Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістра

студента ***Кислякова Якова Андрійовича***

академічної групи ***125м-17-1***

спеціальності ***125 Кібербезпека***

спеціалізації[1]

за освітньо-професійною програмою ***Кібербезпека***

на тему ***Розробка підсистеми самотестування для АСУ легковими автомобілями***

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	д.ф.-м.н., проф. Кагадій Т.С.			
розділів:				
спеціальний	ст. викл. Начовний І.І.			
економічний	к.е.н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2018

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня магістра

студенту ***Кислякову Я.А.*** **академічної групи** ***125м-17-1***
(прізвище та ініціали) (шифр)

спеціальності ***125 Кібербезпека***

спеціалізації[1]

за освітньо-професійною програмою ***Кібербезпека***

на тему ***Розробка підсистеми самотестування для АСУ легковими автомобілями***

1 ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Наказ ректора НТУ «Дніпровська політехніка» від 29.11.2018 № 2025-л_____

2 МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень ***АСУ легковими автомобілями***

Предмет досліджень ***методи захисту АСУ легковими автомобілями***

Мета ***Дослідження існуючого рівня захищеності АСУ легковими автомобілями, розробка та обґрунтування ефективності використання заходів щодо підвищення рівня інформаційної безпеки системи.***

Вихідні дані для проведення роботи ***законодавство України та міжнародні стандарти у сфері кібербезпеки***

3 ОЧІКУВАНІ РЕЗУЛЬТАТИ

Наукова новизна ***висновок про ефективність використання методики аналізу станів керуючого блоку автомобіля як засобу підвищення рівня інформаційної безпеки автоматизованої системи керування легковими***

автомобілями.

Практична цінність ***розробка проектних рішень по підвищенню рівня захищеності автоматизованої системи управління легковими автомобілями***

4 ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Закону України «Про інформацію», НД ТЗІ 1.1-002-99, НД ТЗІ 2.5-004-99, НД ТЗІ 2.5-005-99, НД ТЗІ 3.7-001-99

5 ЕТАПИ ВИКОНАННЯ РОБІТ

Найменування етапів робіт	**Строки виконання робіт** (початок-кінець)
Огляд джерел за темою та напрям досліджень	03.09.18-06.10.18
Методи досліджень	07.10.18-31.10.18
Результати досліджень	01.11.18-24.11.18
Виконання економічного розділу	25.11.18-04.12.18
Оформлення пояснювальної записки	05.12.18-10.12.18

6 РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект ***зниження ймовірності понесення збитку від реалізації несанкціонованих дій зловмисників шляхом впровадження запропонованих мір та засобів підвищення рівня захіщеності АСУ легковим автомобілем.***

Соціальний ефект ***забезпечення захисту даних про стан автомобіля в автоматизованих системах керування легковими автомобілями та підвищення рівня надійності даних систем***

7 ДОДАТКОВІ ВИМОГИ

Завдання видано _____ Кагадій Т.С.
(підпис керівника) (прізвище, ініціали)

Дата видачі: 03.09.18р.

Дата подання до екзаменаційної комісії: 14.12.18р.

Прийнято до виконання _____ Кисляков Я.А.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: ___ с., __ рис., __ табл., 4 додатки, 27 джерел.

Об’єкт дослідження: автоматизована система керування легковими автомобілями «SCar».

Мета дипломної роботи: дослідження існуючого рівня захищеності автоматизованої системи керування легковими автомобілями «SCar», розробка та обґрунтування ефективності використання заходів щодо підвищення рівня інформацийної безпеки системи.

Результати роботи: проведено аналіз стану захищеності автоматизованої системи керування легковими автомобілями «SCar»; розроблено проектні рішення щодо підвищення рівня захищеності об’єкта дослідження; запропоновано використання механізму тестування коректності роботи системи керування як засобу підвищення інформаційної безпеки розглянутої системи.

Практичне значення роботи полягає в розробці проектних рішень по підвищенню рівня захищеності автоматизованої системи керування легковими автомобілями.

Розроблені проектні рішення щодо підвищення рівня захищеності призначені для впровадження та використання у системах керування легковими автомобілями «SCar».

МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, ФУНКЦІОНАЛЬНИЙ ПРОФІЛЬ ЗАХИЩЕНОСТІ, АВТОМАТИЗОВАНА СИСТЕМА КЕРУВАННЯ, ЛЕГКОВИЙ АВТОМОБІЛЬ.

РЕФЕРАТ

Пояснительная записка: ___ с., __ рис., __ табл., 4 приложений, 27 источников.

Объект исследования: автоматизированная система управления легковыми автомобилями «SCar».

Цель дипломной работы: исследование текущего уровня защищенности автоматизированной системы управления легковыми автомобилями «SCar», разработка и обоснование эффективности использования решений по повышению уровня информационной безопасности системы.

Результаты работы: проведен анализ состояния защищенности автоматизированной системы управления легковыми автомобилями «SCar»; разработано проектные решения по повышению уровня защищенности объекта исследования; предложено использование механизма тестирования корректности работы системы управления как средства повышения информационной безопасности рассмотренной системы.

Практическое значение работы заключается в разработке проектных решений по повышению уровня защищенности автоматизированной системы управления легковыми автомобилями.

Разработаные проектные решения по повышению уровня защищенности предназначены для внедрения и использования в системах управления легковыми автомобилями «SCar».

МОДЕЛЬ УГРОЗ, МОДЕЛЬ НАРУШИТЕЛЯ, ФУНКЦИОНАЛЬНЫЙ ПРОФИЛЬ ЗАЩИЩЕННОСТИ, АВТОМАТИЗИРОВАННАЯ СИСТЕМА УПРАВЛЕНИЯ, ЛЕГКОВОЙ АВТОМОБИЛЬ.

ABSTRACT

Explanatory note: ___ p., __ fig., __ tab., 4 application, 27 sources.

The research object is an automized control cars system «SCar».

The purpose of the work is to research current security level of automized informational system «SCar», to design and to substantiate the effectiveness of using measures of increasing its security level.

Got results: analysis of the current security level of automized control cars system «SCar»; solutions of improvement the protection of the researched object were designed; the method of testing the correctness of the system as a way to increase its security level was designed.

In the occupational health and safety section hazards when working with PC users were analyzed, engineering occupational health and safety activities for computer users were developed.

In the economic section evaluated the feasibility of implementing design solutions for information security.

The practical significance of the work lies in the development of complex security measures of increasing the security level of automized automized control cars system.

Solutions designed to improve the security level of automized control cars system «SCar».

MODEL OF THREATS, MODEL OF THE INTRUDER, FUNCTIONALITY SEQURITY PROFILE, AUTOMATED PROCESS CONTROL SYSTEM, CARS.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС	–	автоматизована система;
АСУ	–	автоматизована система управління;
АІС	–	автоматизована інформаційна система;
КЗЗ	–	комплекс засобів захисту;
КС	–	комп’ютерна система;
КСЗІ	–	комплексна система захисту інформації;
НСД	–	несанкціонований доступ;
ОІД	–	об’єкт інформаційної діяльності;
ОЕ	–	об’єкт експертизи;
ОС	–	операційна система;
ПБ	–	політика безпеки;
ПЗ	–	програмне забезпечення;
ПК	–	персональний комп’ютер;
HTTPS	–	Hyper Text Transfer Protocol Secure;
IMEI	–	International Mobile Equipment Identity;
SSL	–	Secure Sockets Layer;
SSH	–	Secure Shell.

ЗМІСТ

с.

ВСТУП

Автомобільна електроніка – це комп’ютер, навчений приймати рішення на основі показань різних датчиків і втручатися в системи управління вузлами і агрегатами для корекції їх роботи. Але будь-яку електронну систему, створену для того, щоб полегшити життя, можна використовувати в прямо протилежних цілях.

У даній роботі розглядається проблема безпеки сучасних автоматизованих систем керування легковими автомобілями. Дана тема є дуже актуальною, тому що на даний момент починають з'являється все більше продуктів, пов'язаних з автоматизацією систем керування автомобілями. Це, по-перше, свідчить про нестачу досвіду виробників, через що вони можуть приділяти недостатньо уваги безпеці своїх систем. По-друге, для підтримки конкурентоспроможності в умовах інтенсивного росту даної галузі необхідно запроваджувати нові сервіси: від надання додаткових користувацьких послуг до запровадження інноваційних механізмів забезпечення інформаційної безпеки.

Метою роботи було дослідження поточного рівня захищеності АСУ легковими автомобілями «SCar» та створення рекомендацій та проектних рішень щодо його підвищення.

Оскільки для реалізації атак зловмиснику необхідно мати не тільки спеціальні знання, а й доступ до автомобіля для того щоб переналаштувати керуючий блок, або ввести до складу електроустаткування додаткові пристрої, то у даній роботі було запропоновано використання системи аналізу дій представників технічної сервісної служби, як засобу підвищення інформаційної безпеки автоматизованої системи керування легковим автомобілем.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Загальна характеристика системи

Сучасні системи керування автомобілем – це спеціалізовані продукти, які являють собою сукупність специфічних реле та модулей для повноцінного контролю за станом автомобиля та забезпечення його захисту. Забезпечення захищеності таких систем є дуже важливим, оскільки вони контролюють роботу усього автомобіля.

Під АС у даній роботі слід розуміти організаційно-технічну систему, що об’єднує у собі розподілений програмно-апаратний комплекс: віддалений сервер, блоки управління, розташовані в автомобілях користувачів, мобільні телефони користувачів, на яких встановлена клієнтська частина системи управління автомобілем, а також фізичне середовище, користувачі сістеми і оброблювана інформація.

Автоматизована система управління легковим автомобілем представляє собою розподілений багатомашинний комплекс, який обробляє інформацію різних ступенів обмеження доступу. Передача даних здійснюється по незахищеному каналу. АСУ легковим автомобілем згідно [1] є АС 3 класу.

Основними фунціями системи управління легковим автомобілем є:

– віддалене керування автомобілем;

– моніторинг стану автомобіля;

– реагування (оповіщення користувача та вживання заходів) на спроби злому/угону автомобіля.

На рисунку 1.1 зображено структурну схему АСУ керування легковим автомобілем. У таблиці 1.1 описані умовні позначення, використані на рисунку 1.1.

