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 забезпечення безпеки критичних ресурсів АСУ ТП”

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

Керівник проекту
кандидат фізико-математичних наук, доцент
_____ Петренюк В.І.
«____» _____ 2025 р.
Рецензент _____
_____

м. Кропивницький

АНОТАЦІЯ

Коробка С.О. Дослідження та програмна реалізація системи забезпечення безпеки критичних ресурсів АСУ ТП. 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 забезпечення безпеки критичних ресурсів АСУ ТП.

Метою розробки є дослідження та програмна реалізація системи забезпечення безпеки критичних ресурсів АСУ ТП.

Об'єктом дослідження є процес забезпечення безпеки критичних ресурсів АСУ ТП.

Предметом дослідження є методи забезпечення безпеки критичних ресурсів АСУ ТП.

Методи дослідження базуються на методах захисту інформації у комп'ютерних мережах, методах математичної статистики, методах розробки програмного забезпечення.

Результат роботи – програмна реалізація системи забезпечення безпеки критичних ресурсів АСУ ТП.

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 Visual C++.

Ключові слова: комп'ютерна інженерія, критичні ресурси АСУ ТП

ABSTRACT

Korobka S.O. Research and software implementation of the system for ensuring the security of critical resources of the ACS TP. 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 that is intended for the system for ensuring the security of critical resources of the ACS TP.

The purpose of the development is the research and software implementation of the system for ensuring the security of critical resources of the ACS TP.

The object of the research is the process of ensuring the security of critical resources of the ACS TP.

The subject of the research is the methods for ensuring the security of critical resources of the ACS TP.

The research methods are based on methods of information protection in computer networks, methods of mathematical statistics, and methods of software development.

The result of the work is the software implementation of the system for ensuring the security of critical resources of the ACS TP.

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 was developed in Visual C++.

Keywords: computer engineering, critical resources of the ACS TP

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

ЕН	–	електронний нотаріус
ЕЦП	–	електронний цифровий підпис
СУБД	–	система управління базами даних
УЦ	–	удостовірюючий центр
CRL	–	список відкликаних сертифікатів
DVCS	–	Data Validation and Certification Server Protocols
http	–	HyperText Transfer Protocol – протокол передачі гіпертексту
HTTPS	–	розширення протоколу HTTP, підтримуюче шифрування
IMAP	–	протокол доступу до електроної пошти Інтернету
MAC	–	код автентифікації повідомлення
OCSP	–	Online Certificate Status Protocol
PKI	–	інфраструктура відкритих ключів
POP3	–	Post Office Protocol Version 3 – протокол поштового відділення
SMTP	–	простий протокол передачі пошти
SSL	–	Secure Sockets Layer – рівень захищених сокетів
SQL	–	Structured Query Language – мова структурованих запросів
TCP	–	протокол управління передачею
TLS	–	криптографічний протокол, захищаючий передачу даних
TSP	–	Time-Stamp Protocol
URL	–	єдиний показник ресурсів
XMPP	–	росширяємий протокол обміну повідомленями й інформацією про присутність

ВСТУП

Актуальність теми. У наші дні практично в будь-якому виробництві використовуються автоматизовані системи управління технологічними процесами (АСУ ТП). Однак автоматизація без виконання вимог інформаційної безпеки може бути критично небезпечним. Розглянемо, чому захист АСУ ТП сьогодні став особливо важливим, які погрози зараз найбільш реальні, і як захистити промислові інфраструктури від зловмисників. Автоматизована система управління технологічними процесами (АСУ ТП) – це ціла група технічних і програмних засобів, призначених для автоматизації процесів управління технологічним устаткуванням на промислових підприємствах. Сьогодні багато експертів одностайні в тому, що основна погроза – це втручання терористичних, екстремістських і вороже настроєних груп у управління автоматизованими системами критично важливих об'єктів, у тому числі й з метою виводу їх з ладу. Деякі експерти зараз прогнозують, що терористичні організації будуть купувати технічну інформацію компаній для здійснення атак. Тому державам так важливо вчасно убезпечити себе від подібних погроз. Галузі, для яких тема захисту АСУ ТП найбільш критична – ті, де можливий максимальний збиток і може постраждати найбільша кількість людей. У першу чергу, це енергетичні компанії й підприємства ПЕК – отут можливі як економічні наслідки, наприклад, порушення поставок нафти або газу, або перебої в електропостачанні населення, так і екологічні або гуманітарні катастрофи. Крім того, під погрозою перебуває транспорт. Ці галузі мають широку розгалужену мережу по всій країні, і безпека на подібних підприємствах – стратегічно важливе завдання для держави.

Мета й завдання дослідження. Метою роботи є дослідження та програмна реалізація системи забезпечення безпеки критичних ресурсів АСУ ТП.

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

– Огляд існуючих систем забезпечення безпеки критичних ресурсів АСУ ТП.

– Дослідження системи забезпечення безпеки критичних ресурсів АСУ ТП.

– Програмна реалізація системи забезпечення безпеки критичних ресурсів АСУ ТП.

Об'єктом дослідження є процес забезпечення безпеки критичних ресурсів АСУ ТП.

Предметом дослідження є методи забезпечення безпеки критичних ресурсів АСУ ТП.

Методи дослідження базуються на методах захисту інформації у комп'ютерних мережах, методах математичної статистики, методах розробки програмного забезпечення.

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

– Удосконалено метод забезпечення безпеки критичних ресурсів АСУ ТП.

– Розроблено вітчизняний продукт забезпечення безпеки критичних ресурсів АСУ ТП, який має більш широкі можливості, на відміну від існуючих аналогів.

Практична цінність отриманих результатів полягає в тому, що розроблені алгоритми дозволяють успішно вирішувати задачі забезпечення безпеки критичних ресурсів АСУ ТП.

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 забезпечення безпеки критичних ресурсів АСУ ТП, 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

Сьогодні підприємства усе серйозніше підходять до інформаційній безпеці свого бізнесу. Однак для захисту складних промислових процесів на підприємствах критичної важливості необхідні спеціалізовані засоби й підходи. Специфіка захисту АСУ ТП від погроз інформаційного характеру полягає в тому, що необдумане застосування мір і засобів захисту може приводити до зниження загальної надійності системи. Впроваджені засоби інформаційної безпеки не повинні створювати нових проблем нормальному функціонуванню АСУ ТП, а усувати існуючі. Тому виробництво змушене балансувати на тонкій грані між безпекою й автоматизацією.

1.2 Область застосування

Число випадків злому промислових систем стає усе більше. Якоюсь мірою це впливає й на ажіотаж навколо цієї теми в ЗМІ, а також зацікавленість підприємств у захисті свого виробництва. Адже, як говориться, ніхто не застрахований...

Не дуже давно в Німеччині була зроблена атака на сталеливарне підприємство. Хакерам удалося віддалено вивести з ладу доменну піч, що привело до поломки встаткування й простою виробництва. Доступ до печі хакери одержали, заразивши шкідливим програмним забезпеченням офісну мережу.

Крім того, можна згадати кібератаку на українських постачальників електроенергії, у результаті чого припинилася подача електроенергії на 80 підстанціях, без світла залишилися більше 200 тисяч чоловік. Паралельно атака була проведена й на call-центр енергокомпанії для відволікання уваги з

відключення встаткування. Після відключення підстанцій хакери змогли впровадитися в систему й приступити до видалення даних з жорстких дисків на робочих станціях і SCADA-серверах, а також змінити налаштування джерел безперебійного живлення. За рівнем атаки можна сміло судити про високу технічну підготовку зловмисників.

Якийсь час назад якийсь зловмисник у США через розважальну систему зміг підключитися до бортового комп'ютера літака й ненадовго змінити тягу одного із двигунів, у результаті чого літак якийсь час летів боком. За словами самого хакеру, протягом декількох років він здійснив біля двох десятків подібних зломів. Ще приклад – закордонний експерт зміг експериментальним шляхом довести можливість дистанційно зламати бортовий комп'ютер автомобіля за допомогою звичайного смартфону й управляти системами машини, включаючи кермо й педалі.

Таким чином, виходячи з вищеперерахованого, дослідження та програмна реалізація системи забезпечення безпеки критичних ресурсів АСУ ТП, 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

Забезпечення безпеки АСУ ТП – короткий огляд сімейства стандартів IEC 62443

Сьогодні питання забезпечення безпеки автоматизованих систем управління технологічним процесом (АСУ ТП) стають усе актуальніше. Якщо кілька років назад ця тема в основному піднімалася серед фахівців, то зараз вона стала цікава всім: власникам систем управління, фахівцям, що займаються їхньою експлуатацією, розробкою й впровадженням, зловмисникам і законодавцям.

Всі експерти в області ІБ погоджуються, що забезпечення безпеки АСУ ТП відрізняється від забезпечення безпеки корпоративних інформаційних систем. Навіть сам термін "інформаційна безпека", настільки звичний ІТ-Фахівцям, як правило, не використовується у відношенні АСУ ТП. У першу чергу це пов'язане з тим, що необхідно приділяти увагу не тільки й не стільки забезпеченню конфіденційності, скільки забезпеченню безперервності й цілісності самого технологічного процесу. Більше того, безпека технологічного процесу в загальному значенні – це насамперед безпека для життя й здоров'я людей і навколишнього середовища. В англомовних джерелах для визначення "комп'ютерної безпеки" у відношенні АСУ ТП використовується особливий термін – cybersecurity (кібербезпека). У наших же реаліях спостерігається явний пробіл не тільки в нормативній і методичній базі в області забезпечення безпеки АСУ ТП, але навіть у термінології.

Для успішної реалізації проектів по захисту АСУ ТП необхідно використовувати підхід, заснований на об'єднанні існуючих (і розроблювальних)

вимог регуляторів, з одного боку, і кращих світових практик – з іншої. Одним з основних наборів міжнародних методичних документів з забезпечення кібербезпеки АСУ ТП є сімейство стандартів IEC 62443 (раніше відоме як ISA 99). Про нього й піде мова далі.

Ризик-орієнтований підхід

Стандарти IEC 62443 пропонують сучасний ризик-орієнтований підхід: безпека розглядається як сукупність безперервних процесів, які необхідно підтримувати на всіх стадіях життєвого циклу системи. Стандарти IEC 62443 задають вимоги до проектування накладених систем управління кібербезпекою АСУ ТП і SCADA і до проектування АСУ ТП із уже закладеними й інтегрованими мірами безпеки.

Загальний підхід до процесів створення системи управління кібербезпекою АСУ ТП, аналізу й управління ризиками почасти схожий з аналогічним, заданим стандартом ISO 27001 для IT-систем. Основою для визначення вимог, пропонованих до проектованої системи, є аналіз ризиків. Наріжними каменями аналізу ризиків є ідентифікація, класифікація й оцінка. Начебто б все знакомо, але диявол криється в деталях – схожість із відомими для IT-Фахівців практиками полягає в тому, що треба зробити. А от те, як це треба робити, істотно відрізняється.

Вибір методики оцінки ризиків залишається на розсуд власника АСУ ТП і залежить від специфіки використовуваних систем. Втім, загальні рекомендації в стандарті описані. Ми у своїй роботі використовуємо методику аналізу ризиків, адаптовану під конкретний об'єкт захисту, що задовольняє вимогам кращих практик, з одного боку, і відповідному українському нормативному документам – з іншої.

Для більшості систем АСУ ТП найбільш важливої є так звана HSE-група наслідків, що приводять до збитку здоров'ю або безпеці людей і навколишнього середовища (Health, Safety and Environmental), а також уведені проектом нормативних документів "наслідку в соціальній, політичній, економічній,

військовій або іншій областях діяльності" (для простоти будемо називати їх ПЕВ). На початку робіт з створення системи управління кібербезпекою АСУ ТП проводиться високорівнева оцінка ризиків, покликана визначити основні фінансові, ПЕВ- і HSE-наслідки у випадку порушення доступності, цілісності або конфіденційності. Високорівнева оцінка дає подання про загальну картину ризиків і критичних систем і є базисом для переходу до більше детального вивчення об'єкта, що захищається.

Наступним кроком при створенні системи управління кібербезпекою є аналіз об'єкта захисту, ідентифікація й класифікація активів АСУ ТП, що підлягають захисту. Незважаючи на те що процес вивчення, описи й класифікації елементів об'єкта захисту заслуговує окремої статті, спробуємо коротенько освітити підхід, описуваний в IEC 62443.

Стадії аналізу й моделювання об'єкта захисту

Сімейство стандартів IEC 62443 пропонує кілька стадій аналізу й моделювання об'єкта захисту. Першою стадією є створення референсної (reference) моделі (або моделей, залежно від складності об'єкта захисту, границь і рамок роботи) об'єкта захисту, що описує "великими мазками" розподіл основних видів діяльності, ТП, АСУ й інших активів на 5 логічних рівнів.

На основі референсної моделі на наступній стадії будується модель активів (asset model), що описує ієрархічну карту основних об'єктів і активів, взаємодія з мережами, територіальними площадками, ключовими підрозділами, що беруть участь у ТП, системами контролю й іншим технологічним устаткуванням. Модель активів будується для того, щоб забезпечити розуміння ієрархічної структури й процесних зв'язків у цілому або окремо виділеного для аналізу об'єкта захисту й дати можливість наочно побачити й визначити критичні процеси й активи.

На наступній стадії будується референсна модель архітектури (reference architecture model). Вона дуже схожа на класичну докладну схему мережі 2-го рівні й відбиває всі основні елементи АСУ ТП, телекомунікаційне встаткування,

лінії зв'язку й т.п. Коректна побудова референсної моделі архітектури надто важливо, тому що на її основі з урахуванням результатів високорівневої оцінки ризиків виконується сегментування об'єкта захисту. При сегментуванні будується так звана модель зонування (zone and conduit model), що розділяє об'єкт захисту (одну або трохи АСУ ТП, розподілену мережу АСУ ТП, організацію в цілому або територіальний об'єкт) на ряд зон. Зони поєднуються за загальними показниками ризику, функціональним і / або технічним характеристикам, логічним або фізичним границям, мережам передачі даних і т.д. І знову IEC 62443 залишає "простір для творчості", дозволяючи адаптувати модель зонування залежно від цілей і завдань побудови захисту й ураховувати специфіку об'єкта захисту.

Для кожної виділеної зони проводиться ідентифікація й класифікація активів, аналіз уразливостей і погроз, моделювання порушників і детальна оцінка ризиків. На основі інформації про поточний стан системи, застосовуваних методах і мірах безпеки, функціональних особливостях технічних засобів і т.д. визначається поточний рівень безпеки для кожної зони. Поняття "рівень безпеки" (security level) також уводиться стандартом IEC 62443 і описує реалізацію вимог до мір безпеки по семи основних напрямках: ідентифікація й автентифікація, контроль використання АСУ, цілісність системи, конфіденційність інформації, управління інформаційними потоками, управління подіями, доступність ресурсів. Кожний напрямок містить ряд вимог, комбінації яких визначають чотири рівні безпеки.

Результати оцінки ризиків і аналізу можливих порушників визначають цільовий рівень безпеки зони. Твердих вимог на вибір цільового рівня стандарт не пред'являє, тобто є широкі можливості для адаптації під будь-який об'єкт захисту залежно від виявлених погроз і ризиків. Можливе компенсування одного напрямку (у випадках технічної неможливості реалізації мер високого рівня) підвищенням цільового рівня по іншому напрямку. За умови, зрозуміло, що така рокіровка закриє актуальні погрози. Також стандарт недвозначно регламентує необхідність при проектуванні визначити міри, що перевищують цільовий рівень захищеності. Це пов'язане з тим, що будь-яка міра захисту із часом втрачає свою

ефективність (поява нових погроз і методів їхньої реалізації, виявлення нових уразливостей, старіння технологій захисту й т.п.). Ступінь "перевиконання плану" з забезпечення захисту залежить від прийнятою організацією періодичності проведення аналізу ризиків і планованого строку перегляду експлуатаційних характеристик системи. У такий спосіб забезпечується ефективність захисних мір на всьому життєвому циклі системи.

Правильно побудовані й проаналізовані моделі об'єкта захисту, адекватно й докладно задані й описані цільові рівні безпеки вкупі з вимогами вітчизняних нормативних документів лягають в основу ТЗ на проектовану систему забезпечення кібербезпеки АСУ ТП. І її ефективність прямо залежить від старанності й подробиці проведеного обстеження й аналізу інформації про об'єкт захисту, від того, чи всі взаємозв'язку (як технічні, так і логічні) між процесами, устаткуванням і персоналом виявлені й проаналізовані, чи всі критичні активи ідентифіковані, чи всі основні ризики розглянуті.

Крім того, стандарт IEC 62443 вимагає впровадження добре відомих фахівцям, знайомим із сімейством ISO 27000, процесів: управління інцидентами, управління змінами, управління конфігураціями, планування відновлення діяльності й безперервності процесу, підвищення поінформованості й т.д. Зрозуміло, з урахуванням специфіки АСУ ТП. Ну й, зрозуміло, IEC 62443, як і всі стандарти й кращі практики в області ІБ, має на увазі підтримку безперервного життєвого циклу процесів безпеки. Такий життєвий цикл, підтримуваний на всіх стадіях існування об'єкта захисту, містить у собі постійний перегляд уже оброблених ризиків, ідентифікацію й аналіз нових, аналіз ефективності вжитих компенсаційних заходів і простору, що змінюється, ризиків і погроз і т.д.

З обліком всі інтересу, що підвищується, до АСУ ТП, у тому числі й з боку зловмисників, часто розповсюджені в області експлуатації АСУ ТП принципи "незмінності й вірності традиціям" серйознішають ризиком. Компенсаційні міри у вигляді профілю безпеки для Windows NT і антивірусу на сервері SCADA настав час переглянути, і сімейство стандартів IEC 62443 дає відмінний методичний посібник для цього.

Червоною лінією проходить головна думка правильного підходу до забезпечення безпеки АСУ ТП, не захист конфіденційних даних, а забезпечення безперервності виробничого процесу. Мало кому цікавий дамп показань із датчиків температури енергоблоків, а от вивести ці датчики з ладу й зупинити виробництво, це більше ласа мета потенційного конкурента.

Напрямків до побудови політики безпеки може бути багато. Я віддаю перевагу наступним акцентам.

Першою метою забезпечення інформаційної безпеки АСУ ТП є максимальний переклад всіх ризиків нападу з віддаленої програмно-мережної площини, на план реальної фізичної присутності нападаючого. Щоб для потенційного порушника, не було різниці розбити молотком цей горезвісний датчик, або підійти до нього з ноутбуком і перепрограмувати його.

Другою метою забезпечення безпеки АСУ ТП плавно випливає з першої, це банальний захист від дурня.

Далі приведу типові проблеми, з якими зіштовхувався у своїй практиці при аналізі захищеності промислових мереж.

1. Високі ризики вірусних заражень. Коли після аналізу однієї АСУ ТП-шної сітки розкрила така банальна ситуація, як відсутність антивірусного захисту. Відповіддю на питання «Чому?» було мова: «А навіщо? Тільки комп'ютери навантажує, все гальмує». Цей милостивий стан тривав до появи в мережі древнього мережного p2p черв'яку, що банально поклав все що міг своїм скаженим трафіком, і виробництво перейшло на ручний режим управління (благо такий режим був). При цьому щогодини простою міг вилитися у відчутні грошові втрати.

2. Відсутність блокування АРМ-ів на фізичному рівні. Що таке АРМ, на типовому такому середнім Українському виробництві? Це банальний такий персональний комп'ютер, на якому крутиться Windows і поверх робочого стола розтягнута «картинка» SCADA. Комп'ютер при цьому беззахисно стоїть на столі оператора. На які тільки хитрування не йдуть оператори, щоб не нудьгувати в

нічну зміну. Спроби засунути завірусовані флешки з іграшками в АРМ-и, випробування різних комбінацій клавіш для згортання інтерфейсу SCADA. Оператори АРМ-ів це вже далеко не дідки, а усе більше й більше «просунута» молодь. Рятує тільки залізний ящик із замком. Чому саме повне блокування за допомогою залізного ящика? У пам'яті свіжий приклад, коли потикавшись у залиті порти USB, спритний оператор, просто відкрутив винтики системного блоку й підключився до внутрішніх інтерфейсів материнської плати.

3. Недостатній поділ між сегментами виробничих мереж. Дуже часто бачив, як в одній мережі крутиться й офісні завдання й технологічні. Отут навіть коментувати нема чого.

4. Множинні крапки входу в мережу АСУ ТП на програмно-мережному рівні. Це проблема випливає із двох попередніх і приводить як правило до вірусних заражень, а в особливо негарних випадку й до легкої реалізації злого наміру. Занадто багато точок підключення переносних пристроїв, занадто багато точок дотику між мережами. В ідеалі крапка входу в мережу АСУ ТП, повинна бути одна. Виділена повністю контрольована машина.

5. Відсутність парольної політики. У звіті говорилося про стандартні інженерні паролі. Це ще квіточки. Паролі найчастіше просто не відносять – для зручності. Ні на інтерфейси контролерів і схеми SCADA, ні на адміністративні облікові записи АРМ-ів і серверів.

