсутності статистичних даних та фінансових звітів, припустимо, що завданий збиток q_c пропорційний кількості населенню району атакованої КС (табл. 3.1).

Таблиця 3.1 - Компоненти системи (КС населеного пункту) с та їх цінності q_c

№ з/п	**КС системи c**	**Цінність q_c**
1.	Центральний диспетчерський пункт «Київ»	3635278
2.	КС «Боярка» (м. Боярка Київської області)	364941
3.	КС «Глушківська» (м. Яготин Київської області)	98695
4.	КС «Лубни» (м. Лубни Полтавської області)	493918
5.	КС «Гребінківська» (м. Лохвиця Полтавської області)	53407
6.	КС «Диканька» (смт Диканька Полтавської області)	330026
7.	КС «Зіньків» (м. Зіньків Полтавської області)	33815
8.	КС «Решетилівка» (смт Решетилівка Полтавської області)	11660
9.	КС «Роменська» (с. Миколаївка Сумської області)	148048
10.	КС «Бердичів» (с. Садки Житомирської області)	844578
11.	КС «Красилів» (м. Красилів Хмельницької області)	604336

3.2 Модель зловмисника та загроз

Формування моделі порушника є обов`язковим етапом створення політики безпеки. Зважаючи на запропоновану задачу, виникає необхідність у передбаченні захисту від зовнішніх порушників, які мають високу кваліфікацією та оснащені потрібними апаратними та програмними засобами для віддаленої реалізації загроз інформаційної безпеки. Їх метою є: отримання доступу до закрітої інформації; отримання можливості внесення відповідних змін до інформаційних потоків у відповідності до своїх намірів; перехоплення управління; виклик відмови в обслуговуванні [16; 22].

За умови володіння інформацією про характерні особливості зловмисника та його мету виникає можливість вибору типових загроз інформаційній безпеці *a,* з використанням яких, порушник зможе досягнути поставленої цілі.

Запропонований підхід пропонує розглядати атаку у вигляді динамічного процесу. Тому виникає необхідність роподілу загроз на етапи *k* у такій послідовності, в якій вони будуть реалізовані зловмисником. З огляду на зазначений вище підхід пропонуємо поділити процес здійснення загрози на 3 етапи (табл. 3.2).

Таблиця 3.2. Загрози інформаційній безпеці a та ймовірності їх виникнення $\boldsymbol{h_a}$

Етап k	**№**	**Загрози** a	**Ймовірності реалізації** $\boldsymbol{h_a}$
1		**Розвідка**	
	4	Обхід механізмів захисту	0,7
2		**Проникнення**	
	1	Віддалене виконання коду	0,9
	3	Переповнення буфера	0,8
	6	Підробка міжсайтового запиту (XSS)	0,6
	7	Введення (залучення, впровадження) операторів SQL	0,5
3		**Реалізація мети**	
	2	Розкриття інформації	0,8
	5	Відмова в обслуговуванні(DoS, DDoS-атаки)	0,7

	8	Підвищення привілеїв	0,4

Припускаємо, що для кожного компоненту системи c застосовуються однотипні технології обробки інформації, а тому наявні вразливості до наведених загроз інформації, при цьому ймовірність здійснення загрози проти кожного з компонентів системи буде однакова $\forall a, \forall c \Rightarrow h_{ac} = h_a$.

Для спрощення вважатимемо, що ймовірність реалізації загрози залежить лише від виду загрози, але не буде залежати від особливостей кожного компоненту, у крайньому випадку доки не буде реалізована система захисту інформації.

3.3 Модель захисника

Вибір механізмів захисту, з орієнтацією на архітектуру обчислювального середовища та модель загроз є наступним етапом розробки політики безпеки. За допомогою методу експертної оцінки визначимо дієвість кожного із механізмів захисту p проти визначених загроз a в системі d_{ap} та вартість їх реалізації w_p (табл. 3.3). Кожен із механізмів захисту p забезпечує певний рівень захищеності.