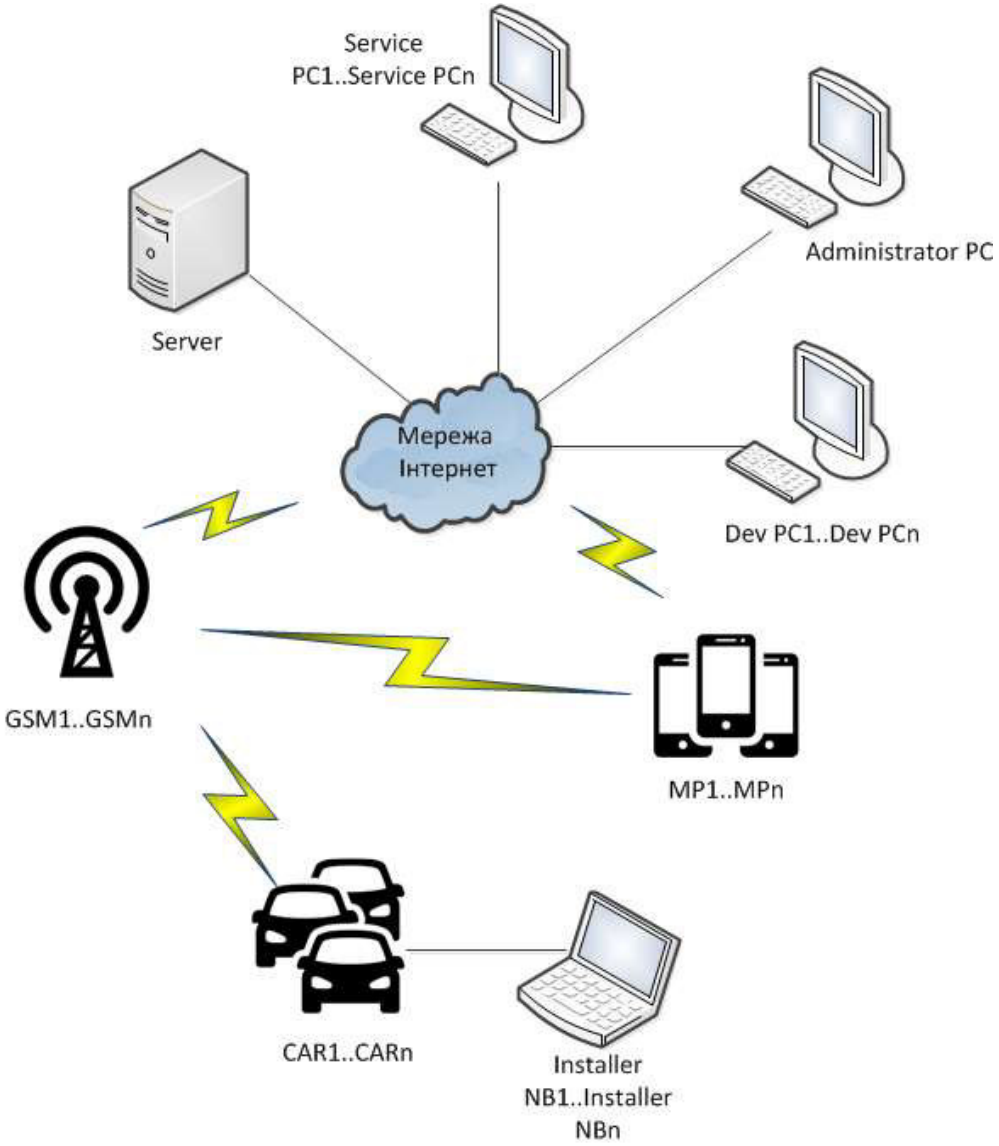

Рисунок 1.1 – Структурна схема АСУ управління легковим автомобілем

Таблиця 1.1 – Умовні позначення

Умовне позначення	Назва	Призначення
	Server	Сервер, на якому обробляються та зберігаються дані
	GSM1..GSMn	Вишка GSM-зв’язку

Продовження таблиці 1.1

Умовне позначення	Назва	Призначення
	CAR1..CARn	Управляючі блоки, що знаходяться в автомобілях користувачів системи
	MP1..MPn	Мобільні телефони користувачів системи, на яких встановлено прграмне забезпечення користувача системи керування автомобілем
	Service PC1…Service PCn	Робочі станції предствників служби підтримки
	Dev PC1…Dev PCn	Робочі станції розробників програмного забезпечення, що використовується в АСУ керування автомобілем
	Administrator PC	Робоча станція адміністратора системи
	Installer NB1..Installer NBn	Портативні комп’ютери представників сервісної служби, які підключаються безпосередньо до блоку керування автомобілем для установки та налаштування програмного забезпечення системи керування автомобілем

Представники служби підтримки мають доступ на віддалений сервер через мережу Інтернет з будь-якої робочої станції по протоколу HTTPS, використовуючи свій обліковий запис для входу у систему через веб-інтерфейс.

Розробники програмного забезпечення АСУ легковим автомобілем через мережу Інтернет передають адміністартору системи оновлений програмний код, який контролює подальше впровадження оновлень програмного

забезпечення. Нові версії програмної частини системи передаються на віддалений сервер через мережу Інтернет по протоколу SSH. Для синхронізації файлів та каталогів серверу та робочої станції використовуєтсья програма Rsync.

Представники сервісної служби отримують доступ до системи під час проведення робіт по встановленню або налагодженню блока управління в автомобілі, шляхом підключення портативного комп'ютера.

Блок управління автомобілем виконує команди користувача, надіслані по GSM або GPRS каналу, та реагує на вплив навколишнього середовща (на підставі показників датчиків, без обробки даних на сервері). Дані про вплив навколишнього середовища та про виконання команд блок управління відпраляє на сервер по GPRS каналу (звідки ця інформація відправляєтья на мобільний телефон користувача, на якому встановлена програмне забезпечення для керування автомобілем) або безпосередньо на телефон користовача по GSM каналу.

Характеристика програмної частини АС приведена у таблиці 1.2.

Таблиця 1.2 – Характеристика програмної частини АС

Назва обладнання	Базова система	Порт
Server	ОС: Ubuntu Server 12.04	-
	ПЗ	
	Rsync 3.1.1	873
	Nginx(Web-сервер) 1.4.7	8080
	Mongodb 2.4.1	27018
CAR1..CARn	ОС: SCar OS	-
MP1..MPn	ОС: IOS 5.0 +, Android 2.3 +	-
	ПЗ	
	SCar iOS App 1.3.4/ SCar Android App 1.3.4	8082

Продовження таблиці 1.2

Назва обладнання	Базова система	Порт
Service PC1…Service PCn	ОС: Будь-яка операційна система	-
	ПЗ	
	Будь-який браузер	8080
Dev PC1…Dev PCn	ОС: Будь-яка операційна система	-
	ПЗ	
	Будь-який браузер	8080
	Brackets 0.37.0-12014	-
	Git 1.8.5.2	873
Administrator PC	ОС: Будь-яка операційна система	-
	ПЗ	
	Rsync 3.1.1	873
	Git 1.8.5.2	4433
Installer NB1..Installer NBn	ОС: Windows XP/Vista/7/8	-
	ПЗ	
	SCar Installer App	-

1.2 Класифікація інформації, що обробляється в АС

В даній роботі для класифікації інформації будемо керуватись наступними законодавчими документами: ЗУ «Про інформацію», НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі». Розглянемо які вимоги висувають зазначені документи.

Відповідно до [2] інформація повинна бути класифікована за режимом доступу, за правовим режимом, а також за типом її представлення в АС. Класифікація є підставою для визначення власником (розпорядником) інформації або АС методів і способів захисту кожного окремого виду

інформації.

Відповідно до статті 28 Закону України «Про інформацію», за режимом доступу інформація поділяється на:

– відкриту;

– з обмеженим доступом (конфіденційна, таємна та службова).

Відкриту інформацію можна поділити на відкриту, яка не потребує захисту, або захист якої забезпечувати недоцільно, та відкриту, яка такого захисту потребує. До другої слід відносити інформацію, важливу для особи, суспільства і держави (відповідно до Концепції технічного захисту інформації в Україні), важливі для організації відомості, порушення цілісності або доступності яких може призвести до моральних чи матеріальних збитків власника інформації.

Для встановлення правил взаємодії активних і пасивних об’єктів АС інформація повинна бути класифікована за типом її представлення в АС (для кожної з визначених категорій встановлюються типи пасивних об’єктів комп’ютерної системи, якими вона може бути представлена).

Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація. Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом. При цьому, у частині 1 статті 13 Закону України «Про доступ до публічної інформації» вказано, що інформація може належати до службової відповідно до вимог частини другої статті 6 Закону України «Про доступ до публічної інформації». Таким чином, обмеження доступу до інформації здійснюється відповідно до закону при дотриманні сукупності таких вимог:

1) виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для

охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя;

2) розголошення інформації може завдати істотної шкоди цим інтересам;

3) шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

На базі викладеного, можна стверджувати, що в досліджуваній АС оброблюється інформація з обмеженим доступом. До службової інформації можна віднести поролі доступу користувачів до системи, керуючі команди, а також інформацію про стан автомобіля.

У таблиці 1.3 приведена класифікація інформації, оброблюваної в АС.

Таблиця 1.3 - Класифікація інформації в АС

Інформація	Ресурс, на якому зберігаються дані	Ресурс, на якому обробляються дані	Властивості інформації		
			К	Ц	Д
Інформація з обмеженим доступом					
1 IMEI керуючого блоку автомобіля	Управляючий блок автомобіля, віддалений сервер	Віддалений сервер	+	+	+
2 Телефонний номер користувача	Управляючий блок автомобіля, віддалений сервер	Віддалений сервер	+	+	+
3 Паролі користувачів	Управляючий блок автомобіля	Віддалений сервер	+	+	+
4 Ідентіфікатори працівників служби підтримки	Управляючий блок автомобіля	Віддалений сервер	+	+	+

Продовження таблиці 1.3

Інформація	Ресурс, на якому зберігаються дані	Ресурс, на якому обробляються дані	Властивості інформації		
			К	Ц	Д
Інформація з обмеженим доступом					
5 Паролі працівників служби підтримки	Віддалений сервер	Віддалений сервер, ПК проедставніків служби підтримки, ПК адміністратора системи	+	+	+
6 Управляючі команди від користувачів	Віддалений сервер	Управляючий блок автомобіля, віддалений сервер, мобільний телефон користувача	+	+	+
6.1 Поставити на сигналізацію					
6.2 Зняти з сигналізації					
6.3 Запустити двигун					
6.4 Запустити двигун					
6.5 Заглушити двигун					
6.6 Заблокувати двигун					
6.7 Відчинити центральний замок					
6.8 Закрити центральний замок					
6.9 Відчинити багажник					
6.10 Увімкнути сервісний режим					
6.11 Увімкнути серену					
6.12 Вимкнути серену					
6.13 Зачинити вікна					

Продовження таблиці 1.3

Інформація	Ресурс, на якому зберігаються дані	Ресурс, на якому обробляються дані	Властивості інформації		
			К	Ц	Д
Інформація з обмеженим доступом					
7 Журнал реєстрації дій користувачів системи	Віддалений сервер	Віддалений сервер	+	+	+
8 Дані про поточний стан автомобіля	Управляючий блок автомобіля, віддалений сервер	Мобільний телефон користувача, ПК представника служби підтримки	+	+	+
8.1 Стан двигуна (запущено/заблоковано/вимкнено)					
8.2 Температура двигуна					
8.3 Температура в салоні					
8.4 Стан дверей (відкриті/закриті)					
8.5 Напруга бортової мережі					
8.6 Стан акумулятора (від’єднано/розрядився/працює)					
8.7 Інформація про стан підключення блоку управління до серверу (підключено/не підключено)					
8.8 Дані про стан охоронних датчиків установлених в автомобілі (датчик удару, нахилу, руху, переміщення)					
9 Геолокаційні дані	Управляючий блок автомобіля, віддалений сервер	Мобільний телефон користувача	+	+	+
10 Історія спрацьовувань системи	Управляючий блок автомобіля, віддалений сервер	Мобільний телефон користувача	+	+	+
11 Дані про баланс на рахунку користувача	Управляючий блок автомобіля, віддалений сервер	Мобільний телефон користувача	+	+	+

Продовження таблиці 1.3

Інформація	Ресурс, на якому зберігаються дані	Ресурс, на якому обробляються дані	Властивості інформації		
			К	Ц	Д
Інформація з обмеженим доступом					
12 Програмний код додатку “SCar”, веб-додатку, веб-серверу, додатку “SCar Installer App”	ПК розробника ПЗ	ПК розробника ПЗ	+	+	+
13 Конфігураційні файли блока управління автомобілем	Управляючий блок автомобіля	Управляючий блок автомобіля, ноутбук представника сервісної технічної служби	+	+	+
14 Ідентифікатор облікового запису адміністратора системи	Віддалений сервер	Віддалений сервер	+	+	+
15 Пароль від облікового запису адміністратора системи	Віддалений сервер	Віддалений сервер	+	+	+

Вся інформація у системі представлена в електронному вигляді.