6. Відновлення програмного забезпечення мережі АСУ ТП. Болюче питання. Скільки разів у вас бувало, що падав сервер у результаті криво, що встало відновлення? Скільки часу йшло на усунення косяка? І якщо у випадку якого-нібуть інтернет-магазина, відновлення сервера після такого збою, означає сиюхвилине відновлення продажів, те аварійна зупинка центрального сервера АСУ ТП на півгодини, може привести до повного перезапуску виробничої лінійки, що може продовжаться не одну годину (новий розігрів казанів, супровідні підготовчі роботи й т.д). Це будуть відчутні грошові втрати. Це-Же нічим не буде вирізняться від самої справжньої диверсії. У результаті, ні про яке

автоматичне відновлення мови йти не може. Всі відновлення прив'язуються тільки до планових зупинок виробництва на ремонт. При цьому виробляється ручний аналіз необхідних патчів і поширення їх по мережі АСУ ТП через єдину крапку входу. Це по правильному, а по неправильному, «Працює й не торкаємо, навіщо ще щось обновляти зайві проблеми наживати!» До речі кажучи, у звіті великий акцент зроблений на віддалених атаках на промислові системи, переповнення буфера й тд. Але це ж квіточки в порівнянні з дірами в системах windows, на яких крутяться всі ці компоненти. Я як те на одному АРМ-і нарахував десяток критичних уразливість що дозволяють захопити повний контроль над машиною.

7. Інженерно-технічний захист і охорона. Це вже трохи виходить із теми інформаційної безпеки, але тому що основна ідея це зниження всіх ризиків нападу по віддаленій програмно-мережній площині, і їхній вивід на план реальної фізичної присутності, те трохи недорогих IP-камер на найбільш критичних вузлах АСУ ТП досить дисциплінує від поспішних рішень.

Тепер небагато про іншу сторону медалі – інсайд і закладки.

Завжди існують ризики наявності недокументованих закладок у керуючих програмах промислових контролерів, ледве менше, можливість інсайда й цілеспрямованого псування керуючих програм обслуговуючим персоналом.

Ризики, що складно закриваються через великі витрати на реалізацію захисти. Армію наглядачів і аудиторів годувати собі мало хто дозволить.

Однак досить корисно збирати й аналізувати статистику роботи вузлів АСУ ТП на предмет збоїв.

Може так трапиться, що вилізуть цікаві закономірності. Які потім розкриють цікавими наслідками, а саме бажанням заробити небагато грошей на «підтримці й відновленні» несумлінними вендорами.

Однією із проблем сучасних АСУ ТП є реалізація масштабних інтеграційних проектів по побудові MES і по інтеграції з бізнес-системами, такими як ERP.

ICS / SCADA / PLC Google / Shodanhq Cheat Sheet

Найчастіше заяви про те, що АСУ ТП доступні з мережі Інтернет, сприймаються скептично. Недавно був опублікований інструмент, що дозволяє самостійно оцінити масштаб погрози. Зверніть увагу, що пристрої й системи, представлені в даному списку, є системами Enterprise-рівня й навряд чи будуть використовуватися для управління холодильниками й мікрохвильовками.

Уразлива система може управляти критично важливим об'єктом і неакуратний обіг з нею може привести до серйозних наслідків. Якщо раптом ви виявили АСУ ТП, доступну в Інтернет, зв'яжіться з її власником або з Computer Emergency Response Team, які допоможуть усунути проблему.

PLCScan

Ця утиліта з відкритим кодом дозволяє виявляти в мережі пристрою, взаємодіючі по протоколах S7comm або Modbus.

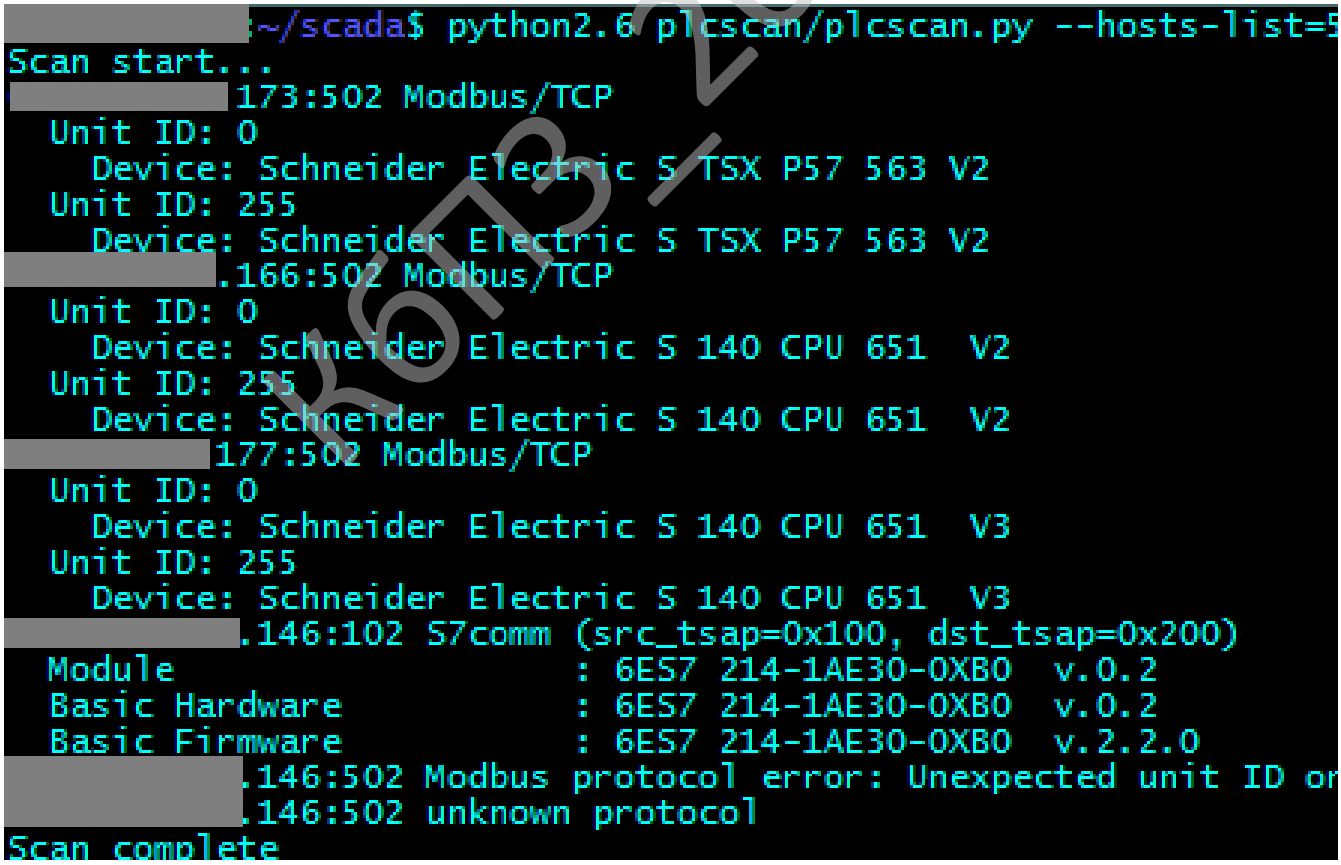

Рисунок 2.1 – Демонстрація використання:

При виявленні пристрою PLCScan намагається одержати інформацію про виробника, тип пристрою, установлених модулях і т.п.

WinCC Harvester

Модуль Metasploit WinCC Harvester може використовуватися після одержання доступу до SCADA WinCC для збору додаткової інформації про проект, користувачів і підключених до системи контролерах.

Siemens SIMATIC WinCC 7.X Security Hardening Guide

Контрольний список може використовуватися для конфігурації WinCC відповідно до вимог безпеки, а також для проведення оцінки захищеності систем у ході аудитів.

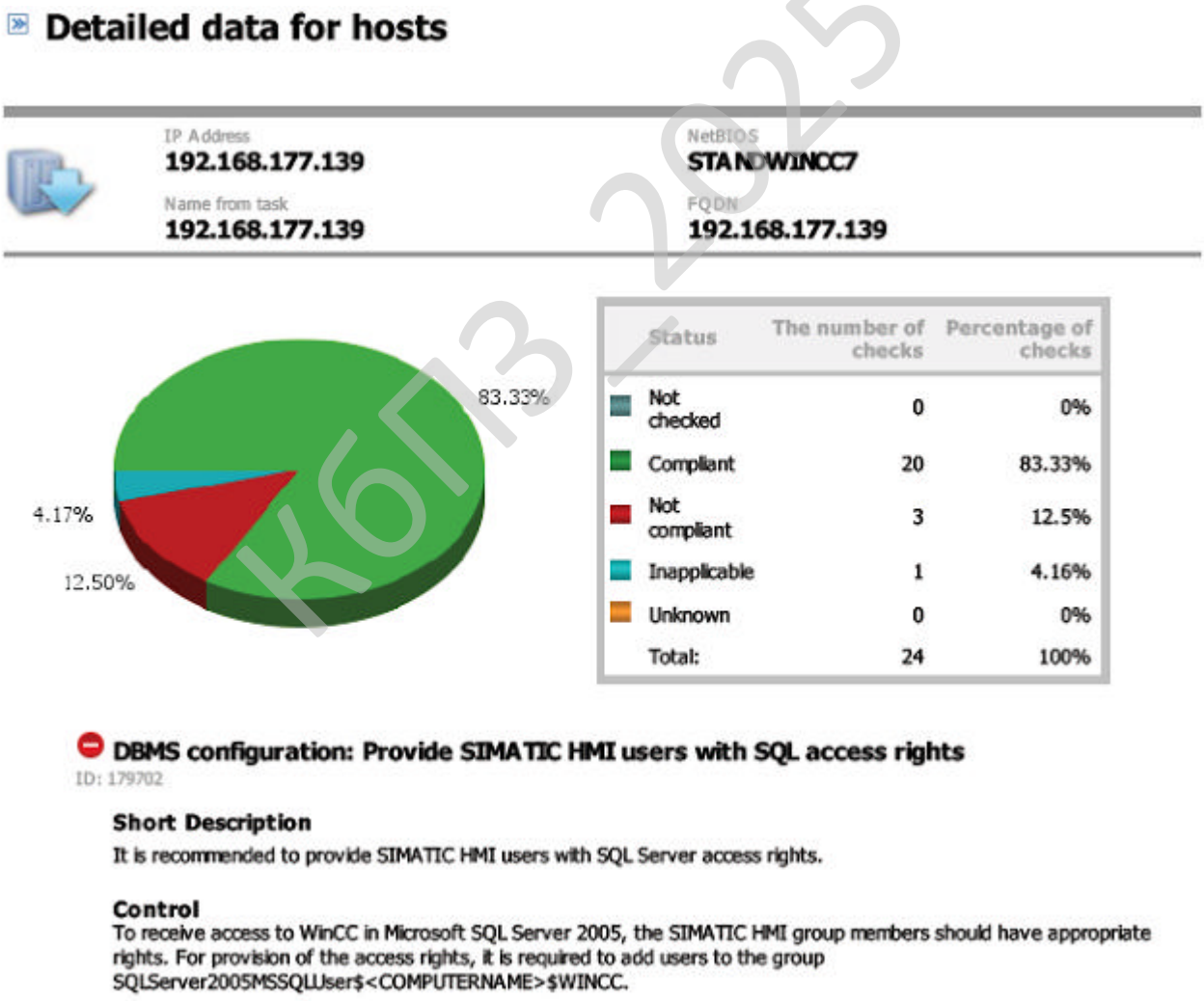

Рисунок 2.2 – Результат роботи MaxPatrol

При оцінці великої кількості систем процедура може бути автоматизована, як це зроблено, наприклад, у системі MaxPatrol.

Siemens WinCC / S7 Under The X-ray

На минулому 16-17 січня в Майами міжнародному симпозіумі по безпеці SCADA-систем експерти Positive Technologies представили доповідь за результатами дослідження безпеки лінійки продуктів Siemens WinCC / S7. Мова йшла зокрема про SIMATIC WinCC / WinCC Flexible / TIA Portal і лінійку S7 PLC; від мережного стека до додатка, від огляду архітектури системи до зворотної розробки прошивання.

S7 password offline bruteforce tool

У ході виступу на симпозіумі експерти Positive Technologies представили також утиліту, що може бути використана для тестування стійкості використовуваних паролів S7 у ході аудитів і тестів на проникнення.

Огляд уразливостей АСУ ТП

Об'єктом дослідження стали уразливості, виявлені з 2020 р. по 1 жовтня 2025 р. Коротко за результатами аналізу можна відзначити кілька фактів:

– За кілька місяців 2025 року було знайдено більше уразливостей АСУ ТП чим за весь попередній рік: відбувається стрімке зростання їхнього числа.

– Проблеми, як і завжди, виявляються в самих популярних продуктах, і близько 65% уразливостей є серйозними або критичними.

– США і Європа лідирують по числу доступних з інтернету систем АСУ ТП, при цьому 40% всіх доступних ззовні SCADA-систем уразливі й можуть бути зламані.

– Більшість проблем безпеки доступних з Інтернету систем АСУ ТП пов'язані з помилками конфігурації (це, наприклад, стандартні паролі) і відсутністю відновлень.

Затребуваність систем АСУ ТП в Україні

Приблизно представити частки різних виробників на ринку систем АСУ ТП можна, оцінивши затребуваність фахівців, що володіють досвідом

роботи з тією або іншою системою, протоколом, технологією або програмою. Як основу для аналізу була взята статистика бази вакансій hh.ua. Найбільш затребуваними виявилися фахівці, що мають досвід роботи з рішеннями компанії Siemens. Чотири із шести найпоширеніших продуктів відносяться до сімейства Siemens SIMATIC:

– Step 7 – розробка систем автоматизації на основі PLC (близько 22,05%);

– WinCC і WinCC Flexible – створення людино-машинного інтерфейсу (18,11% і 3,94% відповідно);

– PCS 7 – побудова комплексних систем автоматизації (7,87%).

У п'ятірку лідерів також входять InTouch HMI компанії Wonderware (12,6%) і пакет ПЗ Genesis від Iconics (5,51%).

Якщо розглядати технології передачі даних, то найбільш популярними з них є Modbus (RTU і TCP / IP) і Profibus / Profinet, що займають приблизно по 33%. Далі йде OPC (25%).

Серед всіх використовуваних з АСУ ТП операційних систем з більшим відривом лідирує Microsoft Windows, досвід роботи з якої потрібно в більшості оголошень у цій сфері. Знання QNX і FreeRTOS зазначені лише в незначній кількості вакансій.

У сегменті програмувальних логічних контролерів (ПЛК, PLC) найчастіше шукають фахівців з рішень Siemens (приблизно 31%). Далі випливають продукти Schneider Electric (11%), ABB (9%), Allen-Bradley (7%) і Emerson (5%).

Аналіз уразливостей

Уразливості часто публікуються без узгодження з розроблювачами, тому для нашого дослідження ми використовували дані з різних джерел, таких як бази знань уразливостей (vulnerability database) і повідомлення виробників, збірники експлойтів (exploit pack), доповіді спеціалізованих заходів, публікації на тематичних сайтах і в блогах.

Цікаво відзначити, що в період з 2020 року до початку 2021 року було виявлено лише 9 уразливостей у системах АСУ ТП, а вже після появи хробака

Stuxnet і галасу, що пішло за цим, за 2021 рік було знайдено вже 64 уразливості. За перші вісім місяців 2025 року стало відомо про 98 новий уразливостей: це більше, ніж за всі попередні роки.

Найбільша кількість уразливостей (42) за звітний період було виявлено в компонентах АСУ ТП виробництва компанії Siemens. На другому місці – системи Broadwin / Advantech (22). На третьому – Schneider Electric (18). Подібна картина у випадку з АСУ ТП, як і взагалі в інформаційних технологіях, пояснюється тим, що найбільша кількість уразливостей виявляється в найпоширеніших рішеннях. Крім того, ряд виробників лише недавно почали активно займатися пошуком і усуненням уразливостей у своїх продуктах (прикладом може служити Siemens ProductCERT).

Уразливості по типі програмно-апаратних компонентів АСУ ТП

Найбільший інтерес для зловмисників представляють такі складові АСУ ТП, як SCADA і людино-машинний інтерфейс (HMI), у яких виявлено 87 і 49 уразливостей відповідно. У програмувальних логічних контролерах різних виробників за звітний період було знайдено 20 уразливостей.

Типи уразливостей

Майже третина уразливостей (36%) пов'язана з переповненням буфера (Buffer Overflow). Дана проблема безпеки дозволяє зловмисникові не тільки викликати аварійне завершення або «зависання» програми, що веде до відмови в обслуговуванні, але й виконати довільний код на цільовій системі. Якщо ж скласти всі типи уразливостей, експлуатація яких дозволяє хакеру запустити виконання коду (наприклад, переповнення буфера, віддалене виконання коду), то вийде частка близько 40% всіх уразливостей. Варто відзначити й велика кількість проблем з автентифікацією і управлінням ключами (Authentication / Key Management) – майже 23%.

Частка усунутих уразливостей АСУ ТП

Більшість недоліків безпеки (81%) були оперативно ліквідовані виробниками – ще до того, як відомості про їх ставали широко відомі, або

протягом 30 днів після нескоординованого розголошення інформації. Однак приблизно кожна п'ята уразливість «закривалася» із серйозною затримкою, а в деяких випадках так і не була усунута.

Наочне подання про те, наскільки серйозно відносяться до проблем інформаційної безпеки різні виробники АСУ ТП, дає частка «закритих» уразливостей. Наприклад, Siemens усунув і випустив відновлення для 98% уразливостей, тоді як Schneider Electric ліквідувала тільки ледве більше половини (56%) виявлених проблем.

Доступність відомостей або ПЗ для проведення атаки

Наявність у відкритому доступі готового засобу для експлуатації уразливості або інформації про неї значно підвищує ймовірність успішної атаки. На даний момент для 35% всіх представлених в АСУ ТП уразливостей існують експлойти, які поширюються у вигляді окремих утиліт, входять до складу пакетів ПЗ для пен-тестів або описані в повідомленнях про уразливість. Аналогічний показник для інших IT-систем у рази менше.

Як правило, кількість опублікованих уразливостей корелює з кількістю опублікованих експлойтів. У період з початку 2021 року по вересень 2025 року було опубліковано 50 експлойтів – у шість разів більше, ніж за шість років з 2020-го по 2021 рік.

Відносно невелика кількість експлойтів, що з'явилися в 2025 році, пояснюється двома факторами:

– упорядкуванням взаємин між виробниками АСУ ТП і дослідниками, політика відповідального розголошення;

– традиційною затримкою між публікацією уразливості й виходом експлойта (його розробка вимагає додаткових витрат).

Ступінь ризику виявлених уразливостей

Майже 65% всіх уразливостей відносяться до високого (значення CVSS v. 2 Base Score > 6,5) або критичного ступеня ризику (доступний експлойт).

Втім, відсутність відомого способу реалізації атаки знижує ймовірність нападу, але не виключає його повністю, оскільки кібератаки на промислові об'єкти проводяться із залученням досвідчених фахівців високого рівня, яким найчастіше попросту не потрібні «експлойт-паки» та інші популярні інструменти.

Неусунуті уразливості АСУ ТП

Уразливості, для яких уже є експлойт, але ще не випущене виправлення, становлять найбільшу небезпеку, тому що для проникнення в систему зловмисникові не потрібні глибокі знання й тривала підготовка. Будь-який школяр, що вирішив похуліганити, може стати причиною величезного збитку. Найгірша ситуація тут складається для продуктів АСУ ТП компанії Schneider Electric: виявлено 6 відкритих уразливостей. На другому місці компанія General Electric (три уразливості), третє місце поділили Advantech / Broadwin і Rockwell Automation – у них по одній відкритій уразливості.

Поширеність систем АСУ ТП в Інтернеті

Щоб зрозуміти, якою мірою всі ці уразливості можуть бути використані зловмисником, було проведене дослідження мережі Інтернет на предмет наявності уразливих систем АСУ ТП. Пошук і перевірка версій систем здійснювалася методами пасивного аналізу з використанням пошукових машин (Google, Yahoo, Bing) і спеціалізованих баз знань, таких як ShodanHQ, Every Routable IP Project. Отримана інформація аналізувалася з погляду наявності уразливостей, пов'язаних з управлінням конфігурацією й установкою відновлень.

Майже третина систем АСУ ТП, до елементів яких є доступ з мережі Інтернет, розташовані в США (31,3%). Друге місце з більшим відривом займає Італія (6,8%), замикає трійку Південна Корея (6,2%). Росія розташувалася на 12 позиції з 2,3%, а в КНР перебувають тільки 1,1% всіх видимих із глобальної мережі систем АСУ ТП.

Результати очікувані, оскільки кількість доступних систем прямо залежить від ступеня автоматизації інфраструктури.

Типи систем АСУ ТП

Найчастіше в глобальній мережі присутні різні компоненти SCADA-систем (включаючи HMI). На їхню частку доводиться 70% всіх виявлених об'єктів. Ще 27% доступних компонентів АСУ ТП – це програмувальні логічні контролери. В 3% випадків були виявлені різні мережні пристрої, використовувані в мережах АСУ ТП (Hardware).

