КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ІМЕНІ ТАРАСА ШЕВЧЕНКА

ФАКУЛЬТЕТ РАДІОФІЗИКИ ЕЛЕКТРОНІКИ ТА КОМП'ЮТЕРНИХ СИСТЕМ

Кафедра радіотехніки та радіоелектронних систем

До захисту допущено: «На правах рукопису»
Завідувач кафедри _____ Ігор АНІСІМОВ
19 грудня 2022 р.

КВАЛІФІКАЦІЙНА МАГІСТЕРСЬКА РОБОТА

на тему:

«Розробка технічних вимог до системи захисту інформації програмно-технічного комплексу бездротового зв'язку»

Виконав:
студент 2-го курсу магістратури
денної форми навчання
спеціальності 172 Телекомунікації та радіотехніка
ОПП «Захист інформації в телекомунікаціях»
Кисельов Максим Денисович _____

Науковий керівник:
к.в.н., доц. Довбня Сергій Якович _____

Рецензент:
к.т.н., доц. Четверіков Іван Олександрович _____

Засвідчую, що у цій магістерській роботі
немає запозичень з праць інших авторів без
відповідних посилань
Студент _____

Робота допущена до захисту в ЕК рішенням кафедри радіотехніки та радіоелектронних систем від 19 грудня 2022 р., протокол № 9.

Завідувач кафедри радіотехніки та радіоелектронних систем,
доктор фіз.-мат. наук, професор
Анісімов Ігор Олексійович _____

Київ – 2022

ЗМІСТ

ВСТУП 3

РОЗДІЛ 1. АНАЛІЗ БЕЗПЕКИ ПТК 5

РОЗДІЛ 2. ДАНІ ОБСТЕЖЕННЯ СЕРЕДОВИЩ ФУНКЦІНУВАННЯ ПТК 8

РОЗДІЛ 3. МОДЕЛЬ ЗАГРОЗ ВИТОКУ ІНФОРМАЦІЇ ЗА РАХУНОК НЕСАНЦІОНОВАНОГО ДОСТУПУ 11

РОЗДІЛ 4. МОДЕЛЬ ЗАГРОЗ ВИТОКУ ІНФОРМАЦІЇ ЗА РАХУНОК НЕСАНЦІОНОВАНОГО ДОСТУПУ 21

РОЗДІЛ 5. ВИМОГИ ДО ЗАХИСТУ ІНФОРМАЦІЇ ПТК БЕЗДРОТОВОГО ЗВ’ЯЗКУ 23

РОЗДІЛ 6. ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ПТК БЕЗДРОТОВОГО ЗВ’ЯЗКУ 29

РОЗДІЛ 7. СТВОРЕННЯ СИСТЕМИ КОМПЛЕКСА РАДІОМОНІТОРИНГУ
РДЖ 33

ВИСНОВКИ 37

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 38

ВСТУП

Висока актуальність роботи на сьогодні обґрунтовується тим, що люди користуються ПТК щодня і з кожним днем таких пристроїв в нашому житті стає все більше і разом з цим росте і ризик витоку інформації, який вже виріс за рамки тільки секретної інформації, а й перейшов на особисту інформацію звичайних користувачів. До ПТК можна віднести смартфони, планшети, розумні годинники та багато інших пристроїв

Смартфони (з англ. smart — розумний, і англ. phone — телефон) — окрема категорія телефонів (як правило, з сенсорним екраном), з великою кількістю оперативної пам'яті і власний потужний процесор, працюють під операційними системами iOS, Android і іншими.

Смартфон володіє багатофункціональністю і більшість користувачів в умовах сьогодення практично не уявляє життя без цього пристрою. Але велика кількість користувачів навіть не цікавиться питаннями безпеки і жертвує цим заради свободи функціональності та задоволення.

Ще за перше півріччя 2018 року по даними GfK і OLX кількість користувачів смартфонів серед активних користувачів інтернету України в віці 16 років і старше досягло 85%. При цьому 50% тих, у кого був досвід покупок в інтернеті, використовує телефон для пошуку товарів і послуг.

Починаючи з 2014 року у світі кожного року продається більше одного мільярда смартфонів. У 2018 році в усьому світі було продано близько 1,56 мільярдів смартфонів.

Також в Україні працює додаток «ДІЯ» що дозволяє мати свої документи та отримувати держпослуги одразу в телефоні.

Це перш за все можливість отримання послуг в електронному вигляді. Таких як – дата народження, вступ до дитячого садка, школи, університету, отримання паспорта та посвідчення водія, реєстрація автомобіля чи нерухомості, землі, шлюб тощо. «ДІЯ» – це можливість розв’язати всі ці

ситуації в один клік за допомогою смартфона, де людина матиме особистий електронний підпис. Те саме стосується й бізнесу.