1.3 Матриця доступу користувачів до інформації

Матриця доступу користувачів до інформації приведена у таблиці 1.4. Можливі операції суб’єктів (користувачів) над об’єктами (інформацією): R – читання, W – запис, D – видалення.

Таблиця 1.4 – Матриця доступу суб’єктів до об’єктів

Інформація	Суб'єкти					
	Розробники ПЗ	Користувач	Представник служби підтримки	Представний сервісної служби	Адміністратор системи	Адміністратор серверу
Інформація з обмеженим доступом						
IMEI керуючих блоків автомобілей	-	R	R	R	-	-
Телефонні номера користувачів	-	R	-	R	-	-
Паролі користувачів	-	R, W	-	R	-	-
Ідентіфікатори працівників служби підтримки	-	-	R, W	-	C, R, W,D	-
Паролі працівників служби підтримки	-	-	R, W	-	C, W	-
Управляючі команди від користувачів	-	R, W	R	R, W	-	-
Журнал реєстрації дій користувачів системи	-	-	R	-	-	-
Дані про поточний стан автомобіля	-	R	R	R	-	-
Геолокаційні дані	-	R	-	R	-	-
Історія спрацьовувань	-	R	R	R	-	-
Дані про баланс на рахунку користувача	-	R	R	R	-	-

Продовження таблиці 1.4

Інформація	Суб'єкти					
	Розробники ПЗ	Користувач	Представник служби підтримки	Представний сервісної служби	Адміністратор системи	Адміністратор серверу
Програмнёий код додатку “SCar”, веб-додатку, веб-серверу, додатку “SCar Installer App”	R, W	-	-	-	-	-
Конфігураційні файли блока управління автомобілем	-	-	-	R, W	-	-
Ідентифікатор облікового запису адміністратора системи	-	-	-	-	R, W	-
Пароль від облікового запису адміністратора системи	-	-	-	-	R, W	-

1.4 Технологія обробки інформації в АС

Технологія обробки інформації в АС дозволяє виконувати над інформацією в електронному вигляді наступні дії: створення, перегляд, редагування, зберігання та видалення. Виконуються ці операції програмними та апаратними засобами АС.

Доступ до системи надається користувачам та працівникам, які забезпечують працездатність системи. Дозвіл на вхід до системи надається на підставі перевірки логину та паролю. Перевірка достовірності паролю під час

аутентифікації виконується на сервері. Ім’я користувача та пароль передаються по мережі у захищеному вигляді по протоколу SSH.

Користувачі для доступа до системи використовують мобільний телефон, на якому встановлено необхідне програмне забезпечення та є підключення до мережі Інтернет.

Видача персональних ідентифікаторів (логінів) та паролів по замовченню для користувачів виконується під час встановлення управляючтого блоку в автомобіль представником сервісної служби. Після цього користувач може змінити свій пароль.

Представники технічної сервісної служби отримують доступ до системи під час першого встановлення управляючого блоку в автомобіль, а потім лише під час обслуговування автомобіля, підключивши безпосередньо до цього блоку свій ноутбук із встановленім додатком. Для доступа до керуючого блоку необхідно отримати фізичний доступ до автомобіля та відчинити капот, попередньо відключивши сигналізацію.

Представники служби підтримки отримують доступ до системи через веб-додаток. Надання доступу до системи через веб-додаток представнику сервісної служби здійснюється після перевірки логіну та паролю працівника. Дані про логін та пароль передаються на сервер по протоколу HTTPS та перевіряються там.

Змінити логін та пароль, а також видати чи видалити обліковий запис представника служби підтримки може лише адміністратор системи.

На сервері зберігається хеш-сумма паролей, розрахована по алгоритму SHA-256.

Користувач, що увійшов до свого облікового запису через додаток на мобільному телефоні може перевірити поточний стан автомобіля (геолокаційні дані, стан двигуна (запущено/заблоковано/вимкнено), темнература двигуна, температура в салоні, стан дверей (відкриті/закриті) напруга бортової мережі, стан акумулятора (від’єднано/розрядився/працює), інформація про стан підключення блоку управління до серверу (підключено/не підключено),

інформація про залишок коштів на рахунку (карта мобільного оператора знаходиться в керуючому блоці автомобіля та використовується для піключення до мережі Інтернет), дані про стан охоронних датчиків, установлених в автомобілі (датчик удару, нахилу, руху, переміщення)), відправити команди на управляючий блок (поставити на сигналізацію, зняти з сигналізації, запустити двигун, заглушити двигун, заблокувати двигун, відчинити центральний замок, закрити центральний замок, відчинити багажник, увімкнути сервісний режим, увімкнути серену, вимкнути серену, зачинити вікна), налаштувати чуттєвість охоронних датчиків та передивитись історію їх спрацьовувань.

Представник служби підтримки, що увійшов до свого облікового запису через веб-додаток отримує доступ до переліку користувачів, активних на даний момент і може здійснювати пошук по їх персональним ідентифікаторам, має можливість переглядати поточний стан автомобіля (те ж саме, що і у користувача, окрім геолокаційних даних) обраного користувача.

Якщо автомобіль знаходиться в сервісному центрі на обслуговуванні, представник технічної служби підтримки має доступ до апаратної та програмної частини керуючого блоку і під’єднавши до нього свій ноутбук із встановленим додатком “SCar Installer App” може переглядати та редагувати конфігураційну інформацію.

Розробник ПЗ вдосконалює програмне забезпечення, що використовується в системі (веб-сервер, веб-додаток, що використовують працівники служби підтримки, SCar Installer App, SCar App). Для того щоб завантажити на сервер оновлену версію програми, розробник спочатку передає через мережу Інтернет адміністратору системи оновлений код, використовуючи систему контроля версій Git. Адміністратор системи заходить на сервер через утіліту rsync, за допомогою якої може виконати синхронізацію файлів та каталогів. Для того щоб отримати доступ до системи адміністратр проходить процедуру аутентифікації, використовуючі свій логін та пароль, які передаються по захищеному протоколу SSH на сервер, де здійснюється

перевірка. Оновлені версії програми користувач системи може завантажити з серверу собі на телефон (мобільний додаток) та обновити прошивку керуючого блоку.

На рисунку 1.2 зображено схему інформаційних потоків між компонентами АС. Цифрам 1-15 на даній схемі відповідає інформацая із відповідним порядковим номером у таблиці 1.3.

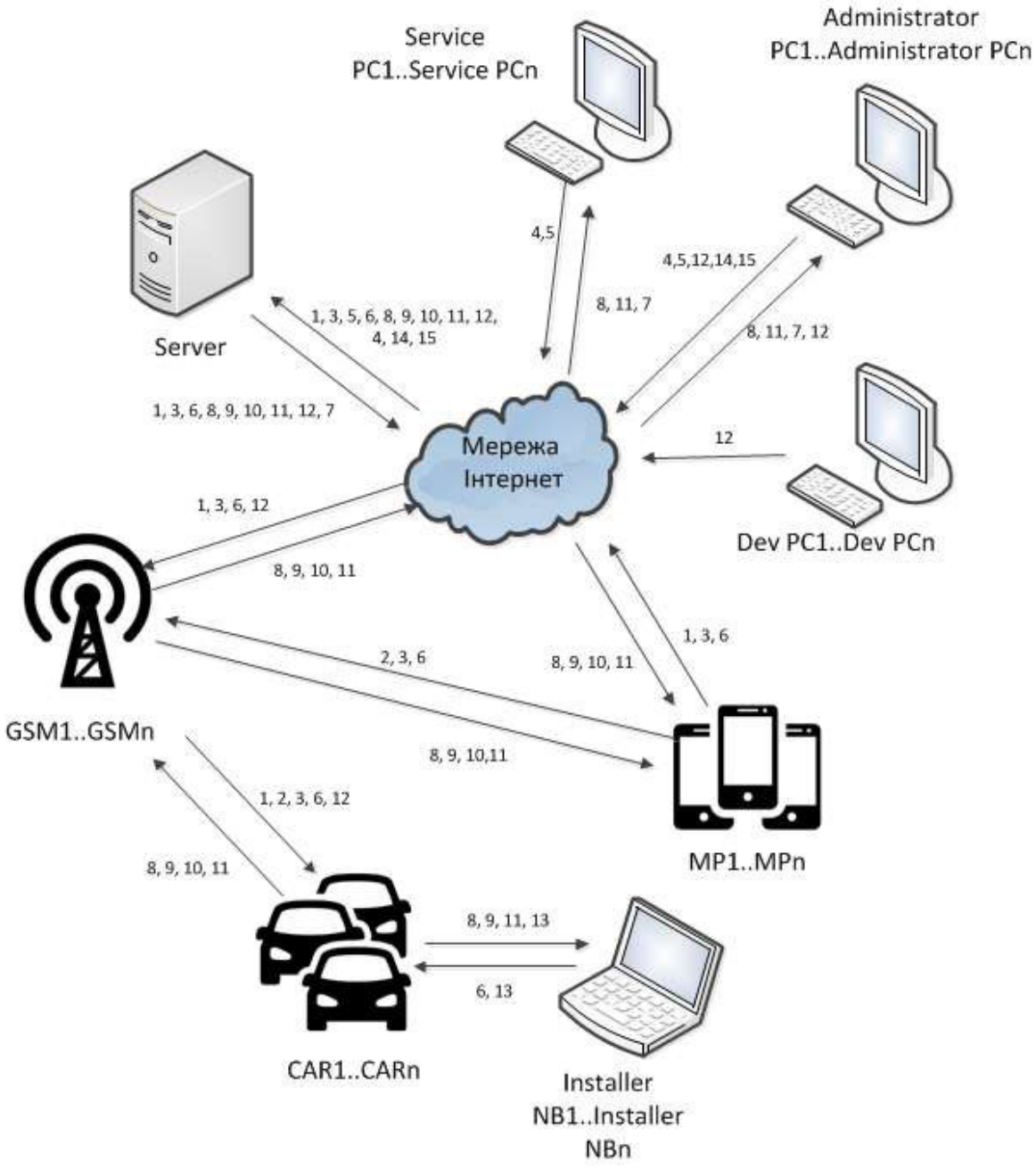

Рисунок 1.2 – Схема основних інформаційних потоків між компонентами АС

1.5 Створення моделі загроз та моделі порушника

Основою для проведення аналізу ризиків і формування вимог до КСЗІ є розробка моделі загроз для інформації та моделі порушника.