Типи уразливостей

Найпоширеніші недоліки безпеки (виявлені в 36% випадків) пов'язані з помилками конфігурації. Сюди відносяться й некоректна парольна політика (наприклад, використання стандартних інженерних паролів), доступ до критичної інформації, помилкове розмежування повноважень. Чверть уразливостей пов'язана з відсутністю необхідних відновлень безпеки.

Найбільше уразливих систем АСУ ТП, які «видні» з Інтернету, – у Швейцарії (100%). Далі йде Чехія (86%), на третім місці Швеція (67%). В Україні уразлива рівно половина доступних ззовні систем АСУ ТП.

Найменше піклуються про безпеку АСУ ТП у Європі: у цьому регіоні уразливі 54% систем промислової автоматизації. На другому місці Північна Америка (39%), потім Азія (32%), де істотну роль грають небезпечні об'єкти Тайваню й Південної Кореї.

2.2 Обґрунтування вибору засобів для побудови системи та мови програмування

Для реалізації програми мною була використана мова програмування Visual C++. У зв'язку з тим, що сьогодні рівень складності програмного забезпечення дуже високий, розробка додатків Windows з використанням тільки якої-небудь мови програмування значно утрудняється. Програміст повинен затратити масу часу на рішення стандартних завдань по створенню

багатовіконного інтерфейсу. Реалізація технології зв'язування й вбудовування об'єктів – OLE – зажадає від програміста ще більш складної роботи. Щоб полегшити роботу програміста практично всі сучасні компілятори з мови C++ містять спеціальні бібліотеки класів. Такі бібліотеки містять у собі практично весь програмний інтерфейс Windows і дозволяють користуватися при програмуванні засобами більш високого рівня, чим звичайні виклики функцій. За рахунок цього значно спрощується розробка додатків, що мають складний інтерфейс користувача, полегшується підтримка технології OLE і взаємодія з базами даних. Сучасні інтегровані засоби розробки додатків Windows дозволяють автоматизувати процес створення додатка. Для цього використовуються генератори додатків. Програміст відповідає на питання генератора додатків і визначає властивості додатка – чи підтримує воно багатовіконний режим, технологію OLE, тривимірні органи управління, довідкову систему. Генератор додатків, створить додаток, що відповідає вимогам, і надасть вихідні тексти. Користуючись їм як шаблоном, програміст зможе швидко розробляти свої додатки. Подібні засоби автоматизованого створення додатків включені в компілятор Microsoft Visual C++ і називаються MFC AppWizard. Заповнивши кілька діалогових панелей, можна вказати характеристики додатка й одержати його тексти, постачені великими коментарями. MFC AppWizard дозволяє створювати одновіконні й багатовіконні додатки, а також додатки, що не мають головного вікна, – замість нього використовується діалогова панель. Можна також включити підтримку технології OLE, баз даних, довідкової системи. Звичайно, MFC AppWizard не всесильний. Прикладну частину додатка програмістові прийдеться розробляти самостійно. Вихідний текст додатка, створений MFC AppWizard, стане тільки основою, до якої потрібно підключити інше. Але працюючий шаблон додатка – це вже половина всієї роботи. Вихідні тексти додатків, автоматично отриманих від MFC AppWizard, можуть становити сотні рядків тексту. Набір його вручну був би дуже стомлюючий. Потрібно

відзначити, що MFC AppWizard створює тексти додатків тільки з використанням бібліотеки класів MFC (Microsoft Foundation Class library). Тому тільки вивчивши мову C++ і бібліотеку MFC, можна користуватися засобами автоматизованої розробки й створювати свої додатки в найкоротший термін. Як уже згадувався, MFC – це базовий набір (бібліотека) класів, написаних мовою C++ і призначених для спрощення й прискорення процесу програмування для Windows. Бібліотека містить багаторівневу ієрархію класів, що нараховує близько 200 членів. Вони дають можливість створювати Windows-додатки на базі об'єктно-орієнтованого підходу. З погляду програміста, MFC являє собою каркас, на основі якого можна писати програми для Windows. Бібліотека MFC розроблялася для спрощення завдань, що стоять перед програмістом. Як відомо, традиційний метод програмування під Windows вимагає написання досить довгих і складних програм, що мають ряд специфічних особливостей. Зокрема, для створення тільки каркаса програми таким методом знадобиться близько 75 рядків коду. У міру ж збільшення складності програми її код може досягати воістину неймовірних розмірів. Однак та ж сама програма, написана з використанням MFC, буде приблизно в три рази менше, оскільки більшість приватних деталей приховано від програміста.

Одною з основних переваг роботи з MFC є можливість багаторазового використання того самого коду. В зв'язку з тим, що бібліотека містить багато елементів, загальних для всіх Windows-додатків, немає необхідності щораз писати їх заново. Замість цього їх можна просто успадковувати (говорячи мовою об'єктно-орієнтованного програмування). Крім того, інтерфейс, забезпечуваний бібліотекою, практично незалежний від конкретних деталей, його що реалізують. Тому програми, написані на основі MFC, можуть бути легко адаптовані до нових версій Windows (на відміну від більшості програм, написаних звичайними методами). Ще однією істотною перевагою MFC є спрощення взаємодії із прикладним програмним інтерфейсом (API) Windows. Будь-який додаток

взаємодіє з Windows через API, що містить кілька сотень функцій. Значний розмір API утрудняє спроби зрозуміти й вивчити його цілком. Найчастіше навіть складно простежити, як окремі частини API зв'язані один з одним! Але оскільки бібліотека MFC поєднує (шляхом інкапсуляції) функції API у логічно організовану безліч класів, інтерфейсом стає значно легше управляти.

Оскільки MFC являє собою набір класів, написаних мовою C++, тому програми, написані з використанням MFC, повинна бути в той же час програмами на C++. Для цього необхідно володіти відповідними знаннями. Для початку необхідно вміти створювати власні класи, розуміти принципи спадкування й уміти перевизначати віртуальні функції. Хоча програми, що використовують бібліотеку MFC, звичайно не містять занадто специфічних елементів з арсеналу C++, для їхнього написання проте потрібні солідні знання в даній області.

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 забезпечення безпеки критичних ресурсів АСУ ТП.

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 АСУ ТП найбільш актуальні в розвинені з погляду промислової автоматизації галузях – це енергетика, нафтогазова галузь, транспорт, металургія, машинобудування. Безпека всієї промислової мережі й АСУ ТП забезпечується застосуванням комплексного послідовного підходу, що враховує специфіку й особливості промислових систем, і заснованого на вимогах і рекомендаціях як міжнародних стандартів, так і українських нормативних документів з забезпечення інформаційної безпеки промислових систем.

Комплексний підхід означає також проведення регулярного аудита стану захищеності АСУ ТП на основі інтерв'ювання фахівців підприємства, аналізу документації, структури й конфігурації систем, а також проведення інструментального аналізу захищеності з метою пошуку уразливостей. На основі отриманих за підсумками аудита даних виробляється аналіз ризиків, у результаті якого визначаються погрози, що представляють небезпеку функціонуванню об'єкта.

Класифікація рішень для інформаційної безпеки АСУ ТП

Приступаючи до побудови архітектури рішення, у першу чергу, варто підібрати вірний тип базового продукту. Умовно всі рішення ІБ АСУ ТП можна розділити на дві категорії:

– Системи моніторингу активності й виявлення погроз. Вони забезпечують тільки моніторинг, нічого не блокують, але стежать за погрозами й проблемами, виявляють їх і повідомляють служби безпеки.

Системи моніторингу активності також підрозділяються по класах, серед них:

– система виявлення комп'ютерних атак і мережних аномалій;

– система моніторингу подій інформаційної безпеки й бездротових мереж;

– система пасивного аналізу уразливостей;

– система аналізу конфігурацій устаткування, правил доступу мережного встаткування;

– а також система контролю цілісності даних і ПЗ.

Наприклад, перші з них, системи виявлення комп'ютерних атак і мережних аномалій, аналізують мережний трафік і виділяють із нього інформацію про мережні потоки (flow), аналіз якої більше ефективний для виявлення погроз у порівнянні із сигнатурними методами й дозволяє виявити в тому числі й атаки на невідомі (zero day) уразливості й вчасно реагувати на підозрілі інциденти.

– Системи запобігання погроз (або управління доступом).

Ще одна класифікація систем інформаційної безпеки АСУ ТП – це розподіл їх на традиційні й спеціалізовані. Класичні системи ІБ можуть використовуватися на промислових підприємствах для побудови архітектури, управління інформаційними потоками. Друга група рішень – спеціалізовані, підходять для компаній важкої промисловості. Це металургія, енергетика, нафтогаз, де більше агресивне середовище (температура, магнітні випромінювання, пил). Якщо системи безпеки перебувають безпосередньо на промислових об'єктах, отут повинні застосовуватися додаткові умови, ураховуватися специфічні вимоги середовища, застосовуватися спеціальний монтаж промислового встаткування, стійке до агресивних середовищ виконання й т.д. Грубо говорячи, спеціалізовані системи повинні бути «розумними», повинні розбиратися в промисловому трафіку, ураховувати саме програмне забезпечення, трафік промислових систем. Однак це не виходить, що традиційні системи безпеки не застосовуються на промислових підприємствах.

На жаль, сьогодні основна проблема безпеки АСУ ТП – це відсутність уваги до її забезпечення. Через те, що технологічні мережі найчастіше досить

статичні, не прийняте що-небудь міняти, устаткування застаріває, використовуються старі версії програмних продуктів і операційних систем з безліччю уразливостей. Відсутність увага до ІБ проявляється й у безконтрольному використанні периферійних пристроїв, флеш-накопичувачів, відсутності політик захисту АСУ ТП і відповідальних осіб.

Також усе реальніше стає ймовірність кібертерроризмау У прогнозі МНС про надзвичайну обстановку на території України відзначається, що в цей час рівень інформаційної безпеки не відповідає рівню погроз у даній сфері, і в 2018 році можливе підвищення хакерських атак з метою створення умов для виникнення техногенних надзвичайних ситуацій. Тому в той час, поки ринок захисту АСУ ТП поки тільки дозріває, важливо нарощувати компетенції для надання ефективної допомоги замовникам у побудові комплексних систем управління й забезпечення інформаційної безпеки.

3.2 Розробка структурної схеми

Сучасним трендом АСУ ТП є впровадження Інтернету речей. Рішення в області Інтернету речей будуються на базі мікропроцесорних систем з використанням різного роду ПЗ, що реалізує, у тому числі, і сучасні технології підключення до зовнішніх мереж зв'язку, які працюють по стандартизованих протоколах. Будь те Wi-fi або Bluetooth. Із цієї позиції різниця між офісною мережею або розумним будинком – невелика. І в того, і в іншого – є можливість підключення до інтернету, наприклад, для віддаленого моніторингу й управління. Але як тільки з'являється підключення до інтернету й програмний рівень, то неминуче виникають і помилки, якими можуть скористатися зловмисники. Тому підходи до забезпечення інформаційної безпеки нових застосувань ІТ повинні бути аналогічні підходам, застосовуваним у класичних випадках забезпечення інформаційної безпеки.

Ринку ще має бути розвиток убік виробництва засобів захисту, які могли б елегантно вбудовуватися в IT-контур «розумних» систем, аналогічно тому, як це відбувається із захистом корпоративних систем. Зараз виробники тільки починають вишиковувати в себе життєвий цикл розробки й супроводу компонентів «розумних» систем, що враховує можливість здійснення у відношенні їх несанкціонованих впливів, включаючи тестування на предмет наявності уразливостей.

Все залежить від того, наскільки й із чим інтегровано те, до чого виходить доступ, і хто власник пристрою. Наприклад, якщо говорити про розумний будинок – можна спробувати одержати доступ до конфіденційних даних домовласника, або, також відключивши сигналізацію, проникнути в будинок. У випадку з виробничим підприємством і промисловим Інтернетом речей – також є ризики. Промислові системи, невміло підключені до інтернету, – це дуже небезпечне явище, що може привести не тільки до зупинки технологічного процесу, але й регіональній катастрофі. Тому виробництво змушене балансувати на тонкій грані між безпекою й автоматизацією. Наприклад, відповідно до інформації, на Shodan – ресурсі, що самостійно сканує Всесвітню мережу й надає інформацію про те, які користувальницькі й промислові пристрої підключені до інтернету із вказівкою їхніх протоколів, доступ через інтернет можливий до цілого ряду критичних пристроїв, починаючи від медичних, закінчуючи системами управління будинками, сонячною енергетикою, розумними будинками та ін.

Застосування технологій IoT досить актуально для ЖКГ (за рахунок інтернету речей можна знизити енерго- і теплоспоживання в житлових будинках), для управління міською інфраструктурою (включаючи транспорт, висвітлення й т.д.), у сільському господарстві (для підвищення врожайності ґрунту й відстеження її параметрів), а також для промислового сектора, де збір і аналіз різних даних дозволяє, зокрема, звістці моніторинг стан устаткування й вчасно попереджати його поломку.

При зваженому підході до реалізації захисту з виявленням основних погроз і вбудовуванням в існуючу систему технологій захисту інформації, безумовно, строки впровадження можуть бути трохи збільшені. Однак мінімізація ризиків, що обіцяє рішення питань безпеки, безумовно, цього коштує.

Насправді, напрямок промислового Інтернету речей у нашій країні тільки починає розвиватися. А раз немає публічних проектів, те немає й інформації про відповідні інциденти в області інформаційної безпеки. Але світових випадків злому промислових систем досить багато. Наприклад, кілька інцидентів було в США. А у звіті Центра досліджень ризиків Кембриджського університету США в 2015 році відзначалося, що якщо зловмисники атакують кілька сегментів американської енергомережі, у результаті чого 15 штатів і Вашингтон без електрики, те економічні втрати можуть досягти $1 трлн. доларів.

Інший відомий випадок відбувся в Європі. У грудні 2014 року в Німеччині була зроблена атака на металургійний завод. Хакерам удалося віддалено вивести з ладу доменну піч, що привело до поломки встаткування. Наскільки відомо, атака складалася з декількох проникнень у системи заводу, і в результаті одна з печей перестала бути керованої. Швидше за все, цей напад було цілеспрямованим, а самі зловмисники – підкованими й в області IT, і в області контрольних систем великих промислових підприємств.

Ще приклад – атака із зараженням вірусом Stuxnet декількох ядерних об'єктів Ірану в 2010 році. У результаті було уражено біля третини центрифуг на заводі по збагаченню урану, а також зірвані строки запуску ядерної АЕС. Це, мабуть, найгучніший випадок на сьогодні.

З більше наближених до України випадків – кібератака на українських постачальників електроенергії, «Прикарпатьеобленерго» і «Київенерго», що привела до перебоїв з електрикою. Проте, хоч на об'єктах і було виявлене шкідливе ПЗ BlackEnergy, однак явних доказів тому, що атакуючі скористалися ним для проникнення в технологічну мережу, поки, наскільки я знаю, немає.

З огляду на той факт, що тематика захисту АСУ ТП – автоматизованих систем управління технологічними процесами – зараз набирає популярність. Цей момент також знайшов відбиття в оновленій доктрині інформаційної безпеки, де особлива увага приділяється блоку погроз із боку закордонних країн у плані впливу на критичну інформаційну інфраструктуру України, підприємства оборонно-промислового комплексу та ін. До речі, показово, що й у недавно проведеному опитуванні 18 з 100 опитаних керівників великих українських компаній також бачать погрозу з боку іноземних урядів.

Тому, сподіваюся, що в самому найближчому майбутньому при впровадженні технологій Інтернету речей безпека буде стояти на чолі кута. Адже зовсім точно можна сказати, що витрати на інформаційну безпеку не порівнянні з можливими негативними наслідками. Адже якщо не боротися з виникаючими погрозами, виникають ризики тимчасової зупинки виробництва, повної втрати бізнесу й навіть катастроф.

Багато чого залежить від того, що диктує ринок. Зокрема, мобільні телефони існують досить давно, але користувальницьких засобів захисту дотепер не так вуж багато, а випадки проникнення вірусів або доступу зловмисників до банківських даних через мобільні пристрої трапляються регулярно. Так може бути й у випадку з Інтернетом речей. Однак, чим перспективніше напрямок, чим більше голосних проектів реалізується (у які застосовуються спеціалізовані програмні платформи, використовуються архітектурні підходи IoT, бездротові протоколи й т.п.), тим швидше йде процес створення інструментів по захисту даних.

Моніторинг аномалій мережної активності в промислових системах

У сфері забезпечення ІБ промислових систем важливим завданням є вибір ефективних заходів і засобів захисту, які повинні запобігати несанкціонованому доступу до управління технологічними процесами, але не створювати перешкоди для роботи АСУ. Домагатися цього дозволяють рішення, що забезпечують безперервне пасивне спостереження за активністю в промислових системах і

мережах, виявлення потенційних погроз і оперативне повідомлення відповідальних служб про виникаючі проблеми. Серед таких рішень можна виділити системи виявлення аномалій мережної активності (Network Behavior Anomaly Detection), застосування яких у промислових системах активно обговорюється експертним співтовариством.

Основною перевагою систем аналізу аномалій є їхнє пасивне застосування. Компоненти систем, відповідальні за збір мережного трафіку, підключаються до дзеркалюючих (SPAN) портів мережних комутаторів або безпосередньо до мережі через TAP-пристрої (це дозволяє не створювати мережні навантаження й не породжує затримок у роботі сервісів) і не взаємодіють прямо із промисловим устаткуванням. Такі системи аналізують мережний трафік і виділяють із нього інформацію про мережні потоки (Flow). Аналіз Flow-статистики більше ефективний для виявлення погроз, чим сигнатурні методи, оскільки дає можливість виявляти, у тому числі, атаки на невідомі (zero day) уразливості, сигнатури для яких ще не випущені.

Є й інші переваги. З обліком того, що штатна взаємодія пристроїв у промисловій мережі повинне бути статичним протягом тривалого часу, розгортання систем виявлення аномалій, їх «навчання», запуск в «бойовому» режимі й безперервній експлуатації значно спрощуються, оскільки не потрібні часті зміни профілю нормального поводження. Нарешті, робота систем аналізу аномалій дозволяє оцінити реальний рівень безпеки й виявити проблеми в системі забезпечення ІБ промислової мережі, причому результати аналізу можуть стати основою її вдосконалювання.

Системи класу Network Behavior Anomaly Detection (NBAD) добре зарекомендували себе при захисті офісних мереж і ЦОДів. Серед пропозицій є як комерційні (наприклад, Lancope StealthWatch, Arbor Networks Pravail NSI, McAfee Network Threat Behavior Analysis), так і безкоштовні (FlowMatrix, FlowBAT, Bro) рішення.

Функціонал цих систем містить у собі наступні можливості:

– виявлення підключення мережних пристроїв і побудова карти мережі;

– створення профілю нормальної мережної взаємодії;

– моніторинг мережної активності в режимі 24/7 для виявлення аномального поводження (аномальні з'єднання, пристрої, час і обсяги трафіку й інші показники);

– виявлення зовнішніх і внутрішніх (пов'язаних з навмисними або помилковими діями персоналу) погроз;

– оперативне оповіщення відповідальних служб про проблеми й передача інформації про їх у суміжні системи безпеки;

– ведення історії змін мережного поводження й допомога при розслідуванні інцидентів;

– формування звітів з різними рівнями деталізації.

Експерти затверджують, що своєчасне застосування рішень, що забезпечують моніторинг мережної активності, дозволило б виявити активність шкідливого ПЗ Stuxnet, Havex і BlackEnergy, оскільки в таких випадках мережне поводження виходить за рамки нормальної взаємодії пристроїв у мережі. Наприклад, не залишилися б непоміченими спроби відновлення прошивання контролера по мережі або збору даних. Незважаючи на всю користь і ефективність традиційних NBAD-систем, вони не можуть виявляти аномальний уміст прикладних промислових протоколів. Ріст числа погроз для систем промислової автоматизації привів до того, що на ринку стали з'являтися рішення, адаптовані для роботи саме в промислових мережах. Їхня робота заснована на тім же принципі пасивного збору трафіку, але вони здатні аналізувати промислові протоколи (deep packet inspection) і виявляти в них аномальні дані. У деяких джерелах цей клас рішень одержав назву Industrial Network Anomaly Detection (INAD).

Зараз відомі наступні закордонні рішення: Dragos Security CyberLens, NexDefense Sophia, C4 Security Fides, SCADAfense. Ці рішення перебувають на

різних стадіях зрілості. Деякі з них існують уже кілька років (наприклад, NexDefense Sophia), а деякі – тільки анонсовані (зокрема, SCADAfense). У кожному разі помітний інтерес виробників і замовників до рішень цього класу.

Розглянуті системи підтримують як відкриті, так і пропрієтарні промислові протоколи, у тому числі DNP3, ModbusTCP, Profinet, ISO-TSAP, AB-PCCC, BACNet, Ethernet / IP і інші. У різних продуктах підтримувані протоколи й функціональні можливості розрізняються.