Таблиця 3.3 - Ймовірності d_{ap} знешкодження загрози a механізмом захисту p та вартість введення такого механізму w_p

№	**Механізми захисту p**	**Індекси загроз інформаційній безпеці a**								**Вартість реалізації w_p**
		1	2	3	4	5	6	7	8	
1	Використання захищених протоколів доступу	0,8	0,9	0,4	0,9	0,7	0,8	0,7	0,8	15
2	Антивірусне ПЗ	0,1	0,9	0,3	0,9	0,3	0,8	0,6	0,1	10
3	Шифрування даних, що передаються	0,8	0,9	0,7	0,8	0,4	0,9	0,9	0,7	20
4	Обробка всіх помилок і виключень	0,7	0,3	0,9	0,6	0,9	0,9	0,4	0,4	10
5	Оновлення вразливих версій ПЗ (Vulnerability management)	0,9	0,9	0,9	0,9	0,9	0,4	0,7	0,6	15
6	Екранування вхідних даних	0,8	0,3	0,8	0,8	0,8	0,7	0,9	0,3	20
7	Метод параметризації запитів	0,4	0,5	0,5	0,7	0,4	0,4	0,9	0,5	5
8	Багатофакторна автентифікація	0,7	0,6	0,3	0,6	0,4	0,8	0,3	0,9	10

3.4 Синтез структури системи захисту інформації

Після отримання необхідних даних, перейдемо до вирішення поставленого завдання - визначення структури СЗІ, що забезпечить мінімальне значення цільової функції (2.2) при заданих обмеженнях (ресурси на побудову СЗІ).

Безпосередньо синтез СЗІ здійснюється з використанням співвідношення (2.3). Результатом цього є сукупність механізмів захисту $\{p\}$ для кожної компресорної станції.

Через те що кількість можливих комбінацій, що аналізуються моделлю досягає значного числа, розв’язуючи цю задачу, використовувалися автоматизовані математичні пакети.

В результаті маємо рішення запропонованої задачі для 3 різних випадків - за умови різних витрат на системи захисту інформації W. (табл. 3.4).

Таким чином, на прикладі побудови СЗІ для САК критично важливої інфраструктури було продемонстровано практичну доцільність наведеного підходу. Низка здійснених експериментів засвідчила, що запропонована модель є адекватною для синтезу структури СЗІ та може бути застосована до систем підтримки прийняття рішень інформаційної безпеки.

Таблиця 3.4 - Встановлені механізми захисту

Компонент системи c	**Сукупність механізмів захисту** $\{x_{cp}\}$		
Виділені ресурси (W)	500	800	1000
КС «Київ»	1,3,4,5,7,8	1,3,4,5,6,7,8	1,2,3,4,5,6,7,8
КС «Бердичів»	1,3,5,7,8	1,3,4,5,7,8	1,2,3,4,5,7,8
КС «Красилів»	1,3,4,6,7	1,3,4,5,6,7	1,3,4,5,6,7,8
КС «Лубни»	1,3,5,7,8	1,3,4,5,7,8	1,3,4,5,6,7,8
КС «Боярка»	1,4,6,7	1,3,4,6,7	1,3,4,5,6,7
КС «Диканька»	1,4,6,7	1,3,4,6,7	1,3,4,5,6,7
КС «Роменська»	1,3,4,7	1,3,4,6,7	1,3,4,5,6,7
КС «Глушківська»	1,4,7	1,4,6,7	1,3,4,6,7
КС «Гребінківська»	1,4,7	1,3,4,7	1,3,4,5,7
КС «Зіньків»	4,7	1,4,7	1,3,4,7
КС «Решетилівка»	4,7	4,7	1,4,7

Де 1,2,3,4,5,6,7,8 - механізми захисту p, що були визначені в таблиці 3.3.

Висновки до розділу 3

В цьому розділі було здійснено оцінку цінностей компонентів системи диспетчеризації «Київтрансгаз», яка в подальшому буде використовуватися для оцінки можливих збитків. Успішна реалізація загрози проти одного із компонентів системи призведе до зупинки постачання газу користувачам (відмова в обслуговуванні), що еквівалентна цінності цього компонента для функціонування системи в цілому. За відсутності статистичних даних та фінансових звітів, припустимо, що завданий збиток пропорційний кількості населення району атакованої КС в якості споживачів газу.