Для створення моделі загроз необхідно скласти перелік суттєвих загроз, описати методи і способи їхнього здійснення.

Необхідно визначити, якими з можливих способів можуть здійснюватися загрози в АС:

– технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо- та радіотехнічні, хімічні та інші канали;

– каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;

– несанкціонованим доступом шляхом підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав’язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп’ютерних вірусів.

Загрози для інформації, що обробляється в АС, залежать від характеристик ОС, фізичного середовища, персоналу, технологій обробки та інших чинників і можуть мати об'єктивну або суб'єктивну природу. Загрози, що мають суб'єктивну природу, поділяються на випадкові (ненавмисні) та навмисні. Мають бути визначені основні види загроз для безпеки інформації, які можуть бути реалізовані стосовно АС і повинні враховуватись у моделі загроз.

Перелік суттєвих загроз має бути максимально повним і деталізованим. Для кожної з загроз необхідно визначити:

– на порушення яких властивостей інформації або АС вона спрямована (рекомендується користуватись чотирма основними градаціями – порушення конфіденційності, цілісності, доступності інформації, а також порушення спостережності та керованості АС);

– джерела виникнення (які суб’єкти АС або суб’єкти, зовнішні по відношенню до неї, можуть ініціювати загрозу);

– можливі способи здійснення загроз.

У кожному конкретному випадку, виходячи з технології обробки інформації, необхідно розробити модель порушника, яка повинна бути адекватна реальному порушнику для даної АС. Модель порушника — абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії і т.ін. По відношенню до АС порушники можуть бути внутрішніми (з числа співробітників, користувачів системи) або зовнішніми (сторонні особи або будь-які особи, що знаходяться за межами контрольованої зони).

Модель порушника повинна визначати:

– можливу мету порушника та її градацію за ступенями небезпечності;

– категорії осіб, з числа яких може бути порушник;

– припущення про кваліфікацію порушника;

– припущення про характер його дій.

Для побудови моделі загроз, таблиця 1.7, використаємо дані стосовно можливих порушників та загроз, приведених у таблицях 1.5, 1.6 відповідно.

Можлива наступна класифікація порушників.

Метою порушника можуть бути:

М1 − отримання необхідної інформації у потрібному обсязі;

М2 − мати можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами;

М3 − нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

Класифікація за рівнем можливостей:

РМ1 − рівень визначає найнижчий рівень можливостей ведення діалогу з АС − можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;

РМ2 − визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;

РМ3 − визначається можливістю управління функціонуванням АС, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування;

РМ4 − визначається повним обсягом можливостей осіб, що здійснюють проектування, реалізацію, впровадження, супроводження програмно-апаратного забезпечення АС, аж до включення до складу АС власних засобів з новими функціями обробки інформації.

Класифікація за рівнем знань:

РЗ1 − володіють інформацією про функціональні особливості АС, основні закономірності формування в ній масивів даних та потоків запитів до них, вміють користуватися штатними засобами;

РЗ2 − володіють високим рівнем знань та досвідом роботи з технічними засобами системи та їхнього обслуговування;

РЗ3 − володіють високим рівнем знань у галузі обчислювальної техніки та програмування, проектування та експлуатації АС;

РЗ4 − володіють інформацією про функції та механізм дії засобів захисту

Класифікація за використовуваними методами та способами:

С1 − використовують виключно агентурні методи одержання відомостей;

С2 − використовують пасивні технічні засоби перехоплення інформаційних сигналів;

С3 − використовують виключно штатні засоби АС або недоліки проектування КСЗІ для реалізації спроб НСД;

С4 − використовують способи і засоби активного впливу на АС, що змінюють конфігурацію системи (підключення додаткових або модифікація штатних технічних засобів, підключення до каналів передачі даних, впровадження і використання спеціального ПЗ тощо).

Класифікація за місцем дій:

МД1 − без одержання доступу на контрольовану територію організації (АС);

МД2 − з одержанням доступу на контрольовану територію, але без доступу до технічних засобів АС;

МД3 − з одержанням доступу до робочих місць кінцевих (у тому числі віддалених) користувачів АС;

МД4 − з одержанням доступу до місць накопичення і зберігання даних (баз даних, архівів, АРМ відповідних адміністраторів тощо);

МД5 − з одержанням доступу до засобів адміністрування АС і засобів керування КСЗІ.

Таблиця 1.5 - Модель порушника

Категорія осіб	Порушник	Мета порушника	Кваліфікація		Характер дій	
			Рівень можливостей	Рівень знань	Використовувані методи	Місце дії
Внутрішні	Адміністратор системи	М1, М2, М3	РМ3	РЗ2	С3	МД5
	Розробник ПЗ	М1, М2, М3	РМ4	РЗ4	С4	МД3
	Представник сервісної служби	М1, М2, М3	РМ3	РЗ2	С1, С3	МД5
	Представних служби підтримки	М1, М2, М3	РМ1	РЗ1	С1, С3	МД3
	Користувач системи	М2	РМ1	РЗ1	С3	МД3
	Адміністратор серверу	М1, М2, М3	РМ1	РЗ2	С4	МД4

Продовження таблиці 1.5

Категорія осіб	Порушник	Мета порушника	Кваліфікація		Характер дій	
			Рівень можливостей	Рівень знань	Використовувані методи	Місце дії
Внутрішні	Технічний персонал, що обслуговує сервер	М3	РМ1	РЗ1	С1	МД2
Зовнішні	Хакери	М1, М2, М3	РМ2	РЗ3	С3	МД1
	Грабіжники/Злочинці	М1, М2, М3	РМ1	РЗ1	С1	МД1

Класифікація загроз за критеріями наведеними у [3] приведена у таблицях 1.7 та 1.8.

Пояснення використаних позначок наведено у таблиці 1.6.

Таблиця 1.6 - Загальна модель загроз

Позначення	Пояснення
СВ	суб'єктивна (випадкова) природа загрози
СН	суб'єктивна (навмисна) природа загрози
О	об'єктивна природа загрози
К	конфіденційність інформації
Ц	цілісність інформації
Д	доступність інформації
С	спостережність системи
НСД	несанкціонований доступ
СП	канали спеціального впливу
ТК	технічні канали

Таблиця 1.7 - Загальна модель загроз

Загроза	Природа загрози	Направлена на порушення властивостей інформації та АС				Спосіб реалізації
		К	Ц	Д	С	
Пошкодження/втрата інформації	СВ, СН, О	-	+	+	-	НСД
Компрометація інформації /НСД	СВ, СН	+	-	-	-	НСД, ТК
Викривлення/підробка інформації	СВ, СН	-	+	-	-	НСД
Порушення доступності	СВ, СН, О	-	-	+	-	НСД
Заперечення автентичності інформації	СВ, СН	-	-	-	+	НСД

Таблиця 1.8 – Зведена таблиця моделі загроз

Загроза	Джерела виникнення	Вразливість
Пошкодження/втрата інформації/ресурсів	Адміністратор системи	Халатність працівників
		Відсутність системи моніторингу за діями администратора
		Відсутність інструкції стосовно дій у надзвичайних ситуаціях
	Представник сервісної технічної служби	Відсутність контролю за внесенням змін до складу обладнання/програмного забезпечення
		Недостатня вмотивованість або незадоволеність персоналу
		Складний інтерфейс користувача

Продовження таблиці 1.8

Загроза	Джерела виникнення	Вразливість
Компрометація інформації /НСД	Адміністратор системи	Відсутність системи моніторингу за діями адміністратора
		Халатність працівників
		Неконтрольоване копіювання інформації
	Розробник ПЗ	Відсутність затвердженої процедури поводження з інформацією з обмеженим доступом
		Халатність працівників
		Використання недокументованих можливостей ПЗ
		Відсутність достатнього контролю за внесенням змін до складу програмного забезпечення
	Представник служби підтримки	Недостатня вмотивованість або незадоволеність персоналу
		Халатність працівників
		Недостатня обізнаність користувача у питаннях інформаційної безпеки
	Представник сервісної технічної служби	Недостатня вмотивованість або незадоволеність персоналу
		Недостатня обізнаність персоналу у питаннях інформаційної безпеки
		Відсутність системи моніторингу за діями педставників сервісної технічної служби

Продовження таблиці 1.8

Загроза	Джерела виникнення	Вразливість
Компрометація інформації /НСД	Хакери	Використання недокументованих можливостей ПЗ
	Грабіжниики/злочинці	Халатність користувача
		Недостатня обізнаність користувача у питаннях інформаційної безпеки
		Недостатня обізнаність персоналу у питаннях інформаційної безпеки
		Відсутність ефективної процедури моніторингу за робочіми місцями віддалених працівників
Викривлення/ підробка інформації	Адміністратор системи	Відсутність системи моніторингу за діями администратора
	Розробник ПЗ	Відсутність достатнього контролю за внесенням змін до складу програмного забезпечення
	Представник сервісної технічної служби	Відсутність системи контролю цілісності
		Халатність працівників
		Відсутність достатнього контролю за внесенням змін до складу програмного/апартного забезпечення
	Хакери	Використання недоліків ПЗ
	Грабіжники/злочинці	Халатність працівників/користувачів
Порушення доступності	Адміністратор системи	Відсутність системи моніторингу за діями администратора

Продовження таблиці 1.8

Загроза	Джерела виникнення	Вразливість
Порушення доступності	Розробник ПЗ	Відсутність достатнього контролю за внесенням змін до складу програмного забезпечення
	Адміністратор серверу	Відсутність плану забезпечення безперервної роботи
		Халатність працівників
	Технічний персонал, що обслуговує сервер	Халатність працівників
	Хакери	Використання недоліків ПЗ
	Грабіжники/злочинці	Використання недоліків радіоканалу передачі даних від автомобіля до радіодежі (зашумлення каналу)
Заперечення автентичності інформації	Представник сервісної технічної служби	Відсутність належного контролю за внесенням змін до обладнання/програмного забезпечення

1.6 Побудова профілю захищеності АСУ легковим автомобілем

АС що розглядається в дипломній роботі відноситься до класу «3», оскільки відповідає вимогам: є багатомашинним багатокористувачевим комплексом, обробляють інформацію різних категорій конфіденційності та передають інформацію через незахищене середовище.

Відповідно до вимог [4], до зазначеної АС висунуті вимоги щодо цілісності, доступності та конфіденційності інформації що обробляється. Для їх

реалізації створимо КСЗІ на базі стандартного функціонального профілю захищеності 3.КЦД.1 та доповнимо його критеріями (ЦА-1, ДР-2, ДС-1):

3.КЦД = { КД-2, КО-1, КВ-1,
ЦА-1, ЦД-1, ЦО-1, ЦВ-1,
ДС-1, ДР-2, ДВ-1,
НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-1, НВ-1}.

Розглянемо детальніше функціональні послуги профілю, наведені у таблиці 1.9.

