Центральноукраїнський національний технічний університет
Механіко-технологічний факультет
Кафедра кібербезпеки та програмного забезпечення

”Допущено до захисту”
Завідувач кафедри кібербезпеки
та програмного забезпечення
д.т.н., професор
_____ Олексій СМІРНОВ
“____” _____ 2025 р.

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА
за другим (магістерським) рівнем вищої освіти
на тему
“Дослідження та програмна реалізація системи аудиту безпеки мережевих ICS/SCADA”

Виконав здобувач вищої освіти
ІІ курсу, групи КІ-24М
ОПП «Комп’ютерна інженерія»
спеціальності 123 «Комп’ютерна інженерія»
_____ Дабич А.В.
«____» _____ 2025 р.

Керівник проекту
кандидат технічних наук, доцент
_____ Буравченко К.О.
«____» _____ 2025 р.
Рецензент _____
_____

м. Кропивницький

АНОТАЦІЯ

Дабич А.В. Дослідження та програмна реалізація системи аудиту безпеки мережевих ICS/SCADA. 123 Комп'ютерна інженерія. Центральноукраїнський національний технічний університет. Кропивницький. 2025.

В даній випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для системи аудиту безпеки мережевих ICS/SCADA.

Метою розробки є дослідження та програмна реалізація системи аудиту безпеки мережевих ICS/SCADA.

Об'єктом дослідження є процес аудиту безпеки мережевих ICS/SCADA.

Предметом дослідження є методи аудиту безпеки мережевих ICS/SCADA.

Методи дослідження базуються на методах захисту інформації у мережі, методах математичної статистики, методах розробки програмного забезпечення.

Результат роботи – програмна реалізація системи аудиту безпеки мережевих ICS/SCADA.

В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

Розроблено зручний інтерфейс користувача. Наведені інструкції по роботі з програмними засобами.

Програма може використовуватися на ПЕОМ з ОС Windows 10/11.

Програму розроблено в середовищі Python.

Ключові слова: комп'ютерна інженерія, аудит безпеки, ICS/SCADA

ABSTRACT

Dabich A.V. Research and software implementation of the network ICS/SCADA security audit system. 123 Computer Engineering. Central Ukrainian National Technical University. Kropyvnytskyi. 2025.

In this final qualification work for the second (master's) level of higher education, software has been developed, which is intended for the network ICS/SCADA security audit system.

The purpose of the development is the research and software implementation of the network ICS/SCADA security audit system.

The object of the research is the process of network ICS/SCADA security audit.

The subject of the research is the methods of network ICS/SCADA security audit.

The research methods are based on methods of information protection in the network, methods of mathematical statistics, methods of software development.

The result of the work is the software implementation of the network ICS/SCADA security audit system.

In the process of working on the software model, an analysis of existing hardware and software tools was performed. All components of the developed software are fully described.

A user-friendly user interface has been developed. Instructions for working with the software are provided.

The program can be used on a PC with OS Windows 10/11.

The program is developed in the Python environment.

Keywords: computer engineering, security audit, ICS/SCADA

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

ALARA – As Low As Reasonably Achievable – настільки низько, наскільки це можливо – принцип прийнятного ризику

FMEA – Failure Modes and Effects Analysis – аналіз видів і наслідків відмов

HCR – Human Cognitive Reliability – Надійність людини як функція його здібностей

HEP – Human Error Probability – Імовірність помилки людини

IRRAS – Integrated Reliability and Risk Analysis System – інтегральна надійність та аналіз ризику систем – пакет прикладних програм

NUREG – Nuclear Regulatory – Стандарт США (керівництво) в атомній промисловості

NRC – Nuclear Regulatory Commission – Комісія з ядерного регулювання США

OHSAS – Occupational Health and Safety Assessment Series – Система менеджменту охорони здоров'я та безпеки персоналу

RRR – Risk Reduction Ratio – коефіцієнт зменшення ризику

RRI – Risk Reduction Interval – інтервал зменшення ризику

THERP – Technique for Human Error Rate Prediction – Методика аналізу помилок людини в техніці (США)

АВНВ – аналіз видів і наслідків відмов

ICS/SCADA, АС – атомна станція

АП – аварійна послідовність

БД – база даних

БП – базисна подія

ВП – вихідна подія

ГНД – галузевий нормативний документ

ДВ – дерево відмов

ДП – дерево подій

ЗІЗ – засоби індивідуального захисту

ІАБ – імовірнісний аналіз безпеки

ІП – ініціююча подія

КС – кінцевий стан

ЛЧ – людський чинник

МНС – Міністерство надзвичайних ситуацій

МОЗ – Міністерство охорони здоров’я

МОН – Міністерство освіти і науки

МП – мінімальні перерізи

ННДІОП – Національний науково-дослідний інститут охорони праці

НД – нормативний документ

НС – надзвичайна ситуація

НП – небажана подія

НВ – небезпечний випадок

ОП – охорона праці

ОПН – об’єкт підвищеної небезпеки

ПНО – потенційно небезпечний об’єкт

ПЛАС – план ліквідації аварійних станів

ПП – прикладна програма

ППР – планово-попереджальний ремонт

ПТЕ – правила технічної експлуатації

РОП – ризик орієнтований підхід

СБ – система безпеки

СТП – стандарт підприємства

СУОП – система управління охороною праці підприємства

ТО – технічне обслуговування

ФБ – функція безпеки

ВСТУП

Актуальність теми. Починаючи з кінця 60-х років минулого століття, промислові системи керування (Industrial Control System; ICS) з'явилися практично у всіх сферах, що мають відношення до сучасного життя: енергетика, промисловість, комунальні системи й інші області.

З моменту винаходу блокового цифрового контролера в 1968 році й до середини 90-х промислові системи керування були практично ізольовані й могли працювати з дуже обмеженим набором вхідних і вихідних даних із зовнішніх джерел.

Однак з появою дешевого устаткування, операційної системи Microsoft Windows, Active Directory і загальної стандартизації, сучасні корпоративні мережі стали одержувати й обробляти дані (а також виконувати інші безліч інших операцій) з мереж за межами традиційних ICS-мереж.

Незважаючи на те, що на даний момент уживає безліч зусиль по сегментації мереж пов'язаних з інформаційними й промисловими технологіями, границі дотепер залишаються розмитими, що доставляємо багато головного болю фахівцям з безпеки, що працює в багатьох індустріях.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи аудиту безпеки мережевих ICS/SCADA.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем аудиту безпеки мережевих ICS/SCADA.

– Дослідження системи аудиту безпеки мережевих ICS/SCADA.

– Програмна реалізація системи аудиту безпеки мережевих ICS/SCADA.

Об'єктом дослідження є процес аудиту безпеки мережевих ICS/SCADA.

Предметом дослідження є методи аудиту безпеки мережевих ICS/SCADA.

Методи дослідження базуються на методах захисту інформації у мережі, методах математичної статистики, методах розробки програмного забезпечення.

Наукова новизна отриманих результатів. У процесі рішення завдань, обумовлених цілями дослідження, отримані наступні результати:

– Удосконалено метод аудиту безпеки мережевих ICS/SCADA.

– Розроблено вітчизняний продукт аудиту безпеки мережевих ICS/SCADA, який має більш широкі можливості, на відміну від існуючих аналогів.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі аудиту безпеки мережевих ICS/SCADA.

Достовірність наукових результатів підтверджена теоретичними викладеннями, даними комп'ютерного моделювання, коректними дослідженнями параметрів на функціонуючій обчислювальній мережі, а також відповідністю отриманих результатів окремим результатам, наведеним у науковій літературі.

Робота апробована на LVII Науково-технічній конференції здобувачів вищої освіти LV науково-технічної конференції «Наука в ЦНТУ: основні досягнення та перспективи розвитку» (2025 р.), основні положення випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти надруковані у статті збірника праць молодих науковців ЦНТУ, випуск №15.

Таким чином, виходячи з вищеперерахованого, дослідження та програмна реалізація системи аудиту безпеки мережевих ICS/SCADA, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти.

1 ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ВИКОРИСТАННЯ

1.1 Призначення системи

Незважаючи на те, що терміни ICS (Промислова система керування) і SCADA (Диспетчерське керування й збір даних) часто використовуються як синоніми, між цими поняттями існує відмінність. Терміном ICS іменується загальна технологія, що включає в себе підкатегорію SCADA. Нижче перераховані приклади підкатегорій, які містить у собі технологія ICS:

Розподілені системи керування (DCS):

– Здійснюють моніторинг і керування процесами в режимі реального часу.

– Звичайно трохи компонент однієї системи перебувають у географічній близькості друг від друга, наприклад, нафтопереробного заводу, вугільної шахти, греблі гідроелектростанції й т.д. Як правило, компоненти розподіленої системи перебувають усередині одного будинку.

Програмувальні логічні контролери (PLC):

– Являють собою захищені компоненти, що управляють платами, які у свою чергу є частиною систем керування процесами.

Диспетчерське керування й збір даних (SCADA):

– У деякому змісті працюють як менеджерів.

– Диспетчерські сервера звичайно не приймають рішень.

– Диспетчерські сервера, як правило, перенаправляють команди від інших систем і людей.

Системи архівних даних

– Збирають і зберігають інформацію стосовно статистики процесів, показань датчиків, уведення/виводу й інші показники.

– Можуть бути необхідні для законодавчого й нормативного регулювання.

– Звичайно інформація зберігається в базах даних, наприклад, в MSSQL або Oracle.

Людино-машинний інтерфейс (HMI):

– Людино-машинні інтерфейси дозволяють інженерові здійснювати візуальний моніторинг всієї ICS-системи.

– Звичайно в графічному виді показують процеси й елементи системи (наприклад, джерела, ретранслятори й потоки інформації).

Вилучений термінал(RTU):

– Невеликі захищені комп'ютери, які збирають і співвідносять дані між фізичними сенсорами й ICS-процесами.

Додаткову складність в ICS-середовища вносять різні комунікаційні протоколи. Нижче перераховані як загальні, так і спеціальні протоколи, які використовуються в системах ICS:

– ANSI X3.28
– BBC 7200
– CDC Types 1 and 2
– Conitel 2020/2000/3000
– DCP 1
– DNP3
– Gedac 7020
– ICCP Landis & Gyr 8979
– Modbus
– OPC
– ControlNet
– DeviceNet
– DH+
– ProfiBus

– Tejas 3 and 5

– TRW 9550

1.2 Область застосування

Типова архітектура ICS-середовища

При проектуванні ICS-середовища повинні задовольнятися вимоги, пов'язані з високою відказостійкістю, законодавчими й нормативними актами й системою відновлення, що серйозно обмежує простір для вибору. Щоб відповідати всім необхідним правилам, більшість ICS-середовищ будуються на базі тртрівневої структури:

– На самому верхньому рівні використовуються людино-машинні інтерфейси й SCADA-сервера, які управляють низькими рівнями на базі набору вхідних параметрів або по команді оператора. Звичайно дані від SCADA-серверів надходять до людино-машинних інтерфейсами й далі відображаються на робочій станції інженера.

– На середньому рівні, як правило, відбувається збір і обробка вхідних і вихідних даних від інших шарів. Пристрою, що працюють на цьому рівні, звичайно називаються Полевими контролерами (Field Controller), які містять у собі Програмувальні логічні контролери (PLC), Інтелектуальні електронні пристрої (IED) і Вилучені термінали (RTU). Польові контролери можуть координувати дії на нижньому рівні на основі рішень, прийнятих на верхньому рівні або відсилати оброблені дані й статистику з нижнього рівня на верхній.

– На нижньому рівні працюють так звані Полеві пристрої, які відповідають за частини, що рухаються, і сенсори, управляють насосами, роботизованими руками й іншими механічними компонентами. Крім того, на цьому рівні звичайно є кілька сенсорів для моніторингу процесів і наступної передачі даних на середній рівень Полевим контролерам для обробки.

Для комунікації між шарами в ICS-середовищах звичайно використовуються різні протоколи. SCADA-сервер, що перебуває на верхньому рівні, спілкується з Полевими контролерами на середньому рівні за допомогою протоколів DNP3 або Modbus. Польові контролери взаємодіють із Полевими пристроями за допомогою протоколів HART, Foundation Fieldbus і ProfiBus.

Хоча проектування мереж, що задовольняють ICS-стандартам, може бути непростим, звичайно в організаціях вирішують це завдання за допомогою поділу ICS-інфраструктури на три зони.

У корпоративних зонах звичайно перебуває корпоративна мережа зі стандартними службами: електронна пошта, печатка, веб, ERP і. т. буд. У цій зоні перебувають усе сервера, що мають відношення до бізнесу, і робітники станції співробітників.

У демілітаризованих зонах (DMZ) звичайно дозволений непрямий доступ до інформації, генеруємой ICS-системою. У цій зоні, як правило, перебувають вторинні сервера з архівними даними й деякі веб- і термінальні додатки.

У зоні керування процесами перебувають три рівні ICS-системи, описані вище. Ця зона повинна бути повністю ізольована від Корпоративної зони, а з боку людино-машинних інтерфейсів і SCADA-серверів у зону керування процесами повинен бути обмежений доступ із правами тільки на читання.

Таким чином, виходячи з вищеперерахованого, дослідження та програмна реалізація системи аудиту безпеки мережевих ICS/SCADA, є актуальною задачею, яка потребує вирішення у даній випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти.

2 ПЕРЕГЛЯД АНАЛОГІЧНИХ ІСНУЮЧИХ СИСТЕМ

2.1 Огляд існуючих систем, технологій, архітектур, програмних рішень за профілем теми випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти

Сучасна промисловість залежить від автоматизованих систем управління для максимізації ефективності та забезпечення гнучкого виробництва. Однак сучасні кіберзлочинці розуміють цю залежність і розробили багато методів для компрометації та пошкодження промислових систем управління (ІСУ).

У цьому розділі буде досліджено, як ІКС вписується в ландшафт кібербезпеки. Ми дізнаємося про загрози, з якими стикаються системи ІКС, обговоримо найкращі практики щодо зменшення кіберзагроз та забезпечення безперебійної промислової діяльності.

Системи промислового керування (ІКС) та операційні технології (ОТ) є критично важливими концепціями в сучасній промисловості. Однак ці два підходи дещо відрізняються, і розуміння цих відмінностей важливе для захисту розгортання ІКС.

Операційні технології – це підмножина промислових технологій, яка контролює обладнання та мережі на підприємствах. Операційні технології перевіряють безперебійну та безпечну роботу виробничих або логістичних об'єктів, включаючи фізичну ефективність, умови навколишнього середовища та фактори кібербезпеки.

Системи промислового управління (СПУ) є підмножиною ОТ , що керують процесами в промислових умовах (включаючи кібербезпеку). Компоненти ІКС включають:

– Диспетчерський контроль та збір даних (SCADA): збирає дані з промислових датчиків та передає цю інформацію до централізованих центрів безпеки.

– Розподілені системи керування (РСК): РСК обробляє складні промислові умови. Наприклад, компанії можуть інтегрувати моніторинг на хімічних заводах або нафтопереробних заводах. Системи використовують розподілені датчики для підвищення ефективності та стійкості.

– Програмовані логічні контролери (ПЛК): ПЛК керують автоматизованими промисловими процесами. Вони дозволяють технічним спеціалістам автоматизувати виробничі та моніторингові функції, включаючи збір даних про загрози, сповіщення та реагування на інциденти.

Чому кібербезпека важлива для ICS?

Системи промислового управління є основоположними для сучасної промисловості. Вони контролюють виробничі лінії , що виробляють товари першої необхідності, керують електростанціями та нафтопереробними заводами , а також допомагають підтримувати та розширювати критично важливу інфраструктуру.

Однак розширення систем ICS принесло нові ризики для кібербезпеки. Кіберзлочинці зараз прагнуть завдати шкоди життєво важливим галузям промисловості за допомогою цілеспрямованих кібератак, часто зосереджуючись на технології ICS для досягнення максимального ефекту. Як наслідок, кібербезпека промислових систем управління стає критично важливою.

Подумайте про ризики, пов'язані з відсутністю захисту мережевої інфраструктури ICS. Кіберзагрози можуть пошкодити обладнання та поставити під загрозу фізичну безпеку працівників. Наприклад, у 2010-х роках шкідливе програмне забезпечення під назвою TRITON вразило системи промислової безпеки по всьому Близькому Сходу.

Ще гірше те, що зловмисники можуть завдати шкоди всьому населенню. Одна з атак, задокументована Verizon, була спрямована на логічні контролери

водопостачальної компанії з метою забруднення водопостачання шкідливими хімічними речовинами. Атака провалилася, але залишається можливою.

У більшості випадків зловмисники завдають компаніям фінансової , а не фізичної шкоди. Атаки на системи контролю та контролю (ICS) часто руйнують продуктивність, виводячи з ладу заводи та обладнання. Наприклад, атака на об'єкти Norsk Hydro у 2019 році зрештою коштувала компанії понад 50 мільйонів доларів.

З огляду на ці цифри та наслідки атак, захист систем ICS має бути пріоритетом кібербезпеки для всіх промислових організацій.

Розуміння ризиків безпеки ICS

Промислова кібербезпека починається з усвідомлення ризиків, з якими стикаються промислові системи управління. Оскільки ICS/OT все більше узгоджуються з IT, виробники стикаються з багатьма критичними ризиками, багато з яких розвиваються та стають все серйознішими.

До поширених вразливостей ICS належать:

– Використання застарілих систем: промислові організації часто повільно оновлюють програмне забезпечення, яке відстає від інших технологій. Непатчені операційні системи та прошивки спонукають зловмисників використовувати слабкі місця. Ця проблема подвоюється, якщо постачальники більше не підтримують застарілі системи. У такій ситуації компаніям нікому порадити їх або надати оновлення.

– Налаштування за замовчуванням: Компанії часто встановлюють промислове обладнання або пристрої Інтернету речей, не змінюючи налаштувань за замовчуванням. Зловмисники можуть швидко отримати доступ до систем ICS за допомогою паролів за замовчуванням , що ставить під загрозу все промислове середовище.

– Відсутність шифрування: Системи ICS покладаються на команди для керування комутаторами та процесами. Однак кіберзлочинці, які отримують доступ до цього трафіку, можуть захопити промислові системи та керувати

виробничим обладнанням. Шифрування вирішує цю проблему, роблячи команди незрозумілими для сторонніх осіб.

– Ризики, пов’язані з віддаленим доступом: постачальники та IT-персонал можуть отримувати віддалений доступ до критично важливих систем для керування налаштуваннями та моніторингу продуктивності. Це являє собою вразливість, якщо компанії не перевіряють з’єднання за допомогою надійних заходів контролю доступу.

Хто використовує вразливості ICS? Розуміння ландшафту загроз

Багато зловмисників використовують ці поширені вразливості ICS. Наприклад, компанії без надійного контролю доступу, сегментації та автентифікації є легкою мішенню для внутрішніх загроз. Інсайдери можуть отримати облікові дані та здійснювати атаки або надавати інформацію зловмисникам-зовнішнім особам.

Однак багато атак відбуваються за кордоном. Так звані атаки національних держав залучають кіберзлочинців, що підтримуються державами. Чудовим прикладом є створений США черв'як Stuxnet, який був спрямований на іранські ядерні об'єкти, але атаки національних держав також здійснювалися з Росії, Китаю, Північної Кореї та Ізраїлю.

Також існують тіньові злочинні угруповання. У 2024 році кількість груп програм-вимагачів, які атакували цілі ICS, зросла на 60%, а кількість атак зросла на 87%. Промислові цілі є привабливими, оскільки компанії не можуть дозволити собі втрачати виробничий час. Наприклад, Colonial Pipeline виплатила зловмисникам-вимагачам 4,4 мільйона доларів у 2021 році, і менші платежі відбуваються щодня.

Зрештою, сторонні облікові записи можуть наражати компанії на ризики ланцюга поставок без належної перевірки та оцінки безпеки. Якщо постачальник зазнає кібератаки, наслідки можуть поширитися на фабрики, які використовують їхню продукцію.

Що відбувається, коли відбуваються атаки на ICS?

Яким би не був задіяний зловмисник, атаки ICS можуть бути руйнівними. Найбільш очевидними наслідками є фінансові. Як зазначалося вище, зловмисники можуть вимагати величезні платежі за програму-вимагач, щоб розблокувати системи. Однак ризики атак ICS виходять за рамки виплат викупу.

На практичному рівні атаки на ICS порушують промислове виробництво , оскільки маніпуляції зі SCADA призводять до нестабільної роботи виробничих ліній та їх зупинки. DDoS-атаки перевантажують та пошкоджують обладнання, що потенційно підвищує ризик пожежі.

Мережі критичної інфраструктури стають ненадійними та потребують детальної оцінки , що може бути головним болем для комунальних підприємств, таких як постачальники електроенергії чи води. Ці проблеми посилюються, якщо зловмисники порушують роботу технологій моніторингу, надаючи неправдиві показники.

Системи безпеки можуть вийти з ладу або викликати хибні тривоги. Фізичний збій може завдати шкоди співробітникам, клієнтам та навколишньому середовищу. Коли це трапляється, порушення нормативних вимог майже гарантовані, а репутаційна шкода завжди є небезпечною.

Найкращі практики безпеки ICS

Кіберзагрози проти критично важливих систем стають дедалі складнішими та руйнівнішими. Зловмисники адаптують свої методи до конкретних компаній та місць розташування. Вони досліджують застарілі системи, промислову архітектуру та заходи безпеки, щоб виявити, здавалося б, незначні вразливості.

У цьому контексті всі промислові організації повинні зміцнити свою позицію в галузі кібербезпеки ІКС. Давайте розглянемо деякі найкращі практики для досягнення цієї мети.

Сегментація мережі

Сегментація середовищ ICS є важливою частиною кібербезпеки для промислових систем керування. Це пояснюється тим, що сегментація мережі

поділяє промислові мережі на області з правами доступу, призначеними певним командам і співробітникам. Команди безпеки можуть контролювати пристрої ICS і виявляти підозрілу активність, гарантуючи, що лише авторизовані користувачі матимуть доступ до конфігурацій або потоків даних.