У загальному виді системи даного класу дозволяють виявляти наступні види активності:

– нелегітимні команди й мережний трафік, що виводять із ладу системи управління;

– присутність у промисловій мережі шкідливого ПЗ, локалізація вогнищ зараження;

– дії зловмисників у промисловій мережі без використання шкідливого ПЗ;

– керуючі команди, що приводять до порушень технологічного процесу;

– команди на зупинку / перезавантаження / перепрошивання / переконфігурацію контролерів;

– команди, що встановлюють неприпустимі / небажані значення ключових параметрів управління технологічним процесом.

З особливостей застосування таких систем відзначимо наступні. Їм потрібне значний час на первісний збір даних для побудови профілю нормального поводження й завдання базової політики безпеки. Але це – плата за невикористання активного сканування, що може створювати проблеми в роботі промислової мережі. Крім того, для підключення до SPAN-порту мережного комутатора або підключення TAP-пристрою, що необхідно для пасивного збору трафіку, потрібне активна взаємодія з мережним устаткуванням (конфігурація, установка в розрив). Однак імовірність того, що ці дії й подальша робота системи

приведуть до проблем, украй мала. Ефективність систем безпеки в цьому випадку незрівнянно вище ризику від їхнього застосування.

Крім систем, орієнтованих на пошук аномалій у мережному трафіку промислових мереж, сталі з'являтися цікаві рішення, націлені на безконтактне виявлення аномалій у роботі промислового встаткування (такий функціонал забезпечує PFP Cybersecurity). Останнє завдання реалізується шляхом спостереження за енергоспоживанням процесора.

Безумовно, вибір конкретного продукту повинен здійснюватися на основі аналізу індивідуальних вимог замовника, особливостей промислових систем і мереж, типу промислового об'єкта. Конче потрібно й ретельне тестування продукту до його введення в експлуатацію. Однак вибір рішень на ринку однозначно є.

Інтеграція бізнес-додатків з виробничими процесами, впровадження рішень класу MES, ERP, розвиток мережних комунікацій між офісними й промисловими сегментами, використання ОС Windows / Linux і IP-протоколів – все це створює потенційну погрозу несанкціонованого доступу до промислових систем з непередбаченим збитком.

Аудит безпеки й аналіз захищеності

Містить у собі аналіз документації, структури й конфігурації систем, проведення інтерв'ю фахівців замовника, а також аналіз захищеності інфраструктури підприємства з визначенням існуючих уразливостей. Підсумковий звіт містить вичерпну інформацію з поточного стану інформаційної безпеки, опис існуючих погроз і рекомендації із протидії їм, методику й опис ходу роботи. У ході аудита перевіряється практична реалізація вимог і рекомендацій IEC 62443, NIST SP 800-82r2, і інших українських і міжнародних стандартів з забезпечення інформаційної безпеки промислових систем.

Побудова системи управління інформаційною безпекою

Розробляється комплексна система управління інформаційною безпекою (СУІБ) підприємства, у тому числі політикові інформаційної безпеки,

корпоративні стандарти й нормативна документація, що регулює процеси управління ІБ. Додатково персонал замовника проходить навчання правилам інформаційної безпеки промислових систем.

Побудова системи забезпечення інформаційної безпеки

Система забезпечення ІБ виявляє й блокує спроби несанкціонованого доступу до технологічної інформації й управління промисловими системами. При її створенні враховуються тенденції розвитку сучасних промислових систем при підключенні до Інтернету, організації віддаленого доступу до встаткування Dial-UP, підключенні до корпоративної мережі, використанні бездротових мереж UMTS / HSDPA / ZigBee / WiFi.

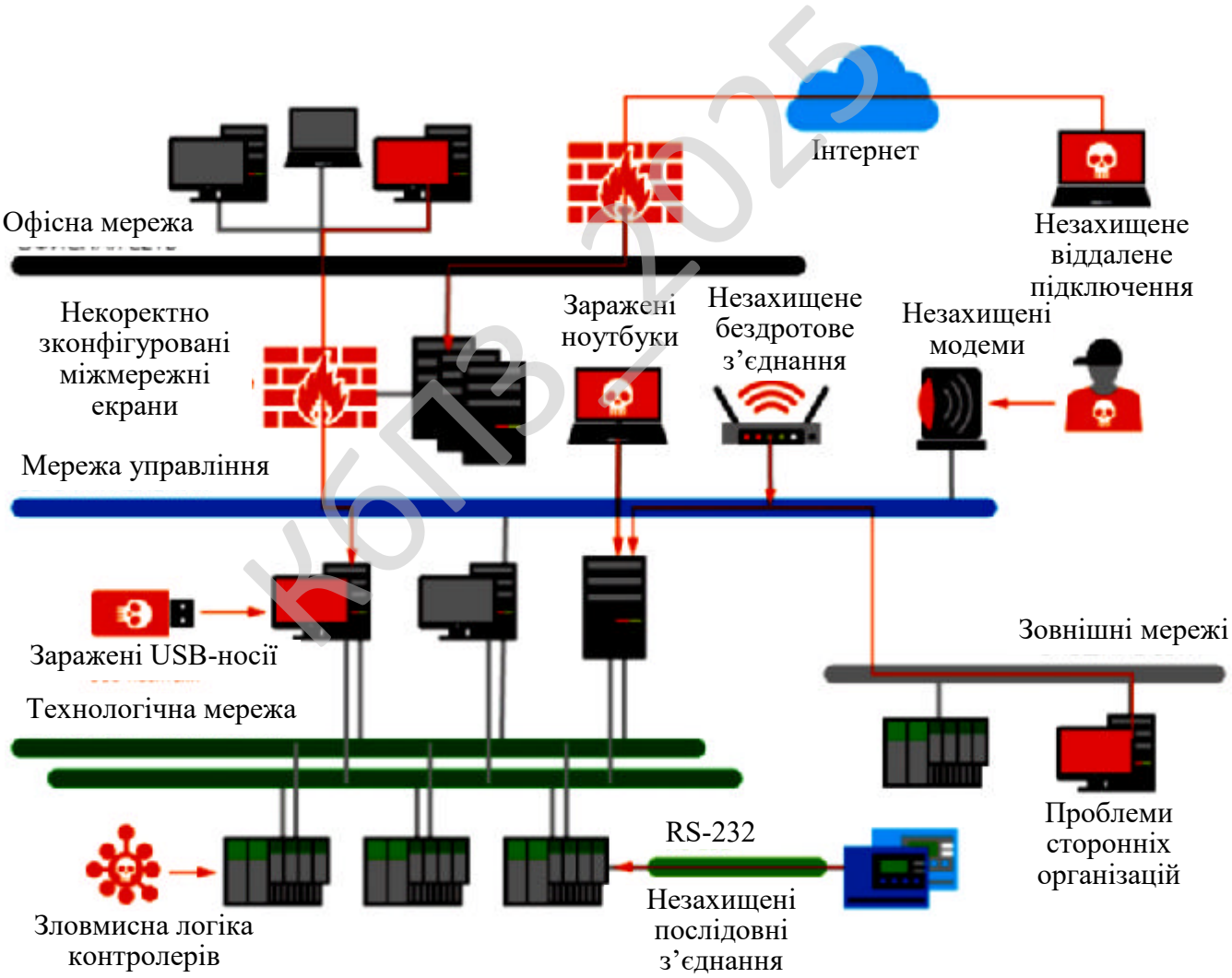

Рисунок 3.1 – Структурна схема системи

На структурній схемі системи наведена типова мережа промислового підприємства й основні погрози інформаційної безпеки.

Під захист попадають основні компоненти промислових систем: робітники станції операторів і інженерів, сервери SCADA і архіву, програмувальні логічні контролери, інтелектуальні виконавчі пристрої й датчики, промислове мережне встаткування, канали зв'язку, шлюзи віддаленого доступу й інші компоненти. Арсенал використовуваних засобів містить у собі односпрямовані шлюзи, промислові міжмережні екрани, рішення для розвідки кіберзагроз, виявлення мережних атак і аномалій, контролю команд, що відправляються на контролери АСУ ТП, системи контролю запуску додатків на серверах і автоматизованих робочих місцях (АРМ) операторів АСУ ТП, сервіси розвідки кіберзагроз.

3.3 Розробка функціональної схеми

Системи технологічного управління (SCADA, Control Systems) і родинні їм інформаційні системи (системи диспетчерського управління, противоаварійної автоматики й т.д.) міцно входять у наше повсякденне життя. Електрика, що висвітлює нас, пальне, яким заправляються наші автомобілі, системи управління дорожнім трафіком і водопостачанням, «розумними будинками» і атомними електростанціями – все це приклади подібних систем. Вони роблять простіше й зрозуміліше процеси управління будь-якими складними технологічними процесами – від передачі електроенергії до збагачення урану. З кожним роком і кожним модернізованим виробництвом їх стає усе більше й більше.

Проблематика захисту автоматизованих систем технологічного управління обговорюється в спеціалізованій пресі й у виступах провідних експертів по інформаційній безпеці (ІБ) досить давно. Однак помітного прогресу в захисті АСУ ТП систем цього класу за минулі 10 років не відбулося. Давайте розберемося, чому.

Найпоширеніші погрози безпеки в даний момент пов'язані із криміналізацією кіберзлочинності, тобто з одержанням грошової вигоди від реалізації тих або інших атак на інфраструктуру.

І з погляду потенційного зовнішнього порушника системи управління технологічними процесами малопривабливі.

Причина цього досить проста. Основна інформація, що циркулює в системах технологічного управління, – це інформація про технологічні процеси (об'єктах фізичного миру, їх стани й динаміку) і про керуючі впливи.

Володіння цією інформацією без фізичного доступу до об'єкта управління не дає можливості зробити крадіжку, що різко обмежує коло потенційних порушників.

Ризики, пов'язані із шахрайськими операціями в АСУ ТП, можна обмежити діями внутрішнього порушника – власного персоналу компанії або компаній-партнерів.

Приміром, для реалізації схем з модифікацією даних по витраті палива на автозаправці треба мати можливість зливу й реалізації цього палива.

Серед монетизуємих зовнішніх атак на ресурси АСУ ТП найпоширенішими залишаються промислове шпигунство (у тих випадках, коли дані технологічного процесу являють цінність для конкурентів) і в рідких випадках – шантаж і замовлені акції проти конкурентів.

Інші інциденти є немонетизуємими: помста звільнених працівників, порушення функціонування шкідливим кодом, випадкові зломи «підлітками».

З вищеописаного треба, що кількість привселюдно відомих порушень функціонування подібних систем украй невелика.

Крім того, у випадку серйозних порушень функціонування процесів, контрольованих системою управління, боротьба з наслідками не буде відрізнятися від боротьби з техногенною аварією.

Системи технологічного управління розраховуються на швидке відновлення після збоїв як у випадку автоматизації, так і без неї.

Та й компанії, експлуатуючі системи автоматизації, все-таки приділяють увагу ІБ систем.

Однак низька ймовірність зовнішніх атак на системи АСУ ТП не знижує актуальність погроз для систем управління.

Відповідно до загальноприйнятої практики актуальність погрози пропорційна як імовірності реалізації погрози, так і можливому збитку від її реалізації.

А якщо говорити про можливий збиток від реалізації погрози, те тут системи управління, особливо системи управління небезпечними виробничими циклами або системи життєзабезпечення цілих міст і областей, будуть поза конкуренцією.

Можливий збиток від реалізації подібних атак включає, крім фінансових втрат, репутаційні ризики й ризики, пов'язані із втратою здоров'я й життя, а також ризики виникнення екологічних катастроф.

Навіть одиничне порушення функціонування систем технологічного управління може привести до катастрофічних наслідків.

Інциденти ІБ у системах технологічного управління при їхньому оприлюдненні викликають великий суспільний резонанс.

Особливості АСУ ТП як об'єкта захисту

Ера після Stuxnet

Найбільш публічним інцидентом, що показує уразливість і можливість експлуатації даної уразливості мереж управління на практиці, з'явився виявлений у липні 2010 р. вірусний код Stunxnet.

Даний вірус містив цільовий код, що задовольняє цілому ряду специфічних вимог і який реалізує повноцінну атаку на системи АСУ ТП виробництва компанії Siemens.

Зокрема, для реалізації потенціалу нападу вірус вимагав наявності частотних конверторів виробництва 2 компаній – «Vacon» (Фінляндія) і «Fararo Paya» (Іран), – працюючих на частотах від 807 до 1210 Гц.

Наявність подібних вимог дозволило більшості експертів, що досліджували даний код, зробити вивід про те, що вірус призначався для крапкової атаки цілком певного виробництва або ряду виробництв.

Відповідно до аналізу, проведеному фахівцями компанії Symantec, шкідливий код Stuxnet-а реалізовував атаку відразу на декількох рівнях: на рівні операційних систем Windows, ПЗ управління АСУ ТП Siemens WinCC/PCS 7 і безпосередньо контролерів програмувальної логіки Siemens S 7-300, що обслуговують конвертори частоти (які, у свою чергу, управляли швидкістю обертання електромоторів).

Атака шкідливого коду Stuxnet на рівні операційної системи не представляла із себе нічого особливого, за винятком експлуатації безпрецедентно високої кількості уразливостей нульового дня – 4 уразливості за раз.

Як правило, шкідливий код, створюваний кіберзлочинцями, не реалізує більше 1-2 подібних уразливостей за раз.

При зараженні звичайного комп'ютера шкідливий код поводився як звичайний вірус, займаючись поширенням своїх копій і спробами встановити зв'язок з командним центром у випадку наявності такої можливості.

Однак при зараженні комп'ютера із установленим ПЗ Siemens WinCC/PCS 7 вірус реалізовував наступний рівень атаки – перехоплення управління контролерами програмувальної логіки Siemens шляхом впровадження в ПЗ управління (використовуючи ще одну уразливість нульового дня – фіксований пароль для роботи З управління із СУБД).

Після чого за допомогою ПЗ управління шкідливий код реалізовував третій рівень атаки, «прошиваючи» на згадку контролерів програмувальної логіки «бойову» частину свого коду.

Існує кілька варіацій вірусу Stuxnet, що відрізняються «бойовим» наповненням.

Але найбільший резонанс у сфері ІБ, що дійшла до уряду ряду країн, викликала одна з варіацій, що проводила час від часу модифікацію частоти,

генеруємой конверторами (і, відповідно, швидкості обертання електродвигунів), спочатку вище максимальної межі обертів, потім – нижче мінімального, далі – установлюючи значення за замовчуванням і приховуючи при цьому зроблені зміни від керуючого ПЗ.

У результаті виконання даних команд відбувалися наступне: електродвигуни розкручували навантаження, що перебуває на них, до граничних обертів і різко зупинялися.

При цьому ПЗ управління й оператори, віддалено контролюючі роботу апаратури, не фіксували ніяких змін у функціонуванні виробничого процесу.

Законодавчі ініціативи

Закордонний досвід

В області захисту систем управління (Control Systems, SCADA) у даний момент існує цілий ряд стандартів і рекомендацій.

Вони включають як галузеві рішення (приміром, у США є присутнім стандарт NERC для систем управління електричними мережами, стандарт ChemITC для хімічної індустрії), так і рекомендації загального рівня (стандарти NIST, ISA і ін.).

Однак яких-небудь обов'язкових вимог до відповідності певним критеріям безпеки для комерційних компаній не пред'являється.

Правове поле України

У правовому полі України існує поняття ключової системи інформаційної інфраструктури, обумовлене як інформаційна система, що здійснює функції управління чутливими для України процесами, порушення її функціонування приводить до значних негативних наслідків.

Передбачається, що система автоматизує функціонування об'єктів, включаючи соціально значимі виробництва або технологічні процеси, порушення штатного режиму функціонування яких приводить до надзвичайної ситуації певного масштабу.

Серед подібних об'єктів, крім інформаційних систем державних органів, присутні системи технологічного управління в нафтогазовій галузі, енергетику, на екологічно небезпечних виробництвах, системи управління життєзабезпеченням міст і т.д.

Способи захисту систем АСУ ТП

Основні погрози ІБ АСУ ТП

Організація забезпечення безпеки АСУ ТП – сукупність погоджених по меті, завданням, місцю й часу заходів, спрямованих на ліквідацію (нейтралізацію) внутрішніх і зовнішніх погроз безпеки інформації в АСУ ТП і на мінімізацію збитку від можливої реалізації таких погроз.

Введення терміна «погроза безпеки інформації» дозволяє об'єднати в одне поняття всі можливі негативні умови й фактори, що впливають прямим або опосередкованим образом на безпеку інформації, тобто на її цілісність, доступність або конфіденційність.

Серед погроз ІБ, властивих АСУ ТП, можна виділити 3 класи: погрози техногенного, антропогенного характеру й несанкціонованого доступу.

Залежно від призначення, розміщення й особливостей функціонування АСУ ТП розрізняється склад конкретних погроз безпеки, отже, і зміст пропонованих вимог по її забезпеченню.

Погрози техногенного характеру – погрози, обумовлені фізичними впливами на компоненти АСУ ТП.

Для захисту від даного класу погроз застосовуються міри й засоби забезпечення безпеки від несанкціонованого фізичного доступу, які запобігають проникненню порушників на охоронювану територію й забезпечують технічний контроль доступу до ключових компонентів АСУ ТП.

До погроз антропогенного характеру відносяться погрози навмисної й ненавмисної дії людей, зайнятих обслуговуванням АСУ ТП, у тому числі помилки персоналу або помилки в організації робіт з компонентами АСУ ТП.

Погрози несанкціонованого доступу для АСУ

ТП розглядаються через наявність взаємодії її компонент із ЛОМ підприємства для передачі інформації про стан технологічного середовища, а також формування керуючих впливів на технологічні об'єкти.

У зв'язку із цим обов'язковими стають заходи щодо формування виділених технологічних мереж передачі даних і використанню периметральних засобів захисту (таких, як засоби міжмережного екранування, виявлення вторгнень криптографічного захисту каналів зв'язку).

Підхід до реалізації системи ІБ АСУ ТП

Реалізація системи ІБ АСУ ТП являє собою комплексне завдання, рішення якого повинне виконуватися на наступних рівнях:

– адміністративному;

– процедурному;

– рівні програмно-технічних мір.

Адміністративний рівень

До адміністративного рівня ІБ відносяться дії загального характеру, що вживаються керівництвом підприємства.

Головна мета мер адміністративного рівня – формування програми робіт із забезпечення ІБ АСУ ТП із урахуванням загальної концепції захисту АСУ ТП.

Основою програми є набір документів, які регламентують високорівневий підхід з забезпечення ІБ, а також описують політикові розвитку системи ІБ АСУ ТП.

Процедурний рівень

Процедурний рівень ІБ АСУ ТП орієнтований на людський фактор.

Головна мета – визначення й виконання вимог з забезпечення безпеки компонентів АСУ ТП за рахунок формування й прийняття пакета організаційної документації, спрямованої на створення й підтримку режиму ІБ АСУ ТП.

Рисунок 3.2 – Функціональна схема системи

Рівень програмно-технічних мір

Рівень програмно-технічних мір утворить основний рубіж забезпечення ІБ АСУ ТП.

На цьому рівні реалізуються наступні сервіси ІБ:

– управління доступом;

– забезпечення цілісності;

– забезпечення безпечної міжмережної взаємодії;

– антивірусний захист;

– аналіз захищеності;

– виявлення вторгнень;

– управління системою ІБ (безперервний моніторинг стану, виявлення інцидентів, реагування).

Конкретні вимоги до перерахованих сервісів пред'являються на підставі аналізу оброблюваної інформації й оцінки погроз безпеки АСУ ТП.

Управління доступом

Рішення завдання розмежування доступу в АСУ ТП, як і в будь-яких інших інформаційних системах, виконується як на мережному, так і на прикладному рівні.

Управління доступом на мережному рівні

Рішення завдання управління доступом на рівні мережної взаємодії виконується за рахунок створення демілітаризованих зон із застосуванням засобів міжмережного екранування.

Подібні зони являють собою крапку обміну інформацією між різними ЛОМ АСУ ТП із системами управління підприємством, забезпечуючи баланс між доступністю й безпекою інформації.

Особливість побудови таких зон при забезпеченні ІБ АСУ ТП полягає в тому, що корпоративна мережа розглядається в якості зовнішнього, недовіреного сегмента.

Тому виділена зона відповідним чином забезпечує як захист інформації, переданої із ЛОМ АСУ ТП у зовнішні системи, так і блокування зовнішніх несанкціонованих звертань до компонентів АСУ ТП.

Управління доступом на прикладному рівні

Програмні засоби блокування несанкціонованих дій, сигналізації й реєстрації можуть бути реалізовані практично у всіх підсистемах забезпечення безпеки АСУ ТП.

Це спеціальні, що не входять у ядро який-небудь ОС програмні й програмно-апаратні засоби для захисту ОС, СУБД і прикладних програм.

Вони виконують функції захисту самостійно або в комплексі з іншими засобами й спрямовані на виключення або утруднення виконання небезпечних для АСУ ТП дій користувача або порушника.

Забезпечення цілісності

Засоби підвищення вірогідності й забезпечення цілісності переданих даних і надійності транзакцій використовуються переважно на ОС і СУБД і засновані на розрахунку так званих «контрольних сум» – повідомлень про збій у передачі пакета повідомлення, у повторі не прийнятого пакета й т.д.