Все це є вагомим привідом звернути увагу на безпеку та загрози смартфонів.

Метою і завданням роботи розробка технічних вимог до системи захисту інформації програмно-технічного комплексу бездротового зв'язку.

В сучасному світі питання безпеки смартфонів та бездротових пристроїв є суттєвою складовою у системах захисту інформації. Більшість сучасних та передових компаній світу проводять серйозну роботу з захисту інформаційної діяльності та розроблять політику інформаційної безпеки з урахуванням можливого впливу смартфонів на загальний стан інформаційної безпеки організації.

РОЗДІЛ 1.
АНАЛІЗ БЕЗПЕКИ ПТК

ПТК володіють не тільки широкою функціональністю, але й широким спектром загроз.

По перше. Уніфіковане системне програмне забезпечення. На більш «сучасні» телефони минулого десятиліття вже можна було встановлювати додаткове програмне забезпечення. Однак програмне забезпечення різних виробників, як правило, виявлялося несумісним між собою. Але в 2007 році була розроблена ОС IOS, а в 2008 ОС Android. Ці операційні системи забезпечили таку необхідну універсальність, і тепер ви можете встановлювати (і видаляти) додатки на будь-який смартфон, що працює під управлінням однієї з цих ОС. Але є небезпека що користувач, наприклад, може встановити шкідливу програму, замасковану під необхідний для нього програмний продукт, який може записувати і пересилати третій стороні всі телефонні розмови, SMS, фотографії та інші конфіденційні дані. А може просто взяти і видалити всі призначені для користувача дані з карти пам'яті пристрою.

По-друге, змінилася функціональність пристрою. Тепер пристрій володіє всілякими датчиками. Якщо раніше телефон мав тільки динамік та мікрофон, то зараз навіть годинник має різноманітний спектр датчиків в придачу. Все що ви можете уявити скоріш за все вже вбудовано у ваш смартфон.

Наявність цих датчиків (сенсорів) ніяк не може пошкодити безпосередньо пристрій, але є в деякому роді проблему для самого його власника. Так, орієнтуючись на GPS-модуль пристрою, можна відстежити його переміщення на місцевості. Звичайно, оператор мобільного мережі і так може стежити за переміщеннями користувача, навіть якщо у нього звичайний телефон десятирічної давності. Але тут мова йде про те, що будь-який бажаючий, який заволодів вашим телефоном всього на кілька хвилин фізично

чи дистанційно, може встановити якийсь додаток, який буде стежитиме за всіма вашими переміщеннями.. Точно так само існують додатки, які постійно або по команді ззовні можуть почати запис і трансляцію про все, що відбувається в даний момент навколо пристрою. Смартфон буде використовуватися як звичайний закладний пристрій.

По-третє, тепер, крім списку SMS, адресної книги і переліку останніх набраних номерів, в смартфоні зберігається серйозна особиста інформація. Можливості IOS та Android дозволяють встановлювати на смартфони та планшети звичайні офісні додатки, а це означає, що в пам'яті пристрою можуть міститися важливі документи, конфіденційне листування по електронній пошті, особисті фотографії і інші дані, які можуть використовувати проти вас. Подібну інформацію необхідно захищати.

І це тільки очевидні відмінності, а питання безпеки залишаються під великим сумнівом.

Можна навести недавні приклади інцидентів пов’язаних з безпекою ОС Android, яка стала найвразливішою платформою в 2019 році.

В цілому в ОС Android в 2019 році було виявлено 414 вразливостей.

До такого висновку прийшли фахівці порталу TheBestVPN в ході аналізу статистики вразливостей в різних операційних системах і програмних продуктах за підсумками 2019 року.

Якщо в 1999 році було зафіксовано тільки 894 уразливості, то через 20 років цей показник збільшився майже в 14 разів – до 12 174. У 2018 році було виявлено найбільшу кількість вразливостей – 16 556, 1 197 з яких містилися в безкоштовній ОС Debian GNU / Linux .

У 2019 лідером цього рейтингу стала ОС Android з 414 виявленими за рік вразливостями. На другому місці слід Debian Linux (360 вразливостей), а на третьому - Windows Server 2016 і Windows 10 (357).

В цілому за весь 2019 рік у програмному забезпеченні було виявлено 12 174 вразливостей. 25,3% всіх проблем дозволяли зловмисникам виконувати

на пристроях довільний код, 17,7% ставилися до вразливостей типу міжсайтового виконання сценарію, а 13,9% - переповнення буфера.