Сегментація мережі також може допомогти обмежити радіус успішних атак. Вона може, наприклад, запобігти поширенню шкідливого програмного забезпечення в мережі. Це особливо корисно для пом'якшення атак типу "відмова в обслуговуванні", які перевантажують промислові мережі трафіком.

В ідеалі, компанії повинні використовувати хмарні брандмауери для впровадження сегментації мережі. Хмарні брандмауери забезпечують контроль доступу до ваших пристроїв ICS. Ви можете забезпечити безперешкодний доступ для співробітників, які мають поважну причину для зміни налаштувань ICS та виключення всіх інших.

Навчання співробітників

Передові засоби безпеки марні, якщо співробітники не дотримуються політик безпеки. Наприклад, компанії повинні навчати співробітників важливості багатофакторної автентифікації (MFA) та безпеки паролів. Забезпечте дотримання політик безпеки пристроїв, дозволяючи підключатися до мережі ICS лише схваленим робочим пристроям.

Крім того, пов’яжіть ризики фішингу з атаками ICS. Працівники повинні знати, як розпізнавати фішингові електронні листи та уникати заражень шкідливим програмним забезпеченням.

Регулярно виправляйте та оновлюйте програмне забезпечення

Як ми вже обговорювали раніше, застарілі системи є поширеними точками збою в кібербезпеці промислових систем керування. Компанії дозволяють програмному забезпеченню для керування застарівати. Підприємства повинні регулярно випускати оновлення, щоб пом'якшити експлойти та випередити зловмисників.

Багатофакторна автентифікація (MFA)

Надійні засоби контролю доступу запобігають несанкціонованому доступу, навіть якщо зловмисники отримують імена користувачів та паролі. Багатофакторна автентифікація (MFA) вимагає унікальних одноразових облікових даних на додаток до паролів. Це допомагає блокувати ненадійних користувачів на межі мережі.

Багатофакторна автентифікація (MFA) ще ефективніша завдяки посиленій безпеці паролів. Користувачам ICS слід регулярно змінювати свої паролі та використовувати надійні, унікальні паролі (без посилання на особисту інформацію).

Менеджери паролів можуть допомогти, забезпечуючи простий інтерфейс для керування обліковими даними. Інтегруйте такі інструменти, як NordPass, із заходами безпеки вашої ICS, щоб послідовно забезпечувати дотримання політик щодо паролів та мінімізувати ризики крадіжки облікових даних.

Безпечний віддалений доступ

ICS зазвичай є віддаленою технологією. Інженери рідко керують обладнанням на місці та залежать від з'єднань між зовнішніми мережами та пристроями ICS. Це відкриває шлях для атак з метою захоплення даних та крадіжки облікових даних. Віртуальні приватні мережі (VPN) допомагають вирішити цю проблему.

VPN допомагають захистити дані компанії, створюючи зашифроване з’єднання для віддаленого доступу співробітників до мережі. Бізнес-VPN гарантує захист віддаленого доступу до критично важливих систем, зменшуючи ризик кібератак.

Використовуйте найновішу інформацію про загрози

Багато атак на системи контролю та контролю (ICS) походять від організованих злочинних колективів та національних держав. Такий рівень організації робить атаки потужнішими, але має й позитивну сторону: цілі можуть досліджувати активні загрози та застосовувати проактивні заходи безпеки.

Використовуйте виявлення загроз та аналітику, щоб випередити зловмисників ICS. Аналітика загроз NordStellar активно відстежує поточні загрози та виявляє витік облікових даних у даркнеті. Маючи ці знання, команди безпеки можуть виявляти критичні загрози та усувати експлойти до того, як відбудуться атаки.

Які відмінності між системами ICS та SCADA?

Перш ніж ми закінчимо, важливо уточнити, чим відрізняються системи ICS та SCADA. Як згадувалося раніше, система супервізійного контролю та збору даних (SCADA) – це система моніторингу , яка збирає дані з промислових датчиків.

SCADA найчастіше асоціюється з розподіленими промисловими середовищами. Наприклад, для нафтопроводів потрібні тисячі датчиків SCADA для контролю структурної цілісності, перевірки безпеки працівників та виявлення потенційних витоків.

ІКС – це загальний термін, що стосується систем, які моніторять та контролюють промислове середовище. SCADA є елементом більшості розгортань ІКС, але ІКС – це більше, ніж просто збір даних. ІКС – це модель керування. Пристрої ІКС аналізують та використовують дані для керування промисловими процесами.

Як NordLayer може допомогти захистити системи ICS?

Кібербезпека ICS є критично важливою в сучасній економіці. Постачальники енергії, виробники, логістичні компанії та всі промислові організації стикаються з серйозними та зростаючими ризиками кібербезпеки. Допомога експертів часто є необхідною, і саме тут може допомогти NordLayer.

Рішення NordLayer щодо кібербезпеки для виробництва допомагають знизити ризики ICS та запобігти руйнівним кібератакам.

Рішення NordLayer для контролю доступу регулюють доступ до ресурсів ICS, блокуючи неавторизованих осіб та забезпечуючи безперешкодний доступ співробітників. Хмарний брандмауер дозволяє детально сегментувати мережу,

зменшуючи поверхню атаки. Інструменти виявлення загроз контролюють вашу мережу, а наш VPN забезпечує безпечний віддалений доступ до всіх пристроїв ICS.

2.2 Обґрунтування вибору засобів для побудови системи та мови програмування

Python – високорівнева мова програмування, яку називають другою за популярністю в світі. Її використовують для розробки вебзастосунків, програмного забезпечення, машинного навчання. Python застосовують для вирішення робочих завдань у компаніях Google, Instagram, Facebook, IBM, NASA, Dropbox, Netflix та інших. Розробники цінують цю мову програмування за простоту у вивченні, ефективність та мультиплатформність.

Python – скриптова мова програмування з досить простим синтаксисом. Для розуміння достатньо порівняти принципи написання найпростішої програми, яка виводить на екран текстове повідомлення. Саме тому мова програмування Python більш доступна для новачків, а професіонали встигли адаптувати її для вирішення великої кількості завдань. Це мультиплатформне рішення, тому знання Python дає можливість працювати у різних сферах: від розробки мобільних застосунків до ігрової індустрії та штучного інтелекту.

У мови програмування динамічна типізація: є можливість передавати до функцій будь-який тип даних без попереднього вказання. Інтерпретованість дозволяє знаходити помилки у коді ще до повної збірки у робочий застосунок. При цьому Python дуже чітко дає зрозуміти, де та через що виникла помилка.

Це мова об'єктно-орієнтованого програмування (ООП). Програмне забезпечення на Python оформлене у вигляді моделей, які можуть бути зібраними у пакети. Тип та структуру кожного об’єкта можна запитати під час виконання програми. Для кожного з об’єктів можна отримати всю інформацію щодо його внутрішньої структури. Окрім того:

– у мови логічний синтаксис, завдяки чому вихідний код легко читати та розуміти;

– гнучкість та масштабованість Python дозволяє адаптувати високорівневу логіку та розширяти складні застосунки, як тільки виникне така необхідність;

– розробка на Python у більшості випадків проходить швидше, ніж на інших мовах програмування;

– Python – інтерпретована мова програмування. Це значить, що код можна написати у будь-якому текстовому файлі на будь-якій платформі, і потім успішно запустити;

– у Python – колосальна спільнота однодумців. Тож будь-які складнощі конкретних розробників вирішуються колективно.

Проте є декілька особливостей, які можна віднести до недоліків. Це повільність (ця мова програмування хоч і універсальна, проте повільніша за інші), велика кількість ресурсів, необхідних для роботи та «прив'язаність» до системних бібліотек.

Мова програмування Python використовується у наступних сферах:

1. Розробка програмних застосунків будь-якого напрямку.

2. Розробка серверної частини мобільних застосунків (найпопулярніший напрямок).

3. Ігри. Багато сучасних ігор для комп'ютерів (наприклад, World of Tanks) частково чи повністю написані на Python.

4. Вбудовані системи для різних пристроїв. Дуже часто Python використовують для написання внутрішніх платформ управління банкоматами.

5. Скрипти та плагіни до уже реалізованих програм для автоматизації процесів чи створення інших рішень.

6. Тестування (автоматизація цього процесу).

7. Машинне навчання. – основна мова для написання алгоритмів і аналітичних застосунків у сфері Machine Learning.

Бібліотеки Python

Різні бібліотеки Python використовують для виконання конкретних завдань. Наприклад, Matplotlib підходить для відображення даних у двовимірній та тривимірній графіці. Pandas підходить для зручної роботи з даними. NumPy дозволяє створювати масиви та керувати ними. Requests використовується для веброзробки. OpenCV-Python відкриває можливості для обробки зображень з метою оптимізації систем «машинного зору».

Найвідоміші фреймворки для мови програмування Python

Фреймворки Python допомагають створити зручне та функціональне середовище для розробки. У них міститься набір інструментів, модулів та бібліотек, корисних для виконання конкретних завдань. Це значно полегшує роботу: наприклад, дає змогу не витрачати час на розписування дій, які повторюються, а використати релевантний інструмент. Тож є можливість позбутися рутинних процесів та сконцентруватися на логіці проєкту.

Серед найпопулярніших фреймворків для Python:

– Django – найстаріший та найвідоміший. Створений для реалізації великих інтерактивних проєктів;

– Pyramid – зручний у налаштуваннях, і дає можливість реалізувати складні нестандартні ідеї;

– Web2py – підходить в першу чергу для вебзастосунків і може використовуватись на будь-яких архітектурах.

Популярні Python IDE

IDE або інтегровані середовища розробки – це програмне забезпечення, яке надає розробникам необхідні інструменти для написання, редагування, тестування та налаштування коду. Для розробки на Python найчастіше використовують IDE PyCharm, IDLE, Spyder та Atom.

2.3 Розгорнута постановка завдання

Згідно з технічним завданням на випускну кваліфікаційну роботу за другим (магістерським) рівнем вищої освіти, реалізації підлягає програмне забезпечення, яке призначено для системи аудиту безпеки мережевих ICS/SCADA.

В процесі розробки випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти необхідно виконати наступний обсяг роботи:

а) провести аналіз існуючих систем-аналогів для виявлення їх позитивних і негативних якостей. Результати аналізу врахувати в подальших розробках;

б) вибрати та обґрунтувати методику побудови системи контролю роботи технологічного обладнання на виробництві в автоматизованому режимі. Розробити функціональну та структурну схеми системи;

в) розробити програмне забезпечення системи, що дозволить реалізувати поставлену технічним завданням задачу. Побудувати блок-схеми алгоритмів програми та підпрограми;

г) організувати інтерфейс користувача з метою формування та виводу на екран ЕОМ повідомлень про некоректні дії користувача та нестандартні ситуації в роботі технологічного обладнання;

д) розробити рекомендації по організаційних та методичних заходах, які забезпечать впровадження системи в промислову експлуатацію та її подальшу успішну експлуатацію;

е) провести розрахунки по визначенню економічної ефективності розробленої системи;

ж) розробити заходи по охороні праці при впровадженні та експлуатації системи, а також розробити заходи з цивільного захисту;

з) сформувати висновки про виконаний обсяг робіт та одержані результати.

3 ОПИС І ОБҐРУНТУВАННЯ ПРОЕКТНИХ РІШЕНЬ

3.1 Опис функціонування системи

Системи безпеки ICS/SCADA захищають промислові системи керування та мережі диспетчерського керування й збору даних, які керують 90% критичної інфраструктури в усьому світі, запобігаючи кібератак, які завдають середньої шкоди в розмірі 5,9 мільйона доларів на інцидент. Системи промислового керування керують електромережами, що обслуговують 7,8 мільярда людей, водоочисними спорудами, що переробляють 147 мільярдів галонів щодня, та виробничими підприємствами, що виробляють товарів на суму 14,2 трильйона доларів щорічно. Ці системи щодня стикаються з 2400 кібератак, причому успішні порушення призводять до збоїв у роботі, які тривають в середньому 23 дні, та загрожують безпеці людей у 47% інцидентів, що потребують комплексного захисту.

Ключові висновки:

– Системи ICS/SCADA контролюють 90% глобальної критичної інфраструктури, і на ці мережі щодня направляється 2400 кібератак.

– Порушення безпеки коштують організаціям в середньому 5,9 мільйона доларів США з 23-денними перебоями в роботі

– 73% систем ICS/SCADA мають невиправлені вразливості через вимоги цілодобової роботи

– Сегментація мережі зменшує успішність атак на 84% за умови правильного впровадження розділення IT/OT

– Відповідність таким стандартам, як NIST SP 800-82 та IEC 62443, запобігає 67% поширених векторів атак.

Безпека ICS/SCADA – це захисні заходи, технології та практики, що захищають промислові системи управління, мережі диспетчерського контролю та

збору даних від кіберзагроз, фізичних атак та операційних збоїв. Безпека ICS/SCADA охоплює комплексний захист операційних технологій, що контролюють промислові процеси у виробничому, енергетичному, водному та транспортному секторах. ICS представляє ширшу категорію операційних технологій, що контролюють промислові процеси, тоді як SCADA спеціально контролює та контролює розподілені активи в різних географічних регіонах.

ІКС включає програмовані логічні контролери (ПЛК), розподілені системи керування (РСК) та людино-машинні інтерфейси (ХМІ), що керують 4,7 мільйонами промислових об'єктів по всьому світу. Системи SCADA збирають дані в режимі реального часу з 23 мільйонів віддалених терміналів (RTU) по всьому світу, що дозволяє операторам контролювати та керувати інфраструктурою, що охоплює тисячі миль. Зв'язок між ІКС та SCADA передбачає функціонування СКАДА як рівня нагляду над компонентами ІКС, що забезпечує централізовану видимість та контроль критично важливих операцій.

Як працює безпека ICS/SCADA?

Безпека ICS/SCADA працює за допомогою багаторівневих захисних механізмів, включаючи сегментацію мережі, спеціалізовані протоколи, системи виявлення вторгнень та контроль доступу, що захищають промислові мережі від кіберзагроз. Мережева архітектура реалізує рівні моделі Purdue, що відокремлюють корпоративні IT від операційних технологій за допомогою демілітаризованих зон та брандмауерів. Промислові протоколи, такі як Modbus, DNP3 та OPC, вимагають протокольно-залежних засобів контролю безпеки, що виявляють шкідливі команди та спроби несанкціонованого доступу.

Механізми безпеки включають односпрямовані шлюзи, що запобігають досягненню 99,9% мережевих атак критично важливих систем керування. Сегментація мережі створює ізольовані зони, зменшуючи поверхню атаки на 73% та обмежуючи порушення в певних областях. Системи виявлення вторгнень щодня відстежують 8,4 мільярда пакетів промислової мережі, виявляючи аномальну поведінку, що вказує на кібератаки або несправності системи.

Чому безпека ICS/SCADA є критично важливою для бізнес-операцій?

Безпека ICS/SCADA має вирішальне значення для бізнес-операцій, оскільки потенційні наслідки включають виробничі втрати в розмірі 1,4 мільйона доларів США щогодини, інциденти безпеки, що щорічно впливають на 10 000 працівників, та збої в інфраструктурі, що порушують роботу мільйонів громадян. Кібератаки на промислові системи зросли на 140% між 2020 і 2024 роками, причому програми-вимагачі були спрямовані на 56% виробничих потужностей і спричиняли середній час простою 21 день. Передові постійні загрози з боку 37 угруповань національних держав активно націлені на критичну інфраструктуру з метою шпигунства та потенційних можливостей порушення роботи.

У 2010 році Stuxnet продемонстрував вразливість ICS, знищивши 1000 іранських центрифуг за допомогою складних маніпуляцій з ПЛК, одночасно відображаючи операторам нормальну роботу. У 2015 році шкідливе програмне забезпечення BlackEnergy порушило роботу українських енергомереж, залишивши 230 000 жителів без електроенергії протягом 6 годин у зимових умовах. У 2017 році шкідливе програмне забезпечення Triton/Trisis було спрямоване на системи безпеки, намагаючись відключити можливості аварійного вимкнення на нафтохімічних об'єктах, що потенційно могло спричинити вибухи.

Поширені вразливості присутні у 73% систем ICS/SCADA, включаючи застарілі технології, яким в середньому 19 років, і які не мають вбудованих функцій безпеки. Плоска мережева архітектура у 61% об'єктів дозволяє зловмисникам рухатися в горизонтальному напрямку після того, як зловмисники порушують захист периметра. Відсутність моніторингу в режимі реального часу у 43% промислових мереж дозволяє зловмисникам діяти непоміченими в середньому протягом 246 днів.

Як організації можуть подолати проблеми безпеки ICS/SCADA?

Організації можуть подолати проблеми безпеки ICS/SCADA, впроваджуючи спеціалізовані стратегії, що враховують унікальні операційні обмеження, включаючи вимоги до цілодобової доступності, 20-річний життєвий

цикл обладнання та критично важливі для безпеки операції, які не терплять перебоїв. Обмеження щодо виправлень впливають на 82% середовищ ICS, де системи не можна вивести з режиму автономного режиму для оновлень, що вимагає компенсуючих елементів керування, таких як віртуальне виправлення та мережева ізоляція. Застарілі системи, несумісні із сучасними інструментами безпеки, вимагають використання технологій-обгорток, що забезпечують захист без модифікації оригінального обладнання.

Спеціалізовані інструменти безпеки для OT, розроблені для промислових протоколів та вимог реального часу, захищають системи, не впливаючи на роботу. Рішення для пасивного моніторингу аналізують мережевий трафік без надсилання пакетів, запобігаючи випадковим збоям у роботі системи, які впливають на 11% активних сканерів. Інструменти інвентаризації активів виявляють 100% підключених пристроїв, включаючи 31%, які зазвичай невідомі операторам, завдяки комплексним процесам виявлення.

Програми навчання персоналу навчають 2,3 мільйона промислових операторів у всьому світі ризикам кібербезпеки та процедурам реагування. Інженерні команди проходять навчання з безпеки операційних систем, що охоплює безпечне програмування для ПЛК, посилення мережевої архітектури та реагування на інциденти. Перехресне навчання між командами IT та операційних систем усуває прогалини в знаннях, і 89% успішних програм потребують управління культурними змінами.

Поширені загрози для ICS/SCADA

Поширеними загрозами для ICS/SCADA є цільове шкідливе програмне забезпечення, дії інсайдерів, компрометація ланцюгів поставок, мережеві атаки та зловживання фізичним доступом, що завдає середньої шкоди в розмірі 5,9 мільйона доларів США за інцидент. Ці загрози використовують вразливості операційних технологій за допомогою складних методів атак, розроблених спеціально для промислового середовища.

Шкідливе програмне забезпечення та програми-вимагачі, спрямовані на SCADA

Шкідливе програмне забезпечення та програми-вимагачі атакують системи SCADA через спеціалізовані варіанти, розроблені для промислових процесів, причому кількість атак зросла на 2000% з 2010 року. Атаки програм-вимагачів на промислові об'єкти вимагають середніх платежів у розмірі 2,3 мільйона доларів США, шифруючи HMI та бази даних історії, критично важливі для операцій. Програма-вимагач EKANS спеціально націлена на промислові системи управління, перевіряючи та завершуючи 64 процеси, специфічні для ICS, до початку шифрування. Методи збереження шкідливого програмного забезпечення використовують інженерні робочі станції, причому 43% атак відбуваються із заражених ноутбуків постачальників під час технічного обслуговування.

Внутрішні загрози та людські помилки

Внутрішні загрози та ризики людських помилок становлять 34% інцидентів безпеки ICS, причому зловмисники завдають збитків у середньому на суму 4,7 мільйона доларів США через саботаж або крадіжку даних. Внутрішні загрози включають співробітників, підрядників та постачальників з доступом до систем, що становить 67% ризиків безпеки, часто без навчання з питань безпеки. Людська помилка спричиняє 52% інцидентів безпеки ICS, включаючи неправильну конфігурацію, переходи за фішинговими посиланнями та випадкове відключення засобів контролю безпеки. Моніторинг привілейованих користувачів виявляє 89% внутрішніх загроз, зменшуючи вплив інцидентів на 71% завдяки ранньому виявленню та реагуванню.

Компроміси в ланцюжку поставок

Компрометації ланцюгів поставок впливають на ICS/SCADA через атаки, спрямовані на постачальників та інтеграторів, які зросли на 430% між 2020 і 2024 роками, торкнувшись тисяч клієнтів нижчої ланки. Атаки на ланцюги поставок, такі як SolarWinds, вплинули на 18 000 організацій, включаючи операторів

критичної інфраструктури, які керують системами живлення та водопостачання. Апаратні імплантати, виявлені у 0,3% поставок промислового обладнання, забезпечують постійний бекдор-доступ, що витримує оновлення прошивки та скидання системи. Вразливості сторонніх компонентів впливають на 73% пристроїв ICS через спільні бібліотеки та вбудовані системи, що вимагають комплексної безпеки ланцюга поставок.

Мережева атака

Методи мережевих атак включають атаки типу «людина посередині», які перехоплюють та змінюють 31% незашифрованого зв'язку ICS, маніпулюючи показаннями датчиків та командами керування. Атаки типу «відмова в обслуговуванні», спрямовані на промислові мережі, спричиняють середній час простою 14 годин, що коштує 940 000 доларів США за інцидент через втрати виробництва. Експлуатація протоколів використовує незахищені за своєю природою промислові протоколи, 67% з яких не мають можливостей автентифікації або шифрування. Мережева розвідка виявляє вразливі системи у 94% промислових мереж протягом 72 годин після першого доступу.

Експлуатація фізичного доступу

Фізичний доступ дозволяє здійснювати експлуатацію шляхом обходу засобів контролю безпеки мережі, причому 23% об'єктів мають недостатній фізичний захист критично важливих систем керування. Атаки на основі USB через знімні носії залишаються ефективними у 61% систем з обмеженим доступом, поширюючи шкідливе програмне забезпечення по ізольованих мережах. Введення несанкціонованих пристроїв, включаючи точки бездротового доступу, щорічно ставить під загрозу 17% захищених об'єктів, створюючи несанкціоновані мережеві мости. Фізичне втручання в датчики та виконавчі механізми призводить до збоїв у процесах, які не виявляються системами кібермоніторингу, зосередженими на мережевому трафіку.

