МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

«На правах рукопису»
УДК 681.3.06

«До захисту допущено»
Завідуючий кафедрою СІКЗ
_____к.т.н. Г.В. Шуклін
«____» _____2023 р.

БАКАЛАВРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 “Кібербезпека”

на тему: **ПОБУДОВА СИСТЕМИ ЗАХИСТУ ІНКАСАТОРСЬКОГО АВТОМОБІЛЯ**

Студента групи СЗД-41 Влащука Богдана Анатолійовича _____
(підпис)

Науковий керівник: к.т.н., доц. Котенко Андрій Миколайович _____
(підпис)

Нормоконтроль ст. викл. Зозуля Сергій Анатолійович _____
(підпис)

КИЇВ – 2023

«ЗАТВЕРДЖУЮ»
Завідувач кафедри СІКЗ
_____ к.т.н. Г.В. Шуклін
(підпис)
«_____»_____ 2023р.

ЗАВДАННЯ

на атестаційну роботу бакалавра

студенту: Влащуку Богдану Анатолійовичу

1.Тема роботи: Побудова системи захисту інкасаторського автомобіля, затверджено наказом від «24 » лютого 2023р. № 26

2.Термін здачі студентом оформленої роботи «____» _____ 2023р.

3. Об'єкт дослідження: процеси захисту інформації від витоку по технічним каналам.

4. Предметом дослідження: технології захисту, які забезпечують захисту інформації від витоку по технічним каналам з інкасаторського автомобіля.

5. Мета роботи: удосконалення та рекомендації щодо застосування методів захисту інформації, яка передається та приймається по технічним каналам в інкасаторському автомобілі.

6.Перелік питань, які мають бути розроблені:

Для досягнення вказаної мети виконуються такі основні задачі:

- аналіз несанкціонованого доступу по технічним каналам, до інформації, яка передається та приймається в інкасаторському автомобілі;
- аналіз та дослідження існуючих методів технічного захисту інформації при переміщенні інкасаторського автомобіля;
- створення рекомендацій щодо захисту інформації, яка передається та отримується по технічним каналам в інкасаторському автомобілі.

7. Дата видачі завдання «____» _____20____р.

Науковий керівник _____ Котенко А.М.
(підпис)

Завдання прийняла до виконання _____Влащук Б.А.

КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання «24» лютого 2023р.

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури	до 26.02.23р.	
2	Обґрунтування актуальності теми роботи	до 27.02.23р.	
3	Написання першого розділу роботи	до 16.03.23р.	
4	Написання другого розділу роботи	до 12.04.23р.	
5	Написання третього розділу роботи	до 08.05.23р.	
6	Написання висновків по роботі	до 11.05.23р.	
8	Підготовка демонстраційних матеріалів	до 18.05.23р.	
9	Підготовка доповіді	до 24.05.23р.	
10	Захист в ДЕК		

Студент: СЗД -41 Влащук Б.А. _____
(підпис)

Науковий керівник: к.т.н., доц. Котенко А.М. _____
(підпис)

Нормоконтроль: ст. викл. Зозуля С.А. _____
(підпис)

ЗМІСТ

РЕФЕРАТ

Дипломна робота містить 47 сторінок, 24 рисунки.

Представлено огляд наявних методів виявлення уразливості, пов`язаних з витоку конфіденційної інформації по технічним каналам під час руху інкасаторського автомобіля. Проведено порівняльний аналіз параметрів. Визначено напрямки, за якими здійснюється вдосконалення засобів технічного захисту інформації в інкасаторському автомобілі. Для оцінювання методів пошуку витоку конфіденційної інформації під часу руху інкасаторського автомобіля визначено підходи щодо показників, які на це впливають. Особливу увагу приділено таким показникам, як потужність інформативного сигналу, який передається по радіотехнічному, оптичному та акустичному каналах. Створено структурну схему та методика технічного захисту інформації при переміщенні інкасаторського автомобіля.

Об’єктом дослідження: є процеси захисту інформації від витоку по технічним каналам.

Предметом дослідження є технології захисту, які забезпечують захист інформації від витоку по технічним каналам з інкасаторського автомобіля.

Мета роботи удосконалення та рекомендації щодо застосування методів захисту інформації, яка передається та приймається по технічним каналам в інкасаторському автомобілі.

Для досягнення вказаної мети виконуються такі основні задачі:

- аналіз несанкціонованого доступу по технічним каналам до інформації, яка передається та приймається в інкасаторському автомобілі;
- аналіз та дослідження існуючих методів технічного захисту інформації при переміщенні інкасаторського автомобіля;
- створення рекомендацій щодо захисту інформації, яка передається та отримується по технічним каналам в інкасаторському автомобілі.

ABSTRACT

Thesis contains 47 pages, 24 figures.

An overview of existing methods for detecting vulnerabilities related to the leakage of confidential information through technical channels while a collection vehicle is moving is presented. A comparative analysis of the parameters is carried out. The directions for improving the means of technical protection of information in a collection vehicle are determined. To evaluate methods for finding leaks of confidential information during the movement of a collection vehicle, approaches to the indicators that affect this are determined. Particular attention is paid to such indicators as the power of the informative signal transmitted via radio, optical and acoustic channels. A structural diagram and methodology for technical protection of information when moving a collection vehicle have been created.

Object of research: processes for protecting information from leakage through technical channels .

The subject security technologies that protect information from leakage through technical channels from the collection vehicle.

The purpose improvement and recommendations on the application of methods for protecting information transmitted and received through technical channels in a collection vehicle.

To achieve this goal, the following main tasks are performed:

- analysis of unauthorized access through technical channels to information transmitted and received in the collection vehicle;

- analysis and research of existing methods of technical protection of information when moving a collection vehicle;

- development of recommendations for the protection of information transmitted and received through technical channels in a collection vehicle.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

БЛОС	Бездротові локальні обчислювальні системи	Wireless local cleaning systems
ОІД	Об`єкт інформаційної діяльності	Object of information activity
СІЗ	Системи інформаційного захисту	Information protection systems
EEPROM	Постійний запам’ятовувач що програмується та очищується за допомогою електрики	Electrically Erasable Programmable Read-Only Memory
NIST	Національний інститут стандартизації та технологій	The National Institute of Standards and Technology
PKI	Інфраструктура публічних ключів	Public key infrastructure
RAM	Пам’ять з довільним доступом	Random Access Memory
RFID	Радіочастотна ідентифікація	Radio frequency identification
ROM	Пам’ять лише для читання	Read Only Memory
SRAM	Статична оперативна пам’ять з довільним доступом	Static random access memory
TDMA	Метод часового поділу	Time division multiple access
WLAN	Метод часового поділу	Wireless Local Area Network
ВЧ	Високі частоти	
ЗЗІ	Засоби захисту інформації	
ІС	Інформаційна система	
ІТС	Інформаційно-телекомунікаційна система	
ОЗП	Оперативний запам’ятовувальний пристрій	

УВЧ Ультра високі частоти

ВСТУП

Завдання захисту інкасаторських автомобілів стають дедалі актуальнішими паралельно з розвитком інформаційних та технічних систем захисту, що лежать в їхній основі.

Актуальність теми Завдання технічного захисту інформації при переміщенні інкасаторського автомобіля на теперішній час прогресирує в напрямку його вдосконалення. Така тенденція зумовлена наступними чинниками:

Прогрес в створенні нових методів і засобів отримання інформації, що дають змогу здійснювати несанкціоноване втручання в процеси передачі та прийому інформації при переміщенні інкасаторського автомобіля, досягає все більшого обсягу інформації на безпечній відстані від руху інкасаторського автомобіля, використовуючи телекомунікації території, де відбувається переміщення інкасаторського автомобіля.

Сучасне досягнення мікроелектроніки, що сприяють створенню технічної бази для різноманітного виготовлення доступних кінцевому споживачеві засобів негласного отримання інформації через технічні канали. Доступність мініатюрних та камуфльованих технічних засобів отримання інформації перетворює завдання несапнкціонованого доступу до інформації з унікальної і ризикованої операції на прибуткові шпали, що збільшує кількість бажаючих легкої наживи діями за межами правового поля.

Оснащенням приміщень, в яких зберігаються гроші, а також останнім часом інкасаторських автомобілів, різноманітною електронною та радіоелектронною апаратурою, фізичні процеси в якій сприяють випадковому неконтрольованому витоку конфіденційної інформації з приміщень та інкасаторських автомобілів.

Виходячи з вищесказаного, ефективний захист інформації з урахуванням цих тенденцій можливий за ширшого використання технічних засобів захисту,

що в свою чергу підтверджує актуальність вибраної теми кваліфікаційної роботи.

Об’єктом дослідження: є процеси захисту інформації в комп`ютерних мережах з виходом в зовнішню мережу Інтернет.

Предметом дослідження є технології захисту, які забезпечують безпеку передачі та отримання інформації через Веб-додатки.

Мета роботи удосконалення та рекомендації щодо застосування методів захисту інформації, яка передається та приймається через Веб-додатки.

Для досягнення вказаної мети виконуються такі основні задачі:

- аналіз кібератак, які спрямовані через Веб-додатки;
- аналіз та дослідження існуючих методів захисту хостів;
- створення рекомендацій щодо захисту інформації, яка передається та отримується через Веб-додатки.

РОЗДІЛ 1 ТЕХНІЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ В ІНКАСАТОРСЬКОМУ АВТОМОБІЛІ

1.1. Особливості витоку інформації з інкасаторського автомобіля

В загальному розумінні витік інформації уявляє собою несанкціоноване перетворення інформації від її джерела до злодія. Саме розуміння "*витік*" є застосовується в достатньо широкому розумінні. Часто приходиться зустрічатись з такими явищами як витік води, витік газу, витік матеріальних цінностей з інкасаторського автомобіля, витік інформації з об`єкта інформаційної діяльності (ОІД). Витік інформації з інкасаторського автомобіля можливий шляхом її розголошення особами, які причетні до нього, втратою цими особами носіїв, на яких зберігається службова та конфіденційна інформація, видобуток інформації за допомогою електромагнітних та акустичних полів, тощо. Простою та дуже небезпечною причиною є бажання осіб, причетних до роботи в обслуговуванні та експлуатації інкасаторських автомобілів розповісти останніми новинами щодо своєї професійної діяльності з рідними або близькими. Таке спілкування породжує передумови для витоку конфіденційної інформації. Засобами перетворення такої конфіденційної інформації можуть бути будь-які її носії.