За останні 20 років компанії стали більш залежати від цифрових даних і хмарних обчислень, що збільшило їх схильність кібератак. У 2019 року в продуктах Microsoft було зафіксовано 668 вразливостей. З 1999 року даний показник складає 6 814, що робить Microsoft найбільш уразливим постачальником за останні 20 років. За нею йдуть компанії Oracle (6 115) та IBM (4 679).

Також дослідники безпеки з групи Tencent Blade виявили в прошивці WLAN системи на кристалі Snapdragon від Qualcomm дві небезпечні вразливості, експлуатація яких може дозволити зловмиснику зламати модем і ядро Android по бездротовій мережі.

Уразливості зачіпають компоненти WLAN Qualcomm Snapdragon 835 і 845. Тести проводилися на пристроях Google Pixel 2 і 3, однак будь-який не оновлений телефон з однією з двох згаданих систем на кристалі вразливий для злому.

Експлуатація першої уразливості (CVE-2019-10538), що отримала високу оцінку небезпеки, дозволяє зловмисникам скомпрометувати бездротову локальну мережу і модем чіпа по бездротовій мережі. Друга проблема пов'язана з переповненням буфера (CVE-2019-10540) і отримала критичну оцінку серйозності, оскільки її експлуатація дозволяє зламати ядро Android з компонента WLAN.

РОЗДІЛ 2.
ДАННІ ОБСТЕЖЕННЯ СЕРЕДОВИЩ ФУНКЦІНУВАННЯ ПТК

Сьогодні спектр ПТК які ми використовуємо у повсякденному житті дуже різноманітний. Смартфони, планшети, розумні годинники всі ці пристрої здатні передавати інформацію без вашого відому.

В якості зразка обрано смартфон компанії APPLE – Apple iPhone 12 64GB Black (MGJ53).

Характеристики даного пристрою наведені на рис.1.

Виробник	Apple
ЗАГАЛЬНІ ХАРАКТЕРИСТИКИ	
Тип корпусу	моноблок
Тип	смартфон
Рік випуску	2020
Стандарт	GSM 1800, GSM 1900, GSM 900, GSM 850 LTE 5G 3G
Операційна система	iOS 14
Матеріал корпусу	метал / скло
Кількість SIM	2
Тип SIM	e-SIM nano-sim
Вага	164 г
Розміри (ШхВхт)	71.5x146.7x7.4 мм
КОМУНІКАЦІЇ	
Навігація	Galileo, A-GPS, GLONASS, GPS, цифровий компас
Інтерфейси	режим модему, Bluetooth, Lightning, NFC, Wi-Fi
Покоління Wi-Fi	6
Частоти Wi-Fi 802.11	ax
Версія Bluetooth	v 5.0
Функції Bluetooth	A2DP (Advanced Audio Distribution)
Покоління мобільного зв'язку	4G (LTE, WiMax), 3G (WCDMA, CDMA2000, UMTS), 3.5G (HSDPA, HSUPA, HSPA, HSPA +), 2G (TDMA, CDMA, GSM), 2.5G (GPRS, EDGE), 5G
ПАМ'ЯТЬ І ПРОЦЕСОР	
Об'єм вбудованої пам'яті	128 Гб
Об'єм оперативної пам'яті	4 Гб
Процесор	Apple A14
Кількість CPU-ядер	6
Графіка	M14

ЕКРАН

Тип екрану	OLED
Діагональ екрану	6.1 "
Співвідношення сторін	19.5: 9
Роздільна здатність дисплея	2532x1170 пикс.
Сенсорний екран	ємнісний
Число пікселів на дюйм	460 ppi
Захист дисплея	Corning Ceramic Shield
Співвідношення екрану до корпусу	86 %

ОСНОВНА КАМЕРА

Кількість мегапікселів основної камери	12 МП
Основний об'єктив	f / 1.6 26 мм
Ультраширокий об'єктив	12 МП f / 2.4 13 мм 120 °
Спалах	світлодіодна
Функції камери	визначення осіб, цифровий Zoom, розпізнавання посмішок, автофокус, геотеги, оптичний Zoom, оптична стабілізація
Сенсори і датчики	Сканер особи, Гіроскоп, Акселерометр, Датчик наближення, Датчик освітлення, Барометр, Компас

Кількість мегапікселів селфі камери	12 МП
Відеозйомка	Full HD (30 к / с), 4K (60 к / с), HD (30 к / с)
Макс. роздільна здатність відео	3840x2160 пікс.
Характеристики об'єктива	f / 2.2

Рис.1.