Що таке стратегії та найкращі практики кібербезпеки ICS/SCADA?

Стратегії кібербезпеки ICS/SCADA – це підходи до глибокого захисту, що поєднують сегментацію мережі, принципи нульової довіри, безпечний віддалений доступ, безперервний моніторинг та планування реагування на інциденти, що зменшує успішність атак на 84%. Ці стратегії враховують унікальні вимоги до операційних технологій, зберігаючи при цьому доступність та безпеку системи.

Як сегментація мережі захищає ICS/SCADA?

Сегментація мережі захищає ICS/SCADA, розділяючи IT- та OT-середовища за допомогою брандмауерів, зменшуючи успішність горизонтального переміщення на 91% під час порушень. Сегментація мережі реалізує модель Пердью, створюючи ієрархічні зони з контрольованим зв'язком між рівнями, що містять 87% атак у початкових зонах компрометації. Мікросегментація в OT-мережах ізолює критичні системи, обмежуючи радіус вибуху під час виникнення інцидентів. Розгортання DMZ між IT- та OT-мережами фільтрує 4,7 мільярда спроб підключення щодня, блокуючи 99,3% несанкціонованого трафіку.

Як принципи нульової довіри застосовуються до ICS/SCADA?

Принципи нульової довіри застосовуються до ICS/SCADA шляхом перевірки кожного з'єднання незалежно від джерела, що зменшує несанкціонований доступ на 94% завдяки постійній перевірці. Архітектура нульової довіри для ICS/SCADA перевіряє всіх користувачів, пристрої та програми, запобігаючи 78% атак на основі облікових даних. Доступ з мінімальними привілеями обмежує користувачів мінімально необхідними дозволами, що містить пошкодження від скомпрометованих облікових записів. Безперервна перевірка відстежує моделі поведінки, виявляючи аномалії у 97% сценаріїв внутрішніх загроз.

Що таке протоколи безпечного віддаленого доступу?

Безпечні протоколи віддаленого доступу замінюють 73% вразливих VPN-з’єднань на зашифровані сервери переходів та рішення для керування привілейованим доступом. Багатофакторна автентифікація запобігає 99,9%

автоматизованих атак на портали віддаленого доступу, що використовуються постачальниками та підрядниками. Запис та моніторинг сеансів відстежують усі віддалені дії, надаючи судово-медичні докази для 100% віддалених сеансів. Контроль доступу на основі часу обмежує вікна з'єднань, зменшуючи вразливість на 67% порівняно з методами постійного доступу.

Як працюють безперервний моніторинг та виявлення аномалій?

Безперервний моніторинг та виявлення аномалій працюють шляхом аналізу 12 мільярдів подій мережі ICS щодня, виявляючи загрози протягом 4 хвилин після початкової активності. Безперервний моніторинг використовує алгоритми машинного навчання для базової оцінки нормальної роботи, а потім виявляє відхилення з точністю 94% та рівнем хибних спрацьовувань 0,3%. Моніторинг активів відстежує зміни конфігурації, виявляючи несанкціоновані модифікації, щомісяця впливають на 31% пристроїв ICS. Моніторинг змінних процесу виявляє маніпулювання показаннями датчиків та командами керування, що вказують на кіберфізичні атаки.

Чому важливі планування реагування на інциденти та проведення навчальних заходів?

Планування реагування на інциденти та практичні навчання є важливими, оскільки плани, специфічні для ICS/SCADA, скорочують час відновлення на 73% порівняно із загальними процедурами реагування на IT. Плани реагування на інциденти враховують унікальні операційні вимоги, надаючи пріоритет критично важливим для безпеки системам та підтримуючи роботу під час інцидентів. Практичні навчання, що проводяться щоквартально, покращують координацію команди, виявляючи прогалини в процесах у 89% симуляцій. Посібники з поширених сценаріїв, включаючи атаки програм-вимагачів та системи безпеки, допомагають у прийнятті рішень, що запобігають паніці.

Що таке стандарти безпеки ICS/SCADA та рамки відповідності?

Стандарти безпеки та структури відповідності ICS/SCADA є базовими вимогами та найкращими практиками для організацій, які дотримуються структур, що зменшує кількість інцидентів безпеки на 67% порівняно з об'єктами, що не відповідають вимогам. Ці стандарти враховують унікальні вимоги до операційних технологій, включаючи продуктивність у режимі реального часу, доступність та безпеку.

Стандарт NIST SP 800-82 надає комплексні рекомендації щодо безпеки ICS, яких прийняли 43% операторів критичної інфраструктури США, враховуючи унікальні вимоги до 240 засобів контролю безпеки. Впровадження зменшує вразливості на 71% завдяки систематичному управлінню ризиками та вибору засобів контролю безпеки. Серія ISA/IEC 62443 представляє міжнародні консенсусні стандарти безпеки промислової автоматизації, що впроваджені в 67 країнах.

Стандарти NERC CIP вимагають від 3000 північноамериканських операторів оптових електричних систем дотримання 45 вимог за 11 стандартами. Порушення призводять до щоденних штрафів у розмірі 1 мільйона доларів, тоді як впровадження запобігає 73% поширених векторів атак за допомогою необхідних заходів контролю. Керівні принципи CISA містять галузеві рекомендації щодо безпеки ICS для 16 секторів критичної інфраструктури, що дозволяє 4700 організаціям отримувати інформацію про загрози.

Специфічні для GCC правила стосуються регіональних вимог безпеки ICS/SCADA, а структура NESA OAE передбачає 33 елементи керування для операторів критичної інфраструктури. Стандарти NCSA Катару вимагають оцінки безпеки ICS для національної інфраструктури, що виявляє вразливості у 94% оцінених систем. Регіональне співробітництво через GCC-CERT обмінюється інформацією про загрози між державами-членами, запобігаючи транскордонним кіберінцидентам.

3.2 Розробка структурної схеми

Незважаючи на важливість правильної ізоляції й інтерес до теми, пов'язаної з експертизою мереж, в інтернеті мало інформації стосовно цього питання. У цьому розділі будуть освітлені найпоширеніші проблеми, пов'язані з ізоляцією мереж, з якими ми зіштовхувалися під час попередніх експертиз. Сподіваємося, що ця інформація допоможе пентестерам глибше поринути в цю тему, а співробітникам, відповідальним за безпеку, відкриє завісу методів, якими користуються зловмисники для одержання доступу до нижніх шарів мережі керування виробничими процесами з боку корпоративної мережі.

Тестування сегрегації мережі звичайно складається з декількох кроків:

– Збір інформації.

– Ідентифікація місця проникнення.

– Доступ до сегрегованої мережі.

Збір інформації

Збір інформації в основному спрямований на ідентифікацію будь-яких незахищених даних, зв'язаних мережею керування виробничими процесами. Ця інформація може розкрити деталі про мережу керування, які допоможуть зловмисникові одержати доступ. Звичайно тут мається на увазі наступне:

– Інформація про персонал, що має відношення до керування процесами - технологи, оператори, IT-персонал і інші ключові люди звичайно володіють конфіденційною інформацією про мережу керування виробничими процесами. Пошук в Active Directory по співробітниках, які виконують вищезгадані ролі, може допомогти в ідентифікації імен робочих станцій і спільно використовуваних мережних ресурсах (кулях), до яких є доступ. Уже цей крок значно скорочує обсяг аналізованих даних і загальна кількість зусиль, необхідних для одержання доступу до мережі керування, оскільки в цьому випадку увага буде зосереджено тільки на певних хостах і кулях.

– Мережні діаграми й проектна документація – ця інформація може допомогти зловмисникові зрозуміти механізми роботи мережі керування процесами на фундаментальному рівні, а також виявити імена хостів і IP-адреси як відправні крапки для наступного збору відомостей. Більше того, в ідеальній ситуації мережна документація може дати повну картину керування, що відбувається в мережі, виробничими процесами й допомогти виявити хости, які потрібно атакувати в першу чергу. Після ідентифікації файлових серверів у корпоративній мережі й інформаційних репозитаріїв (наприклад, SharePoint) мережна документація звичайно шукається у файлах VSD, PDF і DOC / DOCX, що перебувають у директоріях або кулях, що мають відношення до відповідних процесів.

– Документація на мережу керування процесами -ця інформація може містити деталі офіційних процедур, пов'язаних з вилученим доступом, інструкції про авторизацію на хости, що мають відношення до виробничих процесів, і дані про технології (використовуваних і невикористовуваних). У багатьох випадках, у подібній документації втримується надзвичайно важлива й конфіденційна інформація (наприклад, логіни й паролі), що є безцінною під час експертизи сегрегації мережі. Ця документація може перебувати усередині IT-куля й директорій або іноді в папках і кулях, що мають відношення безпосередньо до виробничих процесів.

– Мережні пристрої й бекапи систем – конфігураційні файли файервола, роутера й світча, які перебувають усередині резервної копії в корпоративній мережі, часто допомагають побудувати оптимальну схему проникнення в мережу керування. При вивченні конфігурації мережних пристроїв можна виявити хости в корпоративній мережі, до яких дозволений вилучений доступ через протоколи RDP, VNC і SSH. Якщо в корпоративній мережі перебувають бекапи систем, пов'язаних з керуванням процесами, то із цих даних можна легко витягти хеші й інші конфіденційні відомості. Ця інформація часто може бути отримана через

додатки для IT-керування або мережного резервного копіювання, а також у корпоративні або мережних IT-кулях.

Ідентифікація місця проникнення

Один із ключових моментів на етапі збору інформації – ідентифікація існуючих місць проникнення в мережу керування виробничими процесами з корпоративної мережі. У більшості ситуацій можна знайти наступні типи місць проникнення:

– Jump-сервер (jumpbox) / Термінальний сервер- Доступ до мережі керування процесами з корпоративної мережі часто дозволений через хост, що функціонує як jump-сервер (або jump box). Звичайно вилучений доступ здійснюється через протоколи RDP, VNC і SSH. Хоча іноді використовуються додатки для віртуалізації робітників столів на зразок Citrix. Організації, що приділяють мірам безпеки особлива увага, часто використовують рішення, що підтримують багатофакторну автентифікацію під час вилученого доступу.

У документації часто описуються офіційні процедури для вилученого доступу до мережі керування виробничими процесами. Jump-сервера або термінальних служб також можуть бути ідентифіковані за допомогою аналізу мережних діаграм або конфігураційних файлів файервола для хостів, яким дозволені з'єднання з корпоративної мережі через стандартні порти вилученого доступу. Дослідження робочих станцій персоналу в корпоративній мережі, що має відношення до керування процесами, часто є ефективним способом ідентифікації jump-серверів і протоколу, використовуваного для вилученого доступу:

– VPN-доступ – Обраним користувачам, що звичайно мають відношення до керування процесами, може бути дозволений прямій VPN-доступ з метою вилученого керування мережею. Так само як і у випадку з jump-серверами тут може використовуватися багатофакторна автентифікація.

Іноді для цих користувачів може бути створена окрема група. Вивчення імен і опису груп, у які входять ключові співробітники, що мають відношення до

виробничих процесів, звичайно дозволяє виявити групу користувачів, у яких є VPN-доступ. Далі починається дослідження робочих станцій цих користувачів на предмет присутності VPN-інтерфейсів або додатків, а також активних з'єднань до мережі керування виробничими процесами. Ці робочі станції можуть використовуватися як міст до мережі керування.

– Дводомні хости – У типовій мережі, пов'язаної з керуванням виробничими процесами, трохи хостів можуть бути зконфігурованим як дводомні або за допомогою додаткових правил файервола, які дозволяють доступ до мережі керування. Звичайно в цю категорію попадають сервера, що зберігають архівні дані, використовувані з метою аналізу й поліпшення продуктивності виробничих процесів. Одержання доступу до цим хостам часто дає прямий доступ до мережі керування виробничими процесами без необхідності використання офіційних процедур вилученого доступу. Навіть якщо архівні сервера не дають розширеного доступу до мережі керування, дослідження активних з'єднань допомагає виявити діапазони цільових IP-адрес.

Найбільш надійний спосіб пошуку хостів з архівними даними – аналіз мережної документації й діаграм. Крім того, незайвим буде звернути увагу на імена хостів (архівні хости часто мають імена “HI”, “HIS”, “HIST” або щось у такому дусі). Можна спробувати посканувати порти, однак це завдання ускладнюється тим, що не існує єдиного стандарту портів, використовуваних виробниками. Хоча багато організацій використовують архівні сервера на базі системи OSISoft PI, які можна виявити за допомогою сканування найпоширеніших портів, пов'язаних із цим програмним забезпеченням (https://techsupport.osisoft.com/troubleshooting/kb/2820osi8). У цілому, якщо виробник системи керування відомий або виявлений у процесі аналізу, то далі вивчається загальнодоступна документація на предмет використання розповсюджених портів для наступного сканування в корпоративній мережі.

Ще один ефективний метод виявлення дводомних хостів – обстеження корпоративної мережі за допомогою виконання вилучених команд певним чином

(наприклад, WMI або PSExec) і добування активних з'єднань, мережних інтерфейсів і таблиць маршрутизації. Ці дані потім використовуються для пошуку хостів, що мають доступ до мережі керування виробничими процесами. Хоча цей метод створює багато шуму, забирає багато часу й може видавати величезні обсяги інформації для парсингу, особливо в більших мережах. З іншого боку, фільтрація по отриманим раніше діапазонах IP-адрес, які використовуються мережею керування, значно спрощує завдання.

Доступ до сегрегованої мережі

Після одержання потенційних місць проникнення в мережу керування виробничими процесами наступний крок – дослідження кожного місця на предмет присутності розповсюджених уразливостей з метою одержання доступу до мережі керування. Нижче перераховані найпоширеніші проблеми, які були виявлені під час експертизи різних мереж.

– Небезпечні паролі – Паролі є серйозною проблемою для співробітників, відповідальних за безпеку мережі керування виробничими процесами, з кількох причин. Основна проблема полягає в складності мотивації інженерів і інших користувачів, у яких є доступ до мережі керування, до використання стійких паролів. Найчастіше використовуються ті самі паролі й у корпоративній мережі й у мережі керування, оскільки користувачі не бажають управляти набором паролів і вважають, що ризик злому мережі ніщо малий. Після компрометування корпоративної мережі й злому / одержання паролів ключових співробітників, ті ж самі паролі можуть використовуватися для доступу до мережі керування виробничими процесами через раніше отримані місця проникнення.

Дуже часто використовуються стандартні або слабкі паролі, які встановлені виробником за замовчуванням. Ці паролі ніколи не міняються, щоб уникнути проблем, пов'язаних з відхиленням від стандартної конфігурації. Часто імена користувачів і паролів збігаються (наприклад, operator: operator, manager: manager, supervisor: supervisor) або використовуються варіації ім'я виробника (наприклад, Administrator: siemens).

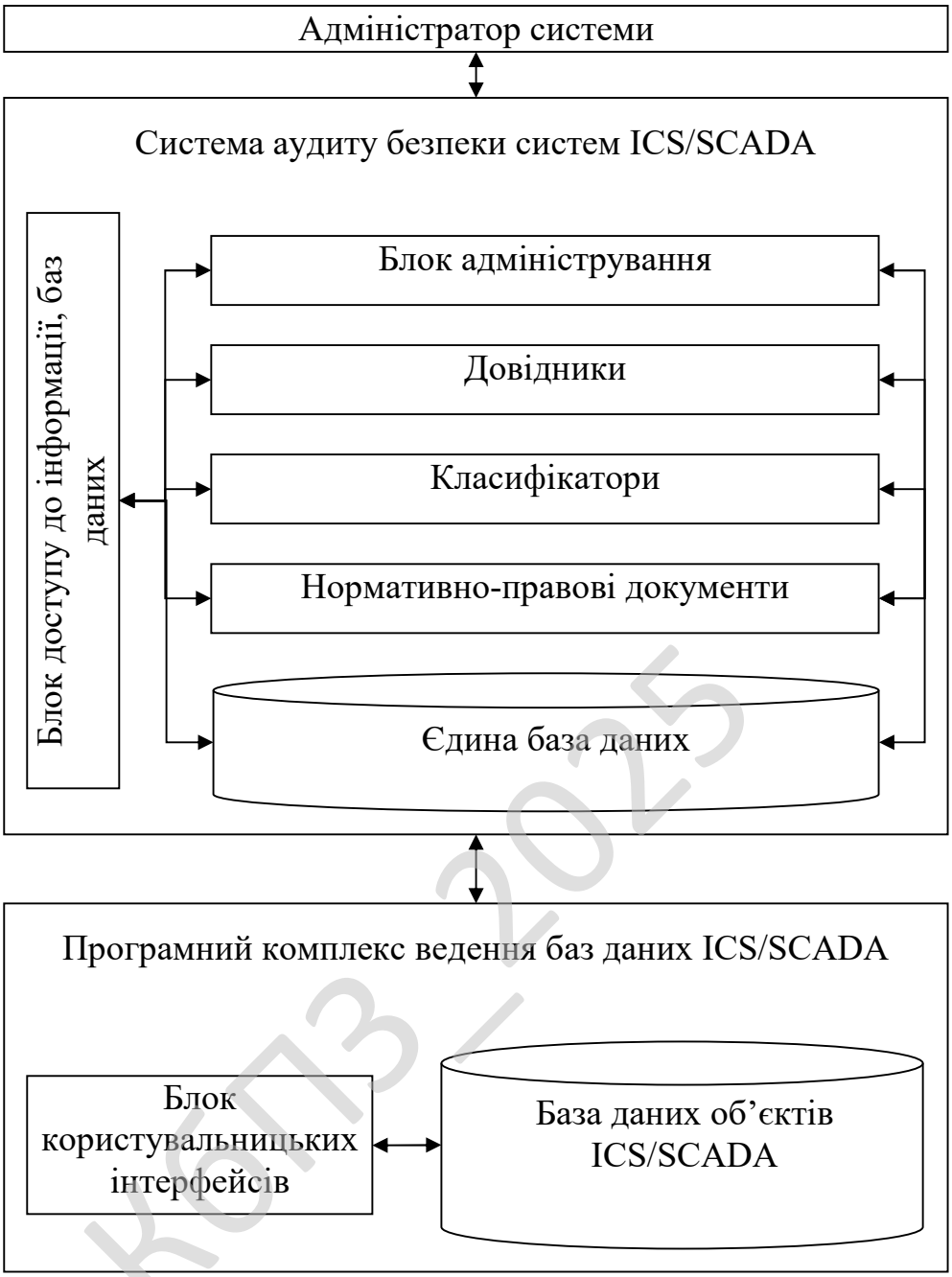

Рисунок 3.1 – Структурна схема системи

Ситуація погіршується ще тим, що політики блокування паролів, використовуваних у виробничих процесах, звичайно не визначені через запобігання випадкових блокувань, які можуть привести до проблем або зупинки всього процесу. Хоча ця ідея й має право на життя, але з іншої сторони зловмисникові відкриваються можливості для прямого підбора облікових записів. Ця проблема в комбінації з попередніми (слабкі й повторно використовувані

паролі) робить атаку по переборі надзвичайно ефективної при спробі одержання доступу до мережі керування виробничими процесами.

– Зберігання паролів у відкритому виді – Облікові записи, використовувані при керуванні технологічними процесами, часто втримуються в документації. Будь-які репозиторії, де зберігається документація мережі керування виробничими процесами, повинні бути досліджені на етапі збору інформації при експертизі сегрегації мережі. Будь-яка знайдена документація повинна бути проаналізована на предмет паролів, використовуваних у місцях проникнення.

– Домен корпоративної мережі підключений до мережі керування – У випадку присутності в корпоративній мережі дводомних хостів або робітників станцій з VPN-доступом ці хости звичайно приєднані до домену в Active Directory. Відповідно, стає можливим одержання доступу до цим хостам прямо за допомогою високопривілійованих облікових записів, використовуваних в Active Directory з боку корпоративної мережі (наприклад, за допомогою облікового запису адміністратора домена). В організаціях, де безпеки приділяється особлива увага, уживають додаткові кроки по обмеженню доступу до цим хостам тільки для певних користувачів або груп. Хоча якщо корпоративна мережа скомпрометована, те досить просто знайти потрібних користувачів і витягти паролі з пам'яті.

– Відкриті уразливі служби – У місцях проникнення можуть використовуватися додаткові служби (наприклад, бази даних або веб-застосунка), уразливі до найпоширеніших атак. Кожний хост, у якого є доступ до мережі керування виробничими процесами, повинен бути просканован на предмет присутності неврахованих служб. У випадку знаходження подібних служб потрібно провести аналіз на предмет наявності уразливостей або розповсюджених помилок у конфігурації, які можуть стати причиною компрометування всього хоста.

Якщо ви коли-або, виконуючи пентести ICS-інфраструктури, зштовхнетеся з однієї з наступних ситуацій, негайно рапортуйте про критичну проблему:

– У корпоративній мережі виявлений трафік Modbus/DNP3.

– З корпоративної мережі є доступ до людино-машинного інтерфейсу (HMI) із правами не тільки на читання.

– Пінгування ядерного реактора за допомогою NMAP приводить до необоротних наслідків.

Сподіваємося, що остання ситуація з вами ніколи не трапиться. У противному випадку, бажаємо вам залишитися цілим і непошкодженим.

Незважаючи на те, що навколо нас багато чого залежить від ICS-технологій, існує явний недолік інформації щодо безпеки подібних систем.

3.3 Розробка функціональної схеми

Для управління системою оператору необхідна інформація, яка б дозволяла:

– швидко оцінити загальний стан об’єкту, тобто в стані нормальної експлуатації, в умовах очікуваної експлуатаційної події чи в аварійному стані і переконатися, що виконуються запроектовані автоматичні дії по забезпеченню безпеки;

– визначити відповідні дії, які необхідно розпочати оператору.

Для виконання ролі оператора устаткування людині потрібна інформація з параметрів окремих систем об’єкту й устаткування.