В багатьох випадках витік розглядають як процес витікання води з крану, який має пошкодження. Що стосується технічного оснащення, яке забезпечує прийом та передачу інформації при переміщенню інкасаторського автомобіля, то в цьому випадку витік розглядають як несанкціоноване поширення носія із захищеною інформацією за межі інкасаторського автомобіля. Однак такий розгляд виявляється хибним, оскільки для інформації не виконується закон збереження маси. Засоби масової інформації (ЗМІ) великою кількістю примірниками розповсюджують різного значення інформацію однак при цьому з джерелом (ЗМІ) нічого не відбувається.

Витік інформації з інкасаторського автомобіля по технічним каналам можна інтерпретувати по аналогії з крадіжкою матеріальних цінносте і який має низку особливостей, які треба враховувати під час організації технічного захисту інформації при переміщенні інкасаторського автомобіля:

- в процесі витоку інформації не виконуються закони збереження маси, що призводить до того, що витік не можна ідентифікувати за рахунок зменшення кількості інформації, яка відображена в її джерелі;
- витік інформації може відбуватися тільки в разі потрапляння її до зацікавленого в ній злодія, на відміну, від витоку певної маси води або маси газу;
- в процесі витоку інформації відбувається її розповсюдження і кількість осіб, які становляться її власниками збільшується, що призводить до того, що вартість інформації стає меншою.

Отже, відповідно першій особливості відбувається ускладнення в своєчасному виявленні витоку інформації при переміщенні інкасаторського автомобіля. Це відрізняє процес витоку матеріальних цінностей, де при дійсності такого явища, достатньо провести ревізію на їх наявність для виявлення витоку цих цінностей унаслідок розкрадання. При здійсненні витоку інформації при переміщенні інкасаторського автомобіля, на перший погляд не спостерігаються ознаки несанкціонованого доступу до неї: цінності та документи, які знаходяться в інкасаторському автомобілі на місці, відбитки печаток на мішках та сейфах не порушені, сліди проникнення в сам автомобіль відсутні. Однак поява непрямих ознак таких як завади, які не дають можливість передавати операторам, які спостерігають за рухом автомобіля, закриття відеокамер в точках пересування автомобіля дає право визначати акт витоку інформації при переміщенні інкасаторського автомобіля. За рахунок ефекту запізнювання за часом ознак, за якими ідентифікується початок процесу витоку інформації з інкасаторського

автомобіля, завдання хоча б часткової нейтралізації негативних наслідків стає достатньо складним.

Відповідно другій особливості важливим є постійно контролювати заходи безпеки інформації, оскільки акти втрати документів, розголошення даних щодо кількості грошей, які перевозить інкасаторський автомобіль, або наявність матеріальних цінностей в ньому та поширення носіїв за межі контрольованої зони не завжди призводять до витоку інформації. Прикладом може бути той факт, що якщо конфіденційну розмову під час переміщення в інкасаторському автомобілі керівника групи забезпечення чути за межами автомобіля через нещільно зачинені вікна, а сам автомобіль пересувається достатньо швидко, то витік інформації відсутній, хоча носій інформації, в даному випадку акустичні хвилі, виходить за межі контрольованої зони – інкасаторського автомобіля. Якщо інкасаторський автомобіль зупинився, а його ведуть злодії, які намагаються скористається інформацією з почутої розмови в особистих чи інших цілях або поділиться нею з іншими зацікавленими в ній зловмисниками, то в цьому випадку відбувається витік інформації з інкасаторського автомобіля.

Узагальнюючи, справедливо розглядати витік інформації як факт порушення її безпеки тільки в тому випадку, якщо вона потрапляє до зловмисника незалежно від того, знає чи не знає про це власник інформації. Якщо з якоїсь причини на цьому шляху передачі інформації відбувається розрив у ланцюжку, то інформація зникає разом з її носієм, а витоку інформації не відбувається.

Таким чином, під витоком інформації з при переміщенні інкасаторського автомобіля слід розуміти не процес поширення носія, а варіант поширення, що закінчується потраплянням інформації до зловмисника. Вихід же носія за межі інкасаторського автомобіля створює передумови для витоку інформації та підвищує загрозу її безпеці. Принциповим є несанкціоноване одержання інформації. Якщо одержувач інформації лигітимний, то витік не відбувається,

а здійснюється лише процес передачі інформації засобами функціонального каналу зв'язку, який спеціально створюється для забезпечення комунікацій у взаємодії присутніх в інкасаторському автомобілі та оператором, який контролює його переміщення.

Спроможність витоку інформації при переміщенні інкасаторського автомобіля характеризується ризиком витоку, а цілеспрямована діяльність зі зміни спроможності витоку уявляє собою процес керування ризиком.

В багатьох випадках крадіжка та витік інформації по технічним каналам розглядаються як автономні корельовані процеси. Якщо під крадіжки розуміти умисне привласнення чужої власності без дозволу її законного володаря, то несанкціоноване зняття інформації в результаті її витоку уявляє собою один із способів її крадіжки.

1.2. Типова структура та види технічних каналів витоку інформації з інкасаторського автомобіля

Фізичний шлях несанкціонованого поширення носія із захищуваною інформацією від її джерела до зловмисника утворює канал витоку інформації. Залежно від виду носія інформації канали її витоку різняться за структурою. Якщо поширення інформації відбувається за допомогою технічних засобів, то відповідний канал називається технічним каналом витоку інформації. Узагальнену структуру типового технічного каналу витоку наведено на рисунку 1.1.

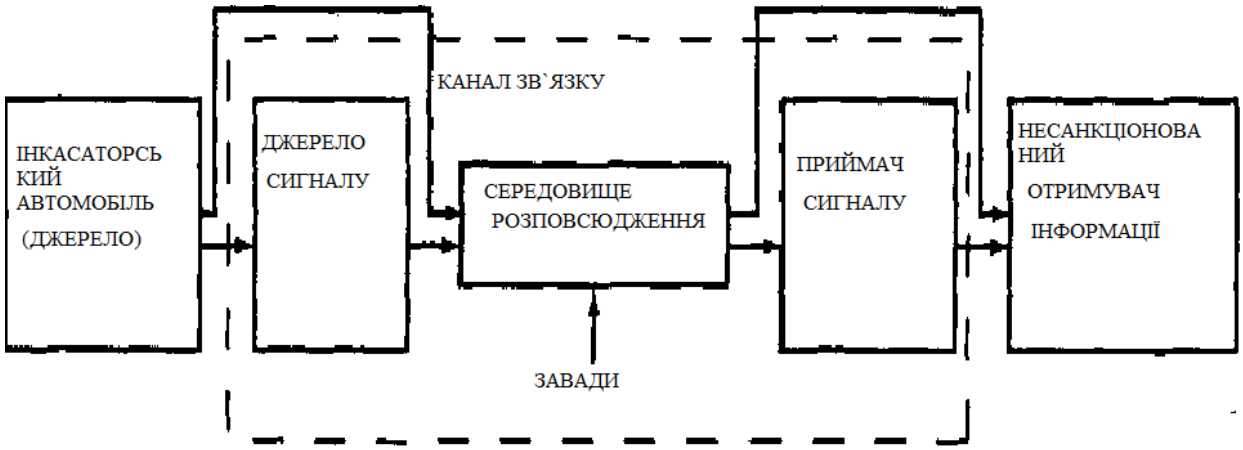

Рисунок 1.1. Функціональна схема технічного каналу витоку інформації при переміщенні інкасаторського автомобіля.

Малюнок показує, що інформативний сигнал, який передається може походити з носіїв, які одночасно виступають їх джерелами, так може передаватися з мобільних носіїв, інформаційне навантаження якого на них зберігається. Прикладами є паролі, які шифрують джерела інформації, можуть переноситися особами, причетними до системи роботи ІА або аномальними поштовхами в просторі від місця знаходження джерела до зловмисника, утворюючи канал витоку інформації. Отже технічний канал витоку інформації якими можуть виступати поверхні самого автомобіля за рахунок відбиття хвиль уявляє собою джерело технічного витоку інформації, середовище розповсюдження носія та особи, яка намагається несанкціоновано отримати цю інформацію. Інформація, яка передається завдяки акустичним, електромагнітним полями та через електричний струм, попередньо запам`ятовується в джерелі сигналів, кожному з яких ставиться у відповідність свій параметр. У зв'язку джерело сигналу, середовище його поширення і приймач сигналу утворюють у сукупності канал зв'язку. Завдання каналу зв'язку полягає в передачі вхідної інформації санкціонованому одержувачу з мінімальними спотвореннями, часовими, енергетичними та іншими витратами.

Канал витоку інформації на носіях у вигляді полів і елементарних частинок містить ті самі елементи, що й канал зв'язку. Відмінність між ними умовна - залежно від одержувача інформації. Учасник каналу зв`язку має доступ до інформації, в той же час в каналі витоку спостерігається учасник, який не має доступу до інформації. Таким учасником є особа, яка намагається несанкціоновано отримати інформацію з використанням засобу негласного отримання інформації, який встановлюється всередині ІА співучасником злочину і який має відношення до функціонування ІА. За відсутності джерела інформації та її одержувача витоку інформації немає. Аналогічним чином, канал зв'язку за допомогою мобільного пристрою існує постійно, але передача інформативного сигналу здійснюється лише тоді, коли сторони по обидва кінця каналу зв'язку починають здійснювати спілкування.

На вхід каналу зв'язку надходить інформація у вигляді первинного сигналу або саме джерело може бути джерелом інформації. Як джерела сигналів можуть бути:

об'єкт спостереження, що відбиває електромагнітні хвилі, зокрема світло; об'єкт, за яким здійснюється спостереження, і при цьому випромінює власні електромагнітні хвилі в діапазоні оптичних частот та діапазоні радіочастот, які виникають за рахунок виділення тепла при русі електронів та акустичні поля, які виникають за рахунок тертя при русі передавачі функціональних каналів зв'язку; ретранслятори у вигляді засобів негласного отримання інформації; джерела побічних електромагнітних випромінювань і наведень (ПЕМВН); радіоактивні матеріали.

З вищесказаного можна зробити висновок, що передавачі сигналів є одночасно джерелами інформації, які можна ідентифікувати за певними ознаками. Лише у випадку, коли надається семантична інформація, вона надходить на вхід іс- |" 111 ика сигналу на носії у вигляді первинного сигналу.