Таблиця 1.9 – Функціональний профіль захищеності інформації в АС

Критерій	Послуга безпеки	Рівень послуги безпеки
Конфіденційність	Адміністративна конфіденційність	КА-2
	Повторне використання об’єктів	КО-1
	Конфіденційність при обміні	КВ-1
Цілісність	Цілісність адміністративна	ЦА-1
	Відкат	ЦО-1
	Цілісність при обміні	ЦВ-1
Доступність	Використання ресурсів	ДР-1
	Стійкість до відмов	ДС-1
	Відновлення після збоїв	ДВ-1
Спостережність	Ідентифікація та автентифікація	НИ-2
	Реєстрація	НР-2
	Достовірний канал	НК-1
	Розподіл обов’язків	НО-2
	Цілісність КЗЗ	НЦ-2
	Самостестування	НТ-1
	Автентифікація отримувача	НВ-1

1.7 Висновок

У розділі виконано обстеження ОІД, описано умови функціонування АС, її структуру та оброблювану інформацію. Побудовано та проаналізовано модель загроз та модель порушника та профіль захищеності.

Постановлено наступні задачі:

– проаналізувати реальний стан захищеності досліджуваної системи з метою виявлення нереалізованих критеріїв побудованого профілю захищеності;

– сформувати рекомендації та проектні рішення щодо реалізації досі не реалізованих критеріїв профілю захищеності з метою поліпшення стану захищеності АСУ легковими автомобілями, а також за допомогою введення необхідних організаційних заходів;

– запропонувати механізм реалізації послуги самотестування (НТ-1), який передбачає впровадження системи тестування функціональних можливостей АСУ легковим автомобілем з метою виявлення некоректної поведінки системи;

– висунути вимоги до реалізації запропонованого механізму (вимоги до програмної реалізації, вимоги до технічної реалізації, користувацькі вимоги);

– описати алгоритм роботи запропонованої системи.

РОЗДІЛ 2. СПЕЦІАЛЬНИЙ РОЗДІЛ

2.1 Оцінка існуючого стану захищеності АС

Перевіримо стан захищеності АС спираючись на методику запропоновану у документах [5, 6] та вимоги до функціональних послуг.

Базова адміністративна конфіденційність. Послуга дозволяє вповноваженому користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів.

Політика адміністративної конфіденційності, що реалізується КЗЗ відноситься до програмно-апаратних комплексів, що обробляють конфіденційну та технологічну інформацію, та усіх категорій користувачів, що мають повноваження на доступ до цих видів інформації. Відкрита інформація має бути доступною для всіх користувачів без винятку.

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача та захищеного об’єкта. Запити на зміну прав доступу повинні оброблятися КЗЗ тільки у випадку, якщо вони надходять від адміністратора або іншого користувача, якому делеговані такі права. Повноваження на доступ користувачів до інформації мають бути засновані на їх функціональних обов’язках.

КЗЗ повинен дозволяти адміністратору або вповноваженому користувачу визначати конкретних користувачів (їх групи), які мають право одержувати інформацію за обмеженим доступом, шляхом керування належністю користувачі, процесів та об’єктів до відповідних доменів.

Можливість розмежування доступу на підставі атрибутів доступу користувачів та захищених об’єктів реалізовано на рівні КА-2 оскільки права доступу до системи для конкретного користувача надає адміністратор системи.

Повторне використання об’єктів. КС забезпечує послугу повторне використання об'єктів, якщо перед наданням користувачеві або процесу в розділювальному об'єкті не залишається інформації, яку він містив, і

скасовуються попередні права доступу до об’єкта. Реалізація даної послуги дозволяє забезпечити захист від атак типу "збирання сміття ".

У складі ОЕ є в наявності функціональні модулі та програмне забезпечення, що дозволяє звільнити вміст поділюваних ресурсів, використовуваних для збереження пасивних об’єктів, а також атрибутів доступу до них. Процедура виконується стандартними засобами ОС Ubuntu Server 12.04.

Мінімальна конфіденційність при обміні. Послуга конфіденційність при обміні дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що в них міститься, під час їх експорту/імпорту через незахищене середовище. Найчастіше дана послуга реалізується з використанням криптографічних перетворень.

Реалізація даної послуги на рівні КВ-1 забезпечує захист від несанкціонованого ознайомлення за рахунок пасивного спостереження за лініями зв'язку або розкрадання носіїв інформації. Прикладом реалізації може служити програмне шифрування файлів перед їх передачею каналами зв'язку або прозоре шифрування файлів перед їх записуванням на диск.

Дана послуга реалізується, оскільки у складі об’єкта експертизи функціонують механізми захисту інформації при обміні, а саме передача інформації по протоколам SSL та SSH.

Базова адміністративна цілісність. Адміністративна цілісність дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від користувачів до захищених об'єктів.

Повинна бути чітко зазначена множина об’єктів, на які поширюється політика адміністративної цілісності, що реалізується КЗЗ. Рівень послуги базова адміністративна цілісність повинна гарантувати реалізацію КЗЗ розмежування доступу на підставі атрибутів доступу процесу і захищеного об’єкту.

КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного захищеного об'єкта шляхом

керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретні процеси і/або групи процесів, які мають право модифікувати об'єкт.

Запит на зміну прав доступу повинні оброблятися тільки у випадку, коли вони надходять від адміністратора або від користувачів, яким надані відповідні повноваження.

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації.

Критерій адміністративна цілісність реалізовано у розглянутій системі, оскільки у складі об’єкта експертизи наявні засоби, що реалізують керування доступом на підставі атрибутів доступу користувачів та об’єктів. Змінювати атрибути доступу об’єктів може лише адміністратор системи.

Обмежений відкат. Послуга дозволить забезпечити можливість відмінити операцію або послідовність операцій і повернути захищений об’єкт до попереднього стану.

Політикою відкату, що реалізуется КЗЗ, повинні бути чітко визначена множина об’єктів КС, яких вона стосується.

КЗЗ повинно включати автоматизовані засоби, що дозволяють авторизованому користувачу або процесу відкатити або відмінити певну множину операцій, виконаних над захищеним об’єктом за певний проміжок часу.

Можливість відмінити певну множину операцій виконаних над інформацію, що зберігається на сервері для повернення її до первинного стану реалізується на стороні сервера шляхом виконання резервного копіювання. Також можливо реалізувати відкат та відміну певної множини операцій, виконаних над програмним кодом прошивки керуючого блоку засобами системи управління версіями GIT. Але оскільки немає можливості відмінити операції, здійснені над конфігураційними файлами керуючого блоку, то можна стверджувати, що послуга ЦО-1 в ас реалізована не в повній мірі.

Мінімальна цілісність при обміні. Дана послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Найчастіше ця послуга реалізується з використанням таких механізмів криптографічного захисту, як цифровий підпис і коди автентифікації повідомлень. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування. Під повнотою захисту, як і для послуги конфіденційність при обміні, треба розуміти множину типів загроз, від яких забезпечується захист. Під ступенем захищеності об'єктів, що експортуються, як правило, слід розуміти криптостійкість використовуваних алгоритмів шифрування.

Рівень ЦВ-1 даної послуги забезпечує мінімальний захист. Дана послуга реалізується, оскільки дані передаються по мережі у захищеному вигляді по протоколам SSL та SSH, які використовують коди автенитифікації повідомлень для забезпечення цілісності повідомлень.

Квоти. Послуга дозволить користувачам керувати використанням послуг і ресурсів.

Політика використання ресурсів, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься.

Політика використання ресурсів повинна визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу.

Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження.

В операційній системі Ubuntu Server існує можливість керування обсягом виділених ресурсів (дисковий простір), що надаються окремому користувачу. Проте, політика використання ресурсів поширюється не на всі інформаційні ресурси АС, тож можна сказати що реалізовано лише рівень послуги ДР-1.

Стійкість при обмежених відмовах. Послуга дозволяє забезпечити доступність послуг і ресурсів ОЕ шляхом забезпечення використання окремих

функцій ОЕ чи ОЕ в цілому після відмови його компонента. Рівні даної послуги ранжируються на підставі спроможності КЗЗ забезпечити можливість КС продовжувати функціонування залежно від кількості відмов і послуг, доступних після відмови.

В ОЕ використовується система резервного електроживлення, а також резервний канал зв'язку, що забезпечує можливість збереження повної працездатності системи протягом деякого часу та продовження виконання функцій з оброблення інформації при відмові системи електроживлення. Можна стверджувати, що дана послуга реалізована на рівні ДС-1, бо в системі також реалізована можливість оповіщення адміністратора про відмову захищеного компонента.

Ручне відновлення. Послуга забезпечує повернення КС у відомий захищений стан після відмови або переривання обслуговування.

Політика відновлення, що реалізується КЗЗ, повинна визначати множину типів відмов КС і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція КС.

Після відмови КС або переривання обслуговування КЗЗ повинен перевести КС до стану, із якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження.

Відновлення можливе на рівні послуги ДВ-1 у випадку відмови чи переривання обслуговування за допомогою відміни певної послідовності операцій.

Захищений журнал. Реєстрація даних в захищеному журналі дозволяє контролювати небезпечні для КС дії.

КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки.

Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події.

КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування.

Адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації.

Дана послуга реалізована не в повній мірі, оскільки ведеться журнал реєстрації дій користувачів системи, за допомогою системи контроля версій ведеться журнал дій розробників ПЗ, але дії представників сервісної технічної служби ніяк не реєструються.

Одиночна ідентифікація та автентифікація. Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до КС.

Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ .

Для надання користувачу можливості виконувати будь-які дії контрольовані КЗЗ, КЗЗ повинен автентифікувати користувача з використанням захищеного механізму.

КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування.

Дана послуга реалізована не в повній мірі, бо процедуру ідентифікації і автентифікації для входу в систему проходять усі користувачі системи окрім представників сервісної технічної служби.

Однонаправлений достовірний канал. Однонаправлений достовірний канал дозволяє користувачу безпосередньо взаємодіяти з КЗЗ.

Політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв'язку між користувачем і КЗЗ.

Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем.

Оскільки в ОЕ є можливості створення захищеного шляху передачі інформації між користувачем і функціональними компонентами ОЕ, що входять до складу КЗЗ, який не може бути імітований, а інформація, що передається по ньому, не може бути отримана або модифікована стороннім користувачем або процесом, можна стверджувати що дана послуга реалізована.

Розподіл обов’язків адміністраторів. Виділення адміністратора дозволить зменшити потенційні збитки від навмисних або помилкових дій користувача.

Політика розподілу обов’язків, що реалізується КЗЗ, повинна виділяти ролі адміністратора і звичайного користувача і призначені їм функції.

Послуга реалізована на рівні НО-3, оскільки серед переліку ролей ОЕ існує декілька адміністративних ролей користувачів (адміністратор системи, адміністратор серверу), а також існує декілька ролей звичайних користувачів.

КЗЗ з гарантованою цілісністю. Послуга характеризує міру здатності КЗЗ захищати себе і гарантувати свою здатність керувати захищеними об’єктами.

Політика цілісності КЗЗ повинна визначати склад КЗЗ і механізми контролю цілісності компонентів, що входять до складу КЗЗ.

В разі виявлення порушення цілісності будь-якого із своїх компонентів КЗЗ повинен повідомити адміністратора і автоматично відновити відповідність компонента еталону або перевести КС до стану, з якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження.

Повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ.