Необхідно, щоб проект сприяв успішному виконанню оператором своїх дій у межах наявного часу, в умовах передбачуваного навколишнього фізичного середовища і психологічного навантаження. Бажано звести до мінімуму необхідність у негайному втручанні оператора. У проекті варто врахувати той факт, що таке втручання прийнятне тільки в тому випадку, коли проектувальник

може довести, що оператор має досить часу для прийняття рішення і відповідних заходів; що необхідна інформація, на основі якої оператор повинен приймати своє рішення, представлена в дохідливій і чіткій формі і що фізичні параметри навколишнього середовища в приміщенні пульту управління та на додаткових пультах управління об'єктом після даної події є прийнятними.

Процедура системного аналізу помилок

Процедура системного аналізу помилок людини має загальні кроки для різних методик [4].

Ця процедура відома в англійській абревіатурі як SHARP – Systematic Human Action Reliability Procedure. Процедура включає сім кроків і два етапи, на яких приймаються рішення. Два перших кроки виконуються системними аналітиками, два подальших – фахівцями з аналізу людського чинника, останні три кроки процедури виконуються спільними зусиллями.

Розглянемо процедуру виконання кожного кроку.

– Крок 1 – Визначення **дій** людини, включаючи дії по ремонту, роботу по програмах, дії по локалізації аварій, тобто всіх дій з помилками персоналу, які погіршують або поліпшують ситуацію.

– Крок 2 – **Скрінінг – відбір** важливих подій, помилок, що мають ключове значення для імовірності аварійної ситуації (наприклад, плавлення активної зони).

– Крок 3 – Розділення – **виділяються** всі дії оператора, що вимагають більш детального аналізу, тобто задача розбивається на більш дрібні, характерними складовими яких будуть:

1. Здатність зрозуміти, що треба робити (для аналітиків), розділення дій по операціях:

– Нездатність визначити систему.

– Нездатність виконати дії.

2. Включення кроків в модель ІАБ.

3. Необхідність (можливість) побудови додаткових аварійних послідовностей, якщо визначилися інші помилки операторів.

– Крок 4 – Уявлення – повне **представлення** всіх помилок і їх аналіз з докладними діями.

– Крок 5 – Визначення **взаємного впливу** елементарних дій (операцій), впливи на наступні етапи;

– Крок 6 – Розрахунки – визначаються **кількісні** значення ймовірностей помилок;

– Крок 7 – Документування.

Обсяг робіт на кожному кроці залежить від типу методики, що використовується.

Визначення базових значень ймовірностей помилок людини

Помилки під час експлуатації частіше складають помилкові дії: або не передбачені, або передбачені в експлуатаційних процедурах, чи процедурах технічного обслуговування; рідше – невиконання окремих дій, що вимагаються. Прикладами є неправильний вибір засобів управління, передача неправильних команд чи інформації, зміна послідовності виконання задач і занадто раннє чи занадто пізнє виконання задач. Такі помилки можуть виникнути в результаті помилок при прийнятті рішень операторами: невірно витлумачених чи нечітких процедур; помилкові показання контрольно-вимірювальних приладів; неправильне розуміння чи просто помилка оператора. Для визначення надійності системи ці можливі помилки потрібно враховувати в проекті.

Значення імовірності помилки у випадку наявності адекватних процедур та їх застосування при виконанні складних робіт зменшується у 50 разів.

Представляє інтерес також таблиця обліку залежності ймовірностей помилки від змін обставин: змін в складі бригади, що виконує роботу, розділення дій за часом і місцем, наявність чи відсутність вказівок на виконання роботи (підказки) і комбінацій названих обставин. Врахування всіх обставин проводиться по нижченаведеному алгоритму. Значення імовірності помилки без

врахування змін обставин (HEP) дорівнює N, в залежності від їх комбінацій – номери для типів помилкових дій людини, приймає значення:

– 1 (одиниця) у разі повних змін;

– (1+N)/2, у разі високих (великих) змін;

– (1+6N)/7, у разі помірних змін;

– (1+19N)/20, у разі низьких (малих) змін;

– N, у разі нульових змін.

Ця таблиця відноситься до методики ASP, що широко використовується для аналізу помилок людини-оператора. При цьому, обставини сильно змінюють імовірність помилки. Наприклад, якщо базова ймовірність N = 0.1, то в залежності від змінених обставин імовірність помилки буде: 0,1; 0,145; 0,23; 0,55; і 1,0 відповідно до різного ступеню залежності.

Побудова дерева помилок персоналу

Дерева аналізу надійності людини вперше були введені в методиці THERP[46]. Події в такому дереві позначаються у вигляді відрізків прямих ліній, розташованих під кутом один до одного.

Відрізки, розташовані **праворуч,** зображають **неуспішні** дії (відмови), які позначаються великими літерами латинського алфавіту, відрізки зліва **– успішні дії**, позначаються малими буквами латинського алфавіту. Поруч з позначенням, звичайно можуть бути пояснюючі надписи й значення ймовірності відповідної події. Дії по відновленню функцій систем позначаються горизонтальними пунктирними лініями.

Відрізки показують послідовність дій. Початок послідовності дій знаходиться вгорі. Кожне дерево, в залежності від числа гілок, має різне число послідовностей. Послідовністю тут будемо називати дії, або їх сукупність, що приводять до якогось результату (на кінець гілки). Так дерево, представлене на рисунку 3.10 містить такі послідовності: abc**, A,** a**B,** ab**C****D,** ab**C**d**.**

Чисельні значення ймовірностей неуспіху проставляються поруч з подіями. Зазначимо, що успіх і відмова є взаємно доповнюючими подіями.

При побудові дерева надійності людини також як і при побудові дерева відмов систем, важливе значення мають всі допущення, припущення і межі. Всі вони повинні бути чітко описані.

Аналіз загального ризику з врахуванням помилок персоналу

При оцінці ризику від промислових об’єктів (ICS/SCADA) необхідно враховувати дії людини, тобто повинен використовуватися комплексний підхід: системний аналіз надійності обладнання, аналіз надійності людини і, в результаті, аналіз загального ризику:

Відмова системи = відмова обладнання + помилка людини.

Наведена формула дещо спрощена, оскільки є взаємодії, які можуть поліпшити або погіршити ситуацію. Розуміти її треба так: оператор остання лінія захисту (в глибоко ешелонованому захисті).

Цілі моделювання подій, пов'язаних з помилками людини:

– представити помилки і їх механізми;

– якісно представляти роль чинників, що впливають на поставлену задачу;

– кількісно описати помилку, що дозволить зробити аналіз чутливості;

– виробити стратегію запобігання помилкам або відновлення функцій оператором.

Основні базисні події, пов'язані з помилками операторів, можуть вводитися в моделі ІАБ на рівні систем – в дерева відмов, або на рівні послідовностей – в дерева подій. Введення в дерева відмов основних базисних подій, пов'язаних з помилками операторів, має деякі переваги:

– отримані при детальному моделюванні відомості враховуються спочатку і використовуються для подальшого аналізу;

– не використовуються консервативні оцінки;

– консервативний відбір для дерев відмов і оцінки базисних подій, пов'язаних з помилками операторів, призводить до того, що завищений рівень людських помилок суперечить повному аналізу. Це сприяє виконанню детального моделювання і кількісних оцінок.

Імовірність відмови системи в цьому випадку визначається з урахуванням можливої помилки оператора, що має всі кількісні характеристики і свій закон розподілу ймовірностей.

У деревах подій врахування людського чинника (HF) може відбуватися як проміжні події із заданими ймовірностями відновлення систем, що відмовили. У випадку складної залежності проміжні події можуть вводитися окремими деревами аналізу надійності людини. Ці дерева можуть мати звичайну форму, або спеціальну, яка розглянута вище.

Отже, в моделях ІАБ дії (помилки) оператора можуть враховуватися в таких варіантах:

– дії зроблені неправильно;

– дії, що призводять до відмов;

– як успішні й аварійні послідовності;

– як дії по відновленню оператором функцій систем, що відмовили;

– при аналізі взаємозалежності і взаємного впливу окремих подій (THERP);

– як типи різних помилок.

В цілому використання методики THERP цілком виправдано для моделювання помилок оператора. Методика проста, зрозуміла й однозначна. Для широкого її застосування необхідно навести зв’язок імовірності помилки оператора від його навченості, досвіду та стану діючої системи управління охороною праці на підприємствах різних галузей України, тобто адаптації методики до конкретних умов.

Застосування імовірнісних моделей для визначення ризику виробництва

Ризик виробництва розуміємо як змінну що характеризує стан безпеки виробництва і дорівнює добутку імовірності небажаної події на величину її наслідків.

Побудова структурно-логічних моделей процесів охорони праці

Якщо маємо випадковий процес дій людини в процесі виробництва, шляхом його дослідження, вивчення й аналізу можливо встановити залежності кінцевих подій від причин та базисних подій, що його складають, а звідсіля і розробка моделей будь-яких НВ на базі наведених вище алгоритмів, визначення (побудова) структурно-логічної моделі НВ як системи технологічного, природного або соціального характеру. Поняття "Система" розуміємо в загальному визначенні, як множину об'єктів разом із відносинами між об'єктами і їх атрибутами (визначення А. Хола). При цьому, на відміну від систем безпеки ICS/SCADA, не завжди існують матеріальні зв'язки між елементами в вигляді трубопроводів або електричних з'єднань. Частіше в системах, що пропонується розглядати, зв'язки між елементами існують тільки в логічному виді. В цьому полягає різниця між системами ICS/SCADA і системами що пропонується розглядати. Відношення системи до того чи іншого типу буде, очевидно, залежати від факторів та обставин, які пов'язані з джерелом небезпек, їх впливу на розвиток та наслідки небажаних подій. Ці фактори та обставини повинні бути проаналізовані фахівцями галузі, відібрані для складання й опису моделі ці з них, що складають замкнуту систему. Важливим етапом цієї роботи буде визначення базисних подій, при цьому обов'язкове дотримання всіх вище приведених вимог щодо базисної події. Фактори та обставини, які будуть прийматися за базисні події, повинні розглядатися як деякі захисні бар'єри, що перешкоджають появі та розвитку небажаної події. Базисна подія у цьому випадку розглядається як відмова захисного бар'єру, людська помилка, чи несприятлива умова для функціонування визначених захисних бар'єрів системи. Подія відмови, як і для технічних систем, не вимагає подальшої розробки, не може бути більше деталізована чи уточнена.

Побудова імовірнісних моделей (ДВ) в цьому випадку, аналіз системи, отримання МП, розрахунок імовірності небажаної події – все це задачі ІАБ, їх вирішення можливо за допомогою коду IRRAS.

Використання ДВ в задачах розрахунку ризиків безпеки систем ICS/SCADA

На основі ДВ досить просто будувати моделі складних технічних систем. Якщо система, ризик якої визначається, сама складається з декількох систем, здатних впливати на наслідки, доцільно вводити моделі дерев подій, що зв'язують роботу систем єдиною логікою. Можливе застосування методу аналізу ДВ і не для технічних систем. Як базисні події в такому випадку мають бути узяті такі події, що впливають на ризик (наслідки) і не можуть бути більш спрощені, при цьому імовірності чи інші їхні імовірнісні характеристики можуть бути знайдені якими-небудь методами. При цьому алгоритм і правила побудови й розрахунку ДВ змінюються відповідно до наведеного нижче алгоритму.

Основні кроки аналізу ризику за допомогою структурно-логічних моделей для будь яких систем:

– Визначити і коротко характеризувати небажану подію, що можлива як підсумкові дії небезпечного або шкідливого чинника.

– Визначити і коротко охарактеризувати початкову подію, що обумовлює дію шкідливого чинника.

– Визначити базисні (незалежні) події, що можуть впливати на процес дії небезпечного чинника за час від початкової події до небажаної події.

– Зробити оцінку інтервалу часу від початкової події до небажаної події.

– Визначити чинники й обставини, що можуть впливати на хід подій за час від початкової події до небажаної події.

– Оцінити зв'язок базисних подій (чинників) і обставин за час від початкової події до небажаної події.

– Визначити можливі міри й засоби запобігання дії шкідливого або небезпечного чинника, і ввести їх у модель базисними подіями.

– Визначити можливе втручання людини в процес і можливі помилки при цьому, і врахувати їх у імовірнісної моделі.

– Зробити оцінку ймовірностей приведених базисних подій.

– Побудувати дерево відмов, визначити ступінь ризику під час дії небезпечного чинника, і можливі шляхи запобігання небажаної події.

При побудові дерева надійності людини також як і при побудові дерева відмов систем, важливе значення мають всі допущення, припущення і межі визначеної системи.

Управління ризиками. Загальна схема

Мету управління ризиком при здійсненні будь-якої діяльності можна визначити як забезпечення безпеки персоналу і навколишнього природного середовища, шляхом встановлення і підтримки прийнятного рівня ризику, при використанні оптимальним чином з максимальною ефективністю наявних матеріальних ресурсів.

Управління ризиками – це діяльність, пов'язана з ідентифікацією, аналізом ризиків безпеки систем ICS/SCADA і прийняттям рішень, спрямованих на мінімізацію негативних наслідків настання вихідних подій (явищ) і/чи зменшення імовірності їхньої реалізації до прийнятних значень. У загальному випадку процес управління ризиками при здійсненні діяльності на об'єкті включає виконання шести процедур (рисунок 3.2).

Планування управління ризиками – це процес прийняття рішень по застосуванню і плануванню управління ризиками для конкретної діяльності. Цей процес може містити в собі:

– Організацію на підприємстві спеціального підрозділу (групи управління ризиками), відповідального за оцінку і управління.

– Вибір методики оцінки ризиків безпеки систем ICS/SCADA.

– Визначення джерел даних для ідентифікації ризику.

– Визначення тимчасового інтервалу для аналізу ситуації.

Дуже важливим буде визначення припустимих (прийнятних) рівнів ризику, які повинні вибиратися на основі чинного законодавства.

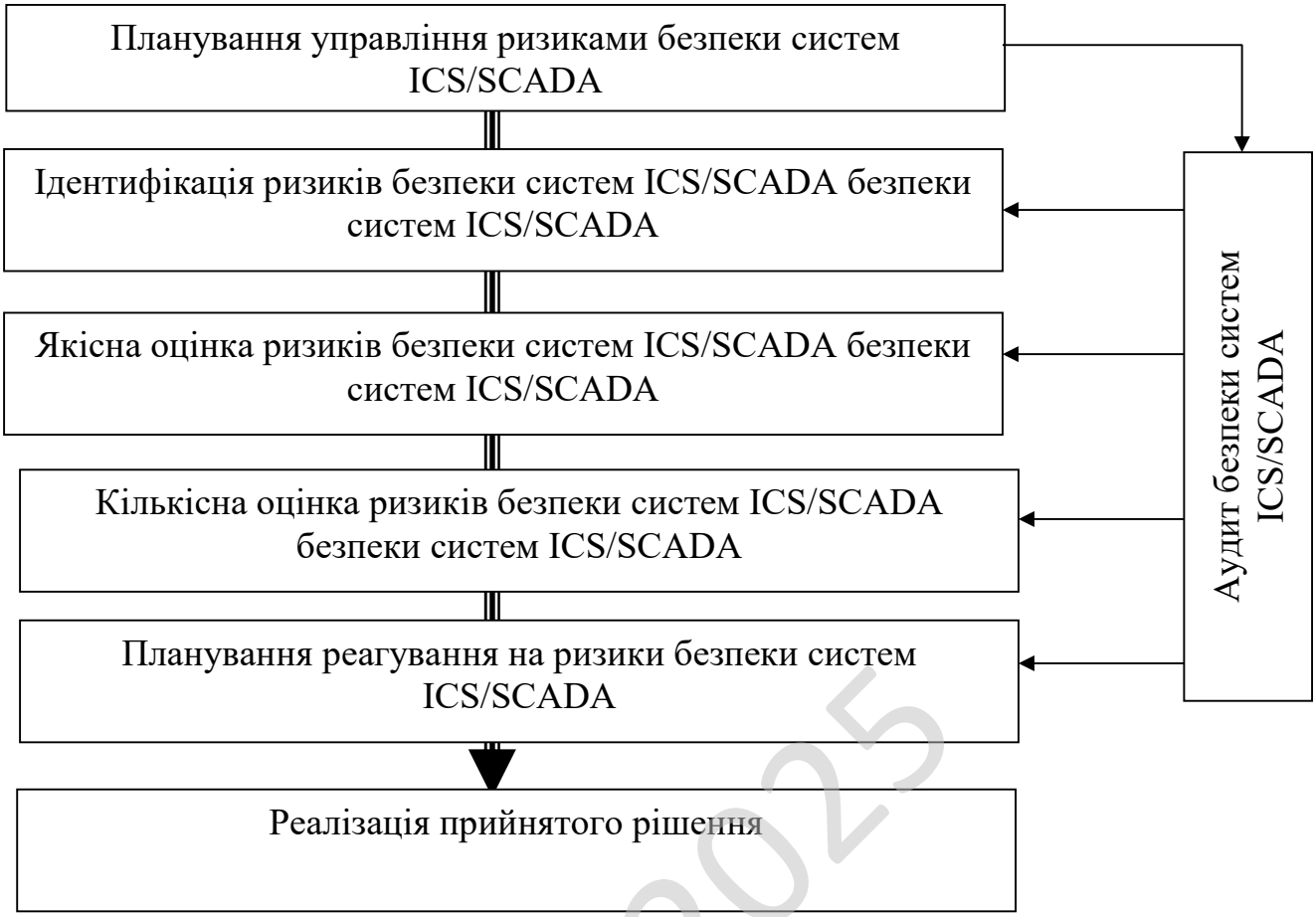

Рисунок 3.2 – Функціональна схема системи

Ідентифікація ризиків безпеки систем ICS/SCADA визначає, які ризики можуть вплинути на діяльність, що розглядається. Характеристики цих ризиків безпеки систем ICS/SCADA повинні бути оформлені документально. Ідентифікація ризиків безпеки систем ICS/SCADA повинна проводитися регулярно протягом усієї діяльності об'єкта. Спеціалізований підрозділ повинний залучати до робіт по ідентифікація ризиків безпеки систем ICS/SCADA всіх учасників процесу: проектантів, експлуатаційників, фахівців інших підрозділів і незалежних експертів. Ідентифікація ризиків безпеки систем ICS/SCADA повинна організовуватися як ітераційний процес. Перші розрахунки потенційного ризику виконують проектанти. У процесі діяльності об'єкту, з урахуванням досвіду експлуатації, уточнюються дані по надійності систем і устаткування,

процедурам управління, помилкам персоналу і робиться перерахунок ризиків безпеки систем ICS/SCADA для об'єкту. Для формування об'єктивної оцінки в завершальній стадії процесу оцінки можуть брати участь незалежні експерти. Приклад ідентифікації ризиків безпеки систем ICS/SCADA, для радіаційних ризиків безпеки систем ICS/SCADA викладений у галузевому нормативному документі НРБУ-97/Д-2000.

Якісна оцінка ризиків безпеки систем ICS/SCADA – це процес якісного аналізу результатів ідентифікації, а також визначення ризиків безпеки систем ICS/SCADA, що вносять найбільший внесок у загальний ризик і які потребують вживання заходів по їхньому зниженню.

Як уже було показано раніше, останній етап якісного аналізу систем полягає в представленні умов невиконання функцій системи у вигляді так званої множини мінімальних перерізів [37]. Набір мінімальних перерізів системи однозначно визначений її деревом відмов і може бути отриманий при використанні спеціальних алгоритмів вибору мінімальних перерізів. Кількісні дані по базисних подіях впливають на важливість самого мінімального перерізу – його відсотковий вклад в імовірність відмов системи.

Якісна оцінка визначає ступінь важливості ризику і складових його подій. Доцільно створити банк даних ризиків безпеки систем ICS/SCADA усієї діяльності на об'єкті, заснований на систематизованих даних, у тому числі даних по впливу ризиків безпеки систем ICS/SCADA на персонал. На цьому етапі можливо визначення чинників найбільшого впливу, що створить передумови управління.

Кількісна оцінка ризиків безпеки систем ICS/SCADA визначає значення імовірності виникнення ризиків безпеки систем ICS/SCADA і впливу їхніх наслідків на діяльність, що допомагає приймати оптимальні рішення й уникати невизначеності (у змісті управління) при цьому. Кількісна оцінка ризиків безпеки систем ICS/SCADA передбачає виконання попередніх процесів, це завершальний етап задачі визначення ризиків безпеки систем ICS/SCADA.

Планування реагування на ризики – це розробка методів і технологій зниження негативних наслідків ризиків безпеки систем ICS/SCADA. Якісне, науково обґрунтоване планування можливе за умови виконання всіх попередніх етапів процесу відповідно до рисунка 3.13. Стратегія планування повинна відповідати типам ризиків безпеки систем ICS/SCADA, їх величині і значимості, наявності ресурсів і тимчасових параметрів. У найбільш небезпечних випадках, можливо потрібно кілька варіантів реагування на ризики. Планування повинне здійснюватися у відповідності зі спеціальною методикою, що враховує специфіку об'єкту, чинні на ньому правила й інструкції.

Реалізація прийнятого рішення проводиться з врахуванням даних моніторингу і контролю параметрів, що проводяться з метою перевірки дотримання вимог встановлених норм. Моніторинг і контроль повинні здійснюватися спеціалізованим підрозділом об'єкту. При цьому повинні постійно контролюватися процес ідентифікації ризиків безпеки систем ICS/SCADA, виконання плану реагування на ризики, оцінка ефективності заходів для зниження ризиків безпеки систем ICS/SCADA, величина залишкового ризику і його прийнятність.

Якісний контроль виконання діяльності подає інформацію, що сприяє прийняттю ефективних рішень по запобіганню нових ризиків безпеки систем ICS/SCADA чи зм'якшення наслідків. Контроль може ініціювати вибір альтернативних стратегій, прийняття коректив, перепланування проекту для досягнення базового плану.

Для цілей моніторингу і перевірки дотримання норм забезпечується належне устаткування і впроваджуються відповідні процедури перевірки. Зазначене устаткування належним чином обслуговується і випробовується, а також калібрується з належною періодичністю на основі еталонів, що відповідають національним чи міжнародним еталонам.