Зазначені на малюнку стрілками шляхи входу і виходу інформації позначають вхід і вихід первинних сигналів з інформацією. Оскільки інформація від

джерела надходить на вхід каналу в мові джерела (у вигляді буквено-цифрового тексту, символів, звуків, сигналів тощо), то передавач здійснює перетворення цієї форми представлення інформації на форму, яка забезпечує запис її на носій інформації, відповідний середовищу розповсюдження. У загальному випадку джерело сигналу виконує такі функції: створює (генерує) поле (акустичне, електромагнітне) або електричний струм, які переносять інформацію;

здійснює запис інформації на носій (модуляцію інформаційних параметрів носія);

підсилює потужність сигналу (носія з інформацією);

забезпечує передачу (випромінювання) сигналу в середовище поширення в заданому секторі простору.

Запис інформації здійснюється шляхом зміни параметрів носія відповідно до рівня первинного сигналу, що надходить на вхід. Якщо носіями інформації є суб'єкти і матеріальні тіла (макрочастинки), то передавач відповідає первісному сенсу цього слова - передавати або переносити, тобто виконує функцію носія. У разі коли інформацію переносять сигнали (поля, електричний струм і елементарні частинки), то передавачі є джерелами сигналів.

Середовище поширення носія - частина простору, в якій переміщується носій від джерела сигналу до його приймача. Середовище поширення може бути у вигляді вільного простору і напрямних ліній. Як напрямні лінії використовують електричні дроти різної конфігурації, хвилеводи, волоконно-оптичні кабелі, звукопроводи та інші конструкції. Їхнє просторове положення визначає маршрут руху носія в просторі. Під час передавання інформації напрямними лініями функціональних каналів зв'язку забезпечуються менші втрати енергії носія на марне опромінення простору і більша безпека інформації, ніж під час поширення носіїв у вільному просторі. Однак при цьому різко зростають витрати на створення та експлуатацію таких каналів

зв'язку.

Приймач сигналу виконує функцію, зворотну функції передавача. Він здійснює:

вибір (селекцію) носія з потрібною одержувачу інформацією;
посилення прийнятого сигналу-носія до значень, що забезпечують знімання інформації;
знімання інформації з носія (демодуляцію, декодування);

перетворення інформації у форму сигналу, доступну одержувачу (людині, технічному пристрою), і посилення первинних сигналів до значень, необхідних для їх сприйняття людиною і технічним пристроєм. Якщо одержувач інформації людина, то інформація з виходу приймача має бути представлена мовою спілкування людей. Якщо технічний пристрій, то форма подання інформації має бути зрозуміла цьому пристрою. Наприклад, якщо одержувач ЕОМ, то з виходу приймача на ЕОМ подається двійкова послідовність у кодах, наприклад, таблиці ASCII DOS, KOI8, Windows тощо. Властивості середовищі дають спроможність передавати довільну інформацію, і це призводить до того, що по відношенню до інформативного сигналу постійно існують завади. Чим наближені параметри інформативного сигналу і завад, тим складніше їх розрізнити при прийнятті інформативного сигналу, а значить і сильніший вплив завад на інформативний сигнал. Це означає, що якщо модуль різниці між частотою завади та частотою радіосигналу, який є носієм інформативного сигналу, більше за ширину смуги пропускання приймача, то завада буде відфільтрована приймачем . Якщо їхні частоти перетинаються, то після демодуляції перешкода накладеться на сигнал, що призведе до зміни інформаційних параметрів сигналу, аж до повного руйнування інформації. Зі зростанням числа сигналів у діапазоні радіочастот постійно зростає і проблема їх електромагнітної сумісності. Але ці заходи погано працюють стосовно джерел перешкод. Наприклад, зростання парку автомобілів у місті підвищує насиченість ефіру перешкодами від їхніх

систем запалювання, які повністю не придушуються встановленими в них фільтрами.

За своєю структурою технічні канали в інкасаторському автомобілі є наступні:

Специфіка витоку інформації по радіоелектронному каналу полягає в тому, що передача та прийом інформативного сигналу відбувається одним із видів полів, а саме завдяки електричним полям, магнітним полям та електромагнітним полям, які визначають діапазон радіохвиль. крім того основою в цьому є електричний струм, який виникає за рахунок направленому руху електронів які пересуваються в металевих дротах. Варто зазначити, що діапазон частот в цьому випадку має великий розмах, а саме від герц до гіга герц.

Виходячи з многовиду властивостей радіоелектронного каналу виникає потреба розділити його на два класи, а саме першим є електромагнітний канал передачі інформативного каналу. Такими носіями є електричне поле, магнітне полк та електромагнітне поле. Другим є електричний канал, передача інформативного сигналу виступає електричний струм.

Що стосується акустичного каналу, то в цьому випадку інформативний сигнал передається за допомогою пружних акустичних хвиль, які розділяються на інфразвуковий діапазон де частота менше $16\ Гц$, звуковий діапазон, де інтервал частот від $16\ Гц$ до $20\ КГц$ та на ультразвуковий діапазон, в якому частота перевищує $20\ КГц$, що спроможні поширюватись в атмосфері, воді та твердому середовищі.

У речовому каналі витік інформації здійснюється шляхом несанкціонованого поширення носіїв із захищуваною інформацією у вигляді речовини, насамперед викинутих чернеток документів і використаного копіювального паперу, забракованих деталей і вузлів, демаскувальних речовин тощо. Демаскувальні речовини у вигляді твердих, рідких і газоподібних відходів або

проміжних продуктів дають змогу визначити склад, структуру і властивості нових матеріалів або відновити технологію їхнього отримання.

При розгляданні систем, за допомогою яких здійснюється поширення інформації за межі інкасаторського автомобіля, необхідно розуміти різницю між технічним каналом витоку інформації від шпигунського, в рамках якого передача інформативного сигналу відбувається зловмисником, який отримав несанкціонований доступ до через технічний канал до джерела передачі інформації. Відмінність між шпигунським каналом та каналом витоку є достатньо умовною, однак під час витоку інформації в шпигунському каналі носієм інформації є особа, яка навмисно здійснює протиправні дії, а в технічному каналі витоку інформації є електричні, магнітні, електромагнітні поля та електричний струм.

Різновид технічних каналів пов`язано з фізикою процесу, який відбувається при застосуванні його. Отже, важливим є враховувати цю фізику при створенні ефективного захисту при передачі інформації від її витоку в ІА.

Самим простим технічним каналом витоку інформації є канал, який уявляє собою передавач, середовище в якому розповсюджується інформація та приймач.

Якщо виток інформації відбувається деякою кількістю послідовних або паралельних каналів, то в цьому випадку сам процес набуває достатньої складності. В таких випадках застосовується властивість інформації, яка полягає в тому, що її можна записати з одного носія на інший. Це пов`язано з тим, що якщо в ІА відбувається передача конфіденційної інформації оператору, то витік можливий не тільки акустичним каналом через двері автомобіля, а й оптичним - шляхом знімання інформації лазерним променем зі скла автомобіля, або через радіоелектронний канал де здійснюється використання встановленого в ІА засобу негласного отримання інформації. Таким чином відбувається створення складного (комбінованого) каналу, за рахунок послідовно з'єднаних акустичного та оптичного або акустичного та

радіоелектронного за схемою «*засіб негласного отримання інформації*» - *середовище розповсюдження* - *радіоприймач* каналів. Виходячи з цих комбінацій такі канали істотно називати *акусто – оптичними* та *акусто – радіоелектронними* відповідно. Для створення каналу витоку інформації таким чином, щоб сам джерело може знаходитись на великій відстані, необхідно застосовувати ретранслятор, що поєднує функції приймача одного каналу витоку інформації та передавача наступного каналу. Якщо для підвищення довжини відстані з якої здійснюється негласне отримання інформації з використанням заклидних пристроїв, які працюють через радіохвилі, то можна розмістити ретранслятор слабкого сигналу засобу негласного отримання інформації в самому автомобілі, а приймати й реєструвати потужніший сигнал ретранслятора на відстані, яка складає декількох кілометрів у мертвій зоні. В цьому випадку даний комбінований канал називають *акусто – радіоелектронними*.

За частотою прояву канали поділяються на постійні та епізодичні. У постійному каналі витік інформації має досить регулярний характер. Наприклад, наявність у кабінеті джерела небезпечного сигналу може призвести до передачі з кабінету мовної інформації до моменту виявлення цього джерела. Регулярність отримання інформації через такий канал робить його досить цінним. Тому розвідка дорожить регулярним джерелом інформації і захищає його від контррозвідки. До епізодичних каналів належать канали, витік інформації в яких має короткочасний, часто випадковий характер.

За способом створення канали витоку можуть бути спеціально організовані та випадкові. Організовані канали створюються зловмисником для регулярного добування інформації. Наприклад, для підслуховування на великій відстані від джерела мовної інформації організовують канал витоку з приміщення шляхом розміщення в ньому закладного пристрою. Характеристики (частота випромінювання, вид модуляції, потужність передавача тощо) цього каналу відомі зловмиснику. Ці знання дають йому змогу безперервно або в певний час прослуховувати всі розмови, що ведуться в приміщенні.

Побічні електромагнітні випромінювання і наведення створюють передумови для утворення випадкових каналів витоку інформації, параметри яких апріорі зловмисникові не відомі. Якщо йому вдасться налаштувати свій приймач на частоту побічного випромінювання, то виникає випадковий канал витоку інформації. Такий канал може бути вельми інформативним, але випадковий характер його утворення і часу роботи (коли ввімкнено випромінювальний технічний засіб) знижує його корисність для зловмисника.

Технічним каналом витоку інформація може передаватися не тільки у відкритому вигляді, вона може бути і закритою. З метою підвищення скритності сигнал на виході перспективних закладних пристроїв закривається, а канал витоку, що використовує ці пристрої, є технічно закритим. У разі перехоплення функціональних каналів зв'язку, якими передається шифрована інформація, утворюється шифрований канал витоку інформації.

Можливості передавання інформації технічними каналами залежать від багатьох чинників: енергії сигналу, ступеня його ослаблення в середовищі розповсюдження, чутливості та роздільної здатності приймача зловмисника.

1.3. Основні показники технічних каналів витоку інформації в інкасаторському автомобілі

Технічний канал витоку інформації характеризується показниками, які дають змогу оцінити ризик витоку. Такими показниками є:

пропускна спроможність технічного каналу витоку;

довжина технічного каналу витоку інформації;

відносна інформативність технічного каналу витоку інформації.