За допомогою засобів контролю цілісності, реалізованих на сервері може бути забезпечено контроль цілісності всіх функціональних модулів ОЕ, що входять до складу КЗЗ, окрім тих, що видносяться до керуючого блоку автомобіля. У випадку порушення цілісності адміністратора буде повідомлено про це. Проте не реалізоване визначення політикою цілісності домену КЗЗ та інших доменів, а також механізму захисту, що використовується для реалізації розподілення доменів. Тож можна сказати, що послуга реалізована на рівні НЦ-1. Для реалізації рівня НЦ-2 потрібно описати обмеження які дозволяють гарантувати, що послуги безпеки доступні лише через інтерфейс КЗЗ і всі запити до доступу до захищених об’єктів контролюються КЗЗ. А також визначити політикою цілісності домен КЗЗ та інші домени та механізми їх захисту. Тож можна стверджувати, що дана послуга реалізована не в повній мірі.

Самотестування при старті. Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС.

Політика самотестування, що реалізується КЗЗ, повинна містити властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ.

Послуга не реалізована оскільки відсутня політика самотестування, яка описувала б властивості КС та реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ.

Автентифікація вузла. Ця послуга дає можливість забезпечити захист від відмови від одержання і дозволяє однозначно встановити факт одержання певного об'єкта певним користувачем. Рівні даної послуги ранжируються на підставі можливості підтвердження результатів перевірки незалежною третьою стороною. Послуга реалізована, оскільки у системі присутні механізми, що виконують процес ідентифікації одним КЗЗ іншого.

Було обрано рівень гарантій Г-2 та проаналізовано, які з його вимог виконуються у розглянутій системі, а які ні.

Архітектура. КЗЗ повинен реалізовувати ПБ. Всі його компоненти повинні бути чітко визначені. Виконується.

Середовище розробки. Не виконується, оскільки у зазначених документах відсутня інформація про етапи кожної стадії життєвого циклу ОС та їх граничні вимоги.

Гарантування того, що процеси розробки і супроводження оцінюваної КС є повністю керованими з боку Розробника.

Розробник повинен визначити всі стадії життєвого циклу КС, розробити, запровадити і підтримувати в робочому стані документально оформлені методики своєї діяльності на кожній стадії. Мають бути документовані всі етапи кожної стадії життєвого циклу і їх граничні вимоги.

Розробник повинен розробити, запровадити і підтримувати в робочому стані документовані методики щодо керування конфігурацією КС на всіх стадіях її життєвого циклу. Система керування конфігурацією повинна забезпечувати керування внесенням змін в апаратне забезпечення, програми ПЗП, вихідні тексти, об'єктні коди, тестове покриття і документацію. Система керування конфігурацією повинна гарантувати постійну відповідність між всією документацією і реалізацією поточної версії КЗЗ.

Послідовність розробки. Не реалізовано, оскільки відсутній точний опис КС на кожній стадії розробки.

Вимоги до процесу проектування (послідовності розробки) забезпечують гарантії того, що на кожній стадії розробки (проектування) існує точний опис КС і реалізація КС точно відповідає вихідним вимогам (політиці безпеки).

На стадії розробки технічного завдання Розробник повинен розробити функціональні специфікації КС. Представлені функціональні специфікації повинні включати неформалізований опис політики безпеки, що реалізується КЗЗ. Політика безпеки повинна містити перелік і опис послуг безпеки, що надаються КЗЗ.

Повинна бути показана відповідність функціональні специфікації, що включатиме модель політики безпеки. Стиль специфікації: неформалізована.

Потрібно показати відповідність проекту архітектури моделі політики безпеки. На стадії розробки ескізного проекту Розробник повинен розробити проект архітектури КЗЗ. Представлений проект повинен містити перелік і опис компонентів КЗЗ і функцій, що реалізуються ними. Повинні бути описані будь-які використовувані зовнішні послуги безпеки. Зовнішні інтерфейси КЗЗ повинні бути описані в термінах винятків, повідомлень про помилки і кодів повернення. Стиль специфікації: неформалізована.

На стадіях розробки технічного проекту або робочого проекту Розробник повинен розробити детальний проект КЗЗ. Представлений детальний проект повинен містити перелік всіх компонентів КЗЗ і точний опис функціонування кожного механізму. Повинні бути описані призначення і параметри інтерфейсів компонентів КЗЗ. Стиль специфікації: неформальна.

Середовище функціонування. Не реалізовано, оскільки не задокументовано перелік усіх можливих параметрів конфігурації, які можуть використовуватись в процесі інсталяції, генерації та запуску ОС.

Вимоги до середовища функціонування забезпечують гарантії того, що КС поставляється Замовнику без несанкціонованих модифікацій, а також інсталюється і ініціюється Замовником так, як це передбачається Розробником.

Розробник повинен представити засоби інсталяції, генерації і запуску КС, які гарантують, що експлуатація КС починається з безпечного стану. Розробник повинен представити перелік усіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації і запуску.

Документація. Не реалізовано, оскільки відсутній детальний опис послуг безпеки, що реалізуються КЗЗ, та настанов адміністратору та користувачам стосовно послуг безпеки.

У вигляді окремих документів або розділів (підрозділів) інших документів Розробник повинен подати опис послуг безпеки, що реалізуються КЗЗ, настанови адміністратору щодо послуг безпеки, настанови користувача щодо послуг безпеки.

В описі функцій безпеки повинні бути викладені основні, необхідні для правильного використання послуг безпеки, принципи політики безпеки, що реалізується КЗЗ оцінюваної КС, а також самі послуги.

Настанови адміністратору щодо послуг безпеки мають містити опис засобів інсталяції, генерації і запуску КС, опис всіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації і запуску КС, опис властивостей КС, які можуть бути використані для періодичної оцінки правильності функціонування КЗЗ, а також інструкції щодо використання адміністратором послуг безпеки для підтримки політики безпеки, прийнятої в організації, що експлуатує КС.

Настанови користувачу щодо послуг безпеки мають містити інструкції щодо використання функцій безпеки звичайним користувачем (не адміністратором).

Випробування комплексу засобів захисту. Не реалізовано, оскільки відсутні детальна методика випробувань усіх механізмів, що реалізують послуги безпеки та не підтверджена достатність тестового покриття.

Розробник повинен подати для перевірки програму і методику випробувань, процедури випробувань усіх механізмів, що реалізують послуги безпеки. Мають бути представлені аргументи для підтвердження достатності тестового покриття.

Розробник повинен подати докази тестування у вигляді детального переліку результатів тестів і відповідних процедур тестування, з тим, щоб отримані результати могли бути перевірені шляхом повторення тестування.

Розробник повинен усунути або нейтралізувати всі знайдені “слабкі місця” і виконати повторне тестування КЗЗ для підтвердження того, що виявлені недоліки були усунені і не з'явилися нові “слабкі місця ”.

Опираючись на проведений аналіз системи, серед критеріїв побудованого профілю можна виділити нереалізовані на даний момент критерії та ті, що реалізовані не в повній мірі.

2.2 Проектні рішення щодо реалізації критеріїв профілю захищеності

Опираючись на проведений аналіз АСУ легковим автомобілем, побудовані моделі загроз та порушника і профіль захищеності, можна запропонувати наступні заходи по підвищенню рівня захищеності системи:

1 Для реалізації послуги НИ-2, необхідно ввести процедуру автентифікації працівників сервісної технічної служби для входу у систему.

2 Для реалізації послуги ЦО-2 пропонується створити захищений журнал реєстрації дій працівників технічної сервісної служби, в який буде заноситись інформація про внесені зміни у конфігураціях, час внесення змін та ідентифікатор працівника, що виконував їх виконував.

3 Для реалізації послуги НЦ-2 необхідно ввести процедуру контролю цілісності програмної частини управляючого блоку, що буде проводитись при старті системи, застосовуючи механізм перевірки контрольної суми.

4 Для реалізації послуги НТ-1 пропонується ввести процедуру самотестування за запитом для перевірки правильності функціонування і цілісність певної множини функцій КС.

5 Реалізувати організаційні заходи, що включатимуть:

– створення пакету документів, зазначених у вимогах до обраного рівня гарантій Г-2;

– створення політики безпеки (ПБ) щодо поводження з ресурсами АС та ознайомити з нею працівників, що обслуговують дану систему, наголошуючи на відповідальності за виконання усіх вимог цієї політики;

– призначення відповідального за дотримання положень ПБ;

– регулярний контроль керівництва над діями користувачів із правами адміністратора системи.

2.3 Реалізація послуги самотестування за запитом (НТ-1)

Послуга "Самотестування" дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій АС. У даній роботі розглядається реалізація послуги самотестування, що

перевіряє коректність роботи критичних функцій системи керування автомобілем.

Для реалізації критерію НТ-1 необхідно ввести можливість застосування відповідних засобів перевірки правильності функціонування компонентів АС, при виконанні певних операцій.

Згідно [5] приведемо перелік властивостей системи та процедур, реалізованих у функціональних компонентах АС, які можуть бути використані для оцінювання правильності функціонування усієї системи:

Таблиця 2.1 – Властивості системи

Компонент системи	Властивість
Керуючий блок	Наявність зв’язку з сервером
	Наявність зв’язку з усіма зареєстрованими датчиками
	Наявність зв’язку з капотним модулем
	Використовуване джерело живлення (основне/резервне)
Капотний модуль	Наявність зв’язку з легітимним керуючим блоком
Геолокаційний модуль	Наявність сигналу з супутників

Таблиця 2.2 – Процедури реалізовані в функціональних компонентах

Компонент системи	Процедура
Керуючий блок	Відкриття центрального замка
	Закриття центрального замка
	Відкриття багажнику
Капотний модуль	Увімкнення тревоги
	Вимкнення тревоги
	Увімкнення режиму Anti-hijack
	Вимкнення режиму Anti-hijack
	Запуск двигуна
	Зупинка двигуна

	Блокування двигуна
	Відміна блокування двигуна
	Блокування капоту

Для перевірки коректності роботи системи необхідно реалізувати набір тестів, використовуваних для оцінювання правильності функціонування різних функціональних компонентів при виконанні операцій.

Система автоматично проходить по всім станам системи і дає можливість користувачу підтвердити чи спростувати коректність роботи функцій.

У запропонованій системі тестування можливо реалізувати частину перевірок в автоматичному режимі, а для реалізації перевірки результатів інших тестів необхідно залучити користувача.

2.3.1 Вимоги до створюваної системи

2.3.1.1 Вимоги до програмної реалізації

Вимоги до методу тестування АСУ легковими автомобілями “SCar” пов'язані з необхідними функціональними можливостями, які спочатку мають бути в нього закладені:

1 Механізм перевірки коректності переходів системи по усім її можливим станам.

2 Можливість реалізації автоматичного тестування властивостей системи, перелічених в таблиці 2.1.

3 Можливість виконання автоматичного тестування при запуску системи, а потім у штатному режимі роботи з інтервалом 5 хвилин.

4 Можливість послідовного запуску усіх процедур, перелічених у таблиці 2.2 та надання можливості користувачу оцінити коректність їх реалізації для перевірки роботи системи.

5 Реалізація обов’язкового запуску тестування за участю користувача після встановлення АСУ автомобілем, після внесення будь-яких змін у

конфигурації системи, а також у процесі штатного функціонування системи за бажанням.

2.3.1.2 Вимоги до технічної реалізації

Вимоги до технічної реалізації:

1 Реєструвати дані про результати тестування у достатньому об'ємі, при якому в журналі реєстрації збережеться час проведення тестування, причина проведення тестування (автоматично, первинний запуск, по запиту користувача) та детальна інформація про усі отримані результати. Зберігати даний журнал у захіщеному вигляді.