Забезпечення безпечного міжмережного взаємодії

Використання Ethernet при створенні мереж передачі даних, голосу й відео добре зарекомендувало себе в корпоративних мережах, де дана технологія успішно застосовується при об'єднанні АРМ, серверів АСУ ТП і контролерів.

У цей час стало можливим використання Ethernet як єдиного середовища передачі даних для самого нижнього рівня АСУ ТП, де розміщаються контрольні датчики й виконавчі механізми, що підключаються по протоколах Modbus/TCP, EtherNet/IP, PROFInet і ін.

Для підключення пристроїв всіх рівнів АСУ ТП рекомендується використання комутаторів Ethernet, здатних забезпечувати захист від таких погроз, як:

– прослуховування трафіку (з використанням атак переповнення таблиці MAC);

– підміна адрес учасників інформаційного обміну (з використанням атак підробки повідомлень протоколу ARP, підробки IP-адрес, підробки MAC-адрес);

– несанкціонована передача трафіку в інші віртуальні сегменти мережі (з використанням атак проходження VLAN);

– атака на сам комутатор і мережу (з використанням особливостей протоколу Spanning Tree, передачі анормального трафіку й ін.).

У деяких випадках доцільне використання технології автентифікації пристроїв і/або користувачів при підключенні до комутирується сети, що (наприклад, по стандарті 802.1x).

Однак не слід забувати, що при здійсненні взаємодії засобів АСУ ТП через мережі загального користування (наприклад, із ЛОМ підприємства) обов'язковим

є створення довіреного (захищеного) каналу зв'язку між взаємодіючими об'єктами з використанням виділених каналів зв'язку й криптографічних засобів.

Антивірусний захист

Хоча прямого підключення до мережі Інтернет не має практично жодна АСУ ТП, у той же час використання різних технологій і протоколів в АСУ ТП створює сприятливе середовище для мережних вірусів, які здатні з великою швидкістю поширюватися в будь-яких мережах передачі даних за допомогою поштових повідомлень, файлів документів, що виконуються файлів, використовуючи уразливості в системному й прикладному програмному забезпеченні АСУ ТП.

Часто перед ініціатором атаки не коштує яких-небудь певних цілей, але навіть у цьому випадку вторгнення можуть вивести компоненти АСУ ТП із ладу, порушити їхню зв’язність, що приведе до позбавлення оператора можливості управляти ТП.

Тому так важливе застосування засобів антивірусного захисту, які забезпечують:

– виявлення й блокування деструктивних вірусних впливів на загальносистемне й прикладне ПЗ, що реалізує виконання критично важливих процесів АСУ ТП, а також на інформацію, необхідну для виконання керованих технологічних процесів;

– виявлення й видалення невідомих вірусів;

– забезпечення самоконтролю даного антивірусного засобу при його завантаженні.

Аналіз захищеності

Засоби аналізу захищеності покликані здійснювати тестування файлових систем, мережних компонентів і баз даних з метою збору інформації про функціонування елементів системи безпеки АСУ ТП.

Виявлення вторгнень

Одним з найважливіших напрямків удосконалювання стану захищеності АСУ ТП при міжмережній взаємодії є застосування систем виявлення мережних атак як на мережному, так і на хостовому рівні.

Засоби виявлення вторгнень мережного рівня

Найчастіше мережні системи виявлення й запобігання вторгнення – єдиний спосіб захисту для нижніх рівнів АСУ ТП, тому що установка антивірусних програм на АРМ, контролери й сервери може бути утруднена або неможлива в принципі.

Подібні системи можуть функціонувати як у режимі перехоплення й блокування небажаних даних, так і в режимі прослуховування, сигналізуючи про проходження небажаного трафіку на консоль системи безпеки.

Засоби виявлення вторгнень хостового рівня

Найбільш ефективним засобом захисту операційних систем від поширення сучасних атак є хостові системи запобігання вторгнень – Host Intrusion Prevention System (HIPS), які розміщаються на всіх операційних системах загального призначення, таких, як Microsoft Windows, Sun Solaris і Linux.

Контролюючи на системному рівні події, що відбуваються в операційній системі й додатках, HIPS дозволяє вчасно блокувати шкідливі впливи хробаків, що самопоширюються, або вірусів, ПЗ, що має несанкціоновано встановлені «закладки», запобігати модифікації файлів, що виконуються, АСУ ТП і т.д.

Управління системою ІБ

Рішення завдання управління системою ІБ АСУ ТП виконується з використанням засобів аудита й контролю захищеності, призначених для відстеження стану захищеності й оповіщення адміністратора у випадку виникнення погроз безпеки.

Принцип роботи зазначених засобів будується на централізованому зборі даних журналювання (системні журнали й журнали аудита безпеки) і виконанні кореляції вступників подій з метою виявлення критичних для системи подій і оповіщення про їх адміністраторів безпеки.

Виділення переліку подій, що підлягають аудитові, а також налаштування правил їхні кореляції виконуються виходячи з існуючих погроз.

Склад реалізованих заходів щодо захисту АСУ ТП

Склад реалізованих мір і набір використовуваних засобів при захисті АСУ ТП залежить від типу оброблюваної в системі інформації.

С точки зору інформаційного забезпечення АСУ ТП забезпечує обробку наступних типів інформації:

– програмно-технічна (склад, структура й характеристики побудови АСУ ТП, її системи забезпечення ІБ, програми системного й прикладного характеру, параметри налаштувань програмно-апаратних засобів, у тому числі засобів захисту інформації);

– керуюча (забезпечує управління потенційно небезпечними об'єктами або процесами);

– контрольно-вимірювальна (відбиває стан потенційно небезпечних об'єктів або процесів, на її основі приймаються рішення по управлінню такими об'єктами або процесами);

– інформація з обмеженим доступом (відповідно до діючих нормативних документів являє собою той або інший вид таємниці).

З метою диференціювання вимог з забезпечення ІБ проводиться розбивка АСУ ТП на наступні підсистеми:

– підсистеми, у яких обробляється інформація обмеженого доступу (не підлягаючому вільному поширенню);

– підсистеми, у яких обробляється загальнодоступна інформація;

– підсистеми, які здійснюють управління критично важливим об'єктом.

Можливе майбутнє – у центрі інформаційної війни

Поняття «кібервійна»

У зв'язку із проблемою захисту систем АСУ ТП на інфраструктурних об'єктах і небезпечних виробництвах всі частіше в ЗМІ й політичних дебатах згадується новий термін – «кібервійна» (cyberwarfare).

У цілому кібервійна визначається як один з видів інформаційної війни (який включає такі методи ведення воєнних дій, як навмисна дезінформація), що припускає нанесення втрати супротивникові за допомогою спрямованого інформаційного впливу на телекомунікаційну інфраструктуру й автоматизовані системи, у тому числі які знаходяться в приватному користуванні.

Серед імовірних цілей при веденні кібервойни, зокрема, називаються мережі управління електроживленням.

У цей час лише кілька країн відкрито заявляють про наявність спеціалізованих армійських підрозділів, призначених для проведення спрямованих атак на IT-інфраструктуру об'єктів супротивника.

При цьому тільки США відкрито надає інформацію про їхню організацію, офіційно включаючи даного підрозділу в структуру армійського командування.

Відповідно до поточної схеми, дані підрозділи включають:

– підрозділ стратегічного командування USCYBERCOM;

– підрозділ американської армії ARCYBER (Army Cyber Command) і підлеглої структури;

– підрозділу десантних військ Marrine Corps Cyberspace Command;

– підрозділу флоту Navy Cyber Command;

– підрозділу ВВС 24AF.

При цьому завданнями армійських підрозділів США є:

– захист комп'ютерних мереж департаменту безпеки;

– забезпечення потенціалу ведення повномасштабних воєнних дій, включаючи як захист, так і напад у межах інформаційного поля.

Можливі наслідки для приватних організацій

У реаліях наявності поняття «кібервійна» варто говорити про наступні практичні аспекти, пов'язаних із захистом систем управління стратегічно важливою інфраструктурою:

– можлива наявність погроз, пов'язаних з порушником, що володіє високим потенціалом нападу (фінансові й технічні ресурси, доступ до Ноу-хау постачальників систем АСУ ТП і засобів захисту інформації);

– у випадку утруднень зовнішньополітичної ситуації можливо різке збільшення ймовірності погроз, пов'язаних із приватними громадянами країн-учасниць конфлікту.

Поки наявність погроз із боку армійських і розвідувальних підрозділів інших країн виглядає фантастикою.

Однак погрози ІБ мають особливість тільки збільшуватися в кількості із часом.

Системи АСУ ТП розраховуються на тривалий період експлуатації, відповідно, повинні розраховуватися й системи забезпечення ІБ.

Обов'язкова умова при цьому – можливість модифікації й прицілу на майбутнє, яким би неприємним воно не виявилося.

Автоматизовані й автоматичні системи технологічного управління міцно інтегровані в наш соціум.

Їхнє функціонування може зачіпати не тільки інтереси окремих промислових компаній – експлуатантів подібних систем, але іноді – всіх і кожного. Імовірність атаки на подібні системи нижче, ніж на багато інші, але відповідальність, пов'язана з їхнім захистом, у деяких випадках незрівнянно вище. Це повною мірою ставиться до значимих і небезпечних областей промисловості й життєзабезпечення міст. Про проблематику захисту подібних систем управління не варто забувати, переносячи плани на черговий рік.

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.

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.

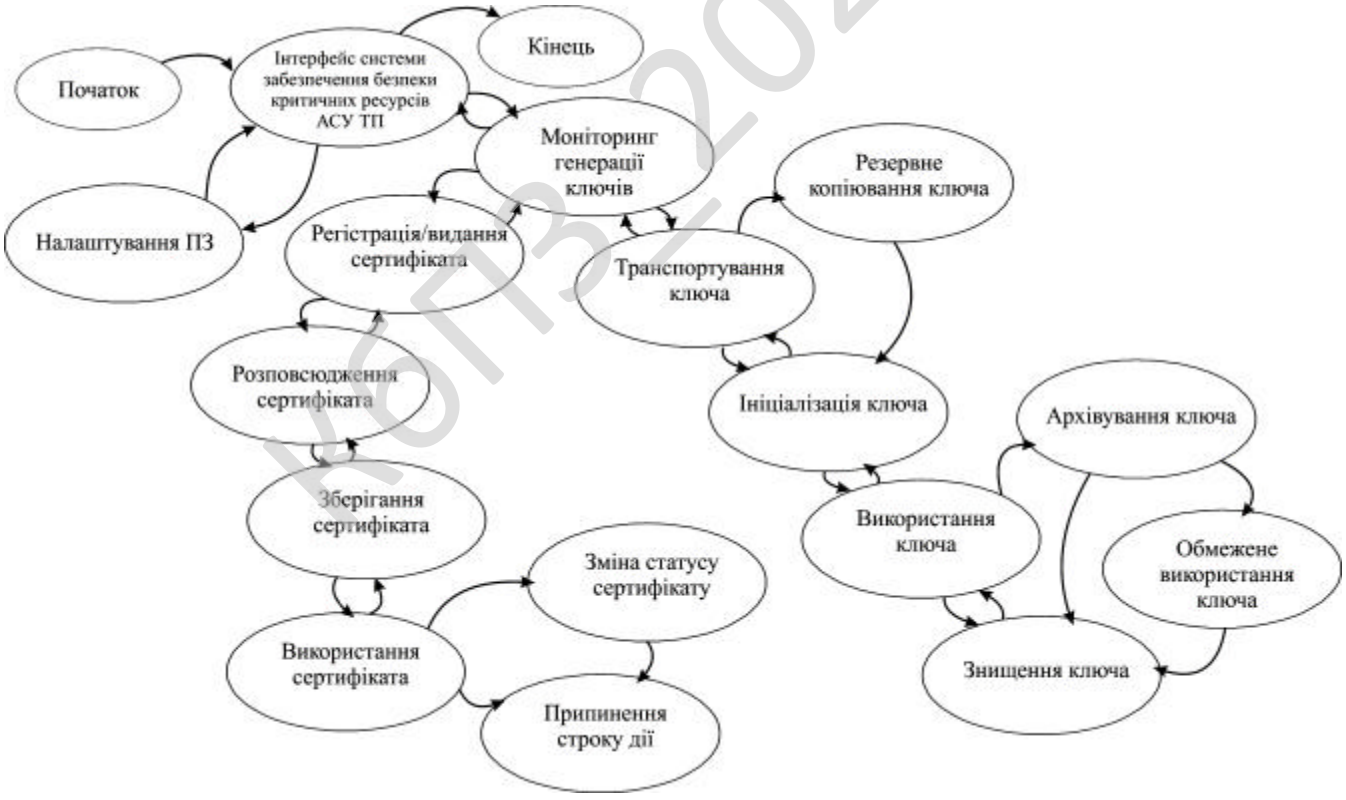

Рисунок 3.3 – Діаграма взаємодії процесів

Модулі діаграми працюють наступним чином:

1. Клієнт посилає повідомлення ClientHello, указуючи найбільш останню версію підтримуваного TLS протоколу, випадкове число й список підтримуваних методів шифрування й стиски, що підходять для роботи з TLS.

2. Сервер хмарного сервісу відповідає повідомленням ServerHello, що містить: обрану сервером версію протоколу, випадкове число, послане клієнтом, що підходить алгоритм шифрування AES й стиски зі списку наданого клієнтом.

3. Сервер хмарного сервісу посилає повідомлення Certificate, що містить цифровий сертифікат сервера.

4. Сервер хмарного сервісу може запросити сертифікат у клієнта, у такому випадку з'єднання буде взаємно автентифіковано.

5. Сервер хмарного сервісу відсилає повідомлення ServerHelloDone, що ідентифікує закінчення handshake.

6. Клієнт відповідає повідомленням ClientKeyExchange, що містить PreMasterSecret відкритий ключ Діффі-Хеллмана.

7. Клієнт і сервер хмарного сервісу, використовуючи PreMasterSecret ключ Діффі-Хеллмана і випадково згенеровані числа, обчислюють загальний секретний ключ Діффі-Хеллмана. Вся інша інформація про ключ Діффі-Хеллмана буде отримана із загального секретного ключа Діффі-Хеллмана (і згенерованих клієнтом і сервером випадкових значень).

8. Клієнт посилає ChangeCipherSpec повідомлення, що вказує на те, що вся наступна інформація буде зашифрована встановленим у процесі handshake алгоритмом AES, використовуючи загальний секретний ключ Діффі-Хеллмана. Це повідомлення рівня записів і тому має тип 20, а не 22.

9. Клієнт посилає повідомлення Finished, що містить хеш MD-5 і MAC, згенеровані на основі попередніх повідомлень handshake.

10. Сервер хмарного сервісу намагається розшифрувати Finished-повідомлення клієнта й перевірити хеш MD-5 і MAC. Якщо процес розшифровки або перевірки не вдається, handshake вважається невдалим і з'єднання повинне бути обірване.

11. Сервер хмарного сервісу посилає ChangeCipherSpec і зашифроване Finished повідомлення й у свою чергу клієнт теж виконує розшифровку й перевірку.

Із цього моменту handshake уважається завершеним, протокол установленим. Весь наступний вміст пакетів іде з типом 23, а всі дані будуть зашифровані AES.

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

Хоча я реалізовував програму сам, було використано підходи Scrum для саморозвитку та пришвидшенню розробки, розглянемо цей метод. Scrum – підхід управління проектами для гнучкої розробки програмного забезпечення. Скрам чітко робить акцент на якісному контролі процесу розробки.

Підхід вперше описали Гіротака Такеучі та Ікуджіро Нонака в статті The New New Product Development Game (Гарвардський Діловий Огляд, січ–лют 1986). Вони відзначили, що проекти, над якими працюють невеликі, крос–функціональні команди, зазвичай систематично продукують кращі результати, і пояснили це, як «підхід регбі». У 1991 році ДеҐрейс та Шталь у книжці Злі проблеми, справедливі рішення послалися на цей підхід, як на Scrum (штовханина; сутичка навколо м'яча (у регбі)), спортивний термін, згаданий в статті Такеучі і Нонака. Кен Швабер на початку 1990–х використовував підхід який привів Scrum в його компанію.

Вперше метод Scrum було представлено на загальний огляд задокументованим, чітко сформульованим та описаним спільно Сазерлендом та Швабером на OOPSLA'96 в Остіні. Швабер та Сазерленд протягом наступних років працювали разом щоб обробити та описати весь їхній досвід та найкращі практичні зразки для індустрії в одне ціле, в ту методологію, що відома сьогодні як Scrum. Швабер об'єднав зусилля з Майком Бідлом в 2001, щоб детально описати метод в книжці Agile Software Development with SCRUM. Не зважаючи на те, що для Scrum нарікли долю управління проектами з розробки ПЗ, він може також використовуватися в роботі команд обслуговувань програмного

забезпечення (software maintenance teams), або як підхід управління розробкою і супроводом програм: Scrum of Scrums.

Scrum – це кістяк процесу, який включає набір методів і попередньо визначених ролей. Головні дійові особи – ScrumMaster, той хто опікується процесами, веде їх і працює як керівник проекту, Власник Продукту, людина, що представляє інтереси кінцевих користувачів та інших зацікавлених в продукті сторін, та Команду, яка включає розробників.

Протягом кожного спринту, 15–30 денного періоду (тривалість визначається командою), працівники створюють функціональний ріст програмного забезпечення.

Набір можливостей, які імплементуються кожного спринту, приходять з етапу, що має назву product backlog (документація запитів на виконання робіт), який має найвищу пріоритетність за рівнем вимог до роботи, що повинна бути виконана.

Запити на виконання робіт (backlog items), що визначені протягом наради з планування спринту (sprint planning meeting), переміщуються в етап спринту. Протягом цієї наради Власник Продукту інформує про завдання, які він хоче, аби були виконані. Тоді Команда визначає, скільки з бажаного вони можуть зробити, щоб завершити необхідні частини протягом наступного спринту. Протягом спринту команда виконує визначений фіксований список завдань (т.з. backlog items). Впродовж цього періоду ніхто не має права змінювати перелік запитів на виконання робіт, що слід розуміти, як заморожування вимог (requirements) протягом спринту.

Product backlog – це документ, який має список вимог до функціональності, які упорядковані згідно зі ступенем важливості. Product backlog представляє список того, що повинно бути реалізовано. Елементи цього списку називається «історіями» (user story) або елементами backlog–у (backlog items). Product backlog відкритий для редагування усім учасникам Scrum–процесу.

Обов'язкові поля:

1. ID – унікальний ідентифікатор, порядковий номер, який використовується для ідентифікації історій у разі їх перейменування.

2. Назва (Name) – стислий опис історії. Він повинен бути однозначним, щоб і розробники і product owner могли зрозуміти, про що йдеться і відрізнити одну історію від іншої.

3. Важливість (Importance) – ступінь важливості даної історії на погляд product owner ’а. Зазвичай являє собою натуральне число, іноді для цієї цілі використовуються числа Фібоначчі. Чим більше значення, тим більше пріоритет.

4. Попередня оцінка (initial estimate) – початкова оцінка об'єму робіт, необхідного для реалізації історії порівняно з іншими історіями. Вимірюється у story point'ах. Приблизно відповідає числу «ідеальних людино–днів».

5. Як продемонструвати (how to demo) – стисле пояснення того, як завершена задача буде продемонстрована у кінці спринта. Дане поле може являти собою код автоматизованого приймального тесту.

Додаткові поля. Іноді, також, використовуються додаткові поля у product backlog, в основному для того, щоб допомогти product owner'у визначитися з його пріоритетами.

Категорія (track). Наприклад, «панель управління» чи «оптимізація». За допомогою цього поля product owner може легко вибрати усі пункти категорії «оптимізація» і задати їм низький пріоритет.

Компоненти (components) – указує, які компоненти (наприклад, база даних, сервер, клієнт) будуть зачеплені при реалізації історії. Дане поле складається з групи checkbox'ів, які відмічаються, якщо відповідні компоненти потребують змін.

Ініціатор запиту (requestor). Product owner може захотіти зберігати інформацію про усіх замовників, зацікавлених у даній задачі. Це потрібно для того, щоб тримати їх у курсі діла про хід виконання робіт.

ID у системі обліку помилок (bug tracking ID) – якщо ви використовуєте окрему систему обліку помилок, тоді у описі історії корисно зберігати посилання на всі дефекти, які до неї відносяться.

Sprint backlog – містить функціональність, обрану Product Owner із Product Backlog. Всі функції розбиті по задачах, кожна з яких оцінюється командою. Кожен день команда оцінює об'єм роботи, який необхідно провести для завершення задачі.

Burndown chart – показує, скільки вже виконано і скільки ще залишається зробити.

Планування спринта (Sprint Planning Meeting)

Проходить на початку нової ітерації Спринта:

– Із Product Backlog обираються задачі, зобов'язання по виконанню яких за спринт приймає на себе команда;

– На основі обраних задач створюється Sprint Backlog. Кожна задача оцінюється у ідеальних людино–годинах;

– Рішення задачі не повинно займати більше 12 годин або одного дня. При необхідності задача розбивається на підзадачі;

– Обговорюється та визначається, яким чином буде реалізовано цей об'єм робіт;

– Тривалість наради обмежена зверху 4–8 годинами в залежності від тривалості ітерації, досвіду команди тощо;

– (перша частина наради) Беруть участь Product Owner + Команда: обирають задачі із Product Backlog;

– (друга частина наради) Бере участь лише команда: обговорюють технічні деталі реалізації, наповнюють Sprint Backlog.