На телефоні встановлено пакет стандартних додатків APPLE рис.1 та є можливість завантажити безліч додатків сторонніх розробників з магазину App Store.

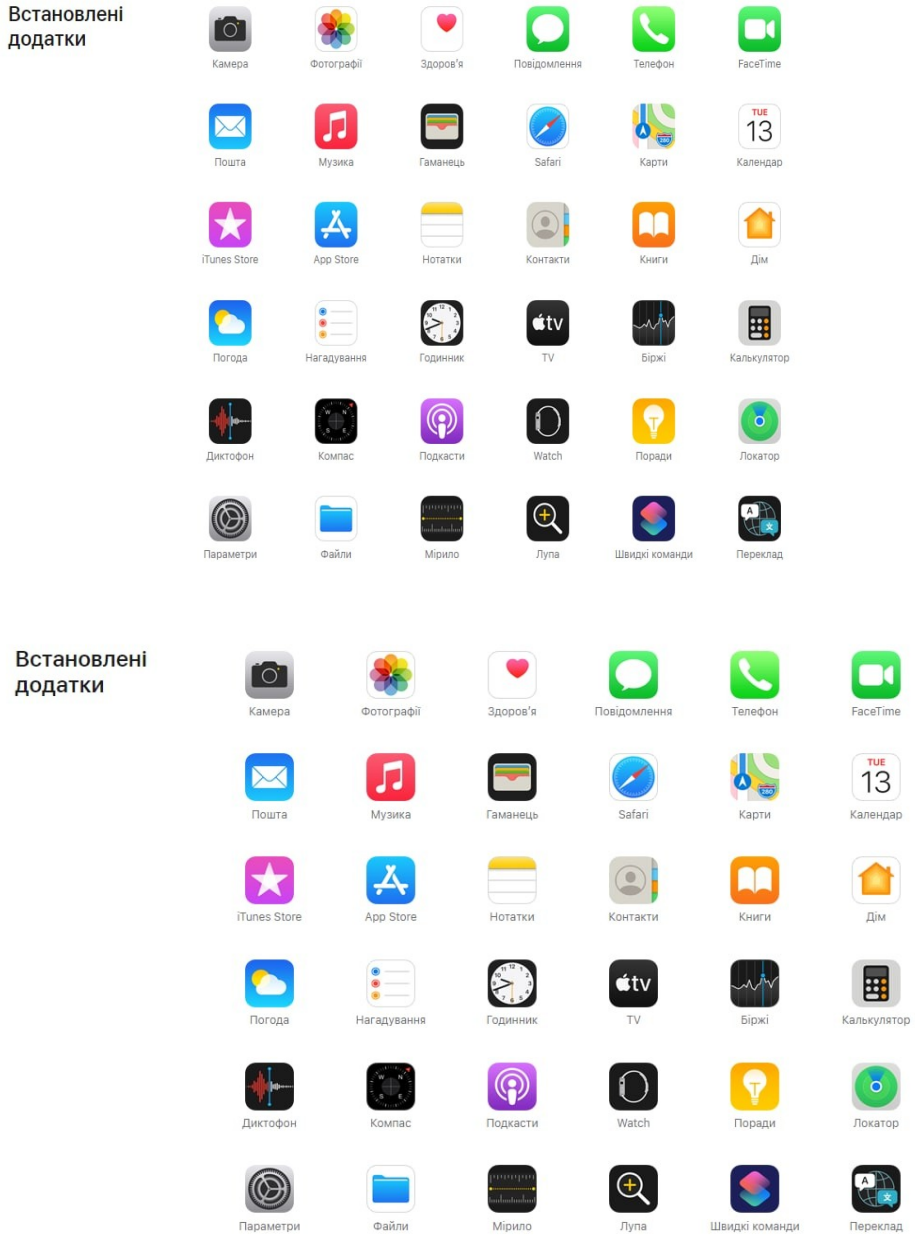

Встановлені додатки
Камера
Фотографії
Здоров'я
Повідомлення
Телефон
FaceTime
Пошта
Музика
Гаманець
Safari
Карти
Календар
iTunes Store
App Store
Нотатки
Контакти
Книги
Дім
Погода
Нагадування
Годинник
TV
Біржі
Калькулятор
Диктофон
Компас
Подкасти
Watch
Поради
Локатор
Параметри
Файли
Мірило
Лупа
Швидкі команди
Переклад
Встановлені додатки
Камера
Фотографії
Здоров'я
Повідомлення
Телефон
FaceTime
Пошта
Музика
Гаманець
Safari
Карти
Календар
iTunes Store
App Store
Нотатки
Контакти
Книги
Дім
Погода
Нагадування
Годинник
TV
Біржі
Калькулятор
Диктофон
Компас
Подкасти
Watch
Поради
Локатор
Параметри
Файли
Мірило
Лупа
Швидкі команди
Переклад

Рис. 2.