За аналогією з каналом зв'язку інтегральні можливості технічного каналу витоку щодо передачі інформації оцінюються його пропускною спроможністю.

Гранична пропускна здатність каналу зв'язку в бітах за секунду має наступне представлення

$$C = A_f \cdot \log_2\left(1 + \frac{P_c}{P_з}\right), \qquad (1.1)$$

де A_f - ширина смуги пропускання каналу зв`язку і вимірюється в герцах, $P_c$ - потужність інформативного сигналу, $P_з$ - потужність завади (білий шум) в смузі пропускання каналу зв`язку відповідно.

З представлення (1.1) слідує, що пропускна спроможність тим більша, чим більша ширина смуги пропускання частот каналу і більше відношення *сигнал/шум* на вході приймача каналу зв'язку. Оскільки пропускна спроможність каналу зв'язку залежить від його смуги пропускання і відношення *сигнал/шум*, то в цьому випадку існує два види каналів, а саме канал вузької смуги та канал широкої смузі, з низькою та високою потужністю сигналу. Найбільшою пропускною спроможністю володіє оптичний канал зв'язку, а найменшою володіє акустичний канал. Стандартний телефонний канал для передачі мовної інформації має смугу $300-3400\ Гц$ і належить до каналу вузької смуги, а шириною $8\ МГц$ для передачі телевізійних сигналів є канали широкої смуги. Якщо ширина спектра інформативного сигналу A_{fc}, дорівнює смузі пропускання частот каналу A_{fk}, то передача інформативного сигналу здійснюється в реальному масштабі часу. Якщо ж $A_{fc} > A_{fk}$, то інформація спотворюється і частково втрачається, як це показано на рисунку 1.2.

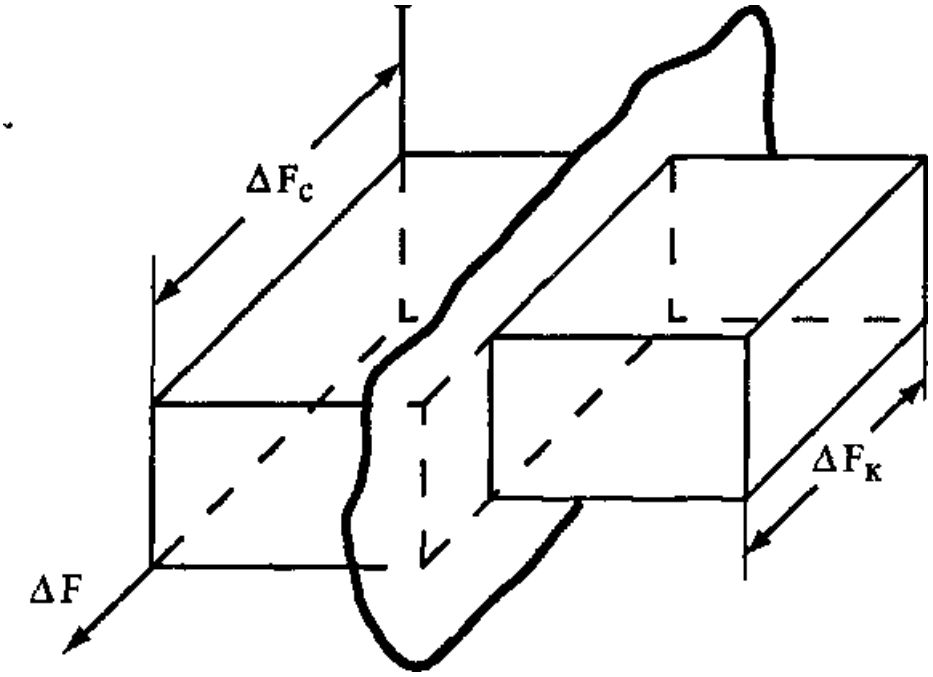

Рисунок 1.2. Графічне представлення обмеження частоти сигналу каналом витоку при переміщенні інкасаторського автомобіля

Для унеможливлення втрати інформації на вході каналу зв'язку застосовується буферний запам'ятовувальний пристрій, на вхід якого надходить з певною швидкістю інформація та з якого інформація зчитується зі швидкістю, що забезпечує узгодження ширини спектра сигналу з шириною смуги пропускання частот каналу. При цьому час передачі збільшується, тобто режим реального часу не забезпечується. Якщо $A_{fc} < A_{fk}$, то спектр сигналу не терпить зріз, але якщо канал більш широкої смуги, то в ньому збільшується рівень завад. В кінцевому результаті відбувається зменшення відношення *сигнал / перешкода*, що також призводить до зниження пропускної здатності каналу зв'язку.

Пропускна спроможність комбінованого каналу визначається пропускною спроможністю простого каналу, що має найменші значення. Як приклад можна навести, що комбінований канал спостереження об'єктів із інкасаторського автомобіля містить широкої смуги оптичний канал "*об`єкт за межами ІА - фотоапарат КА*" і менш ширини смуги радіоелектронний канал "*скидання*" зображення з *КА* одержувачу. Для передавання отриманого під час фотографування обсягу відеоінформації зображення на плівці зчитується з

меншою швидкістю, але протягом більш тривалого часу. У загальному випадку найбільшу пропускну спроможність має оптичний канал витоку інформації, оскільки його смуга пропускання істотно вища за смугу пропускання будь-якого іншого каналу. Найменшу пропускну здатність має акустичний канал витоку інформації.

Іншим показником, який широко застосовується для оцінки можливостей каналу витоку, є його довжина. Довжина технічного каналу витоку інформації оцінюється відстанню від джерела сигналу каналу до його приймача за умови забезпечення під час прийому допустимої якості інформації. Довжина каналу в загальному випадку залежить від показників елементів каналу передавання інформації: енергії сигналу, ступеня його ослаблення в середовищі розповсюдження, чутливості та роздільної здатності приймача зловмисника, рівня перешкод у каналі тощо. Чим довжина каналу більша, тим на більшій відстані від джерела можливе добування інформації і тим менший ризик зловмисника. Якщо довжина каналу більша за відстань від джерела сигналу до межі контрольованої зони, то ризик зловмисника під час видобутку інформації істотно менший, оскільки він може розмістити приймач сигналу за межами контрольованої зони. Тому зловмисник прагне всіма можливими методами збільшити довжину технічного каналу витоку інформації.

Для добування інформації з необхідною якістю необхідно забезпечити на вході приймача каналу мінімально допустиме для кожного виду інформації та носія відношення сигнал/перешкода. Це відношення досягається на різній відстані від джерела сигналу, залежно від потужності сигналу і перешкоди, а також величини (коефіцієнта) ослаблення (загасання) сигналу в каналі. Носії інформації істотно відрізняються за величиною загасання в середовищі поширення: найбільшою мірою зменшується енергія акустичної хвилі, найменшою - електромагнітна хвиля в довгохвильовому діапазоні частот.

За певної енергії сигналу необхідне відношення сигнал/шум забезпечується (без урахування спектральних характеристик коефіцієнта загасання середовища поширення) за вужчої смуги сигналу та каналу. Тому, наприклад, звуження

смуги частот спектра сигналу засобу негласного отримання інформації пристрою збільшує дальність його прийому. Найбільшу довжину, за винятком випадків перенесення матеріальних частинок середовища як носіїв інформації, мають радіоелектронні канали витоку інформації. Довжина складового каналу витоку інформації може бути як завгодно великою.

Якісну оцінку пропускної спроможності та довжини технічних каналів витоку інформації представлено в таблиці 1.1.

Таблиця 1.1.

N° п/п	ВИД КАНАЛУ	Показники простого каналу витоку інформації	
		Пропускна спроможність	Довжина
1	Оптичний	Висока	В МЕЖАХ ПРЯМОГО СПОСТЕРЕЖЕННЯ
2	Акустичний	Низька	МАЛА (одиниці сотні метрів)
3	Радіо-електронний	Висока	ДОВІЛЬНА
4	Дійсний	Низька	ДОВІЛЬНА

Чим ширше пропускна здатність каналу витоку і чим він довший, то більшу потенційну загрозу створює такий канал. Але розглянуті показники не враховують вартість інформації, яка передається. За наявності каналу витоку далеко не вся інформація джерела, що має певну ціну, потрапить до злодія.

Частина її буде загублена в каналі витоку. Отже, ціна інформації, отриманої зловмисником, у загальному випадку завжди буде меншою за ціну інформації джерела. Тому найважливішим показником технічного каналу витоку інформації є його інформативність. Однак інформативність залежить насамперед від інформативності джерела інформації. Тому коректно говорити не про абсолютну інформативність каналу витоку, а про відносну інформативність. Під відносною інформативністю технічного каналу витоку розуміють величину в інтервалі 0-1, що відповідає частці інформації джерела, яка може бути передана каналом, який розглядається. Наприклад, оптичний канал спостереження за об'єктом розвідки в приміщенні протилежного будинку має високу пропускну здатність, але кількість видобутої з його допомогою інформації залежить від роздільної здатності оптичного приймача. Не озброєний оптичним приладом спостерігач може розглянути лише великі об'єкти, а за допомогою спеціального телескопа можна прочитати текст документа в руках людини. Оскільки оптичний приймач є елементом технічного каналу витоку інформації, то його роздільна здатність характеризує відносну інформативність цього каналу. Пропускна спроможність, довжина і відносна інформативність каналу залежать від параметрів його елементів: джерела сигналу, середовища поширення і приймача сигналу.