Розглянувши усі блоки функціональної схеми перейдемо до розгляду діаграми взаємодії процесів, які відбуваються у системі.

3.4 Розробка діаграми процесів

Діаграма процесів розробленої системи зображена на рисунку 3.3. При детальному її розгляді можна побачити як саме проходе взаємодія у розробленій системі. Використовується модель проектування, графічне представлення «потоків» даних в інформаційній системі.

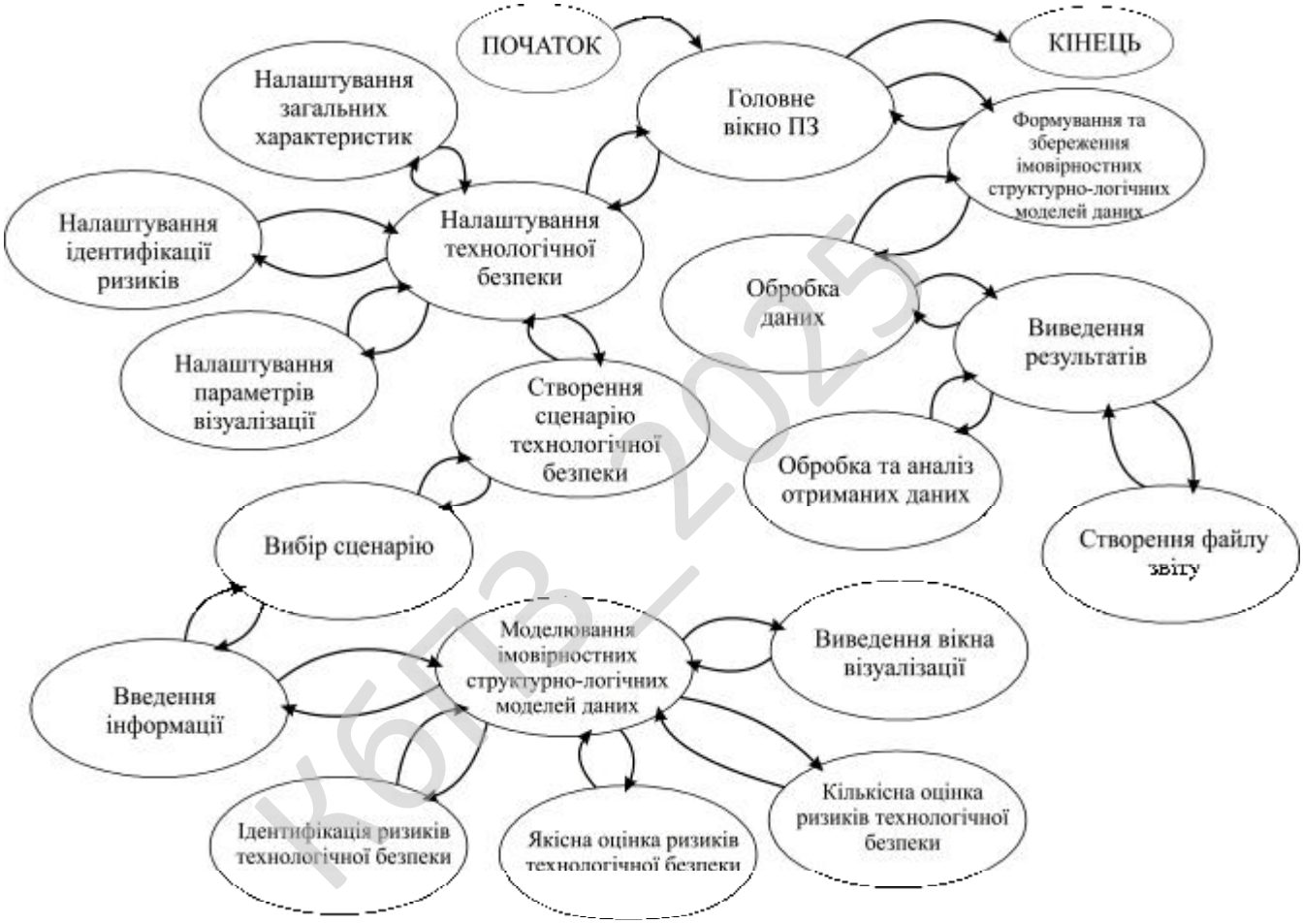

Рисунок 3.3 – Діаграма взаємодії процесів

Діаграма взаємодії процесів використовується для візуалізації процесів обробки даних (структурне проектування). Для розробника вважається звичним спочатку креслити діаграму взаємодії процесів даних рівня контексту, завдяки чому буде показано взаємодію системи. Ця діаграма в подальшому підлягає

уточненню шляхом деталізації процесів та потоків даних з метою показати систему що розробляється.

Діаграми потоків даних містять чотири типи елементів:

– Процеси які являють собою трансформацію даних в рамках описуваної системи.

– Сховища даних (репозиторії).

– Зовнішні по відношенню до системи сутності.

– Потоки даних між елементами трьох попередніх типів.

Таким чином, розглянувши опис системи, структурну, функціональну схеми системи, та діаграму взаємодії процесів перейдемо до опису блок-схем основної програми, та підпрограм, які використовуються, для реалізації системи.

4 РЕАЛІЗАЦІЯ ПРОЕКТУ. РОЗРАХУНКИ І ЕКСПЕРИМЕНТАЛЬНІ ДАНІ, ЩО ПІДТВЕРДЖУЮТЬ ПРАВИЛЬНІСТЬ ПРОЕКТНИХ РІШЕНЬ

4.1 Блок-схеми та опис алгоритмів функціонування системи

Первинною стадією без якої не відбувається розробка програмного забезпечення це звичайно розробка блок-схем. На рисунку 4.1 зображена основна блок-схема програми, на рисунку 4.2 зображено роботу підпрограм.

З яких видно що робота основної програми складається з початкових етапів ініціалізації ПЗ, перевірки наявності ресурсів системи, блоку початку основного циклу з чеканням запиту від користувача в якому відбувається виклик підпрограм та останньої стадії – перевірка поточного стану з завершенням роботи розробленого ПЗ.

При роботі підпрограм виконується основний функціонал системи з циклічними послідовностями, перевіркою поточного стану та поверненням в основну програму прапорів стану виконання.

Опис алгоритмів функціонування системи.

Блок-схеми є першоджерелами стратегії розвитку ПЗ. Тому від точності і детальної блок-схеми залежить результат всієї програми.

При виборі початкової точки відліку при побудові схем було враховано, що виходячи з вибору мови програмування і інших технічних засобів, програма буде об’єктно-орієнтована що вимагає оптимізації програми високого рівня, також те, що при розробці програми слід надати особливу увагу модулю аудиту безпеки систем ICS/SCADA.

При складанні блок-схем програмного забезпечення і напрацювання алгоритмів я зіткнувся з масою проблем, які вимагали напрацювання процедур і функцій над основною проблематикою.

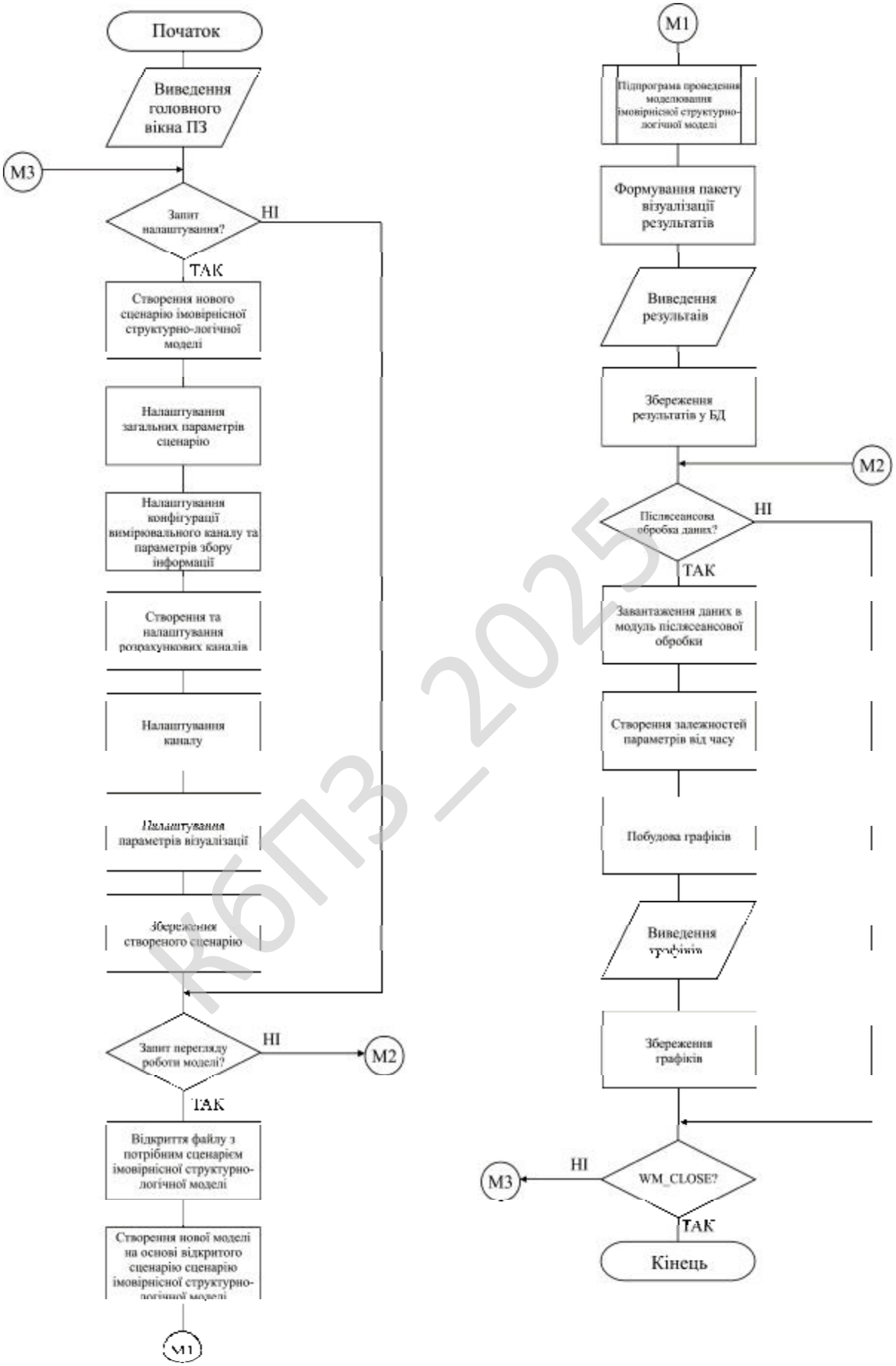

Рисунок 4.1 – Блок-схема основної програми

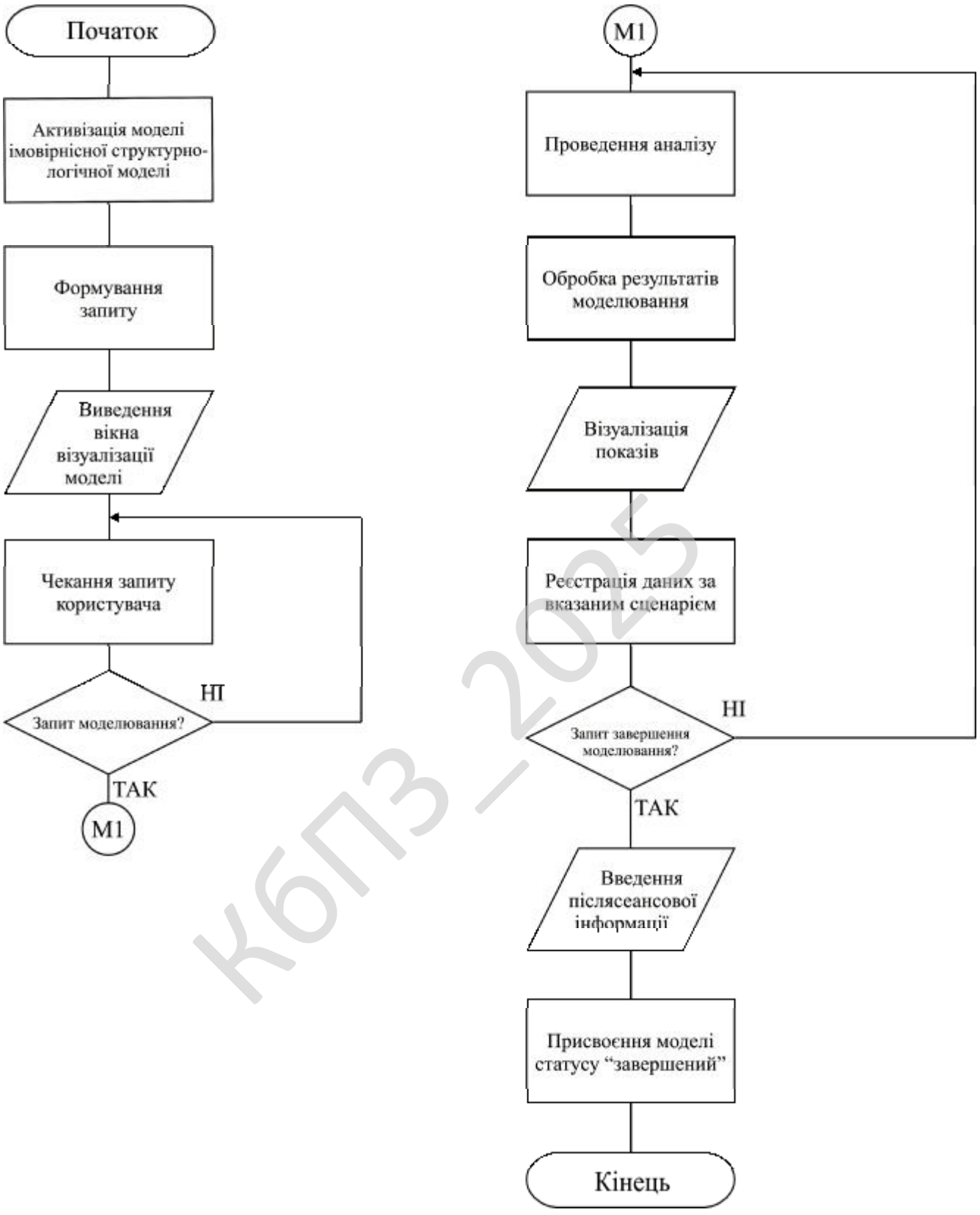

Рисунок 4.2 – Блок-схема роботи підпрограми

Для чого були створені додаткові класи, типи даних і константи, що забезпечило вирішення проблем.

Було використано підходи з використанням UML, це уніфікована мова моделювання, використовується у парадигмі об'єктно-орієнтованого програмування. Є невід'ємною частиною уніфікованого процесу розробки програмного забезпечення.

UML є мовою широкого профілю, це відкритий стандарт, що використовує графічні позначення для створення абстрактної моделі системи, називаної UML-моделлю. UML був створений для визначення, візуалізації, проектування й документування в основному програмних систем. UML не є мовою програмування, але в засобах виконання UML-моделей як інтерпретованого коду можлива кодогенерація.

UML може бути застосовано на всіх етапах життєвого циклу аналізу бізнес-систем і розробки прикладних програм. Різні види діаграм які підтримуються UML, і найбагатший набір можливостей представлення певних аспектів системи робить UML універсальним засобом опису як програмних, так і ділових систем.

Діаграми дають можливість представити систему (як ділову, так і програмну) у такому вигляді, щоб її можна було легко перевести в програмний код. Основною причиною використання мови UML є спілкування розробників між собою.

Крім того, UML спеціально створювалася для оптимізації процесу розробки програмних систем, що дозволяє збільшити ефективність їх реалізації у кілька разів і помітно поліпшити якість кінцевого продукту.

UML прекрасно зарекомендувала себе в багатьох успішних програмних проектах. Засоби автоматичної генерації кодів дозволяють перетворювати моделі мовою UML у вихідний код об’єктно-орієнтованих мов програмування, що ще більш прискорює процес розробки.

Практично усі CASE-засоби (програми автоматизації процесу аналізу і проектування) мають підтримку UML. Моделі розроблені в UML, дозволяють значно спростити процес кодування і направити зусилля програмістів безпосередньо на реалізацію системи.

Діаграми підвищують супроводжуваність проекту і полегшують розробку документації.

UML необхідний:

– Керівникам проектів, які керують розподілом завдань і контролем за проектом.

– Проектувальникам інформаційних систем які розробляють технічні завдання для програмістів.

– Бізнес-аналітикам, які досліджують реальну систему і здійснюють інжиніринг і реінжиніринг бізнесу компанії.

– Програмістам які реалізовують модулі інформаційної системи.

При модифікації системи об'єктний підхід дозволяє легко включати в систему нові об'єкти і виключати застарілі без істотної зміни її життєздатності. Використання побудованої моделі при модифікаціях системи дає можливість усунути небажані наслідки змін, оскільки вони не ламають структури системи, а тільки змінюють поведінку об'єктів.

Система програмної реалізації аудиту безпеки мережевих ICS SCADA у магістерській роботі виступає як навчальний програмний комплекс. Вона моделює процес інвентаризації об’єктів інфраструктури, мережевого сканування технологічного сегмента, застосування правил аудиту та формування текстових і машинно читаних звітів.

Реалізація використовує мову програмування Python і орієнтується на навчальні лабораторні сценарії для аналізу безпеки промислових мереж.

Система працює у режимі командного рядка. Користувач задає список об’єктів контролю з основними характеристиками і ініціює запуск перевірки. Програма послідовно виконує логічні кроки аудиту та формує звіт, який студент може використовувати для подальшого аналізу.

Архітектура побудована модульно і включає підсистеми конфігурації, моделей даних, мережевого сканування, системи правил безпеки, агрегування результатів та генерації звітів.

Загальна архітектура і основні модулі

Система логічно складається з кількох рівнів. На нижньому рівні знаходяться моделі даних, які описують об’єкти контролю, виявлені сервіси та результати аудиту. На наступному рівні працює модуль мережевого сканування, який збирає фактичну інформацію про відкриті порти та доступні протоколи. Далі модуль правил безпеки застосовує набір формалізованих вимог до отриманих даних. На верхньому рівні підсистема звітності перетворює результати в зручну форму для аналізу.

У рамках одного файлу вихідного коду реалізація структуровано за логічними блоками. Спочатку задаються імпорти стандартних бібліотек та глобальна конфігурація. Далі описуються моделі даних. Потім реалізується інвентаризація об’єктів, модуль сканування, модуль правил, формувач звітів і основна керуюча логіка.

Моделі даних

Основу внутрішнього представлення інформації формують класи Asset, ServiceInfo, Finding та AuditResult.

Клас Asset описує окремий об’єкт промислової інфраструктури. У структурі зберігається назва об’єкта, IP адреса, роль у технологічному процесі, зона розміщення, список підтримуваних протоколів та рівень критичності. Рівень критичності задається цілим числом і відображає важливість об’єкта для безперервності виробничого процесу. Наприклад, контролер або захисне реле має вищу критичність ніж робоче місце оператора.

Клас ServiceInfo зберігає інформацію про окремий мережевий сервіс, який система виявляє під час сканування. У моделі фіксується номер порта, протокол транспорту, умовна назва сервісу, а також додатковий текстовий банер, якщо його вдається отримати під час встановлення з'єднання.

Клас Finding описує окреме виявлене відхилення від вимог безпеки. Для кожного результату аудит зберігає ідентифікатор правила, що спрацювало, коротку назву, деталізований опис, рівень важливості, а також привязку до конкретного об'єкта та сервісів. Така структура дає змогу в подальшому агрегувати результати та будувати узагальнені звіти.

Клас AuditResult використовується як контейнер для сукупних результатів аудиту. Він містить словник об'єктів, словник виявлених сервісів і список усіх знайдених відхилень. Додатково зберігається час запуску перевірки, що дає змогу відслідковувати історію аудитів.

Конфігурація і довідкові дані

Для полегшення адаптації системи під конкретні навчальні сценарії конфігурація виділяється в окремий логічний блок. Конфігураційний клас зберігає список портів, які пов'язані з протоколами ICS SCADA, список загальних портів IT сервісів, тайм аут під час сканування, граничні значення для інтерпретації критичності, а також допоміжні словники для експертної оцінки.

Серед портів ICS SCADA виділяються, наприклад, порти 502 для Modbus TCP, 20000 для DNP3, 2404 для IEC 60870 та 102 для S7. Окремо формується список портів для стандартних сервісів загального призначення, таких як HTTP, SSH, RDP або SMB. Поєднання інформації про технологічні протоколи та IT сервіси дає змогу виявляти небезпечні конфігурації, наприклад розміщення панелі веб керування на контролері у польовій зоні.

Модуль інвентаризації об'єктів

Інвентаризація об'єктів у системі реалізується як невеликий сховище в оперативній памяті. Клас InventoryRepository зберігає словник об'єктів, де ключем

виступає IP адреса. Це дає можливість швидко отримувати об’єкт за адресою під час аналізу результатів сканування.

Репозиторій надає методи для додавання об’єкта, пошуку за IP, отримання списку всіх об’єктів та попереднього наповнення даними для навчальної лабораторної роботи. У навчальному режимі студент може або вручну створити список об’єктів, або використати стандартний приклад, який моделює невелику промислову мережу з диспетчерським рівнем, проміжною мережею і польовими пристроями.

Модуль мережевого сканування

Модуль мережевого сканування виконує активну перевірку доступності портів за IP адресами. Реалізація використовує стандартний модуль socket і неблокуючий підхід з тайм аутами. Для прискорення роботи застосовується черга завдань та пул потоків. Це дає змогу паралельно сканувати декілька об’єктів та портів навіть у навчальному середовищі.

Основна функція сканування отримує IP адресу і список портів. Для кожного порта створюється спроба TCP з’єднання. Якщо з’єднання успішне, порт вважається відкритим. Сканер намагається додатково прочитати невелику кількість байтів банера, щоб отримати початковий рядок відповіді сервісу. Якщо банер не доступний, фіксується тільки факт відкритого порта.