Далі було сформовано модель зловмисника та загроз. Володіючи інформацією про мету та характерні особливост зловмисника, є можливість обрати найбільн вірогідні загрози ІБ a, застосовуючи які, він, ймовірно, досягне поставленої мети. Базуючись на цьому та на вразливостях нашої САК було отримано ймовірності реалізації цих загроз.

Вибір механізмів захисту, з орієнтацією на архітектуру обчислювального середовища та модель загроз є наступним етапом розробки політики безпеки. За допомогою методу експертної оцінки визначили дієвість кожного із механізмів захисту p проти визначених загроз a в системі $\boldsymbol{d_{ap}}$ та вартість їх реалізації $\boldsymbol{w_p}$.

І, нарешті, було визначено структуру системи захисту інформації, яка забезпечить мінімальне значення цільової функції (2.2) при заданих обмеженнях (ресурси на побудову СЗІ).

ВИСНОВКИ

У роботі подано вирішення актуальної наукової проблеми побудови системи захисту інформації за умови обмеженості ресурсів та розроблено алгоритм його реалізації на основі методів експертної оцінки, теорії ігор та математичного програмування.

Дослідження дало змогу дійти таких висновків:

1. На основі проведеного огляду й аналізу вихідної інформації було зроблено висновок про доцільність розробки підходу до синтезу структури системи захисту інформації в системах автоматичного керування (САК) критично важливими об`єктами з використанням методів теорії ігор, а також забезпечення рівня захищеності, що є необхідним, використовуючи мінімальну кількість витрат на системи захисту інформації та умови якщо характер атак зловмисника буде комплексним.

2. Розроблено алгоритм побудови СЗІ на основі застосування механізму теорії ігор, а саме: позиційної гри, у тому числі максимінної стратегії, що забезпечує мінімальне гарантоване значення ризику інформації.

3. Для вирішення конкретних завдань дослідження у роботі було використано методи експертної оцінки, методу гілок та границь та математичного програмування.

4. Практичну придатність розробленого підходу було показано на прикладі побудови системи захисту для САК в УМГ «Київтрансгаз». У результаті застосування розробленої моделі синтезовано структуру СЗІ та отримано розподіл механізмів захисту між компонентами системи диспетчеризації. Значною перевагою запропонованого підходу є вирішення поставленої задачі в умовах комплексності атаки зловмисника, тобто такої де поведінка порушника буде змінюватися з часом.

Розглянутий підхід дозволяє створити модель поведінки зловмисників різного типу. У той же час він буде важливим і для випадків циклічно повторюваної атаки порушником.

Подальшу перспективу розвитку підходу вбачаємо в аналізі ситуацій із недостатньою кількістю інформації, за умови коли одна конфліктуюча сторона або обидва супротивника не володіють інформацією щодо виконаних ходів суперника.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Архипов А.Е. Технологии експертного оценивания в задачах защиты информации / А.Е. Архипов // Інформаційні технології та комп'ютерна інженерія: міжнар. наук. техн. журн.—2005. — №1. —С. 89–94.

2. Грайворонський М.В. Безпека інформаційно-комунікаційних систем / М.В. Грайворонський, О.М. Новіков. — К.: BHV, 2009. — 608 с.

3. Глушак В.В. Метод проектування систем захисту інформації з використанням детермінованої гри «захисник-зловмисник» / В.В. Глушак, О.М. Новіков // Наукові вісті НТУУ «КПІ». — 2011. — № 2. — С. 46–53.

4. Мулен Э. Теория игр с примерами из математической экономики / Э. Мулен. — Москва: Мир, 1985. — 200 с.