Найменшу потужність мають сигнали побічного електромагнітного випромінювання та наведень радіоелектронних та електричних приладів. Діаграма спрямованості випромінювання, яка описує характер розподілу в просторі енергії випромінюваного (прийнятого) сигналу. Інтегрально вона оцінюється шириною за рівнем половини потужності випромінюваного поля в градусах у вертикальній площині та горизонтальній площині - шириною діаграми спрямованості. На відміну від антен передавачів і приймачів функціональних радіоканалів зв'язку, ширину яких встановлюють при створенні антен виходячи з просторового розташування джерел і приймачів сигналів, більшість антен джерел сигналів технічних каналів витоку інформації мають так звані випадкові антени. Функції випадкових антен можуть виконувати будь-які

провідники якими протікає електричний струм або в яких виникають високочастотні електричні заряди. Оскільки ці струмопровідні елементи довільно орієнтовані відносно приймача небезпечних сигналів, а їхні розміри не узгоджені з довжиною випромінюваної хвилі, то більш-менш достовірно можна описати діаграму спрямованості випадкової антени тільки після проведення відповідних інструментальних вимірювань. Потужність випромінюваного випадковою антеною електромагнітного поля залежить як від сили струму або величини заряду, так і від ступеня близькості її геометричних розмірів довжині хвилі. Чим вони ближчі, тим вища випромінювана потужність. Оскільки розміри випадкових антен малі, то потужність випромінювання підвищується при збільшенні частоти коливань зарядів або струмів. Основними показниками спектра сигналу, що поширюється в технічному каналі витоку інформації, є ширина і нерівномірність спектра сигналу. Оскільки, на відміну від функціонального каналу зв'язку, від каналу витоку інформації не вимагається безшумне передавання всіх спектральних складових сигналу, а лише тих, що несуть інформацію, яка цікавить зловмисника, то важливо під час оцінювання каналу витоку інформації враховувати ті ділянки спектра, в яких зосереджена основна енергія носія. Такі області стосовно акустичного сигналу називаються фонемами. Наприклад, в акустичному сигналі мовленнєвої інформації під час проходження його через різні середовища. приміщення більшою мірою поглинаються високочастотні складові спектра мови, внаслідок чого на досить великій відстані зникають ознаки індивідуальності голосу людини, яка говорить, але сенс мовного повідомлення залишається зрозумілим тому, хто підслуховує.

1.4. Графічне представлення обмеження частоти сигналу каналом витоку

Здійснення оцінки динамічного діапазону сигналу здійснюється за допомогою значенням виразу $\lg\left(\frac{P_{\max}}{P_{\min}}\right)$. Значимість динамічного діапазону для різних джерел сигналів неоднакова. Для оптичного сигналу він має важливе значення, оскільки описує спектри відбитих сигналів за рахунок властивості поверхні інкасаторського автомобіля. Для акустичного сигналу його інформативність достатньо низька, тому що зміст мовленнєвого повідомлення розуміють навіть за симетричного відносно нуля обмеження аналогового мовленнєвого сигналу та перетворення його на двійкову послідовність перетворення повідомлення.

Середовище поширення характеризується набором фізичних параметрів, що визначають умови поширення носія з інформацією. Основними з них є: швидкість поширення носія в середовищі;

коефіцієнт передачі або ослаблення енергії носія на одиницю довжини; залежність коефіцієнта передачі від частоти сигналу ((*амплітудно – частотна характеристика*);
вид і потужність перешкод сигналу.

Якщо для носія у вигляді радіохвилі швидкість поширення дуже велика і її можна не враховувати, то для носіїв у вигляді матеріальних тіл затримка носія може призвести до час зносу інформації, що міститься на ньому. Наприклад, якщо досить довго не вивозили відходи діловодства з організації, то інформація, що міститься в знайденій на звалищі чернетці документа, може істотно втратити свою первісну ціну.

При будь-якому переміщенні носія в просторі зменшується його енергія. Міра зниження енергії залежить від виду носія і характеристик середовища. Наприклад, бетонна стіна не пропускає світло, істотно послаблює акустичну хвилю і незначно знижує енергію електромагнітної хвилі. Долаючи різного роду перешкоди на шляху руху, зловмисник втомлюється, його рух сповільнюється і може взагалі припинитися. Оскільки будь-який фізичний *сигнал – носій*

інформації може бути описаний моделлю у вигляді сукупності певного набору коливань (*гармонік*), а параметри середовища щодо коливань різних частот відрізняються, то стосовно сигналів середовище розповсюдження може бути представлено у вигляді комплексного коефіцієнта передачі, який має наступне представлення

$$K(c) = \frac{S_{вих.}(c)}{S_{вх.}(c)}\ , \qquad (1.2)$$

де $S_{вх.}(c)$ - спектр сигналу на вході середи розповсюдження, а $S_{вих.}(c)$ - спектр сигналу на виході розповсюдження. Коефіцієнт передачі (1.2) уявляє собою амплітудно-частотну характеристику середовища розповсюдження витоку інформації при переміщення інкасаторського автомобіля в середовищі.

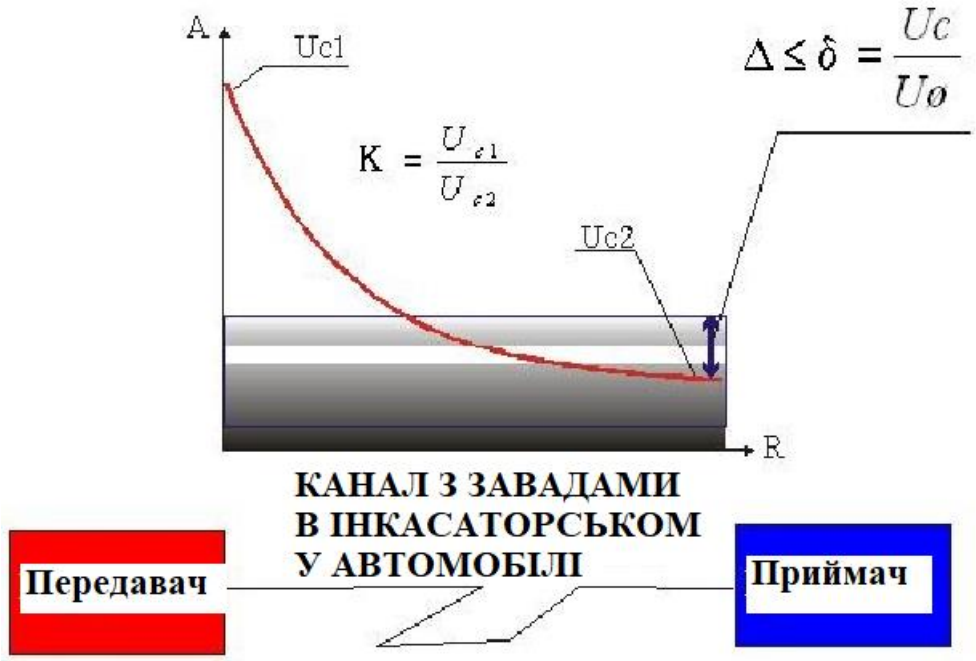

Рисунок 1.3. Джерело АЧХ

Динамічний діапазон приймача характеризується відношенням у логарифмічному масштабі максимального і мінімального рівнів вхідного сигналу, за якого забезпечується необхідний рівень якості сигналу на виході приймача. За малого динамічного відбувається спотворення сигналу великої амплітуди. Оскільки приймачі технічних каналів витоку інформації мають

високу чутливість, то через мінливість коефіцієнта загасання середовища в часі можливий рівень вхідного сигналу, який за певного коефіцієнта посилення спричиняє обмеження вихідного сигналу, що призводить до помітних його спотворень. Наприклад, закладний пристрій, розрахований на рівень акустичного сигналу, який відповідає кільком метрам від джерела звуку, у разі наближення цього джерела до місця знаходження закладного пристрою випромінюватиме радіосигнал зі спотвореною мовленнєвою інформацією. З метою розширення динамічного діапазону приймача в ньому передбачають автоматичне регулювання посилення залежно від середнього рівня вхідного сигналу.

Невідповідність спектральних характеристик і динамічного діапазону приймача відповідним характеристикам вхідного сигналу, вплив зовнішніх перешкод і теплових шумів, нееквівалентне посилення наведеного в антені приймача для різних частот і різних рівнів призводять до частотних і нелінійних спотворень сигналу на вході демодулятора. Оскільки спотворення параметрів сигналу спричиняє зміну інформації, то сигнали на виході демодулятора містять уже змінену інформацію.

Для складових каналів витоку інформації значення всіх розглянутих показників, за винятком потужності сигналу на вході приймача, погіршуються, тому що при будь-якому перетворенні сигналу відбувається зміна його інформативних параметрів, а отже, й інформації. А оскільки якість будь-якого каналу зв'язку оцінюється за подібністю отриманої інформації до переданої, то будь-яке зменшення подібності може трактуватися як погіршення якості інформації. Звичайно, у більшості випадків до якості інформації на виході технічного каналу витоку висувають менш жорсткі вимоги, ніж до функціонального каналу зв'язку. Але далеко не завжди. Під час передавання цифрових даних трансформація чисел може завдати зловмиснику настільки ж великих неприємностей, як і санкціонованому одержувачу.

Висновок до розділу 1

1. Було досліджено, що одним з основних завдань технічного захисту інформації в інкасаторському автомобілі є недопущення можливості витоку конфіденційної інформації під час його переміщення по маршрути, який затверджено.
2. В зонах розташування приймачів на маршруті руху інкасаторського автомобіля необхідно забезпечити таке співвідношення *сигнал / шум*, щоб не можливо було зловмиснику сканувати інформацію, яка потребує захисту.
3. Таке вирішення можливо якщо зменшити сигнал передавача шляхом екранування передавача, збільшити загасання сигналу в каналі, шляхом хибного випромінювання навколо оболонки інкасаторського автомобіля, або збільшити рівень шуму в каналі.
4. Засоби перехоплення інформативних сигналів необхідні для приймання та перетворення сигналів з метою його прийняття.

РОЗДІЛ 2 СИСТЕМИ ЗАХИСТУ ІНКАСАТОРСЬКОГО АВТОМОБІЛЯ

2.1. Основні уразливості в інкасаторському автомобілі

У 2021 році світовий ринок рішень для кіберзахисту автомобілів за рік оцінено у $2 млрд. Такі дані аналітики MarketsandMarkets оприлюднили на початку лютого 2022 року. Зростання продажів під'єднаних і напівавтономних транспортних засобів призвело до збільшення використання електронних компонентів в автомобілі, а це збільшило складність архітектури транспортного засобу і кодування програмного забезпечення, зазначається в дослідженні.
На березень 2022 року автомобілі містять у середньому приблизно 100 млн рядків коду й оснащені складним програмним забезпеченням (ПЗ), розробленим автовиробниками. Щоб забезпечити безпеку і збереження всієї кодової бази автомобіля, OEM-виробники вибирають рішення для захисту кінцевих точок. Ба

більше, очікується, що тенденція мобільної робочої сили, соціальних мереж і хмарних засобів синхронізації вплине на витрати на рішення для захисту кінцевих точок. У 2021 році 80% витрат на рішення для кіберзахисту автомобілів припало на програмне забезпечення, решта - на обладнання.