Щоб відобразити специфіку ICS SCADA, сканер використовує конфігураційні словники і на основі номера порта призначає сервісам опис, наприклад Modbus TCP або DNP3. Для загальних IT сервісів додається опис HTTP, RDP або SSH. Якщо порт не відомий, сервіс позначається як невідомий.

Модуль правил безпеки

Ключовим елементом системи є модуль правил безпеки. Він реалізує просту експертну систему, яка застосовує набір правил до кожного об’єкта та його сервісів.

Кожне правило представляється як окремий об’єкт з ідентифікатором, назвою, текстовим описом, рівнем важливості та функцією оцінювання.

У реалізації присутні приклади правил, які демонструють типові навчальні сценарії. Наприклад, правило виявляє наявність технологічних протоколів ICS у зонах, які задекларовані як польові або проміжні, і одночасну доступність загальних IT сервісів на тих самих об’єктах. Це моделює ситуацію коли контролер має відкритий веб інтерфейс або RDP, що створює додаткову поверхню атаки.

Інше правило оцінює загальну кількість відкритих портів на об’єкті з високою критичністю. Якщо кількість перевищує умовно безпечне значення, правило створює запис про відхилення. Окреме правило може реагувати на наявність сервісів управління з віддаленим доступом у сегменті, який повинен бути ізольованим.

Правила реалізують метод оцінювання, який на вході отримує об’єкт, список сервісів і повертає або об’єкт Finding, або значення відсутності відхилення. Модуль RuleEngine перебирає всі правила для кожного об’єкта, акумулює результати і передає їх у підсистему звітності.

Підсистема формування звітів

Підсистема звітності виконує дві основні функції. Вона створює людинозрозумілий текстовий звіт для пояснювальної записки та одночасно формує структурований JSON для подальшої обробки.

У JSON форматі зберігаються об’єкти, сервіси і повний перелік виявлених відхилень. Така структура дозволяє використовувати звіт у зовнішніх інструментах аналізу або у наступних лабораторних роботах.

Текстовий звіт містить загальну інформацію про час виконання аудиту, перелік перевірених об’єктів з коротким описом, таблицю виявлених сервісів для кожного об’єкта і розділ з відхиленнями. Для кожного відхилення вказується об’єкт, правило, короткий опис проблеми, рівень важливості та коротка рекомендація. У навчальній реалізації рекомендації можуть бути узагальненими, наприклад сегментація мережі, відключення непотрібних сервісів, використання шлюзів прикладного рівня.

Основний керуючий модуль

Основний модуль поєднує всі підсистеми в єдиний сценарій. Під час запуску він створює екземпляр конфігурації, ініціалізує репозиторій об'єктів та наповнює його або типовими прикладами, або вмістом, який можна зчитати з простого JSON файла. Потім створюється екземпляр сканера, який послідовно обробляє всі об'єкти інвентаризації та збирає інформацію про відкриті порти.

Після завершення сканування основний модуль передає отримані дані у RuleEngine. Там до кожного об'єкта застосовується набір правил безпеки. Зібрані відхилення разом з інформацією про сервіси формують структуру AuditResult.

Далі результат передається у ReportGenerator. Програма формує текстовий звіт і виводить його у консоль. Одночасно створюється файл JSON з детальною структурою. Наприкінці основний модуль виводить коротку підсумкову інформацію про кількість об'єктів, кількість виявлених сервісів та кількість знайдених відхилень.

Реалізація орієнтується на безпечне застосування у лабораторних умовах. Студенти працюють з наперед визначеним переліком об'єктів, який моделює реальну промислову мережу, або з тестовим сегментом, що фізично відокремлений від виробничих систем. Код легко адаптується до середовища емуляції мереж, наприклад до віртуальних машин та віртуальних контролерів.

Завдяки використанню Python студенти можуть поступово розширювати реалізацію. Вони додають нові правила, змінюють критерії оцінювання, доповнюють модуль сканування підтримкою додаткових протоколів, інтегрують систему з зовнішніми джерелами даних. У пояснювальній записці це дає змогу продемонструвати як програмні засоби аудиту безпеки ICS SCADA адаптуються до конкретних сценаріїв підприємства.

```
import json
import socket
import threading
import queue
import ipaddress
from dataclasses import dataclass, field
```

```
from datetime import datetime
from typing import Dict, List, Optional, Tuple

# Конфігураційні константи для навчальної системи аудиту ICS SCADA
class ICSAuditConfig:
# Ініціалізація параметрів конфігурації
    def __init__(self) -> None:
# Список портів для типових протоколів ICS SCADA
        self.ics_ports = {
            502: "Modbus TCP",
            20000: "DNP3",
            2404: "IEC 60870 5 104",
            102: "Siemens S7",
        }
# Список загальних IT сервісів які можуть бути небезпечними у технологічному
сегменті
        self.general_service_ports = {
            22: "SSH",
            80: "HTTP",
            443: "HTTPS",
            3389: "RDP",
            445: "SMB",
        }
# Тайм аут для перевірки одного порта
        self.scan_timeout = 1.0
# Максимальна кількість потоків для одночасного сканування
        self.max_threads = 20
# Гранична кількість портів для об’єкта з високою критичністю
        self.critical_asset_port_threshold = 10
@dataclass
class Asset:
# Описує окремий об’єкт ICS SCADA
    name: str
    ip: str
    role: str
    zone: str
    criticality: int = 3
    protocols: List[str] = field(default_factory=list)
    def to_dict(self) -> Dict:
# Перетворення об’єкта у словник для формування звіту
        return {
            "name": self.name,
```

```
            "ip": self.ip,
            "role": self.role,
            "zone": self.zone,
            "criticality": self.criticality,
            "protocols": list(self.protocols),
        }
@dataclass
class ServiceInfo:
# Інформація про виявлений мережевий сервіс
    port: int
    transport: str
    name: str
    banner: str = ""
    def to_dict(self) -> Dict:
# Перетворення інформації про сервіс у словник
        return {
            "port": self.port,
            "transport": self.transport,
            "name": self.name,
            "banner": self.banner,
        }
@dataclass
class Finding:
# Представлення одного виявленого відхилення
    rule_id: str
    title: str
    description: str
    severity: str
    asset_ip: str
    related_ports: List[int] = field(default_factory=list)
    def to_dict(self) -> Dict:
# Перетворення відхилення у словник
        return {
            "rule_id": self.rule_id,
            "title": self.title,
            "description": self.description,
            "severity": self.severity,
            "asset_ip": self.asset_ip,
            "related_ports": list(self.related_ports),
        }
@dataclass
class AuditResult:
```

```
# Сукупні результати аудиту
    started_at: datetime
    assets: Dict[str, Asset] = field(default_factory=dict)
    services: Dict[str, List[ServiceInfo]] = field(default_factory=dict)
    findings: List[Finding] = field(default_factory=list)
    def to_dict(self) -> Dict:
# Перетворення результатів аудиту у словник
        return {
            "started_at": self.started_at.isoformat(),
            "assets": {ip: asset.to_dict() for ip, asset in self.assets.items()},
            "services": {
                ip: [s.to_dict() for s in srv_list]
                for ip, srv_list in self.services.items()
            },
            "findings": [f.to_dict() for f in self.findings],
        }
class InventoryRepository:
# Сховище об’єктів контролю ICS SCADA
    def __init__(self) -> None:
# Створення порожнього сховища об’єктів
        self._assets: Dict[str, Asset] = {}
    def add_asset(self, asset: Asset) -> None:
# Додавання об’єкта до сховища
        self._assets[asset.ip] = asset
    def get_asset(self, ip: str) -> Optional[Asset]:
# Пошук об’єкта за IP адресою
        return self._assets.get(ip)
    def all_assets(self) -> List[Asset]:
# Отримання списку всіх об’єктів
        return list(self._assets.values())
    def preload_sample_assets(self) -> None:
# Попереднє наповнення сховища прикладом промислової мережі
        self.add_asset(
            Asset(
                name="PLC1",
                ip="192.168.10.10",
                role="Польовий контролер лінії",
                zone="Field",
                criticality=5,
                protocols=["Modbus TCP"],
            )
        )
```

```
        self.add_asset(
            Asset(
                name="HMI1",
                ip="192.168.10.20",
                role="Робоче місце оператора",
                zone="Control",
                criticality=4,
                protocols=["Modbus TCP"],
            )
        )
        self.add_asset(
            Asset(
                name="ENG1",
                ip="192.168.10.30",
                role="Інженерна станція",
                zone="Engineering",
                criticality=4,
                protocols=["Modbus TCP", "DNP3"],
            )
        )
        self.add_asset(
            Asset(
                name="HIST1",
                ip="192.168.10.40",
                role="Сервер історії",
                zone="Control",
                criticality=3,
                protocols=[],
            )
        )
```


4.2 Захист розробленого програмного забезпечення

Захист розробленого програмного забезпечення буде відбуватися за допомогою IDEA – симетричний блоковий алгоритм шифрування даних, запатентований швейцарською фірмою Ascom. Відомий тим, що застосовувався в пакеті програм шифрування PGP. У листопаді 2000 року IDEA був представлений

як кандидат у проекті NESSIE в рамках програми Європейської комісії IST (англ. Information Societes Technology, інформаційні громадські технології).

Першу версію алгоритму розробили в 1990 році Лай Сюецзя (Xuejia Lai) і Джеймс Мессі (James Massey) зі Швейцарського інституту ETH Zürich (за контрактом з Hasler Foundation, яка пізніше влилася в Ascom-Tech AG) як заміна DES (англ. Data Encryption Standard, стандарт шифрування даних) і назвали її PES (англ. Proposed Encryption Standard, запропонований стандарт шифрування). Потім, після публікації робіт Біхамом і Шаміра по диференціальному криптоаналізу PES, алгоритм був поліпшений з метою посилення криптостійкості і названий IPES (англ. Improved Proposed Encryption Standard, покращений запропонований стандарт шифрування). Через рік його перейменували в IDEA (англ. International Data Encryption Algorythm).

Так як IDEA використовує 128-бітний ключ і 64-бітний розмір блоку, відкритий текст розбивається на блоки по 64 біт. Якщо таке розбиття неможливо, останній блок доповнюється різними способами певною послідовністю біт. Для уникнення витоку інформації про кожному окремому блоці використовуються різні режими шифрування. Кожен вихідний незашифрований 64 – біт ний блок ділиться на чотири підблока по 16 біт кожен, так як всі алгебраїчні операції, що використовуються в процесі шифрування, відбуваються над 16-бітними числами. Для шифрування і розшифрування IDEA використовує один і той же алгоритм.

Позначення операцій:

- $\boxplus$ Додавання за модулем 2^{16}.
- $\odot$ Множення за модулем $2^{16}+1$.
- $\oplus$ Побітова виключна диз'юнкція.

Фундаментальним нововведенням в алгоритмі є використання операцій з різних алгебраїчних груп, а саме:

Додавання за модулем 2^{16}.

Множення за модулем $2^{16}+1$.

Побітова виключна диз'юнкція (XOR).

Ці три операції несумісні в тому сенсі, що ніякі дві з них не задовольняють дистрибутивному закону, тобто:

$$a \odot (b \oplus c) \neq (a \odot b) \oplus (a \odot c).$$

Застосування цих трьох операцій ускладнює криптоаналіз IDEA в порівнянні з DES, який базується виключно на операції виключає АБО, а також дозволяє відмовитися від використання S-блоків і таблиць заміни. IDEA є модифікацією мережі Фейстеля.

Генерація ключів

З 128-бітного ключа для кожного з восьми раундів шифрування генерується по шість 16-бітних подключів, а для вихідного перетворення генерується чотири 16-бітних підключа. Всього буде потрібно 52 = 8 x 6 + 4 різних подключів по 16 біт кожен. Процес генерації п'ятдесяти двох 16-бітних ключів полягає в наступному:

Насамперед, 128-бітний ключ розбивається на вісім 16-бітних блоків. Це будуть перші вісім подключів по 16 біт кожен – $(K_1^{(1)}K_2^{(1)}K_3^{(1)}K_4^{(1)}K_5^{(1)}K_6^{(1)}K_1^{(2)}K_2^{(2)})$

Потім цей 128-бітний ключ циклічно зсувається вліво на 25 позицій, після чого новий 128-бітний блок знову розбивається на вісім 16-бітних блоків. Це вже наступні вісім подключів по 16 біт кожен – $(K_3^{(2)}K_4^{(2)}K_5^{(2)}K_6^{(2)}K_1^{(3)}K_2^{(3)}K_3^{(3)}K_4^{(3)})$

Процедура циклічного зсуву і розбивки на блоки триває до тих пір, поки не будуть згенеровані всі 52 16-бітних підключа.

Шифрування

Структура алгоритму IDEA показана на рисунку 4.3.

Процес шифрування складається з восьми однакових раундів шифрування і одного вихідного перетворення. Вихідний незашифрований текст ділиться на блоки по 64 біта. Кожен такий блок ділиться на чотири підблока по 16 біт кожен. На рисунку ці підблоки позначені D_1, D_2, D_3, D_4. У кожному раунді використовуються свої підключі згідно з таблицею підключів. Над 16-бітними підключами і підблока незашифрованого тексту проводяться наступні операції:

– Множення за модулем $2^{16}+1 = 65537$, причому замість нуля використовується 2^{16}.

– Додавання за модулем 2^{16}.

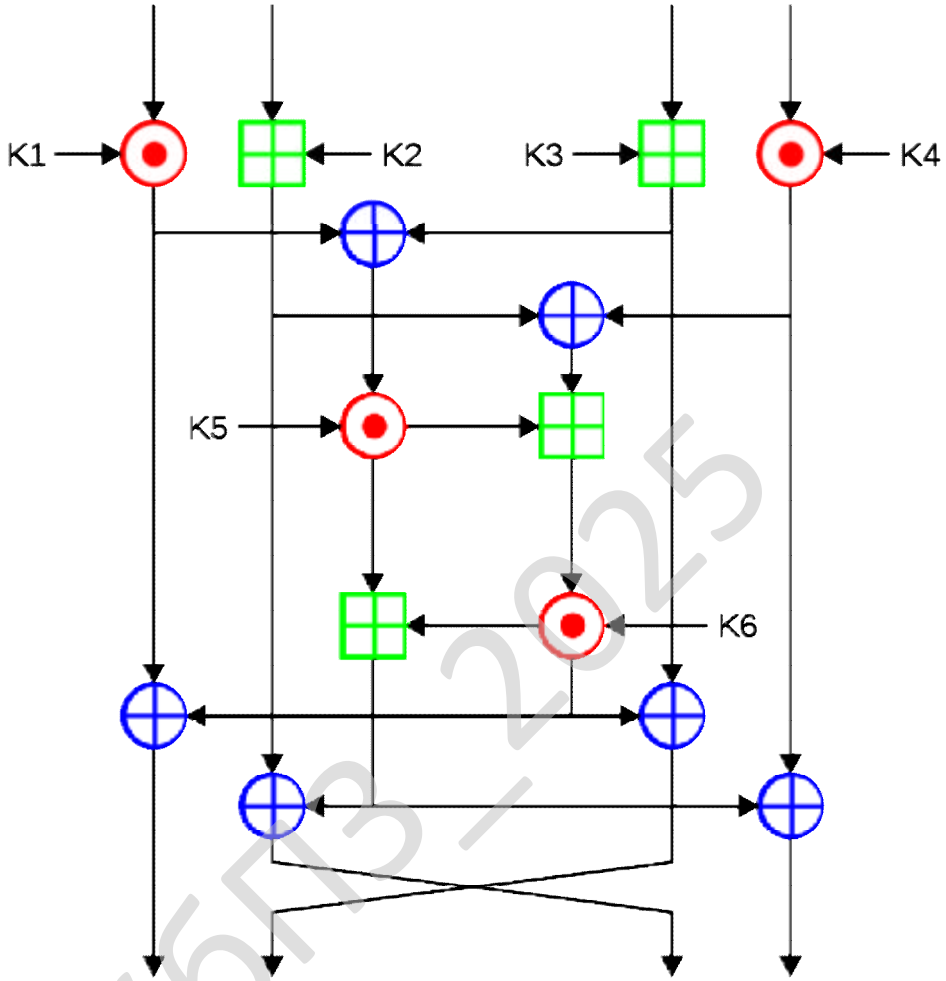

Рисунок 4.3 – Структура алгоритму IDEA

– Побітове виключне АБО.

В кінці кожного раунду шифрування є чотири 16-бітних підблоки, які потім використовуються як вхідні підблоки для наступного раунду шифрування. Вихідна перетворення являє собою скорочений раунд, а саме, чотири 16-бітних підблоки на виході восьмого раунду і чотири відповідних підключа піддаються операціям:

– Множення за модулем $2^{16}+1$.

– Додавання за модулем 2^{16}.

Після виконання вихідного перетворення конкатенація підблоків D_1', D_2', D_3' і D_4' являє собою зашифрований текст.

Потім береться наступний 64-бітний блок незашифрованого тексту і алгоритм шифрування повторюється.

Так продовжується до тих пір, поки не зашифрують всі 64-бітові блоки вихідного тексту.

5 МЕТОДИКА ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ

На рисунку 5.1 зображено інтерфейс програмного забезпечення, розробленого у результаті виконання магістерської роботи.

Розроблене програмне забезпечення аудиту безпеки систем ICS/SCADA складається з наступних функціональних блоків:

– Навігаційне меню: Файл; Сервіс; Структурно-логічна модель; Налаштування; Довідка.

– Вікно вибору необхідного розділу.

– Функціональних кнопок ПЗ.

– Навігаційного меню яке визивається натисканням правої клавіші маніпулятора миші.

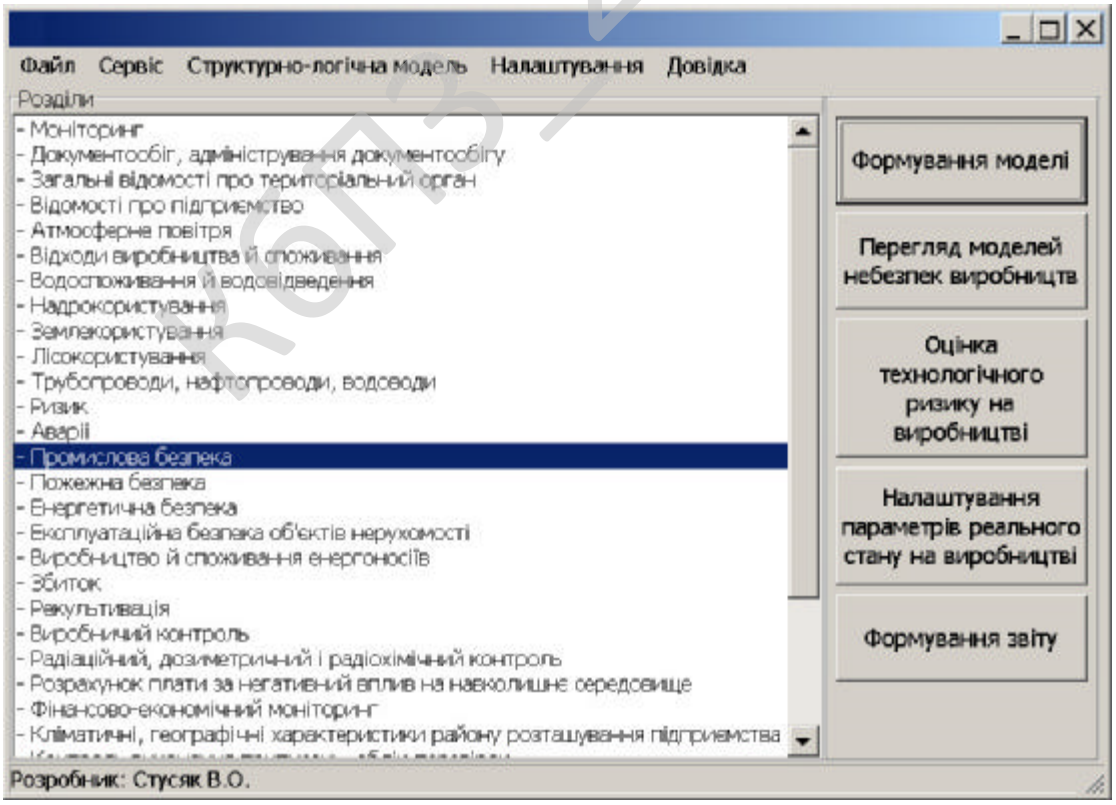

Рисунок 5.1 – Головне вікно розробленого ПЗ

Програма має простий та інтуїтивно зрозумілий інтерфейс, який зображений на рисунку 5.1.

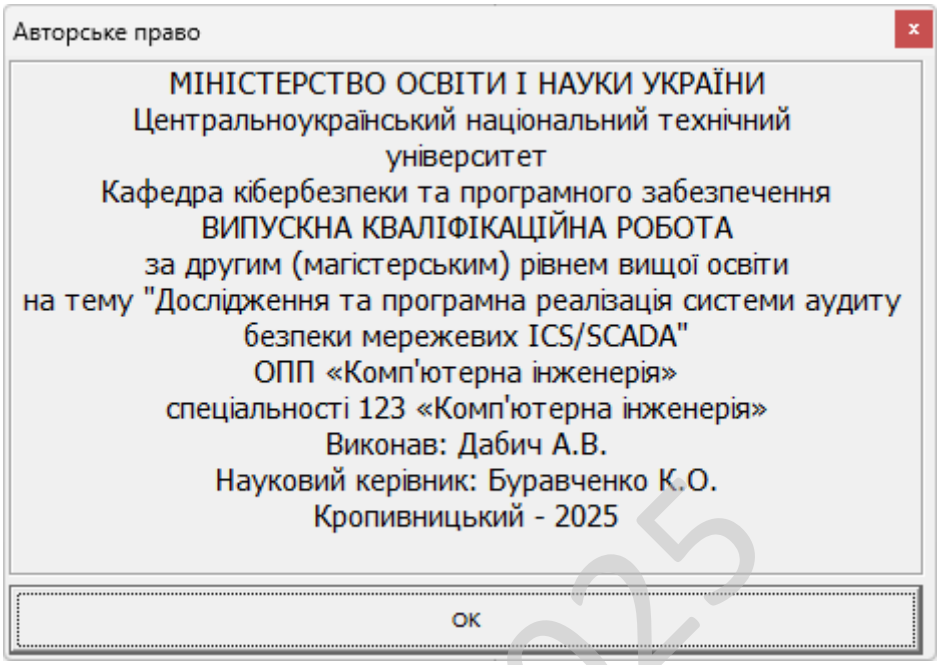

Рисунок 5.2 – Авторське право

Під час роботи над програмою було проведено тестування програмного забезпечення, тобто технічне дослідження, призначене для виявлення інформації про якість продукту відносно контексту, в якому воно має використовуватись.