5. Система диспетчеризації «Київтрасгаз» [Электронный ресурс]. – Режим доступу: http://atep.kpi.ua/files/pdf/kiyivtransgaz_1457089819.pdf

6. Brown G. Defending critical infrastructure / G. M. Brown, J. Carlyle, K. Salmerón // Interfaces. J. — 2006. — 36. — P. 530–544.

7. Brown G.M. Analyzing the vulnerability of critical infrastructure to attack and planning defenses. INFORMS Tutorials in Operations Research / G. M. Brown, J. Carlyle, K. Salmerón // Wood. – 2005. – Hanover: Institute for Operations Research and the Management Sciences, MD. C. 102–123.

8. Garcia M.L. The Design and Evaluation of Physical Protection Systems / M.L. Garcia. – Butterworth-Heinemann, Woburn, MA., 2001. – C. 39-48.

9. Wood A. Power Generation, Operation, and Control. 2nd ed. / A. Wood, B. Wollenberg. – New York: John Wiley and Sons, 1996. – P. 410-430.

10. Flammini F. Critical infrastructure security. Assessment, prevention, detection, response / F. Flammini // WIT Transactions on state-of-the-art in science and engineering. – Southampton: WIT Press, 2012. – Vol. 54.

11. Сташинський О.П. Інформаційна технологія підтримки прийняття рішень диспетчерського персоналу газотранспортного підприємства: дис. канд. техн. наук: 05.13.06 / Олександр Петрович Сташинський. – К., 2015. – 163 с.

12.Назаренко І.П. Інформаційна технологія підтримки прийняття рішень диспетчерського персоналу газотранспортного підприємства: дис. канд. техн. наук: 05.13.06 / Ігор Вікторович Назаренко. – Івано-Франківськ, 2015. – 225 с.

13. Roberts, N. Fault Tree Handbook. NUREG-0492 / N. Roberts, W. Vesely, D. Haasl, F. Goldberg. – Washington, D.C: US Nuclear Regulatory Commission, 1981.

14. Quesada I. An LP/NLP Based Branch and Bound Algorithm for Convex MINLP Optimization Problems // Computers Chem. Eng. — 1992. — 16 (10/11). [Электронный ресурс] / I. Quesada, I.E. Grossmann. – Режим доступу: — http://repository.cmu.edu/cgi/viewcotent.cgi?artcle=1176&context=cheme.

15. Глушак В.В. Синтез структури системи захисту інформації з використанням позиційної гри захисника та зловмисника / В.В. Глушак, О.М. Новіков // Системні дослідження та інформаційні технології. – 2013. – № 2. – С.89-100

16. Калиберда Е.А. Анализ уязвимостей по степени их влияния на защищённость и качество структурно-сложных информационных систем / Е.А. Калиберда, А.А. Рыбкин // Вестн. Ом. ун-та. – 2014. – № 2. – С. 130–135.

17. Назаренко І.В. Застосування технології розподіленого вводу-виводу в системах автоматичного керування технологічним обладнанням компресорного цеху / І.В. Назаренко, М.Я. Николайчук, В.Д. Ференець // Нафтогазова енергетика. – 2013. – № 2. – С. 79-84. – Режим доступу: http://nbuv.gov.ua/UJRN/Nge_2013_2_9

18. Positive research 2018. [Электронный ресурс]. – Режим доступу: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Positive-Research-2018-rus.pdf

19. Vulnerability Details : CVE-2011-2962 [Электронный ресурс]. – Режим доступу: https://www.cvedetails.com/cve/CVE-2011-2962/

20. PT-2013-39: Некорректная проверка входных данных в Wonderware Information Server [Электронный ресурс]. – Режим доступу: https://www.securitylab.ru/lab/PT-2013-39

21. PT-2014-17: Ненадежное шифрование данных учетных записей в Wonderware Information Server [Электронный ресурс]. – Режим доступу: https://www.securitylab.ru/lab/PT-2014-17

22. Топ 10 OWASP 2017. Десять самых критичных угроз безопасности веб приложений [Электронный ресурс]. – Режим доступу: https://www.owasp.org/images/9/96/OWASP_Top_10-2017-ru.pdf