РОЗДІЛ 3.
МОДЕЛЬ ЗАГРОЗ ВИТОКУ ІНФОРМАЦІЇ ЗА РАХУНОК НЕСАНЦІОНОВАНОГО ДОСТУПУ

Загалом загрози для мобільних пристроїв можуть бути класифіковані на 4 основні категорії:

- прикладні (програмні) загрози;
- вебзагрози;
- мережеві загрози;
- фізичні загрози.

3.1 Прикладні загрози

Загрози на рівні програм або прикладні є найбільш обговорюваними в літературі загрозами. Програми можуть бути цільовим вектором для порушення безпеки пристрою та його системи до якої він підключається (наприклад, корпоративної мережі). Загрози можуть бути спричинені шкідливими або зловмисними програмами, особливо тими, що завантажуються із стороннього джерела, а також вразливими додатками.

Наприклад, зловмисне програмне забезпечення може запустити програмний код для виконання певних дій у смартфоні – надсилання небажаних запитів повідомлення, надати можливість дистанційно керувати пристроєм, або непомітно викрасти дані користувача, такі як списки контактів, паролі від електронної скриньки та фотографії, без відома або дозволу користувача.

У поспіху скоротити час виходу на ринок розробники створюють додатки з функціональністю, а про безпеку забувають чи ставлять її на останній план. Існує велика кількість програм, які містять лазівки безпеки, якими може скористатися зловмисник.

Хоча вразливі додатки можуть не розроблятися із шкідливим наміром, вони можуть спричинити значні ризики для безпеки та конфіденційності для користувачів. Як приклад – можна отримати географічні координати користувача на основі додатків соціальних мереж.

Завантажені або попередньо встановлені програми можуть представляти багато типів проблем безпеки для мобільних пристроїв. "Зловмисні програми" можуть виглядати чудово на сайті завантаження, але вони розроблені для того, щоб робити різноманітні речі, такі як захоплення паролів, отримання інформації, збирання особистої інформації про кінцевих користувачів без їх відома, вчиняти шахрайство, збирати інформацію для націленої реклами.

Навіть ліцензоване програмне забезпечення можна використовувати в шахрайських цілях.

3.1.1. Шкідливий програмний засіб

Шкідливий програмний засіб (*malware*) – це програмне забезпечення, яке виконує зловмисні кроки на телефоні. Без вашого відома зловмисне програмне забезпечення може стягувати плату за телефонний рахунок, надсилати непотрібні повідомлення у список контактів або надати зловмиснику контроль над пристроєм.

3.1.2. Електронне відстеження (шпигунське чи рекламне програмне забезпечення)

Шпигунське програмне забезпечення призначене для збору або використання приватних даних без відома чи схвалення.

Дані, на які зазвичай спрямовано шпигунське програмне забезпечення, включають історію телефонних дзвінків, текстові повідомлення, місцезнаходження користувача, історію браузера, список контактів, електронну пошту та приватні фотографії. Ця викрадена інформація може бути використана для крадіжок особи або фінансових шахрайств.

Рекламне програмне забезпечення, як правило, встановлюється мимоволі кінцевим користувачем і є звичайною складовою вільного програмного забезпечення, наприклад, програм для обміну файлами. Він збирає інформацію про користувача, яку можна використовувати для націленої реклами у вигляді банерів, спливаючих вікон та вторгнення в конфіденційність через відстеження файлів cookie для співвіднесення поведінки в Інтернеті та для виявлення конкретної особи, яка допомагає в націлених атаках. Надзвичайно поширене сьогодні. Майже кожен додаток відслідковує активність для таргетування реклами.

3.1.3. Вразливі програми

Вразливі програми – програми, які містять недоліки, які можна використовувати в зловмисних цілях. Такі вразливості дозволяють зловмиснику отримувати доступ до конфіденційної інформації, виконувати небажані дії, зупиняти функціонування служби належним чином або завантажувати програми на пристрій без відома користувача.

3.1.4. Програма-вимагач

Програма-вимагач або програма-шантажист – це тип шкідливої програми, який злочинці встановлюють на пристроях. Програми, які вимагають викуп, надають злочинцям можливість віддалено заблокувати пристрій. Після цього програма відображає спливаюче вікно з повідомленням, що пристрій заблокований і що не можна отримати до нього доступ, не заплативши викуп. Користувачі не зможуть видалити шкідливий додаток традиційними засобами для видалення, як це було б зазвичай, тому що система або навіть антивірусний інтерфейс користувача завжди "охоплені" користувацьким інтерфейсом зловмисного програмного забезпечення.