Тестування включає як процес пошуку помилок або інших дефектів, так і випробування програмних складових з метою їх оцінки.

Проводилась оцінка:

– відповідності поставленим вимогам;

– правильна відповідь для усіх можливих вхідних даних;

– виконання функцій за прийнятний час;

– практичність;

– сумісність з ОС та стороннім ПЗ.

Оскільки число можливих тестів для програмних компонент практично нескінченне, тому стратегія тестування полягала в тому, щоб провести всі можливі тести з урахуванням наявного часу та ресурсів.

Як результат ПЗ тестувалось стандартним виконанням програми з метою виявлення помилок або інших дефектів.

Проводилось тестування форматом білої скриньки засноване на аналізі керуючої структури програми.

Програма вважається повністю перевіреною, якщо проведено вичерпне тестування маршрутів (шляхів) її графа управління.

У цьому випадку формуються тестові варіанти, в яких:

– Гарантується перевірка всіх незалежних маршрутів програми.

– Знаходяться гілки True, False для всіх логічних рішень.

– Виконуються всі цикли (у межах їхніх кордонів та діапазонів).

– Аналізується правильність внутрішніх структур даних.

Недоліки тестування "білої скриньки":

– Кількість незалежних маршрутів може бути дуже велика.

– Повне тестування маршрутів не гарантує відповідності програми вихідним вимогам до неї.

– У програмі можуть бути пропущені деякі маршрути.

– Не можна виявити помилки, поява яких залежить від даних.

Переваги тестування "білої скриньки» пов'язані з тим, що принцип «білої скриньки» дозволяє врахувати особливості програмних помилок:

– Кількість помилок мінімально в «центрі» і максимально на «периферії» програми.

– Попередні припущення про ймовірність потоку керування або даних у програмі часто бувають некоректними. У результаті типовим може стати маршрут, модель обчислень за яким опрацьована слабо.

– При записі алгоритму програмного забезпечення у вигляді тексту на мові програмування можливе внесення типових помилок трансляції (синтаксичних та семантичних).

– Деякі результати в програмі залежать не від вихідних даних, а від внутрішніх станів програми.

Обрано умови розповсюдження – Shareware.

Під умовно-безплатним програмним забезпеченням можна розуміти спосіб або метод розповсюдження комерційного ПЗ на ринку (тобто на шляху до кінцевого користувача), при якому випробувачеві пропонується обмежена за можливостями (не повнофункціональна або демонстраційна версія), терміном дії (тріал версія) або версія з вбудованим набридливим нагадуванням про необхідність оплати використання програми.

В угоді про використання (ліцензії для кінцевого користувача, EULA) також може бути обумовлена заборона на комерційне або професійне (не тестове) її використання.

Основний принцип умовно-безплатного ПЗ – «спробуй, перш ніж купити» (try before you buy). ПЗ що поширюється як умовно-безплатний, надається користувачам безоплатно. Звичайно користувач платить тільки за час завантаження файлів через Інтернет або за носій (CD диск, флешку, ключ). Протягом певного терміну, що становить зазвичай тридцять днів, він може користуватися програмою, тестувати її, освоювати її можливості.

Якщо після закінчення цього терміну користувач вирішить продовжити використання ПЗ, він зобов'язаний купити його (зареєструватися), заплативши авторові певну суму.

В іншому випадку користувач повинен припинити використання ПЗ та видалити його зі свого комп'ютера.

6 НАУКОВА НОВИЗНА

У випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для системи аудиту безпеки мережевих ICS/SCADA.

Метою розробки є дослідження та програмна реалізація системи аудиту безпеки мережевих ICS/SCADA.

Об'єктом дослідження є процес аудиту безпеки мережевих ICS/SCADA.

Предметом дослідження є методи аудиту безпеки мережевих ICS/SCADA.

Методи дослідження базуються на методах захисту інформації у мережі, методах математичної статистики, методах розробки програмного забезпечення.

Наукова новизна отриманих результатів. У процесі рішення завдань, обумовлених цілями дослідження, отримані наступні результати:

– Удосконалено метод аудиту безпеки мережевих ICS/SCADA.

– Розроблено вітчизняний продукт аудиту безпеки мережевих ICS/SCADA, який має більш широкі можливості, на відміну від існуючих аналогів.

7 МАРКЕТИНГОВЕ ТА ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ ІТ-ПРОЄКТУ

7.1 Визначення цільової аудиторії кінцевого готового продукту

Результати дослідження та розробки системи аудиту безпеки мережевих ICS/SCADA насамперед зацікавлять промислові підприємства, де автоматизація процесів є основою виробництва. Це можуть бути енергетичні компанії, нафтогазові комплекси, транспортна інфраструктура або підприємства хімічної промисловості. Для таких структур стабільність роботи систем керування має критичне значення, а будь-який збій або втручання з боку зловмисників може призвести до мільйонних збитків. Тому система аудиту безпеки, яка здатна своєчасно виявляти відхилення, несанкціоновані дії чи потенційні загрози, є стратегічно важливим елементом їхнього функціонування.

Крім того, ця розробка може зацікавити державні органи, які відповідають за кіберзахист критичної інфраструктури. Враховуючи постійне зростання кількості кібератак на промислові об’єкти, впровадження подібних систем може бути частиною державних програм із цифрової безпеки. Це допоможе не лише підвищити рівень захищеності об’єктів, але й створити єдину базу аудиту для аналізу тенденцій та обміну інформацією між секторами.

Також розробка буде цікавою для консалтингових компаній, що спеціалізуються на аудиті інформаційної безпеки. Вони зможуть використовувати її як інструмент для комплексної оцінки ризиків клієнтів і надання рекомендацій щодо посилення безпеки. Окрім цього, навчальні заклади та науково-дослідні установи можуть застосовувати систему як навчальну платформу для підготовки фахівців у галузі кіберзахисту промислових систем.

У ширшому сенсі, подібна система може бути корисною навіть для невеликих підприємств, які починають автоматизувати свої виробничі процеси.

Зазвичай такі компанії мають обмежені ресурси для повноцінної служби безпеки, тому впровадження автоматизованої системи аудиту стане для них ефективним і доступним способом забезпечення кіберзахисту. Таким чином, потенційне коло зацікавлених користувачів охоплює як великі корпорації, так і середні або навіть малі підприємства, які прагнуть підвищити рівень надійності своїх технологічних систем.

7.2 Оцінка привабливості шляхом застосування методів експертних оцінок

Для визначення привабливості системи аудиту безпеки мережевих ICS/SCADA було проведено експертне опитування серед фахівців у галузі автоматизації, промислової кібербезпеки та адміністрування критичних інфраструктур. Експертам запропонували оцінити систему за п’ятьма критеріями: ефективність виявлення загроз, простота інтеграції з існуючими ICS/SCADA-рішеннями, зручність візуалізації аудиту, вартість впровадження та рівень автоматизації процесів. Кожен критерій оцінювався за 10-бальною шкалою, а потім підсумковий результат визначався за середньозваженою оцінкою.

За підсумками оцінювання, система отримала середній бал 8,9 із 10. Найвищу оцінку – 9,5 бала – було отримано за зручність аналізу журналів подій та автоматичну генерацію звітів. Експерти відзначили, що можливість віддаленого доступу до аналітики в реальному часі значно спрощує контроль над системою безпеки. Також високі оцінки отримала гнучкість налаштувань, що дозволяє адаптувати систему під різні типи виробничих середовищ.

Найнижчі оцінки (близько 8 балів) були отримані за вартість впровадження, оскільки для деяких малих підприємств первинні інвестиції можуть здатися значними. Проте експерти підкреслили, що з точки зору довгострокової вигоди система є економічно доцільною, оскільки окупається протягом одного року за рахунок зменшення простоїв і запобігання аваріям. У

цілому, експертний аналіз підтвердив високу ринкову привабливість розробки, підкресливши її відповідність сучасним вимогам кіберзахисту промислових систем.

Таким чином, метод експертних оцінок показав, що система має реальні перспективи для впровадження у промислових середовищах і здатна конкурувати з дорогими закордонними аналогами, залишаючись гнучкою та адаптивною до потреб українського ринку.

7.3 Вибір методу оцінки вартості ПЗ

Для оцінки вартості системи аудиту безпеки ICS/SCADA найдоцільніше застосувати витратний метод у поєднанні з елементами порівняльного аналізу. Витратний метод дозволяє розрахувати реальні фінансові вкладення, необхідні для розробки, впровадження та підтримки системи, включно з оплатою праці спеціалістів, придбанням обладнання, ліцензуванням компонентів та тестуванням. Цей підхід забезпечує прозорість фінансового планування й дозволяє визначити точну собівартість продукту.

Разом із тим, порівняльний метод дає можливість співставити вартість розробленої системи з уже існуючими аналогами на ринку. Це допоможе визначити конкурентну ціну та зробити продукт привабливішим для клієнтів. У сфері кібербезпеки та автоматизації такий підхід особливо актуальний, адже дозволяє враховувати не лише технічні параметри, а й репутаційну цінність рішення.

Використання сукупного підходу дозволяє отримати більш точну й реалістичну оцінку вартості. Наприклад, якщо система демонструє високий рівень автоматизації аудиту, зменшуючи потребу в ручній праці фахівців, це може суттєво підвищити її ринкову цінність. Також важливо врахувати витрати на майбутні оновлення, технічну підтримку та адаптацію системи під різні виробничі стандарти.

У результаті саме комбінований підхід – витратно-порівняльний – є найефективнішим для об’єктивної оцінки вартості такої системи. Він забезпечує баланс між фінансовою точністю, ринковою доцільністю та стратегічною конкурентоспроможністю розробки.

7.4 Розрахунок економічної ефективності від впровадження реалізованого ПЗ як фактору його привабливості

Підприємство використовує систему автоматизованого керування технологічними процесами (ICS/SCADA) для контролю виробничих об’єктів. До впровадження системи аудиту безпеки спостерігались періодичні збої в роботі обладнання, несанкціоновані зміни у налаштуваннях контролерів та відсутність централізованого моніторингу подій. Це призводило до простоїв, втрати даних та підвищення операційних витрат. Метою впровадження системи аудиту є підвищення рівня кіберзахисту промислової інфраструктури, запобігання зупинкам технологічного процесу та забезпечення відповідності стандартам ISA/IEC 62443. Вхідні дані зафіксовано в таблиці 7.1.

Розрахунок економічного ефекту показує: зменшення збитків від інцидентів – 720 000 грн/рік, економія на зовнішніх аудитах безпеки – 150 000 грн/рік, сукупний річний ефект – 870 000 грн/рік, термін окупності (Payback Period) – 0,69 року (~8 місяців), коефіцієнт економічної ефективності – 145%, річна економія після окупності – 770 000 грн.

Додаткові (немонетарні) переваги: підвищення надійності виробництва – зменшення кількості аварій і простоїв обладнання, покращення контролю доступу – аудит дій операторів та адміністраторів у реальному часі, відповідність міжнародним стандартам безпеки, зростання довіри партнерів – можливість підтвердження сертифікації безпеки під час перевірок, оптимізація внутрішніх процесів – автоматизація аналізу журналів подій і формування звітів для керівництва.

Таблиця 7.1 – Вихідні дані для розрахунку

Показник	**До впровадження**	**Після впровадження**	**Економічний ефект**
Кількість технічних збоїв через несанкціоновані дії або зловмисне втручання (на рік)	8	2	–6
Середні збитки від одного інциденту (зупинка виробництва, ремонт, відновлення даних)	120 000 грн	40 000 грн	–80 000 грн
Річні витрати на аудит безпеки (зовнішні перевірки)	300 000 грн	150 000 грн	–150 000 грн
Вартість впровадження системи аудиту (одноразово)	—	—	600 000 грн
Річні витрати на обслуговування системи	—	—	100 000 грн

Таким чином, аудит безпеки в ICS/SCADA є не просто інструментом кіберзахисту, а складовою стійкої виробничої політики, що поєднує економічну доцільність і технологічну безпеку підприємства.

7.5 Пропозиція алгоритму просування проєкту розробки ПЗ

Просування проєкту системи SIEM має починатися з глибокого розуміння її цільової аудиторії. Основними користувачами є компанії, що мають складну мережеву інфраструктуру та обробляють великі обсяги конфіденційних даних. Перший крок – створення демонстраційної версії системи або пілотного проєкту, який дозволить потенційним клієнтам побачити реальні результати аналізу загроз і оцінити ефективність автоматизації процесів. Візуалізація даних, приклади реальних сценаріїв реагування та наочні графіки стануть переконливим аргументом на користь рішення.

Далі слід зосередитись на комунікації через професійні спільноти та конференції з кібербезпеки. Виступи на форумах, публікації аналітичних матеріалів або кейсів використання системи дадуть змогу сформувати довіру серед фахівців галузі. Водночас важливо підтримувати онлайн-присутність через офіційний сайт, сторінку проєкту в LinkedIn, спеціалізовані форуми та освітні платформи. Це забезпечить доступність інформації про продукт для широкого кола користувачів. На наступному етапі можна запропонувати гнучку модель ліцензування. Наприклад, надати можливість безкоштовного тестового періоду для компаній, які бажають оцінити функціонал перед купівлею. Такий підхід сприяє формуванню лояльності та довіри. Важливо також підготувати набір матеріалів для технічних директорів і IT-менеджерів, у яких чітко показати, як система скорочує час реагування на загрози, знижує кількість інцидентів і дозволяє ефективніше використовувати ресурси команди безпеки.

Фінальним кроком має стати формування партнерських програм з провайдерами хмарних сервісів, консалтинговими компаніями та інтеграторами IT-рішень. Це розширить канали просування системи, дозволяючи їй виходити на нові ринки без значних маркетингових витрат. Також варто забезпечити підтримку користувачів і регулярні оновлення продукту – це допоможе не лише утримати клієнтів, а й створити довгострокову екосистему навколо розробки.

7.6 Оптимізація каналів збуту та шляхів реалізації ПЗ

Оптимізація каналів збуту системи SIEM повинна бути побудована на поєднанні прямих і партнерських шляхів реалізації. Основну ставку варто зробити на співпрацю з компаніями, які вже працюють у сфері IT-консалтингу або надають послуги з адміністрування корпоративних мереж. Вони можуть виступати посередниками, які пропонуватимуть систему своїм клієнтам як частину комплексних рішень із кібербезпеки. Така стратегія дозволяє не лише зменшити витрати на прямий маркетинг, а й розширити охоплення аудиторії через уже сформовану базу довіри партнерів.

Також ефективним інструментом може стати використання моделі підписки (SaaS). Це дає змогу компаніям почати користуватись системою без великих одноразових витрат, сплачуючи за фактичне використання. Такий підхід особливо привабливий для малого та середнього бізнесу, який часто має обмежений бюджет на безпеку, але потребує якісного захисту.

Ще одним напрямом оптимізації є створення відкритого API, що дозволить іншим розробникам інтегрувати SIEM у власні рішення. Це розширює потенційну клієнтську базу та створює додатковий ефект взаємодії з іншими системами безпеки. Крім того, варто приділити увагу роботі з навчальними закладами – співпраця з університетами може не лише розширити знання про продукт, а й підготувати майбутніх фахівців, які у своїй професійній діяльності обиратимуть знайомі технології.

Загалом, оптимізація збуту повинна спиратись на поєднання партнерських програм, цифрових каналів комунікації та освітніх ініціатив. Такий підхід створює не лише ринкову присутність продукту, а й підвищує його цінність у професійному середовищі.

7.7 Визначення ключових факторів успіху конкретного проєкту

Успіх проєкту системи мережевої SIEM багато в чому визначається її здатністю забезпечити надійність, точність і масштабованість. У першу чергу, система має ефективно збирати й аналізувати величезні обсяги даних у режимі реального часу, виявляючи потенційні загрози до того, як вони завдадуть шкоди. Висока продуктивність і мінімальна кількість хибних спрацьовувань – це ті показники, які безпосередньо впливають на рівень довіри користувачів і конкурентоспроможність продукту.

Не менш важливим є зручний інтерфейс і можливість адаптації системи під специфіку конкретного підприємства. Якщо рішення легко інтегрується у вже існуючу IT-інфраструктуру, воно стає привабливим як для технічних фахівців, так і для управлінців, які цінують простоту впровадження. Система, яка не потребує складного налаштування, має більші шанси на швидке поширення.

Стабільне оновлення бази загроз і постійна підтримка користувачів також є визначальними факторами успіху. У сфері кібербезпеки зволікання може мати серйозні наслідки, тому здатність оперативно реагувати на нові виклики робить продукт конкурентним і надійним.

Не можна оминути увагою й репутацію розробників. Відкрита комунікація з клієнтами, публічність результатів тестування, участь у профільних конференціях – усе це формує довіру до компанії й підвищує авторитет продукту на ринку. Коли клієнти бачать, що система розвивається, отримує оновлення і вдосконалюється, вони сприймають її як живий, надійний і перспективний інструмент.

Таким чином, поєднання технічної якості, гнучкості, професійної підтримки та репутаційної стабільності формує основу успіху будь-якої SIEM-системи. Це не просто програмний продукт, а стратегічне рішення, яке допомагає компаніям вибудовувати культуру безпеки та впевнено рухатись у цифровому середовищі.

8 ЗАХОДИ З ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ

8.1 Вступ

Законом України “Про охорону праці” [3] регламентуються загальні положення державної політики в галузі охорони праці, а реалізуються ці положення нормативно-правовими актами про охорону праці, зокрема Наказом Міністерства соціальної політики України № 207 від 25.04.2018 р. та №508/31960 «Про затвердження Вимог щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями» [5], яким затверджено нормативно-правовий акт з охорони праці НПАОП 0.00-7.15-18, «Правила охорони праці під час експлуатації електронно-обчислювальних машин», та «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» ДСанПіН 3.3.2-007-98.

Програмісти у процесі роботи мають негативний вплив на органи зору, а також мають значну розумову напругою і нервово-емоційне навантаження. Руки (суглоби пальців та м'язи рук) при роботі з клавіатурою мають теж істотне навантаженням. До шкідливих факторів, які впливають на робітників галузі інформаційних технологій (ІТ) спеціалісти відносять високочастотні електромагнітні коливання (випромінювання) роботи апаратної частини ЕОМ та виділення шкідливих газів.

Ці шкідливі фактори можуть привести до професійних захворювань.

Керуючись нормативно-правовими актами «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» ДСанПіН 3.3.2-007-98 [5], та «Вимоги щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями» НПАОП 0.00-7.15-18 розглянемо шкідливі чинники роботи персоналу.

Щоб запропонувати заходи щодо зменшення негативного впливу

комп’ютера на організм людини визначимо фактори, які можуть викликати професійне захворювання і впливають на працездатність програміста.

8.2 Шкідливі і небезпечні фактори при роботі з комп’ютером

Працівники, задіяні на роботах, пов'язаних з періодичною або постійною роботою за комп'ютером, піддаються впливу факторів виробничої небезпеки, основними з яких є наступні:

1. Фізичні:

– Підвищений рівень напруги в електричному ланцюзі, замикання якої може пройти через тіло працюючого;

– Підвищений рівень рентгенівського випромінювання;

– Підвищений рівень ультрафіолетового випромінювання;

– Підвищений рівень інфрачервоного випромінювання;

– Можливість ураження статичною електрикою;

– Запиленість повітря робочого приміщення;

– Підвищений вміст важких (+) аероіонів;

– Нерівномірний розподіл яскравості в полі зору;

– Підвищений рівень пульсації світлового потоку;

2. Хімічні: підвищений вміст у повітрі вуглекислого газу, озону, аміаку, фенолу, формальдегіду та інше

3. Психофізіологічні:

– Напруга зору;

– Напруга пам'яті;

– Напруга уваги.;

– Тривале статичне напруження;

– Підвищений обсяг інформації, що обробляється в одиницю часу;

– Монотонність праці в окремих випадках;

– Нераціональна організація робочого місця.

До основних шкідливих факторів при роботі з комп'ютером відносять: тривале сидяче положення, електромагнітне випромінювання, навантаження на зір, перевантаження кистьових суглобів, можливість захворювань органів дихання, алергії, порушення нормального перебігу вагітності та інше.

8.3 Аналіз санітарно-гігієнічних умов праці на робочому місці програміста

Розглянемо умови праці у приміщенні, в якому працюють програмісти. Геометричні розміри приміщення наведено у таблиці 8.1.

Таблиця 8.1 – Розміри приміщення

Найменування	Значення, м
Ширина	4
Довжина	5
Висота	3

Таблиця 8.2 – Площа та обсяг приміщення, на одного працюючого*

Геометрична характеристика	Одиниця виміру	Нормативне значення*	Фактичне значення
Площа, S	$м^2$	не менше 6.0	6,6
Об'єм, V	$м^3$	не менше 20.0	20

* Згідно ДСанПіН 3.3.2.007-98 (Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин).

У зазначеному приміщенні працюють троє людей. За даними, які наведено у таблиці 8.1, та таблиці 8.2, можна зробити висновок, що площа та об’єм приміщення у розрахунку на одне робоче місце програміста не відповідають нормативним вимогам ДСанПіН 3.3.2-007-98 «Державні санітарні правила і

норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» [5], але відповідають нормативним вимогам Наказу Міністерства соціальної політики України № 207, від 14.02.2018 «Про затвердження Вимог щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями» [5] та НПАОП 0.00-1.28-10 «Правила охорони праці під час експлуатації електронно-обчислювальних машин»). Таним чином можна зробити висновок, що санітарно-гігієнічні умови праці на робочому місці програміста відповідають вимогам.