2 Своєчасність тестування. Своєчасний аналіз станів системи (при запуску та у штатному режимі з інтервалами 5 хвилин), що проводиться в автоматичному режимі є дуже важливим, оскільки при своєчасному виявленні проблеми можливо у короткі строки отримати дані про причини їх виникнення та уникнути небажаних наслідків.

3 Захищеність. Можливість оцінювання результатів роботи системи в тестовому режимі лише власником після входу до системи шляхом проходження процедури авторизації для уникнення некоректної оцінки результатів роботи системи тестування зловмисником.

4 Розширюваність. Виконання цієї вимоги дозволить модифікувати програмну систему в ході її життєвого циклу і реалізувати тестування нових процедур.

2.3.1.3 Користувацькі вимоги

Вимоги до призначених для користувача можливостей по роботі з системою:

– можливість формування повідомлень про виявлені аномалії. Система тестування коректності роботи АСУ автомобілем повинна повідомляти власника автомобиля у разі виявлення проблем у роботі;

– можливість запуску системи тестування за бажанням користувача у штатному режимі роботи системи;

– зручність та інтуїтивно зрозумілий інтерфейс користувача.

2.3.2 Опис алгоритму роботи системи тестування

Згідно до зазначених вимог та цілей, тестування коректності роботи АСУ автомобілем побудовано на основі виконання послідовності із n процедур, що охоплюють усі функціональні можливості даної системи та контролю за відповідністю очікуваному результату, що здійснює користувач. Сам набір та порядок проходження по станам системи і розроблюється в період визначення функціональних можливостей системи, коли будується концепція нормальної діяльності системи. На даному етапі визначаються критичні функції системи, коректність роботи яких необхідно гарантувати. На рисунку 2.1 приведена блок схема алгоритму роботи запропонованої системи тестування.

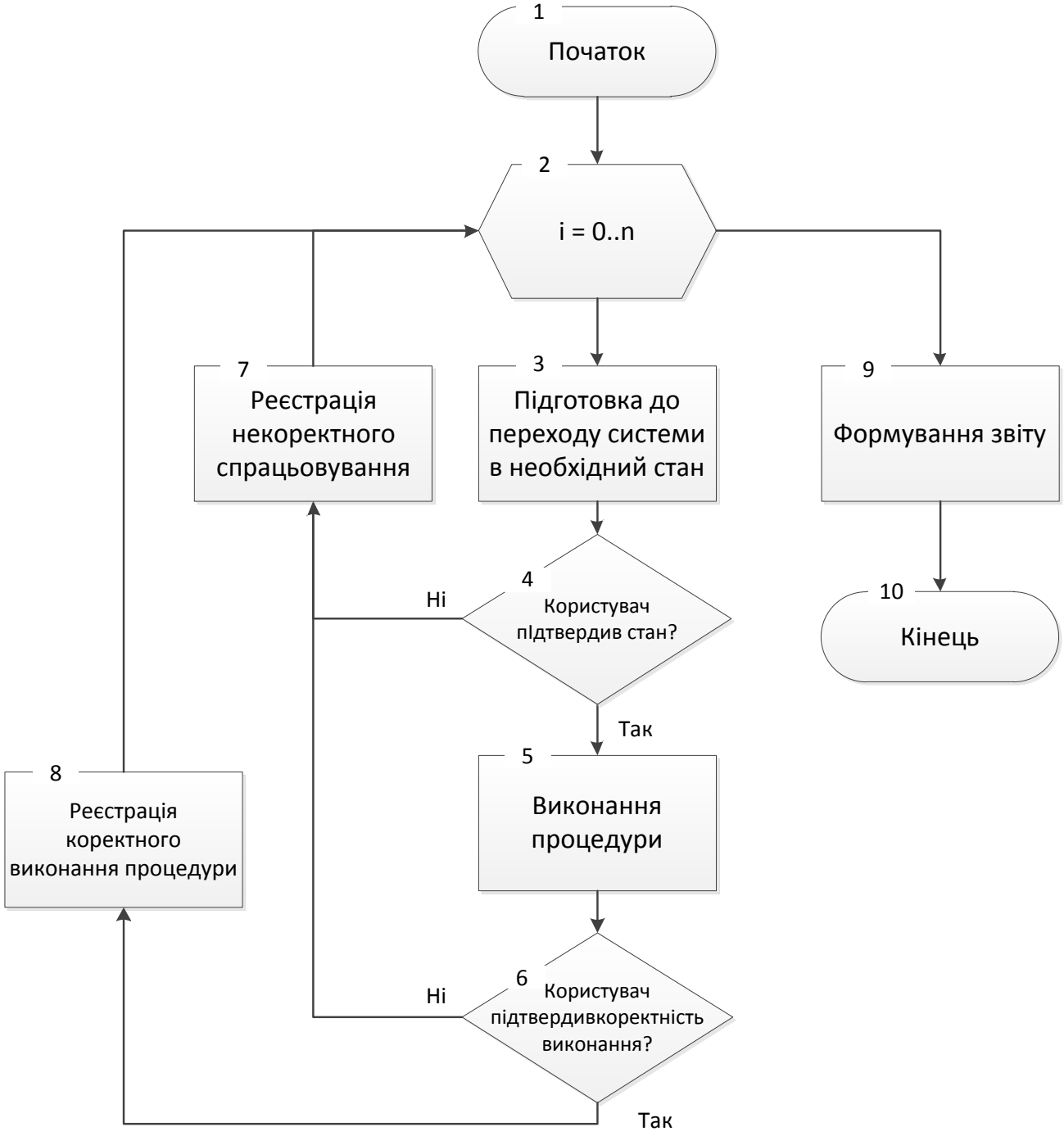

Рисунок 2.1 – Блок-схема алгоритму роботи системи тестування

Запропонована система дозволяє своєчасно виявити збої у роботі системи управління автомобілем, які могли виникнути під час встановлення або налагодженя керуючих блоків автомобіля, що виконують працівники техничної сервісної служби. На даний момент цей аспект є слабким місцем в захищеності АСУ легковими автомобілями «SCar» та релізація

запропонованого методу сумісно із веденням журналу реєстрації змін внесених в конфігураційні файли керуючого блоку дозволить знизити ризик від реалізації загроз, пов'язаних із неконтрольованою модифікацією файлів налаштувань.

2.4 Висновок

У даному підрозділі було проаналізовано реальний стан захищеності досліджуваної системи, виявлено нереалізовані критерії побудованого профілю захищеності, розроблено проектні рішення по підвищенню рівня захищеності АСУ легковими автомобілями шляхом реалізації досі не реалізованих критеріїв профілю захищеності (НИ-2, ЦО-2, НЦ-2, НТ-1), а також за допомогою введення необхідних організаційних заходів. Було запропоновано механізм реалізації послуги самотестування (НТ-1), який передбачає впровадження системи тестування функціональних можливостей АСУ легковим автомобілем з метою виявлення некоректної поведінки системи. Було висунуто вимоги до програмної та технічної реалізації запропонованої системи, а також користувацькі вимоги. Було описано алгоритм роботи запропонованої системи.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Для економічного обґрунтування розробки підсистеми самотестування для АСУ легковими автомобілями необхідно здійснити наступні розрахунки:

– капітальні витрати на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов’язані з виготовленням апаратури, приладів, програмного забезпечення;

– річні експлуатаційні витрати на утримання і обслуговування об'єкта проектування;

– річний економічний ефект;

– показники економічної ефективності розробки підсистеми самотестування для АСУ легковими автомобілями.

3.1 Розрахунок (фіксованих) капітальних витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

3.1.1. Визначення витрат на розробку моделі розслідування інцидентів кібербезпеки із врахування критеріїв захищеності інформації

3.1.1.1 Визначення трудомісткості розробки підсистеми самотестування для АСУ легковими автомобілями

Трудомісткість розробки розробку підсистеми самотестування визначається тривалістю кожної робочої операції:

$$t = t_{тз} + t_{в} + t_{а} + t_{з} + t_{обр} + t_{зз} + t_{р} + t_{д}, \text{ годин,}$$

де $t_{тз}$ – тривалість складання технічного завдання, $t_{тз} = 8$;

$t_{в}$ – тривалість вивчення ТЗ, літературних джерел за темою тощо, $t_{в} = 16$;

ta – тривалість аналізу реального стану захищеності досліджуваної системи з метою виявлення нереалізованих критеріїв побудованого профілю захищеності, $ta = 25$;

$t_З$ – тривалість формування рекомендацій та проектних рішень щодо реалізації досі не реалізованих критеріїв профілю захищеності з метою поліпшення стану захищеності АСУ легковими автомобілями, а також за допомогою введення необхідних організаційних заходів, $t_З = 40$;

$t_{обр}$ − тривалість розробки механізму реалізації послуги самотестування (НТ-1), який передбачає впровадження системи тестування функціональних можливостей АСУ легковим автомобілем з метою виявлення некоректної поведінки системи, $t_{обр} = 34$;

$t_{ЗЗ}$ – тривалість розробки вимог до реалізації запропонованого механізму (вимоги до програмної реалізації, вимоги до технічної реалізації, користувацькі вимоги), $t_{ЗЗ} = 60$;

tp – тривалість розробки алгоритму роботи запропонованої системи, $tp = 30$;

$t_Д$ – тривалість підготовки технічної документації, $t_Д = 6$.

Таким чином,

$$t = 8 + 16 + 25 + 40 + 34 + 60 + 30 + 6 = 219 \text{ годин},$$

3.1.1.2. Розрахунок витрат на розробку підсистеми самотестування для АСУ легковими автомобілями

Витрати на створення програмного продукту Кпз складаються з витрат на заробітну плату виконавця програмного забезпечення *Ззп* і вартості витрат машинного часу, що необхідний для опрацювання програми на ПК *Змч*:

$$К_{пз} = З_{зп} + З_{мч} = 21024 + 85{,}56 = 21109{,}56 \text{ грн.}$$

$$З_{зп} = t\, З_{пр} = 219*96 = 21024 \text{ грн.}$$

де t – загальна тривалість створення ПЗ, годин;

Зпр – средньогодинна заробітна плата програміста з нарахуваннями, грн/годину.

Вартість машинного часу для налагодження програми на ПК визначається за формулою:

$$З_{мч} = t_д \cdot С_{мч} = 6 \cdot 14{,}26 = 85{,}56 \text{ грн.}$$

де $t_д$ – трудомісткість підготовки документації на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч} = 0{,}8 \cdot 10 \cdot 1{,}64 + \frac{3500 \cdot 0{,}5}{1920} + \frac{2200 \cdot 0{,}2}{1920} = 14{,}26 \text{ грн.}$$

У складі ОЕ є в наявності функціональні модулі та програмне забезпечення, що дозволяє звільнити вміст поділюваних ресурсів, використовуваних для збереження пасивних об’єктів, а також атрибутів доступу до них. Процедура виконується стандартними засобами ОС Ubuntu Server 12.04 та оскільки воно підтримується вільним товариством, то є безкоштовним.