Щоденна нарада (Daily Scrum Meeting)

Відбувається кожен день протягом спринта. Є «пульсом» ходу спринта. Нараді властиві наступні обмеження:

– починається точно вчасно;

– всі можуть спостерігати, але говорять тільки обрані;

– триває не більш ніж 15 хвилин;

– проводиться в одному і тому ж місці протягом одного спринта.

Протягом наради кожен член команди відповідає на 3 запитання:

– Що зроблено з моменту попередньої щоденної наради?

– Що буде зроблено з моменту поточної наради до наступної?

– Які проблеми заважають досягненню цілей спринта? (Над рішенням цих проблем працює ScrumMaster. Зазвичай це рішення проходить за рамками щоденної наради і у складі осіб, що безпосередньо займаються даною перешкодою).

Демонстрація (Sprint Review Meeting):

– Проходить у кінці ітерації (спринта).

– Команда демонструє внесок функціональності до продукту всім зацікавленим особам.

– Залучається максимальна кількість глядачів.

– Усі члени команди беруть участь у демонстрації (одна людина на демонстрацію або кожен показує, що зробив за спринт).

– Обмежена 4–ма годинами в залежності від тривалості ітерації і змін у продукті.

Ретроспектива (Sprint Retrospective):

– Члени команди висловлюють свою думку про минулий спринт.

– Відповідають на два основних запитання: Що було зроблено добре у минулому спринті?; Що потрібно покращити в наступному?

– Виконують покращення процесу розробки (вирішують питання та фіксують вдалі рішення).

– Обмежена 1–3ма годинами.

Під час роботи над бакалаврською дипломною роботою було створено блок-схеми. Перед їх розглядом необхідно провести роз’яснення який саме тип блок-схем використовується.

Блок-схема це представлення задачі для її аналізу або розв'язування за допомогою спеціальних символів (геометричних образів), які позначають такі елементи, як операції, потік, дані тощо. Блок вхідних та вихідних даних прийнято позначати паралелограмом, блок обчислень (обробки) даних – прямокутником, блок прийняття рішень – ромбом, еліпсом – початок та кінець алгоритму.

У інформаційних технологіях функціональна схема складається з функціональних блоків, які являють собою конструктивно відособлені частини (елементи або пристрої) автоматичних систем, які виконують певні функції. Функціональні блоки на схемі позначають прямокутниками, всередині яких надписують їх найменування відповідно до функцій, що виконуються. Зв'язки між функціональними блоками (внутрішні впливи) позначаються лініями зі стрілками, які вказують напрям впливів.

Функціональні схеми можуть виконуватися в укрупненому і розгорненому вигляді. У першому випадку на схемі зображають найважливіші блоки системи і зв'язки між ними.

У другому варіанті схема відображається більш детально, що полегшує її читання та ілюструє принцип роботи.

Основні елементи схем алгоритму це термінатор, процес, рішення, зумовлений процес (підпрограма), дані та з'єднувач.

Термінатор це елемент відображає вхід із зовнішнього середовища або вихід з неї (найчастіше застосування – початок і кінець програми). Всередині фігури записується відповідна дія.

Процес це виконання однієї або кількох операцій, обробка даних будь-якого виду (зміна значення даних, форми подання, розташування). Всередині фігури записують безпосередньо самі операції.

Рішення це показує рішення або функцію перемикального типу з одним входом і двома або більше альтернативними виходами, з яких тільки один може бути обраний після обчислення умов, визначених всередині цього елементу. Вхід в елемент позначається лінією, що входить зазвичай у верхню вершину елементу.

Якщо виходів два чи три то зазвичай кожен вихід позначається лінією, що виходить з решти вершин (бічних і нижній). Якщо виходів більше трьох, то їх слід показувати однією лінією, що виходить з вершини (частіше нижній) елемента, яка потім розгалужується. Відповідні результати обчислень можуть записуватися поруч з лініями, що відображають ці шляхи.

Зумовлений процес (підпрограма) це символ відображає виконання процесу, що складається з однієї або кількох операцій, що визначені в іншому місці програми (у підпрограмі, модулі). Всередині символу записується назва процесу і передані в нього дані.

Дані це перетворення у форму, придатну для обробки (введення) або відображення результатів обробки (виведення). Цей символ не визначає носія даних (для вказівки типу носія даних використовуються специфічні символи).

З'єднувач це символ відображає вихід в частину схеми і вхід з іншої частини цієї схеми. Використовується для обриву лінії та продовження її в іншому місці (приклад: поділ блок-схеми, що не поміщається на листі). Відповідні сполучні символи повинні мати одне (при тому унікальне) позначення.

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 системи забезпечення безпеки критичних ресурсів АСУ ТП.

На рисунку 4.1 зображена основна блок-схема програми, на рисунку 4.2 зображено роботу підпрограми.

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

підпрограми та останньої стадії – перевірка поточного стану з завершенням роботи розробленого ПЗ.

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

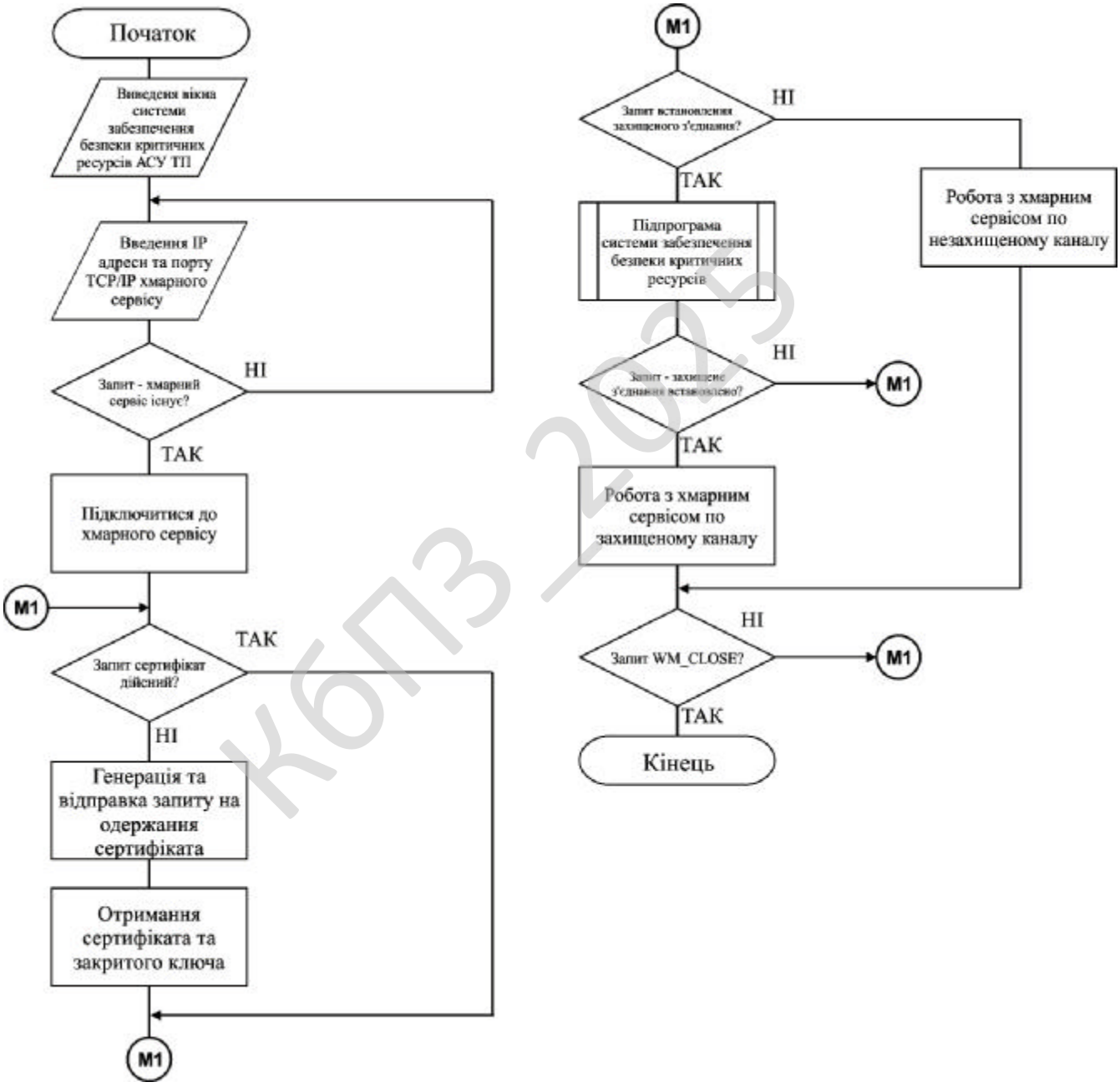

Рисунок 4.1 – Блок-схема основної програми

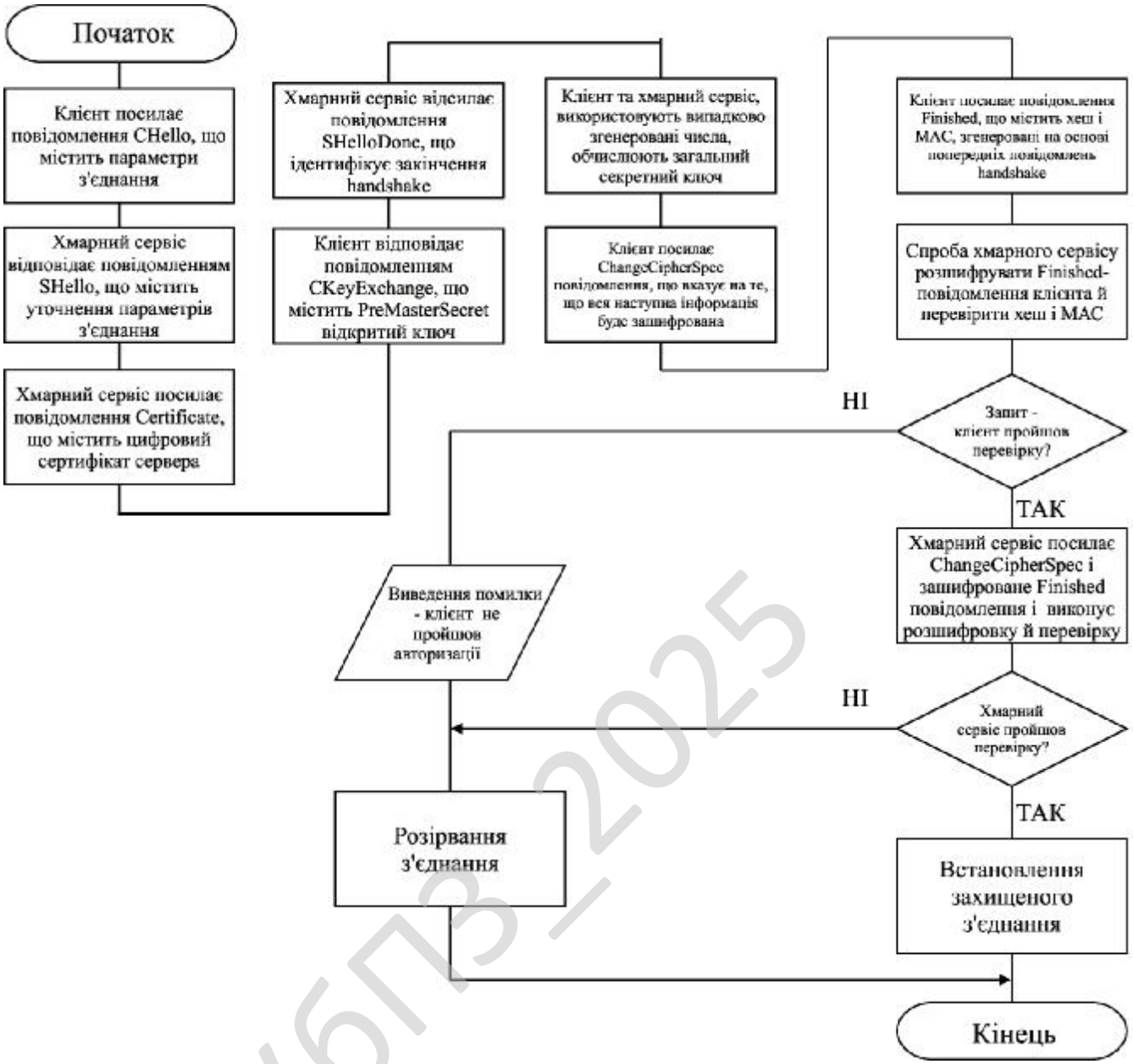

Рисунок 4.2 – Блок-схема роботи підпрограми

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.

Redmine – вільне серверне ПЗ для управління проектами та відстежування помилок. До системи входить календар-планувальник та діаграми Ганта для візуального представлення ходу робіт за проектом та строків виконання. Redmine написано на мові Ruby і є ПЗ розробленим з використанням відомого веб-фреймворку Ruby on Rails, що означає легкість в розгортанні системи та її адаптації під конкретні вимоги. Для кожного проекту можна вести свої вікі та форуми.

Функціональні можливості:

– Ведення декількох проектів.

– Гнучка система доступу з використанням ролей.

– Система відстеження помилок.

– Діаграми Ганта та календар.

– Ведення новин проекту, документів та управління файлами.

– Сповіщення про зміни за допомогою RSS-потоків та електронної пошти.

– Власна Wiki для кожного проекту.

– Форуми для кожного проекту.

– Облік часових витрат.

– Налаштування власних (custom) полів для задач, затрат часу, проектів та користувачів.

– Легка інтеграція із системами керування версіями (SVN, CVS, Git, Mercurial, Bazaar и Darcs).

– Створення записів про помилки на основі отриманих листів

– Підтримка LDAP автентифікації.

– Можливість самореєстрації нових користувачів.

– Багатомовний інтерфейс (у тому числі українська мова).

– Підтримка СКБД: MySQL, PostgreSQL, SQLite.

Діаграма Ганта (*Gantt chart*, також стрічкова діаграма, графік Ганта) – це популярний тип діаграм, який використовується для ілюстрації плану, графіка робіт за будь-яким проектом. Є одним з методів планування та управління проектами.

Діаграма Ганта являє собою відрізки (графічні плашки), розміщені на горизонтальній шкалі часу. Кожен відрізок відповідає окремому завданню або підзадачі. Завдання і підзадачі, складові плану, розміщуються по вертикалі. Початок, кінець і довжина відрізка на шкалі часу відповідають початку, кінцю і тривалості завдання. На деяких діаграмах Ганта також показується залежність між завданнями.

Діаграма може використовуватися для представлення поточного стану виконання робіт: частина прямокутника, що відповідає завданню, заштриховується, відзначаючи відсоток виконання завдання; показується вертикальна лінія, що відповідає моменту «сьогодні».

Часто діаграма Ганта використовується спільно з таблицею зі списком робіт, рядки якої відповідають окремо взятій задачі, зображеній на діаграмі, а стовпці містять додаткову інформацію про задачу.

Система відстеження помилок Багтрекер – прикладна програма для допомоги розробникам програмного забезпечення (програмістам, тестувальникам тощо) враховувати і контролювати помилки, знайдені у програмах, питання щодо функціональності, рішення та оновлення, побажання користувачів, а також стежити за процесом їх виконання.

Кожному, хто розробляв програмні продукти, добре знайоме співвідношення «20/80» – останні 20 % роботи тривають 80 % часу.

Як це не парадоксально, але нічого дивного в цій пропорції немає, адже саме на завершальній стадії починається тестування проекту, коли виявляються помилки, і що більший проект, то більше буде знайдено помилок.

Водночас досить часто виявляється, що більшість цих помилок були відомі та могли бути виправлені з меншими витратами на попередніх стадіях роботи, але не були вчасно описані, а потім загубилися серед інших важливих завдань.

Отже, система відстеження помилок у найпростішому варіанті – це процес, що включає в себе виявлення помилки, її опис, виправлення і перевірку цього виправлення, тобто процес «стеження» за багом протягом всього як його життєвого циклу, так і життєвого циклу розробки в цілому.

Сукупність інформації про дефект. Головний компонент такої системи – база даних, що містить відомості про виявлені дефекти. Ці відомості можуть включати в себе:

– номер (ідентифікатор) дефекту;

– хто повідомив про дефект;

– дата і час виявлення дефекту;

– версія продукту, в якій виявлено дефект;

– серйозність (критичність) дефекту та пріоритет рішення;

– опис кроків для відтворення дефекту (неправильної поведінки програми);

– відповідальний за усунення дефекту;

– обговорення можливих рішень та їх наслідків;

– поточний стан виправлення дефекту;

– версії продукту, в якій дефект виправлений.

Крім того, розвинені системи надають можливість прикріплювати файли, які допомагають описати проблему, наприклад, дамп пам'яті або скріншот.

Використання. Основна перевага систем відстеження помилок полягає в забезпеченні чітких централізованих оглядів, запитів на розробку (включаючи помилки і виправлення) та їх стан. У корпоративному середовищі, системи відстеження помилок можуть бути використані для генерації звітів по продуктивності програмістів виправлення помилок. Однак, це може іноді

приводити до неточних результатів, тому що різні помилки можуть мати різні ступені пріоритету та серйозності, що пов'язано з складністю їх фіксації.

Життєвий цикл дефекту. Як правило, система відстеження помилок використовує той чи інший варіант «життєвого циклу» помилки, стадія якого визначається поточним станом помилки.

Типовий життєвий цикл дефекту:

1. Новий – дефект зареєстрований тестувальником.

2. Призначений – призначений відповідальний за виправлення дефекту.

3. Дозволений – дефект переходить назад у сферу відповідальності тестувальника. Як правило, супроводжується резолюцією, наприклад:

– Виправлено (виправлення включені у версію таку-то).

– Дубль (повторює дефект, що вже знаходиться в роботі).

– Не виправлено (працює відповідно до специфікації, має занадто низький пріоритет, виправлення відкладено до наступної версії тощо).

– «В мене все працює» (запит додаткової інформації про умови, в яких дефект проявляється).

4. Далі тестувальник проводить перевірку виправлення, залежно від чого дефект або знову переходить у стан «Призначений» (якщо він описаний як виправлений, але не виправлений), або у стан «Закрито».

5. Відкрито повторно – дефект знайдено знову в іншій версії.

Система може надавати адміністраторові можливість налаштування користувачі, які можуть переглядати і редагувати помилки залежно від їх стану, переводити їх в інший стан або видаляти.

У корпоративному середовищі, система відстеження помилок може використовуватися для отримання звітів, що показують продуктивність програмістів при виправленні помилок. Однак, часто такий підхід не дає достатньо точних результатів через те, що різні помилки мають різну ступінь серйозності та складності. При цьому серйозність проблеми прямо не стосується складності її усунення.

4.2 Захист розробленого програмного забезпечення

Для захисту розробленого програмного забезпечення запропоновано використовувати алгоритм Madryga. Алгоритм Madryga складається із двох вкладених циклів. Зовнішній цикл повторюється вісім разів (для гарантії надійності число циклів можна збільшити) і полягає в застосуванні внутрішнього циклу до відкритого тексту. Внутрішній цикл перетворює відкритий текст у шифртекст і виконується однократно над кожним 8-бітовим блоком (байтом) відкритого тексту. Таким чином, весь відкритий текст послідовно вісім разів обробляється алгоритмом. Ітерація внутрішнього циклу оперує з 3-байтовим вікном даних, називаним робочим кадром (рисунок 4.3). Це вікно зрушується на 1 байт за ітерацію. (При роботі з останніми 2 байтами дані покладаються циклічно замкнутими). Перші два байти робочого кадру циклічно зрушуються на змінне число позицій, а для останнього байта виконується операція XOR з декількома бітами ключа. У міру переміщення робочого кадру всі байти послідовно циклічно зрушуються й піддаються операції XOR із частинами ключа. Послідовні циклічні зрушення перемішують результати попередніх операцій XOR і циклічного зрушення, причому на циклічне зрушення впливають результати XOR. Завдяки цьому процес у цілому оборотний. Оскільки кожний байт даних впливає на два байти ліворуч і на один байт праворуч від себе, після восьми проходів кожний байт шифртексту залежить від 16 байтів ліворуч і 8 байтів праворуч.

При шифруванні кожна ітерація внутрішнього циклу встановлює робочий кадр на передостанній байт відкритого тексту й циклічно переміщає його до третього з кінця байту відкритого тексту. Спочатку весь ключ піддається операції XOR з випадковою константою й потім циклічно зрушується вправо на 3 біти (ключ і дані рухаються в різних напрямках, щоб мінімізувати надлишкові операції з бітами ключа). Молодші три біти молодшого байта робочого кадру зберігаються, вони визначають циклічне зрушення інших двох байтів. Далі конкатенація двох старших байтом циклічно зрушується вліво на змінне число

біт (від 0 до 7). Потім над молодшим байтом робочого кадру виконується операція XOR з молодшим байтом ключа. Нарешті робочий кадр зміщається вправо на один байт і весь процес повторюється.