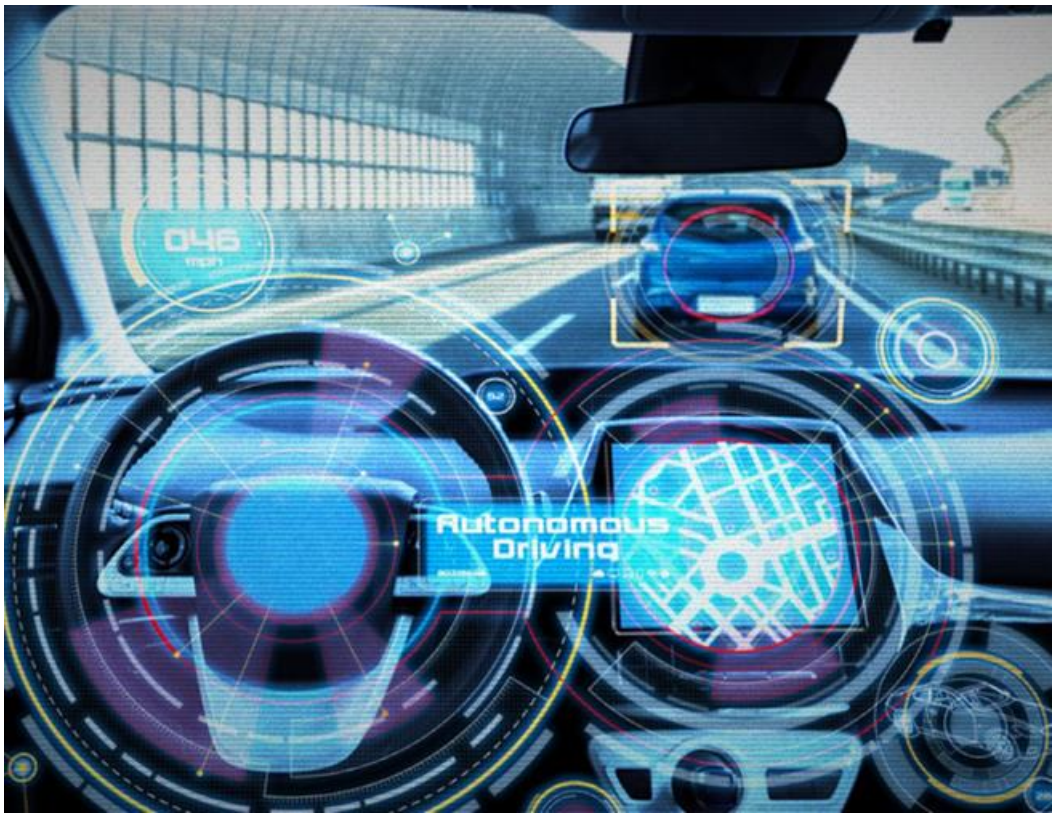

Рисунок 2.1. Вид з середини інкасаторського автомобіля

ПЗ у сфері кібербезпеки всередині автомобіля вимагає реалізації декількох функцій безпеки, як-от захищені протоколи, управління ідентифікацією та доступом, виявлення вторгнень і рівні абстракції для криптографічних функцій. Ці функціональні можливості потім використовуються функціональними електронними блоками управління (ЕБУ) для захисту комунікацій і запобігання створенню чорних ходів. Тому очікується, що сегмент ПЗ займатиме найбільшу частку на ринку автомобільної кібербезпеки.

У 2021 році найбільша частка ринку, що розглядається, припала на Азіатсько-Тихоокеанський регіон, за яким йдуть Європа та Північна Америка. Зростаюча обізнаність людей про засоби активної та пасивної безпеки і збільшення продажів автомобілів середнього класу і люкс є ключовими факторами, що стимулюють ринок автомобільної кібербезпеки в Азіатсько-Тихоокеанському

регіоні. Деякі виробники комплектуючих перенесли свої заводи з виробництва автомобілів у країни, що розвиваються, через низьку вартість робочої сили, простоту ведення бізнесу і доступність сировини. Кілька відомих напівпровідникових компаній також мають свої виробничі центри в Азіатсько-Тихоокеанському регіоні. Це допомагає їм підтримувати ефективний ланцюжок поставок своєї продукції для автовиробників.

Зростаючі продажі автомобілів, оснащених системами і значне зростання індустрії спільного використання автомобілів, ймовірно, призведуть до збільшення попиту на автомобільні рішення з кібербезпеки в Азіатсько-Тихоокеанському регіоні. Виробники комплектуючих в Японії та Південній Кореї зосереджені на розробці самокерованих автомобілів. Очікується, що це підстьобне попит на відповідні рішення з кібербезпеки.

2.2. Побудова системи захисту інкасаторського автомобіля

У середині серпня 2021 року стало відомо про те, що для запобігання викраденню і крадіжці даних автовиробники перевірятимуть ПЗ своїх машин на наявність недоліків у системі безпеки й обмінюватимуться інформацією про тенденції кібератак. Для цього створено організацію Car Connected Cybersecurity Consortium, до якої увійдуть понад 90 членів.

Популярні моделі Volkswagen і Ford зламані

У середині квітня 2020 року британський журнал Which? звинуватив виробників двох найпопулярніших автомобілів у Європі - Volkswagen і Ford - у тому, що вони недбало ставляться до кібербезпеки. Докладніше тут.

Зупинка всього 20% автомобілів у годину пік повністю паралізує транспортний рух у місті

За словами вчених із Технологічного інституту Джорджії, у майбутньому кількість безпілотних автомобілів зросте до 10 млн. Про це стало відомо 30 липня 2019 року. Вчені побоюються, що кіберзлочинці зможуть паралізувати міський трафік, зламавши лише невелику частину безпілотних автомобілів. Головними наслідками таких кібератак на безпілотні автомобілі стануть дорожньо-транспортні пригоди, а також величезні затори, в які потраплять

машини швидкої допомоги з пораненими, хворими і вмираючими людьми. Дослідники змоделювали ситуацію, як злам кількох безпілотних автомобілів може вплинути на міський трафік у Мангеттені (район Нью-Йорка). За словами дослідників, зупинка всього 20% автомобілів у годину пік повністю паралізує транспортний рух у місті. Місто буде розділене на кілька секторів, що дасть змогу переміщатися між кварталами, однак дістатися в інший кінець уже буде неможливо. Злом і примусова зупинка 10% автомобілів у годину пік призведе до блокування руху машин швидкої допомоги. Результати дослідження також показали, що такі наслідки можуть виникнути і в будь-який інший час дня. Дослідники рекомендують інженерам безпілотних автомобілів пов'язувати машини кількома цифровими мережами, щоб запобігти доступу зловмиснику до кожного автомобіля шляхом компрометації однієї або двох мереж.

У 2017-2018 роках модно публічно говорити про "мислячі" машини і про небезпеку, що походить від роботів, які вийшли з-під контролю, або, як їх називають, роботів-убивць. Є навіть відповідні законодавчі ініціативи, наприклад, "Campaign to Stop Killer Robots"[3]. Попри очевидну сумнівність небезпеки автономної смертоносної зброї вже зараз проти неї виступають видатні люди. Наприклад, лист із попередженням про небезпеку підписали астроном Стівен Гокінг, підприємці Ілон Маск і Стівен Возняк, лінгвіст Ноам Хомскі та інші не менш відомі особистості.
Так, цілком можливо, ця загроза колись виникне, але, найімовірніше, вона виявиться всього лише нешкідливою страшилкою. Насправді в нашому стрімко мінливому світі є інші, менш відомі, але куди більш реальні небезпеки, породжувані новими технологіями. Одна з них - інформаційна небезпека сучасних автомобілів. Цю проблему виявили і розкрили 2012 року двоє: у минулому аналітик Агентства Національної Безпеки США, а на той час інженер із безпеки в Twitter Чарлі Міллер і на той момент глава фірми IOActive Кріс Валачек. Пізніше з'ясувалося, що роботу фінансувало оборонне агентство DARPA.

Паралельно з двома хакерами проблемою інформаційної безпеки автомобілів займалися в Центрі безпеки вбудованих автомобільних систем (The Center for Automotive Embedded Systems Security, CAESS), створеному спільно Каліфорнійським університетом у Сан-Дієго та Університетом штату Вашингтон. На його сайті є низка корисних статей. Невідома раніше небезпека породжена вразливістю телематичних систем, якими комплектуються сучасні автомобілі. Не якесь гіпотетичне, а цілком реальне зовнішнє вторгнення може позбавити водія можливості керувати машиною і зробити її джерелом небезпеки не тільки для тих, хто всередині, а й для оточуючих. За останні роки ми стали свідками терористичних актів з використанням вкрадених автомобілів. А тепер уявіть собі, що автомобіль реальність, а не фантастика.

Причина вразливості криється в процесі активної комп'ютеризації автомобілів, що почався в 90-ті роки. Насамперед окремі елементи автоматизації стали об'єднувати в мережі промислових контролерів CAN[4], а по-друге, для зв'язку із зовнішнім світом було запропоновано найрізноманітніші телематичні системи. Доступність ззовні до всіх систем від фар до гальм створила можливість для хакерської атаки на автомобіль з усіма витікаючими звідси наслідками. Перше повідомлення про злом автомобіля, оснащеного телематичною системою, було зроблено в журналі Forbes у 2013 році.[7] А 2015 року в Wired вийшла гучна стаття[8], де дуже жваво з відео показано те, як Міллер і Валачек захопили Jeep Cherokee і, дистанційно керуючи ним, робили все, що вони хотіли, попри спроби водія припинити це неподобство. Зрештою вони загнали нещасного в яр. Утім усе це відбувалося за згодою власника машини, пізніше він став автором статті. За всієї його брутальності експеримент пройшов без порушень, оскільки Міллер і Валачек відносять себе до етичних або білих хакерів (білих шапок). Вони повідомили про скоєне компанії Chrysler, як заведено в таких випадках, за 9 місяців, щоб вона могла провести необхідні заходи щодо відкликання машин.