3.2 Загрози вебрівня

Загрози вебрівня або Інтернет-загрози, хоча ці загрози не характерні лише для мобільних пристроїв ризики безпеки та конфіденційності для мобільних пристроїв через загрози вебрівня реальні. Однією з ключових загроз на вебрівні є фішинг, який використовує електронну пошту чи інші додатки для соціальних медіа, щоб надсилати мимовільні повідомлення користувачів на вебсайт із фішингу, розроблений для того, щоб обдурити користувачів у наданні конфіденційної інформації, такої як облікові записи користувачів.

Оскільки мобільні пристрої майже постійно підключені до Інтернету і часто використовуються для доступу до Інтернет-сервісів, вебзагрози створюють постійні проблеми для мобільних пристроїв.

3.2.1. Загрози відмови у обслуговуванні (DoS) / (DDoS)

Хоча реальні атаки DoS та DDoS фіксують заголовки відомих ЗМІ, важливо, щоб організації також повністю розуміли вплив ненавмисних, нешкідливих відключень мобільних пристроїв. На сьогоднішній день більшість DoS-атак були рідкісними і короткочасними роздратуванням, з якими більшість організацій відносно добре могли справлятись. Якщо на ядро Інтернету впливає зловмисна атака чи ненавмисний вихід з ладу, ми всі страждаємо, оскільки Інтернет став нашою «життєвою кров'ю» з точки зору того, як ми працюємо, живемо, граємо та вчимося. З точки зору мобільних пристроїв, фокус може обертатися навколо власних мереж і даних користувачів, мереж та служб передачі даних, які організації.

3.2.2. Ботнет

Боти це один із найскладніших та найпопулярніших видів кіберзлочинності сьогодні. Вони дозволяють хакерам одночасно контролювати багато мобільних пристроїв або комп'ютерів і перетворювати їх на «зомбі», які працюють як частина потужного «ботнету» для поширення вірусів, генерування спаму та вчинення інших видів злочинів та шахрайств в

Інтернеті. Боти підкрадаються до пристрою людини різними способами. Боти часто поширюються по Інтернету, шукаючи вразливі незахищені пристрої для зараження. Коли вони знаходять підходящий пристрій, вони швидко заражають його, а потім повідомляють про свого господаря. Їх мета – залишатися прихованими, поки їм не буде доручено виконати завдання.

Зростання підключених до Інтернету пристроїв дозволяє ботам розвиватися. Ми починаємо бачити, що пристрої, викрадаються та перетворюються на ботів для DDoS, створюючи змішану загрозу із загрозою DoS / DDoS, згаданою вище, тим самим збільшуючи бар'єр для виявлення та попередження їх.

3.2.3. Розширені стійкі загрози (APT)

Смартфони, планшети та інші мобільні пристрої потрапляють під цілеспрямовані атаки, відомі як APT(Advanced Persistent Threats), призначені для крадіжки конфіденційних даних. Мобільні пристрої, що використовуються в організаціях, часто є точкою входу для атаки в стилі APT, спрямованої на певних осіб, щоб отримати доступ до корпоративної інформації. Типи технологічних організацій, які потребують інвестицій у захист від цих загроз, включають контроль додатків, запобігання втрат даних, управління пристроями.

3.2.4. Фішинг

Фішинг шахрайства полягає в наданні цінних даних зловмисникам. Це може включати імена користувачів, паролі, іншу особисту інформацію, фінансові дані тощо. У більшості випадків це відсутність можливості перевірити джерело повідомлення (ніякого способу перегляду повних заголовків в електронній пошті) та труднощі при перегляді повних посилань на малому форм-факторі мобільного пристрою.

3.2.5. Рекламні атаки

Загрози для мобільних пристроїв можуть виникати через мобільну шкідливу рекламу (або зловмисну рекламу), яка є просуванням шкідливих

додатків, схожих на законні програми або програми, які претендують на "безпечні. На відміну від оголошень, що відображаються у веббраузерах ПК, оголошення, що відображаються в мобільних додатках, розміщуються за допомогою коду, який є частиною самих програм. Це може представляти чорний вхід у пристрій. Існують приклади зловмисного програмного забезпечення в магазині Google Play . Додатки для Android через сторонні магазини, деякі навіть встановлюють та виконують рекламне програмне забезпечення на пристрої.