Таким чином, капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{пр} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} =$$

$$= 21109{,}56 + 2000 + 1500 = 24609{,}56 \text{ грн.}$$

де $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн;

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення, тис. грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, $К_{навч}$=2000 грн;

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, $К_{навч}$=1500 грн.

3.1.1 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_{в} + С_{к} + С_{ак}, \quad грн.$$

де $С_{в}$ - вартість відновлення й модернізації системи ($С_{в} = 0$);

$С_{к}$ - витрати на керування системою в цілому;

$С_{ак}$ - витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак}$ = 0 грн.).

Витрати на керування системою інформаційної безпеки ($С_{к}$) складають:

$$С_{к} = С_{н} + С_{а} + С_{з} + С_{ел} + С_{о} + С_{тос}, \text{ грн.}$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються ($С_{н}$ = 6000 грн.).

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_{з}$), складає:

$$С_з = З_{осн} + З_{дод}, \text{ грн.}$$

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 16000 грн. Для виконання контролю за самотестуванням системи працюватиме один спеціаліст на 0,3 ставки. Додаткова заробітна плата – 10% від основної заробітної плати. Отже,

$$С_з = 16000*0,3*12 + 16000*0,3*12*0,1= 63360 \text{ грн.}$$

Ставка ЄСВ для всіх категорій платників з 01.01.2016 р. складає 22%.

$$С_{єв} = 63360*0,22 = 13939,2 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.},$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=1,6 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р$ = 1920 год.);

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,64 грн./кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$$С_{ел} = 1,6*1920*1,64 = 5038,08 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат - 3% (Стос = 24609,56 *0,03=738,29 грн).

Витрати на керування системою інформаційної безпеки ($С_к$) визначаються:

$$С_к = 6000 + 63360 + 13939,2 + 5038,08 + 738,29 = 89075,57 \text{ грн.}$$

Отже, річні поточні витрати на функціонування системи інформаційної безпеки складають 89075,57 грн.

3.2 Оцінка можливого збитку від атаки на вузол або сегмент мережі

Автоматизована система управління легковим автомобілем контролює роботу усього автомобіля та представляє собою розподілений багатомашинний комплекс, який обробляє інформацію різних ступенів обмеження доступу.

3.2.1 Оцінка величини збитку

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки.

Необхідні *вихідні дані* для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 10 годин;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 5 годин;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 6 годин;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 6000 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 8000 грн./міс.;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), 4 осіб.;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 50 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 2 млн. грн. у рік;

$П_{зч}$ – вартість заміни встаткування або запасних частин, грн;

I – число атакованих сегментів корпоративної мережі, 1;

N – середнє число атак на рік, 13.

Автоматизована система управління легковим автомобілем контролює роботу усього автомобіля та представляє собою розподілений багатомашинний комплекс, який обробляє інформацію різних ступенів обмеження доступу.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = П_п + П_в + V,$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_П = \frac{\sum Зс}{F} \cdot t_п = \frac{6000 \cdot 50}{176} \cdot 10 = 17045{,}45 \quad \text{грн},$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч).

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч},$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн..;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, 0 грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ВИ} = \frac{\sum Зс}{F} \cdot t_{ви} = \frac{6000 \cdot 50}{176} \cdot 6 = 10227{,}27 \text{ грн.}$$

Витрати на відновлення сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{ПВ} = \frac{\sum Зо}{F} \cdot t_в = \frac{8000 \cdot 4}{176} \cdot 5 = 909{,}09 \text{ грн.}$$

$$П_в = 10227{,}27 + 909{,}09 = 11136{,}36 \text{ грн.}$$

Втрати від зниження очікуваного обсягу прибутків за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із средньогодинного обсягу прибутку і сумарного часу простою сегмента корпоративної мережі:

$$V = \frac{O}{Fг} \cdot (t_П + t_В + t_{ВИ})$$

$$V = \frac{2000000}{2080} \cdot (10 + 5 + 6) = 20192{,}3 \text{ грн.}$$

де $F_г$ – річний фонд часу роботи філії (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 год.

$$U = 17045{,}45 + 11136{,}36 + 20192{,}3 = 48374{,}11 \text{ грн.}$$

Таким чином, загальний збиток від атаки на сегмент корпоративної мережі організації складе:

$$B = \sum_i \sum_n U = \sum_1 \sum_{13} 48374{,}11 = 532115{,}22 \text{ грн.}$$

3.2.2 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B \cdot R - C \text{ грн.},$$

де B – загальний збиток від атаки у разі перехоплення інформації, тис. грн.;

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці (30%);

С – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки:

$$E = 532115{,}22*0{,}3 - 89075{,}57 = 79559 \text{ грн.}$$

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки:

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці,}$$

де E – загальний ефект від впровадження системи інформаційної безпеки грн.;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = \frac{79559}{24609{,}56} = 2{,}86, \quad \text{частки одиниці,}$$

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$\text{ROSI} > (\text{N}_{\text{деп}} - \text{N}_{\text{інф}})/100),$$

де $N_{деп}$ – річна депозитна ставка, (17 %);

$N_{інф}$ – річний рівень інфляції, (11%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$2,86 > (17 - 11)/100 = 2,86 > 0,06.$$

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{2,86} = 0,34, \quad \text{років.}$$

3.4 Висновок

Відповідно до проведених розрахунків економічної ефективності розробка підсистеми самотестування для АСУ легковими автомобілями можна дійти висновку, що запропоновані рішення є економічно доцільні, оскільки згідно із значенням коефіцієнта повернення інвестицій (ROSI = 2,86) кожна гривня, вкладена в розробку підсистеми самотестування приноситиме додатковий прибуток в розмірі 2,86 грн. Термін окупності складає 0,34 роки (124 дні).

ВИСНОВКИ

В ході дослідження питань пов’язаних із станом захищеності автоматизованих систем керування легковими автомобілями було виконано поставлені цілі:

– виконано обстеження ОІД, описано умови функціонування АС, її структуру та оброблювану інформацію;

– побудовано та проаналізовано модель загроз та модель порушника;

– побудовано профіль захищеності та проаналізовано кожен його критерій;

– розроблено проектні рішення по підвищенню рівня захищеності АСУ легковими автомобілями шляхом реалізації досі не реалізованих критеріїв профілю захищеності (НИ-2, ЦО-2, НЦ-2, НТ-1), а також за допомогою введення необхідних організаційних заходів;

– запропоновано механізм реалізації послуги самотестування (НТ-1), який передбачає впровадження системи тестування функціональних можливостей АСУ легковим автомобілем з метою виявлення некоректної поведінки системи;

– висунуто вимоги до програмної та технічної реалізації запропонованої системи, а також користувацькі вимоги;

– описано алгоритм роботи запропонованої системи;

– обґрунтовано економічну доцільність впровадження запропонованих проектних рішень.

ПЕРЛІК ПОСИЛАНЬ

1 НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» / ДСТСЗІ СБ України – Київ, 1999.

2 НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі», затверджений наказом ДСТСЗІ СБ України від 04.12.2000 р. № 53.

3 Постанова Кабінету Міністрів України «Про затвердження Правил захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.06 р. № 373.

4 Закон України «Про доступ до публічної інформації».

5 НД ТЗІ 2.7-010-09 «Методичні вказівки з оцінювання рівня гарантій. коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу».

6 НД ТЗІ 2.7-009-09 «Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу».

7 НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу»

8 НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу».

9 Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».

10 Закон України «Про інформацію».

11 Міжнародний стандарт ISO/IEC 27001.

12 Положення про державну експертизу в сфері захисту інформації.

13 Helman P., Liepins G., Richards W. Foundations of Intrusion Detection // Proc. of the 15th Computer Security Foundations Workshop. 1992. p.120.

14 Ryan J., Lin M., Miikkulainen R. Intrusion Detection with Neural Networks. AI Approaches to Fraud Detection and Risk Management: Papers from the 1997 Workshop (Providence, Rhode Island), p. 79. Menlo Park, CA: AAAI. 1997.

15 Bace R. An Introduction to Intrusion Detection Assessment for System and Network Security Management. 1999.

16 Kumar S., Spafford E. A Pattern Matching Model for Misuse Intrusion Detection // Proc. of the 17th National Computer Security Conference. 1994. p. 125.

17 Allen J., Christie A., Fithen W., McHugh J., Pickel J., Stoner E. State of the Practice of Intrusion Detection Technologies. Carnegie Mellon University. Networked Systems Survivability Program. Technical Report CMU/SEI-99-TR-028 ESC-99-028. 2000, January.

18 Denning D. E. An intrusion detection model // IEEE Trans. on Software Engineering, 1987, SE-13. p. 232.

19 Garvey T. D. Lunt T. F. Model-based intrusion detection // Proc. of the 14th National Computer Security Conference. 1991.

20 Teng H. S., Chen K., Lu S. C. Adaptive real-time anomaly detection using inductively generated sequential patterns // Proc. of the IEEE Symposium on Research in Computer Security and Privacy.1990. p. 284.

21 Червяков Н. И., Малофей О. П., Шапошников А. В., Бондарь В. В. Нейронные сети в системах криптографической защиты информации // Нейрокомпьютеры: разработка и применение. 2001, No 10.

22 Fu L. A Neural Network Model for Learning Rule-Based Systems // Proc. of the International Joint Conference on Neural Networks. 1992. I. p. 348.

23 Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с.

24 А.Ю. Щеглов Защита компьютерной информации от несанкционированного доступа. – Наука и техника, Санкт-Петербург, 2004. – 384 с.

25 В.Г. Олифер, Н.А. Олифер Компьютерные сети. Принципы, технологии, протоколы – Спб.: Питер, 2001. – 672 с.

26 Система перехвата и дешифровки GPRS (Электр. ресурс) / Спосіб доступу URL: http://itbuben.org/blog/1474.html.

27 НД ТЗІ 3.1-001-07 «Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи».

ДОДАТОК А. Відомість матеріалів дипломного проекту

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	1 Розділ	26	
6	А4	2 Розділ	17	
7	А4	3 Розділ	11	
8	А4	Висновки	1	
9	А4	Перелік посилань	3	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК

на дипломну роботу магістра на тему:
Розробка підсистеми самотестування для АСУ легковими автомобілями
студента групи 125м-17-1
Кислякова Якова Андрійовича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на __ сторінках та містить __ рисунків, __ таблиць, __ джерела та __ додатка.

Актуальність теми полягає в необхідності вдосконалення організації захисту інформації підсистеми самотестування для АСУ легковими автомобілями.

Зміст та структура дипломної роботи дозволяють розкрити поставлену тему повністю.

Студент показав достатній рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота виконана самостійно. У роботі було проведено аналіз стану захищеності автоматизованої системи керування легковими автомобілями; розроблено проектні рішення щодо підвищення рівня захищеності об’єкта дослідження; запропоновано використання механізму тестування коректності роботи системи керування як засобу підвищення інформаційної безпеки розглянутої системи.

Це підтверджує самостійність обробки даних, практичні рекомендації та висновки.

Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому дипломна робота задовольняє усім вимогам і може бути допущена до захисту, а його автор Кисляков Яків Андрійович заслуговує на оцінку «_____».

Керівник дипломної роботи,
д.ф.-м.н., проф. Т.С. Кагадій

Керівник спец. част.,
ст. викл. кафедри БІТ І.І. Начовний