Температура повітря в приміщенні визначається впливом температури зовнішнього повітря і тепловою енергією, яка виділяється всередині приміщення. Джерелами виділення теплоти в даному приміщенні є електроустаткування, освітлювальні прилади, а також люди. У світлий час доби джерелом надлишкового тепла є сонячна радіація. Згідно Постанови № 42 від 01.12.1999 Головного державного санітарного лікаря України, робота, виконувана в даному приміщенні, відноситься до категорії Іа. В цьому випадку людина витрачає енергії до 120 ккал у годину. Вологість повітря в приміщенні визначається впливом багатьох факторів, серед яких: вологість атмосферного повітря, виділення вологи людьми (при диханні та випарами з поверхні шкіри).

Мікроклімат повітряного середовища в приміщенні характеризується запиленістю та загазованістю повітря. Мікроклімат приміщення визначається діючим на організм людини поєднанням, вологості, температури, швидкості руху повітря та інтенсивності теплового випромінювання. Аналіз мікроклімату складається з визначення зазначених вище факторів і порівняння результатів із встановленими нормами.

У таблиці 8.3 наведено оптимальні та фактичні значення параметрів мікроклімату як для категорії ваги робіт Іа, так і розглянутого приміщення. У приміщеннях, де встановлено ЕОМ, рекомендується застосування тільки оптимальних значень показників мікроклімату.

Проведений аналіз показує, що показники мікроклімату в приміщенні відповідають установленим нормам. Штучне опалення застосовується у холодний період року.

В літню пору застосовується кондиціонер.

Для боротьби з пилом робляться регулярні провітрювання та вологі прибирання приміщенні.

Таблиця 8.3 – Оптимальні і фактичні значення параметрів мікроклімату

Пора року	Оптимальні для Іа			Фактичні		
	Температура, °С	Вологість, %	Швидкість повітря, м/с	Температура, °С	Вологість, %	Швидкість повітря, м/с
Холодна	22-24	40-60	0,1	21-22	46-54	0,1
Тепла	23-25	50-70	0,1	24-25	50-65	0,11

У приміщенні знаходяться наступні джерела шуму: принтер *XEROX PHASER 3020BI*, електродвигуни вентиляторів ЕОМ.

Одним з найважливіших факторів, які впливають на ефективність трудової діяльності людини, та попереджають травматизм і професійні захворювання програмістів є освітлення на робочому місці.

З 2019 року діють Державні будівельні норми України “Природне і штучне освітлення” – ДБН В.2.5-28:2018 [1], у яких прописані вимоги до використання всіх освітлювальних приладів, у тому числі світлодіодних.

Працю працівника, який постійно працює за комп’ютером, згідно ДБН В.2.5-28:2018 [1], можна віднести до роботи з малою точністю (найменший розмір об'єкта має розрізнення від 1 до 5 мм) V-го розряду зорової роботи, з великою контрастністю об'єкта розрізнення (символів на екрані дисплея), з темним тлом (підрозряд зорової роботи В).

Приміщення можна віднести до 1-ої групи приміщень, у яких проводиться розрізнення об'єктів зорової роботи при фіксованому напрямку лінії зору того, що працює на робочу поверхню.

Для такого типу приміщень і розряду зорової роботи нормоване значення коефіцієнта природної освітленості (КПО) робочої поверхні (при поєднаному, спільному освітленні), повинен становити не більше 1,5%, освітленість при штучному висвітленні повинна становити 300 Лк. [1], Крім того все поле зору повинне бути освітлено достатньо рівномірно – ця основна гігієнічна вимога. Оскільки яскраве світло на ділянці периферійного зору значно збільшує напруженість очей і, як наслідок, призводить до їх швидкої стомлюваності, ступінь освітлення приміщення і яскравість екрану комп'ютера повинні бути приблизно однаковими.

8.4 Розробка заходів з умов поліпшення охорони праці

Згідно аналізу умов праці в розглянутому приміщенні, ми одержали наступні результати:

– розмірі приміщення, у розрахунку на одному працюючого, відповідають нормативам;

– мікроклімат відповідає нормативному значенню;

– акустичні умови роботи не перевищують нормативних значень;

Таким чином можна припустити, що основною причиною можливого зниження працездатності програміста є психофізіологічний фактор, тому основна пропозиція буде така: дотримання позитивної психологічної атмосфери в колективі та регламентованого режиму праці та відпочинку, організація робочого місця з урахуванням ергономічних вимог.

Рекомендовані заходи: регулярні періодичні наочні огляди персоналом шляхів для евакуації людей із приміщення, відповідно до плану евакуації (який повинен розташовуватись на видному місці у приміщенні), включення до

колективного договору мінімально можливого вмісту аптечок з обов'язковою наявністю масок-клапанів, або іншого спорядження для штучного дихання. Регулярна періодична перевірка параметрів заземлення та занулення (вимірювання опору ланцюга).

Регулярна наочне знайомство персоналу із шляхами для евакуації людей із приміщення відповідно до плану евакуації, забезпечення розподільних щитів спеціальними розетками з заземлюючими контактами; організація заземлення всіх приладів і пристроїв, які працюють при напрузі вище 36 В.

8.5 Розрахункова частина

Проведемо розрахунок штучного освітлення за методом коефіцієнту використання світлового потоку для приміщення ширина якого складає 4 м, довжина – 5 м, висота – 3 м.

Для того, щоб визначити потрібну кількість світильників, які повинні забезпечити нормований рівень освітленості, необхідно враховувати, що, з одного боку середня освітленість робочих місць з постійним перебуванням людей повинна бути не менш як 200 люкс, а з іншого – штучне освітлення при системі комбінованого освітлення для зорової роботи найвищої точності повинна складати 300 лк та вимогу ДБН В.2.5-28:2018, що створювати освітленість більше ніж 300 лк при світлодіодних світильникх дозволяється тільки за наявності обґрунтування.

Таким чином для розрахунку приймаэмо середню освітленість робочих місць 300 Люкс [1].

Визначимо світловий потік, що падає на робочу поверхню за формулою [6]:

$$F = E \cdot S \cdot K \cdot Z / n,$$

де:

F – світловий потік, що розраховується, Лм;

E – нормована мінімальна освітленість, Лк; E = 300 Лк. [1];

S – площа поверхні, на яку падає світловий потік, м^2 [1];

Z – відношення середньої освітленості до мінімальної (зазвичай приймається рівним 1.1... 1.2, у нашому випадку Z = 1,1);

K – коефіцієнт запасу, що враховує зменшення світлового потоку світильників в результаті їх забруднення в процесі експлуатації (його значення залежить від типу приміщення і характеру робіт, що проводяться в ньому, в нашому випадку K = 1,5) [1];

n – коефіцієнт використання світлового потоку, (відношення світлового потоку, що падає на розрахункову поверхню, до сумарного потоку всіх ламп і обчислюється в долях одиниці; залежить від характеристик світильника, розмірів приміщення, забарвлення стін і стелі, що характеризуються коефіцієнтами відбиття від стін ($\rho_{стін.}$) і стелі ($\rho_{стелі}$), значення коефіцієнтів дорівнюють $\rho_{стін}$ = 50% і $\rho_{стелі}$ = 50% [6].

Обчислимо індекс приміщення за формулою:

$$i = S/(h\cdot (A+B)),$$

де:

S – площа поверхні, на яку падає світловий потік, м^2 [1];

h – розрахункова висота підвісу, h = 3 м;

A – ширина приміщення, A = 4 м;

B – довжина приміщення, B = 5 м.

Підставимо всі значення у формулу та визначимо індекс приміщення:

$$i=0,74.$$

Знаючи індекс приміщення, знаходимо n = 0.29 (з табличних даних коефіцієнтів використання світлового потоку (n) світильників відповідного типу [6]). Підставимо всі значення у формулу, визначимо світловий потік: F=43043 Лм.

Будемо використовувати світильники (світлодіодні панелі) Matt White Армстронг 36W 6000К, світловий потік яких $F_л$ = 3000 Лм.

Число ламп визначається по формулі:

$$N = F/F_л$$

де:

F – світловий потік,

$F_л$ – світловий потік одного світильника.

Підставимо всі значення у формулу та визначемо індекса приміщення:

$$N = 43043/3000 = 14{,}34 \text{ шт.}$$

Приймаємо необхідну кількість світильників 15 шт.

Висновки до розділу

Дотримання всіх необхідних умов праці не лише сприяє збереженню здоров'я працівників, а також підвищує ефективність виробництва в цілому.

З цих міркувань було здійснено аналіз приміщення, призначеного для праці програмістів, проведено розгляд небезпечних та шкідливих факторів, що негативно впливають на програмістів під час роботи. Виконано розрахунок штучного освітлення, як одного з ключових факторів впливу на працездатність та здоров'я програміста. Розроблено заходи з охорони праці.

9 ОСНОВНІ ВИСНОВКИ

Програмне забезпечення, створене в результаті виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти, призначено для системи аудиту безпеки мережевих ICS/SCADA.

В межах України в недостатній мірі представлені вітчизняні розробки в цій області.

У випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти наведені теоретичне узагальнення й рішення наукового завдання дослідження методів аудиту безпеки мережевих ICS/SCADA.

Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем аудиту безпеки мережевих ICS/SCADA.

– Досліджена система аудиту безпеки мережевих ICS/SCADA.

– На основі отриманих результатів досліджень створена програмна реалізація системи аудиту безпеки мережевих ICS/SCADA.

Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання аудиту безпеки мережевих ICS/SCADA.

Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Розроблене програмне забезпечення має простий, дружній та зручний інтерфейс користувача, що забезпечує легкість у освоєнні роботи програмного продукту, зручність у використанні, і не потребує особливих спеціальних знань.

При створені програмного забезпечення було використано об’єктно-орієнтований підхід, що відповідає сучасним тенденціям у галузі розробки комерційних програмних систем.

Програма реалізована на мові високого рівня Python. Дана мова програмування дозволяє найбільш ефективно обробляти дані. Це дозволило мінімізувати строк розробки програмного забезпечення, і, як слід, зменшити витрати на його розробку. Запропоноване програмне забезпечення ділиться на загальне програмне забезпечення, що поставляється із засобами обчислювальної техніки й спеціальне програмне забезпечення, що спеціально розроблене для даної конкретної системи й включає програми, що реалізують її функції.

Програма призначена для виконання під управлінням багатозадачної операційної системи Windows 10/11.

Даються необхідні рекомендації з установки розробленого програмного забезпечення.

Для підвищення рівня безпеки запропоновано застосовувати алгоритм IDEA.

В цілому створене програмне забезпечення підтверджує правильність використаних проектних рішень та повністю відповідає вимогам технічного завдання. Створене програмне забезпечення має потенційну можливість для подальшого вдосконалення і застосування у різних галузях.

Проведено маркетингове та економічне обґрунтування ІТ-проєкту, що дозволило визначити ключові фактори успіху даного проекту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Дабич А.В. Дослідження та програмна реалізація системи аудиту безпеки мережевих ICS/SCADA // Збірник праць молодих науковців ЦНТУ. – Вип. 15. – Кропивницький: ЦНТУ, 2025.

2. Corey J. Ball. Hacking APIs. No Starch Press. 2022. 353 p.

3. Kevin Beaver. Hacking for Dummies. John Wiley & Sons. 2022. 419 p.

4. Mark S. Merkow. Practical Security for Agile and DevOps. CRC Press. 2022. 236 p

5. Derek Fisher. Application Security Program Handbook. Manning Publications. 2021. 155 p.

6. Cameron Wyatt PH.D. Kali Linux Tutorial. Independently published. 2021. 60 p.

7. Alex Matrosov, Eugene Rodionov, Sergey Bratus. Rootkits and Bootkits. No Starch Press. 2019. 450 p.

8. Петрик В.М., Присяжнюк М.М., Аль-Файюмі Халед та ін. «Системи інформаційної зброї та технології інформаційної війни»: підручник / Петрик В.М., Присяжнюк М.М., Аль-Файюмі Халед, Жарков Я.М., Смірнов О.А, Буравченко К.О., Давидюк А.В., Кононович В.Г., Корчинский В.В., Кудирко В.М., Фесенко А.О.; за заг. ред. В.М. Петрика, М.М. Присяжнюка.– К.: Видавничий центр “Кафедра”, 2025.– 320 с.

9. Усік, П.С., Смірнова, Т.В., Буравченко, К.О., Смірнов, О.А., Улічев, О.С., Смірнов, С.А. «Дослідження технологій забезпечення кібербезпеки банківських систем з використанням штучного інтелекту». *Кібербезпека: освіта, наука, техніка.* 2025. Том 1 № 29. С.704–716, 2025

10. Kuznetsov, O., Frontoni, E., Kuznetsova, K., Arnesano, M., Smirnov, O. «A secure biometric authentication architecture for blockchain-driven cyber-physical systems». *Security and Privacy of Cyber Physical Systems Emerging Trends*

Technologies and Applications, 2025, pp. 193–224.

11. Kuznetsov, O., Atzeni, G., Arnesano, M., Randieri, C., Smirnov, O. «Secure IoT-based smart wheelchair system: From implementation to security enhancement strategy». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 225–257.

12. Kuznetsov, O., Smirnov, O., Kuznetsova, T., Shaikhanova, A., Svatowsky, I. «Privacy-utility trade-offs in IoT networks: A comparative analysis of differential privacy mechanisms for sensor data aggregation». *Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications*, 2025, pp. 589–622.

13. Lakhno, V., Malyukov, V., Smirnov, O., Bebeshko, B., Chubaievskiy, V., Zhumadilova, M., Malyukova, I., Smirnov, S. «Multifactorial Model for Targeted Attacks Counteracting Within the Framework of a Multi-Step Quality Game with Fuzzy Information». *8th International Symposium on Intelligent Informatics, ISI 2023*, 2025. vol 389. pp 377-389. Springer, Singapore.

14. Kuznetsov O., Frontoni E., Kuznetsova Y., Smirnov O., Moskovchenko I. «Trust-Based Security Architecture for Edge Computing: A Simulation Study of Dynamic Trust Evolution and Attack Detection». *CEUR Workshop Proceedings,* 2024, 3909, pp. 227–241.

15. Kuznetsov, O., Frontoni, E., Kryvinska, N., Chevardin, V., Smirnov, O. «Wireless Network Encryption Stream Ciphers, Computational Modeling, and Security Analysis». *Computational Modeling and Simulation of Advanced Wireless Communication Systems*, 2024, pp. 379–402.

16. Kuznetsov, O., Frontoni, E., Kryvinska, N., Smirnov, O., Imoize, G.L. «Computational Modeling of Enhanced Spread Spectrum Codes for Asynchronous Wireless Communication». *Computational Modeling and Simulation of Advanced Wireless Communication Systems*, 2024, pp. 403–447.

17. Ткаченко, О., Ільєнко, А., Улічев, О., Мелешко, Є., Смірнов, О. «Правові засади поширення інформаційних впливів в соціальних мережах».

Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2024. № 2(26), С. 170–188.

18. Смірнова Т.В., Конопліцька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». *Кібербезпека: освіта, наука, техніка.* 2024. №4(24), С. 6-27.

19. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». *Кібербезпека: освіта, наука, техніка.* 2024. №3(23), С. 111-131.

20. Батрак О., Смірнова Т., Гнатюк В., Одарченко Р., Смірнов О. «Дослідження показників ефективності функціонування та перспектив розвитку систем IP-телефонії». *Підводні технології,* 2024, № 13, с. 28-35.

21. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». *CEUR Workshop Proceedings*, 2023, 3628, pp. 106-115.

22. Akhalaia, G., Iavich, M., Iashvili, G., Prysiazhnyy, D., Smirnova, T. «Secure Encrypted Connection on Georgian Website». *CEUR Workshop Proceedings,* 2023, 3550, pp. 313-320.

23. Al-Mudhafar Aqeel, A.M., Smirnova, T., Buravchenko, K., Smirnov, O. «The method of assessing and improving the user experience of subscribers in software-configured networks based on the use of machine learning». *Advanced Information Systems*, 2023, 7(2), pp. 49-56

24. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchev, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». *CEUR Workshop Proceedings,* Volume 3530, 2023, pp. 256-265.

25. Kuznetsov, O., Kandiy, S., Frontoni, E., Smirnov, O. «Trade-offs in Post-Quantum Cryptography: A Comparative Assessment of BIKE, HQC, and Classic McEliece». *CEUR Workshop Proceedings,* Volume 3504, 2023, pp. 1-11.

26. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskyi, V., Khorolska, K., Bebeshko, B. «Selection of a Rational Composition of İnformation Protection Means Using a Genetic Algorithm». *In: Rajakumar, G., Du, KL., Vuppalapati, C., Beligiannis, G.N. (eds) Intelligent Communication Technologies and Virtual Mobile Networks. Lecture Notes on Data Engineering and Communications Technologies*, vol 131. 2023. Springer, Singapore. pp. 21-34.

27. Смірнова Т.В., Гнатюк С.О., Бердибаєв Р.Ш., Сидоренко В.М., Жигаревич О.К., «Система корелювання подій та управління інцидентами кібербезпеки на об'єктах критичної інфраструктури». *Кібербезпека: освіта, наука, техніка*, №*3*(19), 2023, С. 176-196.

28. Смірнов О.А. Козлов Я.О., Смірнова Т.В. «Дослідження застосування SIEM-систем для забезпечення кібербезпеки та захисту інформації». *ІІ Міжнародна науково-практична Інтернет-конференція «Інновації та перспективні шляхи hозвитку інформаційних технологій (ІПШРІТ-2023)»* м.Черкаси 6 грудня 2023 року – Черкаси: ЧДТУ.– 2023. – С.251-252.

29. Козлов Я.О., Смірнова Т.В., Смірнов О.А. «Дослідження SIEM-систем для забезпечення кібербезпеки». *VII міжнародна науково-практична конференція "Інформаційна безпека та комп'ютерні технології" до 30-ти річчя кафедри кібербезпеки та програмного забезпечення,* м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 26.

30. Козлов Я.О., Козірова Н.Л., Смірнов О.А. «Дослідження структури та принципу роботи SIEM-системи». *VII міжнародна науково-практична конференція "Інформаційна безпека та комп'ютерні технології" до 30-ти річчя кафедри кібербезпеки та програмного забезпечення,* м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 59.

31. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А., Коваленко А.С. «Дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення комп'ютерних систем управління АЕС, важливих для безпеки». *Системи управління, навігації та зв'язку*, 2023, вип.

2(72), С. 170-178.

32. Smirnov, O., Neskorodieva, T., Fedorov, E., Rudakov, K., Neskorodieva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» *CEUR Workshop Proceedings,* Volume 3187, 2022,

33. Smirnov O.A., Al-Oraiqat A.M., Ulichev O.S., Meleshko Ye.V., Al-Rawashdeh H.S., Polishchuk L.I. «Modeling strategies for information influence dissemination in social networks». *Journal of Ambient Intelligence and Humanized Computing* Volume 13, Issue 5. Springer, Cham. 2022, pp. 2463-2477.

34. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». *Проблеми інформатизації та управління,* № 2(70). 2022. С. 28-37.

35. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Системи управління, навігації та зв'язку,* 2022, № 3(69). С. 93-98.

36. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Вісник Хмельницького національного університету. Серія: «Технічні науки»,* № 2 (307). С. 46-52. 2022.

37. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» *Системи управління, навігації та зв'язку*, 2022, № 1(67). С. 84-89.

38. Smirnov O., Kuznetsov A., Zhora V., Onikiychuk A., Pieshkova O. «Hiding Messages in Audio Files Using Direct Spread Spectrum». *11th IEEE*

International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2021, Cracow, Poland, 22-25 September 2021. P. 414-418

39. Smirnov O., Kuznetsov A., Lokotkova I., Kuznetsova T., Florov S., Lebid O. «Using Orthogonal Signals to Hide Information in Images». *4 IEEE International Conference on Advanced Information and Communication Technologies (AICT) – 2021*, Lviv, Ukraine, September 21-25, 2021. P. 255-260.

40. Smirnov O., Kuznetsov A., Girzheva O., Kiian A., Nakisko O., Kuznetsova T. «Advanced Code-Based Electronic Digital Signature Scheme». *2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020,* Kharkiv, 6 October 2020-9 October 2020, P. 358-362.

41. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova K. «Data hiding scheme based on spread sequence addressing». *CEUR Workshop Proceedings* Volume 2805, 2020, Pages *44-58.*

42. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». *International Journal of Computing*; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256.

43. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». *CEUR Workshop Proceedings*. Volume 2740, 2020, Pages 102-114.

44. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». *Journal of theoretical and applied information technology* Vol.98. No 21, 2020, P. 3334-3346.

45. Smirnov O., Kuznetsov A., Arischenko A., Chepurko I., Onikiychuk A., Kuznetsova T. «Pseudorandom sequences for spread spectrum image steganography». *CEUR Workshop Proceedings* Volume 2654, 2020, Pages 122-131.

46. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New

technique for data hiding in cover images using adaptively generated pseudorandom sequences». *CEUR Workshop Proceedings* Volume 2654, 2020, Pages 1-14.

47. Smirnov O., Lutsenko M., Kuznetsov A., Kiian A., Kuznetsova T., «Biometric cryptosystems: overview, state-of-the-art and perspective directions». *Lecture Notes in Networks and Systems*, vol 152. Springer, Cham. 2021, pp 66-84.

48. Smirnov O., Kuznetsov A., Onikiychuk A., Makushenko T., Anisimova O., Arischenko A. «Adaptive pseudo-random sequence generation for spread spectrum image steganography». *2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, Ukraine, Kyiv, May 14-18. 2020. P. 161-165.

49. Smirnov O., Kuznetsov A., Kiian A., Babenko V., Perevozova I.,Chepurko I. «New Approach to the Implementation of Post-Quantum Digital Signature Scheme». *2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT),* Ukraine, Kyiv, May 14-18. 2020. P. 166-171.

50. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». *2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT),* Ukraine, Kyiv, May 14-18. 2020. P. 172-177.

51. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.

52. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». *CEUR Workshop Proceedings* Volume 2616, 2020, Pages 125-136.