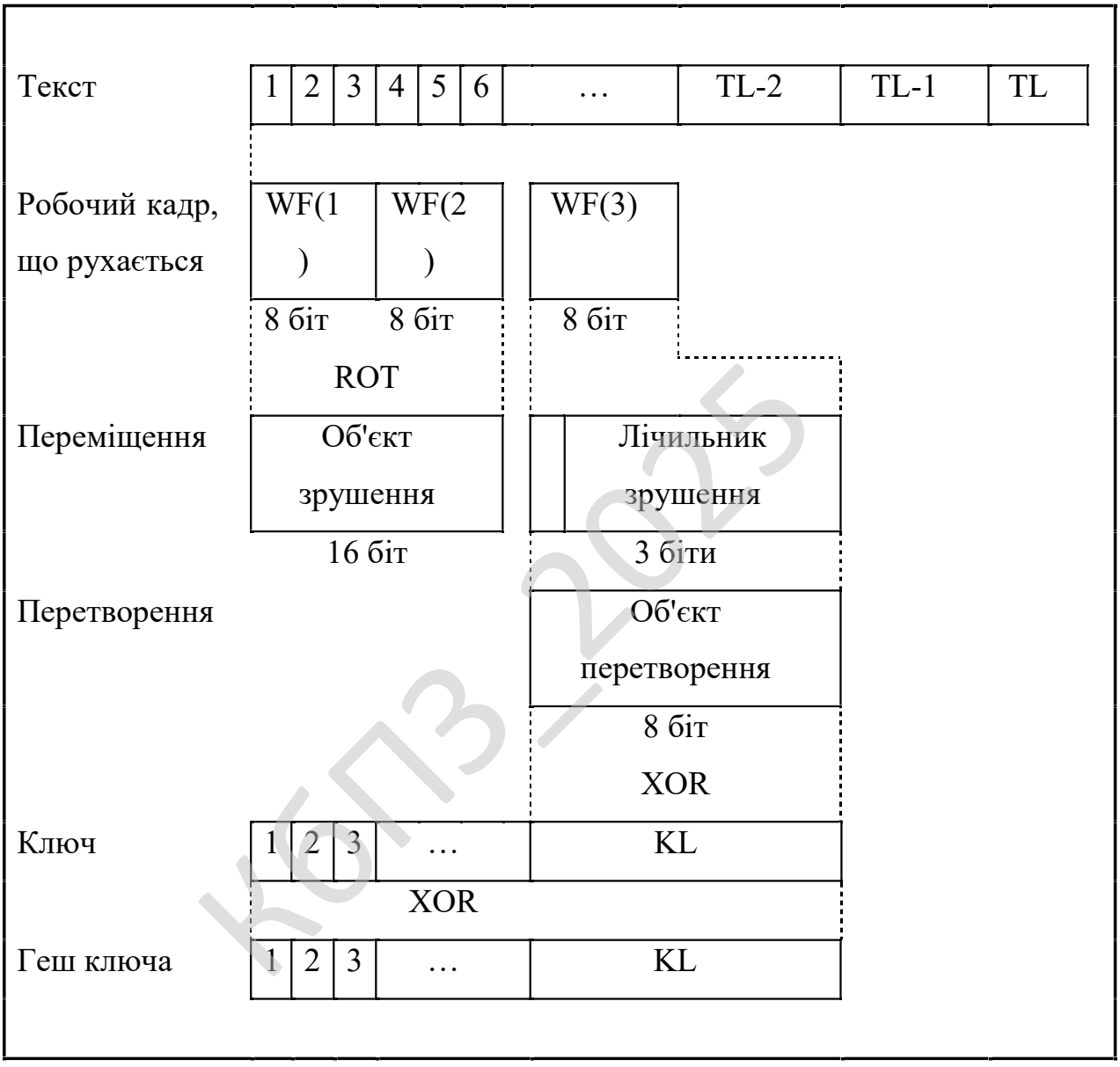

Рисунок 4.3 – Одна ітерація алгоритму Madryga

Випадкова константа призначена для перетворення ключа в псевдовипадкову послідовність. Довжина константи повинна бути рівній довжині ключа. При обміні даними абоненти повинні користуватися однієї й тією же константою. Для 64-бітового ключа Madryga рекомендує константу

0x0fle2d3c4b5a6978. При розшифруванні процес повторюється у зворотному порядку. У кожній ітерації внутрішнього циклу робочий кадр установлюється на байт, третій ліворуч від останнього байта шифртексту, і циклічно зрушується у зворотному напрямку до байта, розташованого на 2 байти уліво відносно останнього байта шифртексту. 2 байти шифртексту в процесі циклічно зрушуються вправо, а ключ – уліво. Після циклічних зрушень виконується операція XOR.

5 МЕТОДИКА ВПРОВАДЖЕННЯ СИСТЕМИ В ПРОМИСЛОВУ ЕКСПЛУАТАЦІЮ

Розглянемо розроблене ПЗ системи забезпечення безпеки критичних ресурсів АСУ ТП яке зображено на рисунку 5.1. З рисунку можна побачити що інтерфейс головного вікна розподілено на наступні функціональні розділи:

– Функцій введення серверних даних.

– Функціональних кнопок ПЗ – функціонал системи відповідно до технічного завдання.

– Розділу виведення результату роботи системи.

– Навігаційного меню яке викликається натисканням правої клавіші маніпулятора миші.

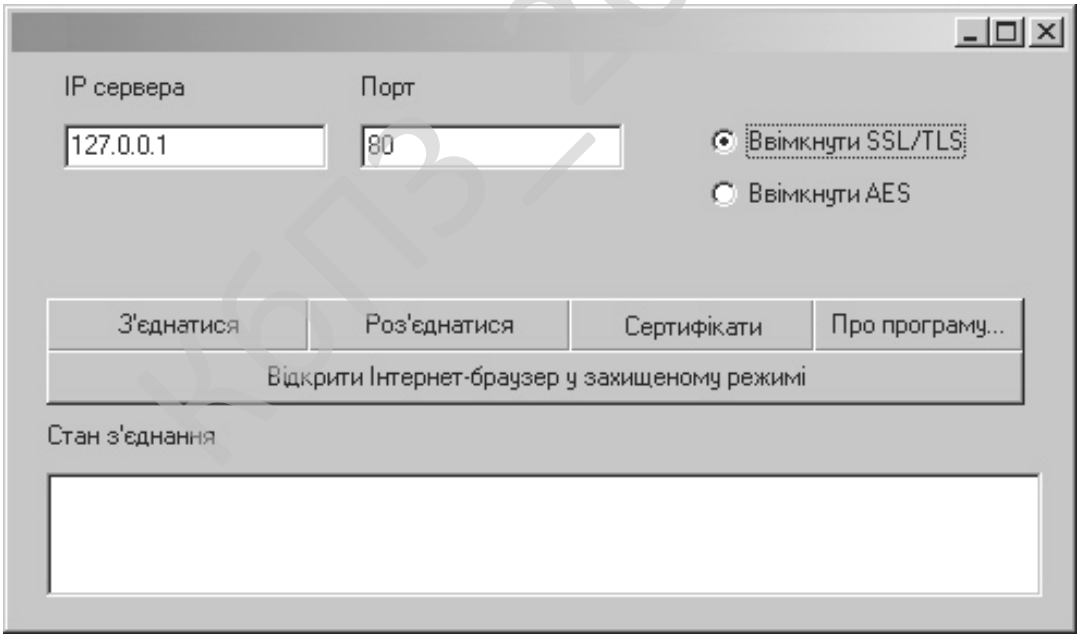

Рисунок 5.1 – Головне вікно ПЗ

Розроблена програма має дуже простий і інтуїтивно зрозумілий інтерфейс з користувачем. Кожен, хто в достатньому обсязі володіє операційним

середовищем Windows без особливих складностей освоїть і цю програму, оскільки її інтерфейс інтуїтивно зрозумілий.

Якщо програма не видала ніяких помилок, і працює, то можна використовувати, інакше слід слідувати інструкціям, які пропонує програма.

На рисунку 5.2 зображено авторські дані розробленого програмного забезпечення.

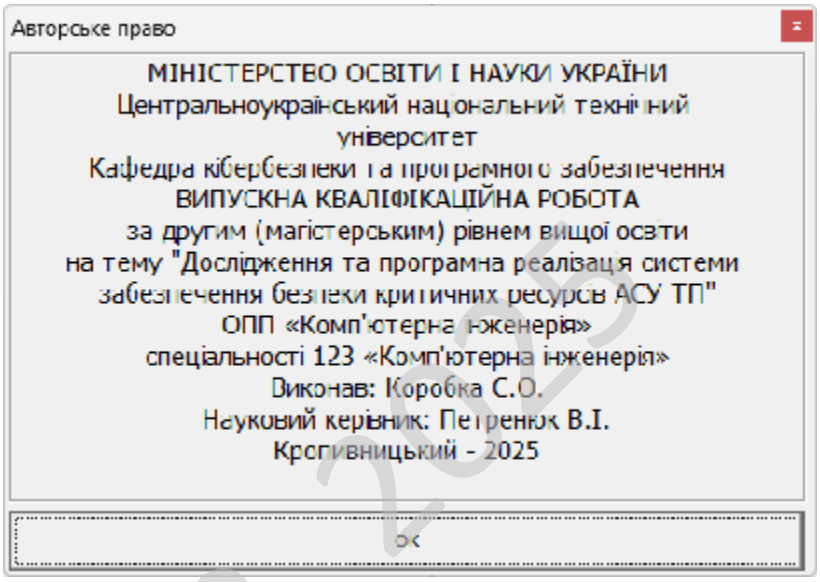

Рисунок 5.2 – Авторське право

Розглянемо процес впровадження програмного забезпечення, це процес налаштування програмного забезпечення під певні умови використання, а також навчання користувачів роботі з програмним продуктом. Впровадження програмного забезпечення це усі дії, що роблять розроблену програмну систему готовою до використання. Даний процес є частинною життєвого циклу програмного забезпечення.

Загалом процес розгортання складається з кількох взаємопов'язаних дій із можливими переходами між ними. Ця активність може відбуватися як з боку виробника так і з боку споживача. Оскільки кожна програмна система є унікальною, то усі процеси та процедури під час розгортання важко передбачити.

Тому, "розгортання" можна трактувати як загальний процес відповідно до певних вимог та характеристик. Розгортання може здійснюватись програмістом і в процесі розробки програмного забезпечення.

До діяльностей пов'язаних із розгортанням програмного забезпечення відносять:

– Випуск.

– Встановлення та активація.

– Деактивація.

– Адаптація.

– Обновлення.

– Вмонтування.

– Відстежування версій.

– Видалення.

– Вилучення з обігу.

При впровадженні програмного забезпечення потрібно урахувати наступні дії:

– Виділення критичних, з точки зору загального результату, процедур в діяльності організації. Коли набір таких процедур визначений, необхідно в першу чергу використовувати ІТ рішення для автоматизації операцій усередині саме цих процедур. Таким чином, розроблене ІТ рішення автоматично стає життєво важливим і затребуваним для організації, а також буде забезпечена публічність процесу впровадження.

– Розширення нормативної бази організації шляхом включення до неї регламентів, що описують порядок виконання процедур автоматизованих процесів. В іншому випадку є небезпека виникнення неузгодженості між автоматизованими процедурами та іншими процесами організації.

– Виконання робіт з загальної стандартизації існуючої діяльності організації, коли виділяються кращі практики виконання процедур і включаються в ІТ рішення за принципом найбільшої корисності для більшості учасників.

Відсоток таких процедур щодо загального обсягу автоматизації може бути невеликий, але це надає процесу побудови рішення вагу в організації за рахунок збільшення його необхідності.

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.

Проводилось тестування чорної скриньки.

Основне місце програми тестів «чорної скриньки» – інтерфейс ПЗ. Відомі: функції програми. Досліджується: робота кожної функції на всій області визначення.

Ці тести демонструють:

– Як виконуються функції програми.

– Як приймаються вихідні дані.

– Як виробляються результати.

– Як зберігається цілісність зовнішньої інформації.

При тестуванні «чорної скриньки» розглядаються системні характеристики програм, ігнорується їхня внутрішня логічна структура. Вичерпне тестування, як правило, неможливе.

Наприклад, якщо в програмі 10 вхідних величин і кожна приймає по 10 значень, то кількість тестових варіантів становитиме 10^10. Тестування «чорної скриньки» не реагує на багато особливостей програмних помилок.

Тестування «чорної скриньки» (функціональне тестування) дозволяє отримати комбінації вхідних даних, які забезпечують повну перевірку всіх функціональних вимог до програми.

Програмний виріб тут розглядається як «чорна скринька», чию поведінку можна визначити тільки дослідженням його входів та відповідних виходів. При такому підході бажано мати:

– Набір, утворений такими вхідними даними, які призводять до аномалій у поведінці програми (назвемо його ITc).

– Набір, утворений такими вхідними даними, які демонструють дефекти програми (назвемо його OT).

Будь-який спосіб тестування «чорної скриньки» повинен:

– Виявити такі вхідні дані, які з високою ймовірністю належать набору ITc;

– Сформулювати такі очікувані результати, які з високою імовірністю є елементами набору OT.

Принцип «чорної скриньки» не альтернативний принципу «білої скриньки». Скоріше це доповнює підхід, який виявляє інший клас помилок.

Тестування «чорної скриньки» забезпечує пошук наступних категорій помилок:

– Некоректних чи відсутніх функцій.

– Помилок інтерфейсу.

– Помилок у зовнішніх структурах даних або в доступі до зовнішньої бази даних.

– Помилок характеристик (необхідна ємність пам'яті і т.д.).

– Помилок ініціалізації та завершення.

Обрано умови розповсюдження – proprietary software. Програмне забезпечення, на яке зберігаються як немайнові, так і майнові авторські права.

Отримавши або придбавши таке програмне забезпечення, користувач отримує обмежені права користування ним: може бути заборонено або закрито доступ до коду (вивчення), внесення змін, тиражування, розповсюдження та перепродаж. Програмне забезпечення вважається власницьким, якщо наявне хоча б одне з перелічених обмежень.

Найчастіше основним методом захисту майнових прав на власницьке ПЗ, поза ліцензійною угодою, власник обирає закриття сирцевого коду, захищаючи свій продукт від модифікації і вбудовуючи системи обмеження користування через авторизацію. Таке програмне забезпечення називається закритим. Проте, код власницького продукту може бути і відкритим, але власник може обмежити права користувача умовами користувацької ліцензії.

Власницьке програмне забезпечення та комерційне програмне забезпечення не є синонімами – власницьким може бути і безплатне (тобто, некомерційне) програмне забезпечення.

На противагу власницькому ПЗ існує вільне програмне забезпечення, автори і власники якого дозволяють вивчати, модифікувати і поширювати свій продукт. Саме визначення власницького програмного забезпечення виникло в результаті діяльності громадського руху вільного програмного забезпечення (представленого Фондом вільного програмного забезпечення та іншими організаціями) і осмислення умов свободи користування програмами. Визначенням власницького програмного забезпечення є не невідповідність хоча б одній з базових умов вільного програмного забезпечення. Сама назва власницьке ПЗ підкреслює визначальне значення власника у способі використання і можливостях розвитку цього програмного забезпечення.

6 НАУКОВА НОВИЗНА

У випускній кваліфікаційній роботі за другим (магістерським) рівнем вищої освіти розроблено програмне забезпечення, яке призначено для системи забезпечення безпеки критичних ресурсів АСУ ТП.

Метою розробки є дослідження та програмна реалізація системи забезпечення безпеки критичних ресурсів АСУ ТП.

Об'єктом дослідження є процес забезпечення безпеки критичних ресурсів АСУ ТП.

Предметом дослідження є методи забезпечення безпеки критичних ресурсів АСУ ТП.

Методи дослідження базуються на методах захисту інформації у комп'ютерних мережах, методах математичної статистики, методах розробки програмного забезпечення.

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

– Удосконалено метод забезпечення безпеки критичних ресурсів АСУ ТП.

– Розроблено вітчизняний продукт забезпечення безпеки критичних ресурсів АСУ ТП, 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 практичної реалізації системи безпеки критичних ресурсів АСУ ТП можуть бути цікавими насамперед для промислових підприємств, які використовують автоматизовані системи управління технологічними процесами. Це компанії, що працюють у галузях енергетики, хімічного виробництва, транспорту, нафтогазового комплексу та харчової промисловості – усюди, де стабільність технологічних процесів безпосередньо впливає на прибутковість і безпеку. Для них система безпеки АСУ ТП стає не просто елементом технічного захисту, а ключовою умовою безперервності виробництва. Особливу зацікавленість можуть проявити ІТ-департаменти та відділи кібербезпеки підприємств, адже вони відповідають за захист промислових мереж від кібератак. У сучасних умовах, коли промислові об’єкти дедалі частіше стають мішенню зловмисників, впровадження ефективних засобів моніторингу, контролю доступу й реагування на загрози є критично важливим.

Результати дослідження також можуть бути корисними для державних структур, які займаються розробкою політик національної безпеки у сфері промислової кібербезпеки. Такі системи допомагають сформувати стандартизовані підходи до захисту критичної інфраструктури, що особливо актуально в контексті сучасних ризиків і вимог міжнародних стандартів. Крім того, навчальні та наукові заклади, які готують фахівців із промислової автоматизації та інформаційної безпеки, можуть використовувати цю систему як навчальний інструмент для вивчення взаємодії між ІТ-рівнем і технологічними процесами. Таким чином, розробка має широкий спектр потенційних користувачів – від промисловців до освітян і державних аналітичних центрів.

7.2 Оцінка привабливості шляхом застосування методів експертних оцінок

Для оцінки привабливості впровадження системи безпеки АСУ ТП було проведено експертне опитування серед спеціалістів промислових підприємств, IT-аналітиків і представників державних установ, які займаються регулюванням кіберзахисту. Критеріями оцінки виступали: рівень технічної складності, ефективність виявлення загроз, вартість впровадження, зручність інтеграції з існуючими системами, надійність та економічна доцільність.

Результати експертного аналізу показали, що система отримала середню оцінку 8,9 з 10 можливих. Найвищі бали експерти надали функціям моніторингу в реальному часі, сегментації мережі та можливості централізованого управління безпекою. Зокрема, відзначалося, що система здатна запобігати інцидентам ще на ранніх етапах, знижуючи ризик зупинки виробництва.

Експерти підкреслили, що важливою перевагою є масштабованість рішення – його можна адаптувати як для невеликого виробничого цеху, так і для енергетичного комплексу. Серед потенційних викликів називали потребу у високій кваліфікації персоналу та початкову вартість впровадження, але більшість учасників погодилися, що окупність системи виправдовує інвестиції.

Таким чином, експертна оцінка підтвердила доцільність реалізації системи безпеки критичних ресурсів АСУ ТП, оскільки вона забезпечує не лише технічну, а й стратегічну вигоду – підвищення стійкості виробництва й зниження операційних ризиків.

7.3 Вибір методу оцінки вартості ПЗ

Оцінюючи вартість впровадження системи безпеки АСУ ТП, доцільно застосувати комбінований підхід, який поєднує витратний та дохідний методи. Витратний метод дозволяє детально розрахувати реальні фінансові витрати на

створення системи – придбання серверного обладнання, програмного забезпечення, ліцензій, навчання персоналу, технічну підтримку та обслуговування. Це дає об’єктивне уявлення про початкову інвестицію.

Дохідний метод, у свою чергу, дозволяє оцінити економічну вигоду від зниження ризиків. Наприклад, запобігання навіть одному серйозному інциденту може заощадити підприємству сотні тисяч гривень, не кажучи вже про втрату даних чи репутаційні збитки. Також до переваг належить підвищення ефективності виробництва, адже стабільна робота АСУ ТП без збоїв зменшує простої обладнання й втрати продуктивності.

Використання саме такого підходу дозволяє не лише врахувати поточні витрати, а й показати реальну віддачу від інвестицій у вигляді зниження витрат на аварійні ремонти, запобігання інцидентам і підвищення надійності технологічних процесів.

Крім того, комбінований метод є універсальним і може бути використаний для залучення інвесторів або грантових коштів, оскільки демонструє як економічну ефективність, так і соціально-технологічну користь проєкту.

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

Підприємство працює у сфері енергетики й використовує АСУ ТП для контролю за технологічними процесами, обладнанням і потоками енергії. До впровадження системи кібербезпеки спостерігалися випадки несанкціонованого доступу, збій у роботі сенсорів та мережевих компонентів, що призводило до тимчасових зупинок технологічних ліній.

У середньому протягом року фіксувалося близько 5 інцидентів, які спричиняли простої виробництва від 1 до 4 годин. Це призводило до значних фінансових втрат, адже одна година простою системи коштувала підприємству

близько 100 000 грн. Крім того, відсутність централізованого контролю підвищувала ризик порушення безпеки даних і роботи критичних об’єктів.

Мета проєкту – впровадження системи забезпечення безпеки критичних ресурсів АСУ ТП, яка включає сегментацію мережі, міжмережеві екрани, систему виявлення вторгнень (IDS/IPS), контроль доступу, резервне копіювання даних і централізований моніторинг. Вхідні дані зафіксовано в таблиці 7.1.