3.2.6. Загрози при завантаженні

При завантаженні і відкритті файлів з інтернету потрібно бути обережним. Часто буває, що шкідливе програмне забезпечення як правило, буває замасковане під пакет оновлення або документ. І після відкриття цього файлу зловмисник отримає контроль над пристроєм до того, як жертва дізнається про це, і навіть якщо власник телефону відразу ж виявить, нічого не зможе вдіяти, щоб запобігти захопленню пристрої шкідливим ПЗ. Хакер матиме доступ до всіх даних і можливість копіювати або видаляти їх, а також мати доступ до мікрофона, камери та всіх зображень на пристрої та Bluetooth.

3.2.7. Вразливість браузера

Інтернет браузер може мати вразливості програмного забезпечення. Просто відвідавши небезпечну вебсторінку, ви можете запустити експлойт, який може встановлювати зловмисне програмне забезпечення або виконувати інші дії на вашому пристрої [7].

3.3 Загрози мережевого рівня

Однією з відмінних особливостей мобільних пристроїв є можливість підключення. Типове з'єднання, що підтримується мобільними пристроями, що на даний момент, включає стільникову / мобільну мережу, локальні бездротові мережі та зв'язок на невеликих відстанях (NFC). Безпека зв'язку на мережевому рівні - це ще одна активна дослідницька область.

3.3.1. Мережеві експлойти

Мережеві експлойти використовують недоліки в мобільній операційній системі або іншому програмному забезпеченні, яке працює в локальних або стільникових мережах. Підключившись, вони можуть перехопити підключення до даних і знайти спосіб ввести зловмисне програмне забезпечення на ваш телефон без вашого відома

3.3.2. Електронне прослуховування (Wi-Fi та Bluetooth)

Аналізатори Wi-Fi перехоплюють дані, що передаються по повітрю між пристроєм і точкою доступу Wi-Fi. Багато програм не застосовують належних заходів безпеки, відправляючи незашифровані дані по мережі, які можуть бути легко перехоплені. Спільне шифрування так само погано. Публічні місця, такі як кафе, ресторани і книжкові магазини, можуть мати захищене WPA2, але є імовірність, що будь-який користувач з паролем зможе розшифрувати ваші пакети.

Загрози Bluetooth також серйозні. Люди, які весь час залишають Bluetooth, увімкнутим залишаються вразливими для сполучення з різними пристроями та завантаження шпигунських програм. Bluejacking – це атака в старому стилі, коли хтось використовує пристрій увімкнутий Bluetooth іншої людини. Bluejacking – це відправка непрошених даних (vCards) для відкриття Bluetooth-пристроїв в цій області. Останнім часом це використовувалося для маркетингу, але багато сучасних смартфони менш уразливі для використання стека Bluetooth.

3.3.3. Виявлення місцезнаходження

Відстеження місцеположення через керовані користувачем додатки про місцезнаходження, де хтось заходить і навмисно ділиться своїм місцезнаходженням. Такі програми, як Facebook, Tinder, Twitter, Uber тощо, тримають та обмінюються інформацією про те, де ви точно знаходитесь в цей момент, не кажучи вже про історію, де ви були.

Виявлення локації шляхом обходу посилених заходів безпеки LTE (4G) з атаками на IMSI або на міжнародні ідентифікатори. Відбувається тріангулювання певних мобільних пристроїв для визначення їх місцезнаходження, це є загрозою, яка може бути використана для багатьох цілей, наприклад, злочинцями, які націлених на високопрофільних осіб та професіоналів.

3.3.4. Публічні мережі

Відомо, що кмітливі кібер-зловмисники користуються публічними мережами готелів чи конференцій, щоб отримати доступ до мобільних пристроїв.

3.4 Загрози фізичного рівня

Фізична безпека мобільних пристроїв не менш важлива. Оскільки мобільні пристрої, як правило, невеликі та портативні, їх можна легко вкрасти або замінити. Втрачений або вкрадений пристрій може використовуватися для отримання доступу до даних користувача, що зберігаються на пристрої, або як точка входу в корпоративну мережу користувача.

3.4.1. Викрадені дані через втрату, крадіжку чи знешкодження пристроїв

Втрачені або викрадені мобільні пристрої є значним ризиком для безпеки та конфіденційності даних. Мобільний пристрій цінний не лише тим, що сам апарат може бути перепроданий третім особам на чорному ринку, але ще важливіше через чутливі особисті та корпоративні дані, які він може містити. Витік даних для мобільних пристроїв /смартфонів/ планшетів - це можливий наслідок, який може мати юридичні наслідки, наслідки порушення даних тощо.