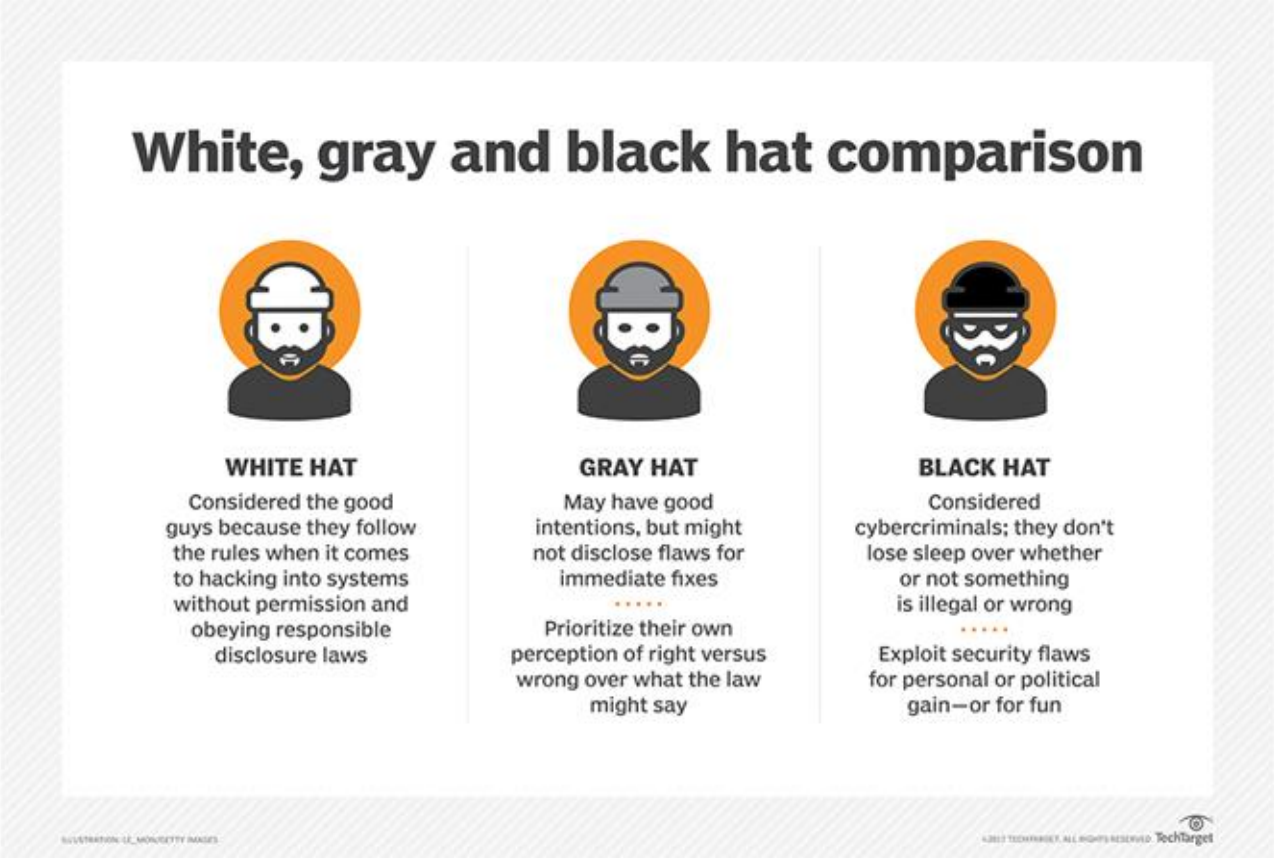

Рисунок 2.2. Розподіл зловмисників по групам

Білі шапки вважаються хорошими хлопцями, тому що під час злому систем вони дотримуються прийнятих правил і визнають відповідальність перед законом. Сірі шапки можуть мати добрі наміри, але виявивши вразливості, вони не завжди повідомляють про них негайно. При цьому, самі себе вони вважають хорошими, а закон може помилятися.

Чорні шапки вважаються кіберзлочинцями. Вони не розрізняють легальне від нелегального, використовують виявлені вразливості в особистих або політичних цілях, а може просто для задоволення.

За своїм впливом на громадську думку цю та ще кілька супутніх публікацій можна порівняти зі знаменитою книжкою "Небезпечний на будь-якій швидкості" (Unsafe at Any Speed: The Designed-In Dangers of the American Automobile), опублікованою у США 1965 року Ральфом Нейдером, де автор розкрив проблеми безпеки американських моделей тих років. Під впливом книги автомобільна промисловість в усьому світі помітно переорієнтувалася, зробивши безпеку одним із найважливіших пріоритетів.

2.3. Рекомендації щодо забезпечення технічного захисту інформації в інкасаторському

У цивілізованому світі на можливі загрози відреагували серйозно, про них написали масові видання, зокрема англійська Guardian[9]. Найцікавіші статті на тему автомобільного хакерства (car-hacker) публікуються у Wired. У 2016 році вийшла цілком серйозна книга The car hacker's handbook, її текст є у відкритому доступі.

Міллер і Валачек зосередили свою увагу на вразливостях телематичних рішень тих чи інших вендорів. Виробники автомобілів серйозно поставилися до загрози Jeep hack і внесли відповідні зміни до телематичних систем, що припиняють можливості зовнішнього управління автомобілем. Рішення було нескладним, оскільки можна використовувати системи виявлення вторгнень, відомі як IDS/IPS. Більшість телематичних систем допускає виконання необхідного апргейду, а для випадку, коли це неможливо, було створено спеціальні захисні пристрої, їхня ціна не перевищує $150.

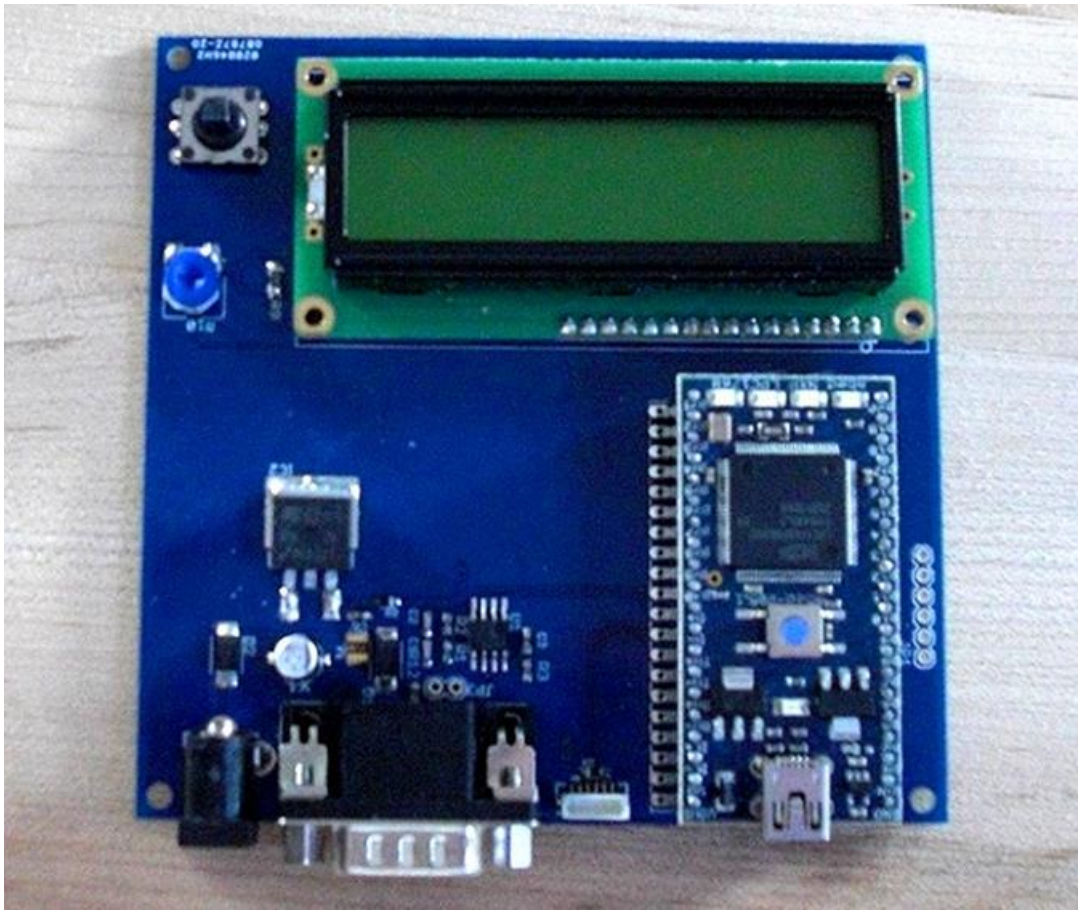

Рисунок 2.3. Засіб для захисту від вторгнення в інкасаторський автомобіль

Після того, як проблему Jeep hack було вирішено, розкрилася інша, набагато серйозніша. Вона пов'язана з недосконалістю стандартів, за якими будуються мережі контролерів CAN (Controller Area Network). Ідея CAN була запропонована в середині 80-х німецькою компанією Robert Bosch, яка задумувала її як економічний засіб для об'єднання контролерів. Актуальність цього завдання зрозуміла будь-кому, хто хоч раз бачив системи комунікації в об'єктах автоматизації. Це кілометри і кілометри кабельної проводки, якими обплутані і промислові об'єкти, і енергетичні агрегати, і навіть літальні апарати. Традиційний спосіб зв'язку розподілених по об'єкту контролерів джгутами проводів за своєю технічною складністю, за ціновими і за ваговими параметрами для такого масового виробу, яким є автомобіль, виявився непридатним. Було потрібне альтернативне рішення, що скорочує кількість дротів, тому було запропоновано протокол CAN, для якого достатньо будь-якої дротової пари.

Перехід на CAN дає змогу заощадити кілька кілограмів міді на кожному автомобілі і спрощує проводку.