Таблиця 7.1 – Вихідні дані для розрахунку

Показник	**До впровадження**	**Після впровадження**	**Економічний ефект**
Кількість інцидентів безпеки за рік	5	1	–4
Середня тривалість простою під час інциденту	2,5 год	0,5 год	–2 год
Втрати підприємства за 1 годину простою	100 000 грн	20 000 грн (мінімізовано за рахунок резервування)	–80 000 грн
Річні втрати від інцидентів	1 250 000 грн	10 000 грн	–1 240 000 грн
Вартість впровадження системи безпеки	—	900 000 грн	—
Щорічні витрати на обслуговування	—	120 000 грн	—

Розрахунок економічного ефекту демонструє наступне: зменшення збитків від простоїв АСУ ТП – 1 240 000 грн/рік, економія на аварійних ремонтах і ручному відновленні даних – орієнтовно 200 000 грн/рік, загальний річний економічний ефект – 1 440 000 грн/рік, чистий економічний ефект – 1 320 000 грн/рік, термін окупності – 0,68 року (~8 місяців), коефіцієнт рентабельності (ROI) – 147%.

Додаткові (немонетарні) переваги: зменшення ризику несанкціонованого доступу до АСУ ТП і саботажу технологічних процесів, підвищення надійності виробництва за рахунок резервування критичних вузлів і моніторингу, покращення репутації підприємства як безпечного й технологічно стійкого партнера, відповідність міжнародним стандартам безпеки (IEC 62443, ISO/IEC 27001), що відкриває можливості для участі в міжнародних проектах, можливість централізованого управління безпекою та швидкого реагування на загрози.

Таким чином, економічна ефективність проєкту проявляється не лише у прямій фінансовій економії, а й у довгостроковому підвищенні стабільності, безпеки та конкурентоспроможності підприємства в умовах зростання кіберзагроз.

7.5 Пропозиція алгоритму просування проєкту розробки ПЗ

Просування системи безпеки критичних ресурсів АСУ ТП має ґрунтуватися на демонстрації її практичної ефективності. Першим етапом має стати створення демонстраційної лабораторії, де потенційні замовники зможуть побачити роботу системи в реальних умовах. Візуалізація результатів, таких як виявлення вторгнень або швидке реагування на збої, викликає довіру та сприяє прийняттю рішення про впровадження. Далі варто представити систему на галузевих конференціях і виставках з промислової автоматизації та кібербезпеки. Це дозволить залучити увагу фахівців, інвесторів і представників великих підприємств. Важливо також створити серію публікацій у фахових виданнях, які б демонстрували аналітичні дані щодо ефективності системи у запобіганні

кіберінцидентам. Наступним етапом може стати партнерство з інтеграторами промислових систем, які зможуть пропонувати рішення своїм клієнтам у складі комплексних проєктів модернізації АСУ ТП. Така стратегія дозволить скоротити цикл продажу та вийти на нові ринки без значних маркетингових витрат. Просування також має передбачати підготовку технічних спеціалістів і сертифікацію персоналу, адже саме людський фактор є вирішальним у сфері промислової безпеки. Таким чином, правильний алгоритм просування передбачає поєднання демонстрації ефективності, освітньої підтримки та стратегічного партнерства.

7.6 Оптимізація каналів збуту та шляхів реалізації ПЗ

Для ефективної реалізації проєкту варто використовувати багаторівневу модель збуту, яка передбачає як прямі продажі великим промисловим підприємствам, так і співпрацю з інтеграторами промислових систем. Прямий контакт із клієнтом дозволяє краще враховувати специфіку його АСУ ТП, тоді як партнерська модель відкриває доступ до нових ринків через уже існуючі канали.

Додатково варто запровадити модель обслуговування за підпискою, коли клієнт платить не за продукт, а за послугу захисту. Це зручно для підприємств, які не можуть відразу інвестувати в повну систему, але готові користуватися її функціоналом поступово. Такий підхід забезпечує стабільний потік доходів і підвищує лояльність клієнтів. Розширення збуту можна забезпечити через цифрові платформи, де система пропонується у вигляді модульного рішення з можливістю кастомізації під конкретні потреби замовника. Онлайн-демонстрації, вебінари та кейси успішного впровадження допоможуть привернути увагу потенційних покупців.

Важливим елементом оптимізації є післяпродажний супровід: оперативна підтримка, оновлення, консультації. Це створює позитивний користувацький досвід і формує репутацію розробника як надійного партнера.

7.7 Визначення ключових факторів успіху конкретного проєкту

Ключовими факторами успіху такого проєкту є технологічна надійність, адаптивність і довіра користувачів. Система має бути здатною працювати безперервно, швидко реагувати на загрози та адаптуватися до змін у структурі АСУ ТП. Надійність у цій сфері – це не просто характеристика, а запорука безпеки підприємства.

Не менш важливим фактором є професіоналізм команди розробників і спеціалістів, які забезпечують впровадження. Їхній досвід і компетентність у промислових технологіях дозволяють уникати критичних помилок і гарантувати ефективну інтеграцію системи.

Ключову роль відіграє також постійне вдосконалення системи – оновлення алгоритмів, впровадження нових модулів аналізу, підтримка відповідності міжнародним стандартам безпеки. Це підвищує довіру клієнтів і забезпечує довгострокову життєздатність продукту.

І, нарешті, успіх проєкту визначається здатністю налагодити партнерські відносини з промисловими підприємствами. Там, де є комунікація, взаємна довіра та готовність до спільного вдосконалення, система безпеки АСУ ТП стає не просто програмним продуктом, а стратегічним елементом захисту бізнесу.

8 ЗАХОДИ З ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ

8.1 Вступ

Аналізуючи умови працівників ІТ-сфери, на перший погляд, може здатися, що працівники сфери інформаційних технологій не схильні до ризиків на виробництві, та якщо більш глибоко розглянути умови і специфіку праці фахівців сфері ІТ-індустрії, можна виявити ряд факторів які будуть мати негативний сплив на стан охорони праці, та на самого ІТ-фахівця зокрема.

Сюди можна віднести як невідповідність освітлення, так і високий рівень шуму, що негативно позначатимуться як на емоційному так і на фізичному стані фахівця, призводитимуть до зниження ефективності праці та виробничих травм.

Також, важливим моментом охорони праці ІТ-фахівця є врахування його психологічних можливостей (швидкість реакції, особливості пам'яті та уваги, емоційний стан тощо). Для того, щоб забезпечити ефективну роботу ІТ-фахівця, потрібно враховувати та максимально компенсувати такі негативні фактори як: надмірне нервово-емоційне навантаження, довготривалі статичні перевантаження, обмежена рухова активність.

Всі ці чинники призводить до різноманітних відхилень у стані здоров’я, зокрема до перевтоми, зниження фізичної та розумової працездатності, неврозів, захворювань серцево-судинної системи тощо.

Метою даного розділу є огляд конкретних умов праці спеціаліста у сфері ІТ-індустрії. Завданнями для даного розділу є: аналіз умов праці на робочому місці фахівця ІТ-індустрії, розробка конкретних рекомендацій щодо покрашення умов праці фахівців ІТ-індустрії, огляд пожежної безпеки на ІТ-підприємстві та розрахунок системи загального штучного освітлення виробничого приміщення де працюють ІТ-фахівці.

8.2 Аналіз умов праці на робочому місці ІТ-фахівця

На робочому місці ІТ-фахівця (або програміста) виникають небезпечні та шкідливі для безпечної життєдіяльності фактори:

– підвищений рівень шуму;

– недостатній рівень освітленості;

– шкідливі речовини;

– підвищений рівень електромагнітних випромінювань радіочастот;

– висока напруга електричної мережі;

– статична електрика та інші.

Робота супроводжується також підвищеним ступенем напруженості трудового процесу. При систематичному впливі виробничих факторів, які не відповідають нормативним показникам, зростає рівень професійно зумовленої захворюваності працюючих та можуть виникнути професійні захворювання органів зору, руху, нервової системи. Таким чином, вивчення умов праці на робочому місці програміста є необхідною умовою запобігання негативних наслідків впливу небезпечних та шкідливих факторів. Робоче місце, добре пристосоване до трудової діяльності інженера, правильно і доцільно організоване, щодо простору, форми, розміру забезпечує йому зручне положення при роботі і високу продуктивність праці при найменшому фізичному і психічному напруженні.

Нормування параметрів проводиться в залежності від періоду року та категорії важкості виконуваних робіт. Для постійних робочих місць, якими є робочі місця ІТ-фахівців, встановлені оптимальні параметри мікроклімату, а за неможливості їх дотримання використовують допустимі параметри. Робота ІТ-фахівця за важкістю відноситься до Іа (роботи, що виконуються сидячи і не потребують фізичного напруження) та Іб (роботи, що виконуються сидячи, стоячи або пов'язані з ходінням та супроводжуються деяким фізичним напруженням) категорій. В таблиці 8.1. наведені оптимальні параметри

мікроклімату в приміщеннях.

Виміряні за допомогою приладів температура та вологість у приміщеннях праці ІТ-фахівців повинні відповідати зазначеним у таблиці для теплого періоду року.

Таблиця 8.1 – Параметри мікроклімату для приміщень з ПК

Період року	Параметр мікроклімату	Величина
Холодний	Температура повітря в приміщенні; відносна вологість; швидкість руху повітря	22...24°С; 40... 60%; до 0,1 м/с
Теплий	Температура повітря в приміщенні; відносна вологість; швидкість руху повітря	23...25 °С 40...60% 0,1...0,2 м/с

Слід зазначити, що для нормалізації параметрів мікроклімату слід використовувати у приміщеннях кондиціювання повітря, або забезпечити подачу свіжого повітря системами вентиляції. Норми подачі свіжого повітря наведені у таблиці 8.2.

Таблиця 8.2 – Норми подачі свіжого повітря в приміщення

Характеристика приміщення	Об'ємна витрата свіжого повітря, що подається в приміщення, $м^3$ на одну людину в годину
Об'єм до 20 $м^3$ на людину 20... 40 $м^3$ на людину Більше 40 $м^3$ на людину	Не менше 30 Не менше 20 Може біти використана природна вентиляція

Створення сприятливих умов праці і правильне естетичне оформлення робочих місць на виробництві має велике значення як для полегшення праці, так і для підвищення його привабливості, позитивно впливає на продуктивність праці. Забарвлення приміщень і меблів повинні сприяти створенню сприятливих умов для зорового сприйняття, гарного настрою. У службових приміщеннях, у яких виконується одноманітна розумова робота, що вимагає значної нервової напруги і великого зосередження, забарвлення повинно бути спокійних тонів – мало насичені відтінки холодного зеленого або блакитного кольорів.

При розробці оптимальних умов праці програміста необхідно враховувати освітленість. Раціональне освітлення робочого місця є одним з найважливіших факторів, що впливають на ефективність трудової діяльності людини, що попереджають травматизм і професійні захворювання. Правильно організоване освітлення створює сприятливі умови праці, підвищує працездатність і продуктивність праці. Освітлення на робочому місці програміста повинно бути таким, щоб працівник міг без напруги зору виконувати свою роботу. Стомлюваність органів зору залежить від ряду причин: недостатність освітленості; надмірна освітленість; неправильний напрям світла. Недостатність освітлення приводить до напруги зору, ослабляє увагу, приводить до настання передчасної стомленості. Надмірно яскраве освітлення викликає засліплення, роздратування і різь в очах. Неправильний напрямок світла на робочому місці може створювати різкі тіні, відблиски, дезорієнтувати працюючого. Всі ці причини можуть призвести до нещасного випадку або профзахворювань. [2]

8.3 Пропозиції щодо підвищення працездатності ІТ-фахівців

Поява та впровадження нових інформаційно-комунікаційних технологій зумовлює необхідність подальшого вдосконалення охорони праці фахівців ІТ-індустрії. Все це потребує розробки нових нормативно-правових актів з регламентації праці та відпочинку фахівців ІТ-індустрії і стандартів підприємств,

центрів комп'ютерної техніки, центрів інформаційних технологій, сучасних комп'ютерних класів. Для підвищення розумової працездатності то зорової роботи повинна здійснюватися ергономічна оптимізація в рамках системи «оператор-термінал», яка сприятиме результативній фізичній та інтелектуальний працездатності і відновленню психосоматичного здоров'я фахівців ІТ-індустрії. Всі наведені заходи щодо вдосконалення охорони праці фахівців ІТ-індустрії повинні контролюватися службою охорони праці та комісією з охорони праці підприємства. Особливе значення у соціальному захисті цієї категорії працівників належить прийняття комплексного договору, який може забезпечити фахівців додатковими пільгами та компенсаціями.

Для більшого розуміння, пропозиції щодо підвищення працездатності ІТ-фахівців, розіб'ємо на декілька категорій:

1. Середовище і розпорядок праці. Для мінімізації негативних ефектів, що пов'язані з перевтомленням ІТ-фахівців, потрібно чітко прописати і реалізувати графік періодів праці-відпочинку, щоб фахівець міг можливість переключити увагу, дати можливість відпочити очам, мозку, елементарно, встати розім'яти ноги. Також потрібно зробити максимально комфортними умови мікроклімату у офісному приміщенні, де працюють ІТ-фахівці. Мається на увазі встановлення і експлуатація, коли виникає необхідність, кондиціонерів, опалення, та системи вентиляції, задля попередження перегрівання, переохолодження ІТ-фахівців, і подальшої неможливості ними виконувати свої функції. Також, за можливості, нами пропонується введення практики віддаленої праці ІТ-фахівцями, якщо роботодавець не може забезпечити оптимальні і безпечні умови в офісному приміщенні, або якщо фахівця вони не влаштовують із певних причин.

2. Фізичні і психоемоційні чинники. Першим і найважливішим чинником, що впливає на працездатність ІТ-фахівців є робоче місце, і саме тому, роботодавець має забезпечити максимальний його комфорт і безпеку. Гарантією цих факторів може слугувати сертифікація меблів, що використовуються на підприємстві ІТ-галузі. Тому нами пропонується закупівля тільки меблів, які

пройшли сертифікацію на відповідність. Під психоемоційними чинниками ми розуміємо гарне самопочуття фахівців, позитивний настій, гарний психологічний клімат у колективі, тощо. Задля того, щоб психоемоційні чинники мали максимально позитивний ефект, керівництву слід поводити заходи, які сприятимуть укріпленню і покращенню міжособистісних стосунків у колективі, таких як психологічні тренінги, таймбілдінг, спортивні змагання і естафети. Також, сюди можна віднести розробку і впровадження системи мотивації працівників, як фінансової, так моральної і адміністративної.

8.4 Розрахунок системи загального штучного освітлення виробничого приміщення де працюють ІТ-фахівці

Приміщення з ПК повинні мати природне і штучне освітлення, яке відповідало б вимогам ДБН В.2.5-28-2006 «Природне і штучне освітлення», ДСАНПІН 3.3.2.007-98 «Гігієнічні вимоги до організації роботи з візуальними дисплейними терміналами електронно-обчислювальних машин».

Приміщення для роботи із ПЕОМ повинні мати природне й штучне освітлення. Віконні прорізи повинні бути орієнтовані на північ або на північний схід, забезпечувати коефіцієнт природної освітленості не менш 1,5% і мати жалюзі або штори. Віконні прорізи повинні мати регульовані пристрої для відкривання, а також жалюзі, завіски, зовнішні козирки тощо. Приміщення із ПЕОМ повинні бути обладнані системою загального рівномірного освітлення. У виробничих і адміністративно-суспільних приміщеннях, де переважно ведеться робота з документами, допускається комбінована система штучного освітлення. Штучне освітлення має здійснюватися системою загального рівномірного освітлення, яка включає суцільні або такі, що перериваються, лінії світильників, розташованих збоку робочих місць (переважно ліворуч), паралельно лінії зору користувачів ПК. Світильники повинні мати розсіювачі світла. У світильниках місцевого освітлення можна використовувати лампи накалювання. При

розміщенні ПК по периметру приміщення лінії світильників штучного освітлення повинні розміщуватися локально над робочими місцями. Система освітлення робочого місця користувача ПК має відповідати наступним вимогам (рис. 8.1).

Рисунок 8.1 – Вимоги до системи освітлення робочого місця користувача ПК

Освітленість на робочому столі користувача в зоні розташування документів має бути в межах 300-500 лк. Якщо цей рівень освітленості неможливо забезпечити системою загального освітлення то допускається застосування світильників місцевого освітлення, але при цьому не повинно бути відблисків на поверхні екрану (яскравість відблисків не повинна перевищувати 40 кд/м^2) та перевищення його освітленості більше ніж 300 лк. Яскравість світильників загального освітлення, а також яскравість стелі при застосуванні

системи відбитого освітлення не повинна перевищувати 200 кд/м^2. Величина коефіцієнта пульсації освітленості не повинна перевищувати 5%. Що стосується розподілу яскравості в полі зору працюючих за дисплеями ПК, то відношення значень яскравості робочих поверхонь не повинно перевищувати 3:1

Проведемо розрахунок штучного освітлення за методом коефіцієнта використання світлового потоку для приміщення ширина якого складає 6 м, довжина – 7 м, висота – 2,9 м. У зазначеному приміщенні працює 7 людей.

Для того, щоб визначити потрібну кількість світильників, які повинні забезпечити нормований рівень освітленості, визначимо світловий потік, що падає на робочу поверхню за формулою [1]:

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

де:

F – світловий потік, що розраховується, Лм;

E – нормована мінімальна освітленість, Лк; *E = 300 Лк;*

S – площа освітлюваного приміщення (у нашому випадку S=6 х 7 = 42 *м*^{2});

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

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

n – коефіцієнт використання світлового потоку, (відношення світлового потоку, що падає на розрахункову поверхню, до сумарного потоку всіх ламп і обчислюється в долях одиниці [8]; 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%.

Обчислимо індекс приміщення за формулою:

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

де:

S – площа приміщення, *S* = 42 *м*^{2}*;*

h – розрахункова висота підвісу, *h* = 2,9 *м (співпадає з в*исотою стелі, т.я. лампи освітлення закріплюються на стелі)*;*

A – ширина приміщення, *A = 6 м;*

B – довжина приміщення, *B* = 7 *м.*

Підставимо всі значення у формулу та визначимо індекс приміщення: i=1,4.

Знаючи індекс приміщення, за довідковими даними знаходимо *n = 0,29 (з табличних даних коефіцієнтів використання світлового потоку (n) світильників з відповідним типом лампам) [8]*. Підставимо всі значення у формулу, визначимо світловий потік: *F=71689 Лм.*

Для розрахунку будемо використовувати *світлодіодні стельові панелі* Delux LED Panel 41 44Вт., світловий потік яких $F_л$ = 3600 *Лм.*

Кількість світильників визначається по формулі:

$$N=F/F_л$$

де:

F – світловий потік,

$F_л$ – світловий потік однієї лампи.

Підставимо всі значення у формулу та визначимо кількість світильників приміщення:

$$N= 71689 / 3600=19,9 \text{ шт.}$$

Приймаємо необхідну кількість *світлодіодних світильників* 20 шт.

8.5 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 умов праці на робочому місці ІТ-фахівця, 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 умов поліпшення охорони праці.

9 ОСНОВНІ ВИСНОВКИ

Програмне забезпечення, створене в результаті виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти, призначено для системи забезпечення безпеки критичних ресурсів АСУ ТП.

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 забезпечення безпеки критичних ресурсів АСУ ТП.

Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем забезпечення безпеки критичних ресурсів АСУ ТП.

– Досліджена система забезпечення безпеки критичних ресурсів АСУ ТП.

– На основі отриманих результатів досліджень створена програмна реалізація системи забезпечення безпеки критичних ресурсів АСУ ТП.

Розроблені під час виконання випускної кваліфікаційної роботи за другим (магістерським) рівнем вищої освіти алгоритми дозволяють успішно вирішувати завдання забезпечення безпеки критичних ресурсів АСУ ТП.

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 Visual C++. 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 Madryga.

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. Коробка С.О. Дослідження та програмна реалізація системи забезпечення безпеки критичних ресурсів АСУ ТП // Збірник праць молодих науковців ЦНТУ. – Вип. 15. – Кропивницький: ЦНТУ, 2025.

2. Loren Kohnfelder. Designing Secure Software. No Starch Press. 2022. 332 p.

3. Samir Kumar Rakshit. Ethical Hacker's Penetration Testing Guide. BPB Online. 2022. 509 p.

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

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

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

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

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

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

10. 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.

11. 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

12. 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.

13. 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.

14. 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.

15. 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.

16. 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.

17. 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.

18. 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.

19. 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.

20. 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.

21. 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.

22. 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.

23. 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.

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

25. 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

26. 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.

27. 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.

28. 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.

29. 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.

30. 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.

31. 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.

32. 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.

33. 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.

34. 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,

35. 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.

36. 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.

37. 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.

38. 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.

39. 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.

40. 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

41. 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.

42. 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.

43. 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.*

44. 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.

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

46. 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.

47. 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.

48. 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.

49. 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.

50. 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.

51. 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.

52. 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.