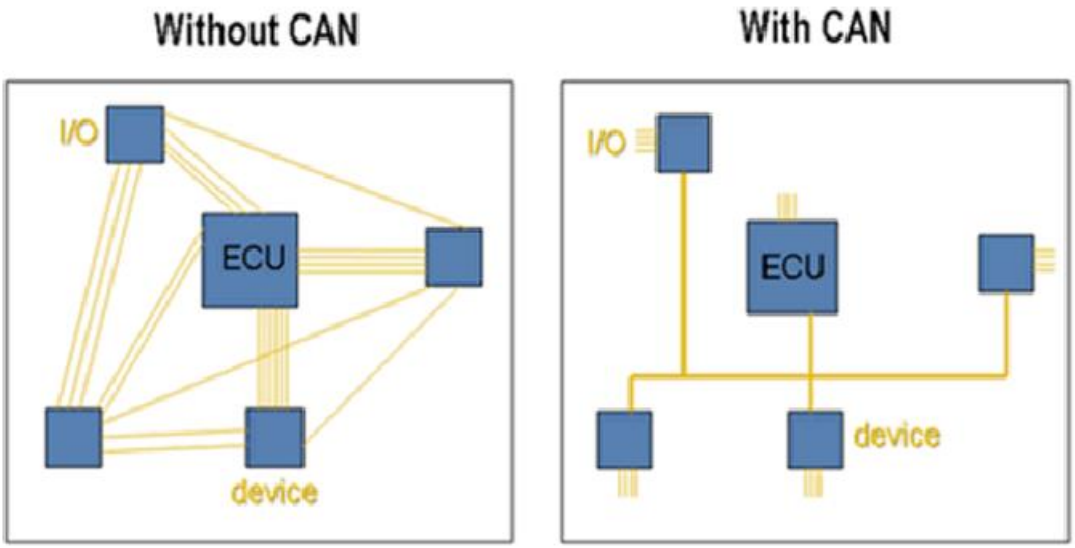

Рисунок 2.4. Система забезпечення живлення без CAN та з CAN

Протокол CAN було створено 1983 року, а 1993-го його було прийнято як стандарт ISO 11898 Міжнародною організацією зі стандартизації та схвалено урядовими органами більшості країн світу. Він створений без припущення про можливість зловмисного вторгнення в роботу мережі, тому не дає навіть теоретичної можливості виявити адресовані CAN шкідливі дії. Станом на 2018

рік CAN є невід'ємною частиною будь-якого автомобіля.

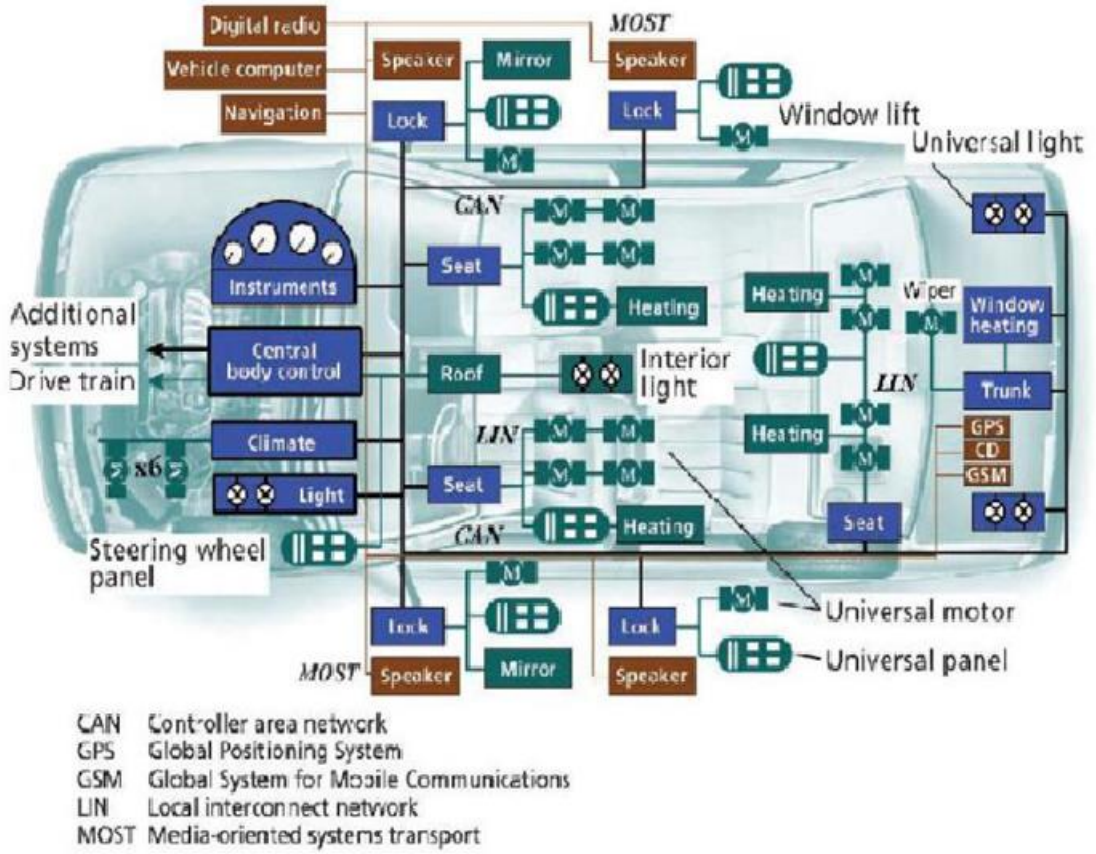

Рисунок 2.5. Загальна схема системи захисту інкасаторського автомобіля.

Об'єктом атаки CAN стає система обміну повідомленнями, так званими фреймами. За логікою своєї роботи CAN - це зменшений Ethernet. Їх об'єднує необхідність виявлення і виправлення наслідків колізій, тобто тих випадків, коли передавач звертається до носія, зайнятого в цей момент іншим передавачем. В Ethernet це називають множинним доступом з контролем несучої і виявленням колізій (CSMA/CD, Carrier Sense Multiple Access with Collision Detection). У CAN цей механізм простіший - якщо трапляється колізія, передавач повторює спробу. За нормальних умов для встановлення зв'язку потрібна обмежена кількість спроб, але, якщо передавач з якоїсь причини "занадто нав'язливий", його переводять у пасивний. Саме цей тип дії є незахищеним і може стати предметом атаки. Тобто атакувальник може перепрограмувати електронний контролер (ECU) або блок керування двигуном або ж просто відключити той чи інший контролер. Без перегляду стандарту ISO 11898 цю вразливість виключити неможливо, це мінус. Але є і плюс. На відміну від Jeep hack впровадження

можливе тільки за безпосереднього контакту з автомобілем, дистанційно нашкодити не можна. З цієї причини особисті автомобілі меншою мірою схильні до загрози, ніж ті, які в прокаті або каршенінгу, а ці форми користування постійно розширюються.

За кілька років виникла ціла низка компаній, які професійно займаються інформаційною безпекою автомобілів, з найвідоміших - це Trend Micro, а також молоді Argus і NNG.

Висновки до розділу 2

1. При дослідженні уразливостей ІА було встановлено, що відповідне програмне забезпечення, яке встановлюється на борту автомобіля потребує постійного ретельного тестування.
2. Динамічний спосіб реалізовано у вигляді вбудованого в рушій браузера аналізатора коду, який перевіряє всі звернення веб-додатка до рушія і виявляє аномальну активність на основі таких звернень. Через незмінне зниження продуктивності браузера та необхідності його постійного адаптування під конкретні веб-додатки подібний метод так і не був доопрацьований у повноцінне комерційне рішення.
3. Водночас потенційно цей метод дає змогу виявляти з великою точністю активності, які не є звичайними для веб-додатками. На теперішній час захист веб-додатків виконує сам браузер, надаючи можливість створення виконання різних движків. При цьому ускладнено доступ до нативних функцій операційної системи.
4. Використання *Secure Sockets layer* з'єднання забезпечує надійний захист від підробки програмного забезпечення та кібератак "*людина по середині*". Тим самим виходить програмне забезпечення, яке передано розробником, і це програмне забезпечення має доступ не до всіх функцій операційної системи.

5. Отже, динамічний метод аналізу коду є найперспективнішим способом аналізу аномальних активностей, і необхідний подальший більш глибинний аналіз цього методу з погляду продуктивності та виявлення необхідних аномалій.

ВИСНОВКИ

1.У роботі був проведений аналіз слабких місць інкасаторського автомобілю щодо технічного захисту оболонки його на те, щоб не було можливості ззовні сканувати інформацію, яка передається з середини автомобіля під час його переміщення.

2.В ході роботи було встановлено, що при теперішньому розвитку електроніки необхідно враховувати всі можливі витоки з технічних каналів.

3.В інкасаторському автомобілі можуть бути встановлені маячки, які оповіщають зловмисника про маршрут слідування автомобіля. Для запобіганню цьому необхідно перед стартом інкасаторського автомобіля перевірити на їх наявність в ньому.

4. На інкасаторському автомобілі повинно бути встановлено спеціальні відеокамери, які фіксують все, що відбувається за межами інкасаторського автомобіля під час його переміщення.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ ТА ДЖЕРЕЛ

1. International Forum of Educational Technology & Society [Електронний ресурс]. – Режим доступу : http://ifets.ieee.org/.

2. Automated Testing of Desktop. Web. Mobile. [Електронний ресурс] // Ranorex Company. – Режим доступу : http://www.ranorex.com/

3. Category:Software testing tools [Електронний ресурс] // Вікіпедія – вільна енциклопедія. – Режим доступу :

https://en.wikipedia.org/wiki/Category:Software_testing_tools

4. 5 Best Test Automation Tools [Електронний ресурс] // automated-360 blog . – Режим доступу : http://automated- 360.com/automation-tools/5-besttestautomation-tools

5. List of Testing Tools. [Електронний ресурс] // guru99 – professional courses. – Режим доступу : http://www.guru99.com/list-of-testingtools.html

6. Тестування програмного забезпечення. [Електронний ресурс] // Вікіпедія – вільна енциклопедія.

7. DOU. Тестирование. Фундаментальная теорія. [Електронний ресурс]:

Gennadii Mishchevskii. – 2015. – Режим доступу :

https://dou.ua/forums/topic/13389/

8. Broken Authentication [Електронний ресурс]. – Режим доступу: https://www.owasp.org/index.php/Top_10-2017_A2-Broken_Authentication

9. Статья «Внедрение SQL кода» [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/Внедрение_SQL-кода

10. Kali Linux [Електронний ресурс]. – Режим доступу: https://www.kali.org

11. .Сканер Nmap [Електронний ресурс]. – Режим доступу: https://nmap.org

12. OWASP Testing Guide [Електронний ресурс]. – Режим доступу:

https://www.owasp.org/index.php/OWASP_

Testing_Guide_v4_Table_of_Contents

13. Стаття «Metasploit инструкция по применению» [Електронний ресурс].

– Режим доступу: https://cryptoworld.su/metasploit