Дані також можуть бути викрадені через напади на мобільні телефони, смартфони чи планшети. У цих випадках зловмисник має можливість відновити інформацію протягом більш тривалого періоду часу, оскільки попередній власник або

користувач пристрою, як правило, більше не очікує спроби використання їх інформації. Наприклад, продаючи вживаний пристрій на платформах онлайн-оголошень, без належної перевірки пристрою, яке було б підтверджено, можна залишити особисту інформацію на смартфоні, яка може бути відновлена іншимм власником та використана для атак проти попереднього власника. Дійсно, було показано, що багато пристроїв операційної системи Android насправді не захищають дані з пристроїв. Система iOS це робить, але існує тривалий ризик доступу до даних третіх сторін, якщо стерту не було належним чином перевірено.

3.4.2. Несанкціонований доступ

Багато користувачів смартфонів не мають блокування екрану або паролю доступу на своїх смартфонах. Ця широка відсутність безпеки робить будь-який мобільний пристрій спокусливою ціллю для несанкціонованого доступу, що згодом може призвести до витоку даних та зараження системи. Деякі з наслідків полягають у тому, парольна фраза чи PIN використовується для шифрування файлової системи, а наявність пароля дозволяє розробити такі функції, як автоматична чистка під час введення помилкових паролів.

3.4.3. Загроза у вигляді подарунка

Як правило, багато людей отримують USB-накопичувачі або інші пристрої в якості подарунка під час відвідування галузевих подій. Занепокоєння викликає те, що люди зі шкідливим наміром, використовують можливості для щоб подарувати електронний пристрій, який попередньо завантажений шкідливим програмним забезпеченням. Подарунок мобільного телефону чи планшета,викликає занепокоєння, оскільки вони мають дуже різні профілі загрози. Коли ці пристрої використовуються або підключаються до мережі чи персонального комп’ютера організації, шкідливе програмне забезпечення може встановлюватися та запускатися.

РОЗДІЛ 4.
ОЦІНКА РИЗИКІВ ВИТОКУ ІНФОРМАЦІЇ ЗА РАХУНОК НЕСАНКЦІОНОВАНОГО ДОСТУПУ

У цьому розділі оцінено наскільки ризикований може бути виток інформації за допомогою того чи іншого засобу. Результати оцінювання наведені в Таблиці 1 де оцінки виставлені за шкалою від 1 до 10 де 1 це майже безпечно, а 10 дуже небезпечно

Таблиця 1.

Загроза витоку інформації	Оцінка
Шкідливий програмний засіб	4
Електронне відстеження	8
Вразливі програми	8
Програма-вимагач	7
Ботнет	10
Загрози відмови у обслуговуванні (DoS) / (DDoS)	10
Розширені стійкі загрози (APT)	10
Фішинг	8
Рекламні атаки	6
Загрози при завантаженні	8
Вразливість браузера	5
Мережеві експлойти	10
Електронне прослуховування (Wi-Fi та Bluetooth)	9
Виявлення місцезнаходження	3
Публічні мережі	6
Викрадені дані через втрату, крадіжку чи знешкодження пристроїв	4
Несанкціонований доступ	8
Загроза у вигляді подарунка	6

РОЗДІЛ 5.
ВИМОГИ ДО ЗАХИСТУ ІНФОРМАЦІЇ ПТК БЕЗДРОТОВОГО ЗВ’ЯЗКУ

6.1 Загальні вимоги

Організація повинна створити, впровадити, експлуатувати, постійно контролювати, аналізувати, підтримувати в робочому стані та покращувати документовану СМЗІ в контексті цілісної ділової діяльності організації та ризиків, із якими вона стикається. Для цілей цього міжнародного стандарту, використовуваний процес заснований на моделі PDCA.

6.2 Створення та менеджмент СМЗІ

6.2.1 Створити СМЗІ

Організація має зробити таке.

a) Визначити область застосування та межі СМЗІ у термінах характеристик бізнесу, організації, її розташування, активів та технологій, також включаючи подробиці та обґрунтування будь-яких винятків із галузі застосування.

b) Визначити політику щодо СМЗІ у термінах характеристик бізнесу, організації, її розташування, активів та технологій, яка:

1) включає структуру для встановлення цілей і встановлює загальний сенс керівництва та принципів дії щодо захисту інформації;

2) враховує ділові та законодавчі чи нормативні вимоги, а також договірні зобов'язання із захисту;

3) дорівнює контексту стратегічного менеджменту ризиків організації,

якому буде відбуватися створення ЗМІЗ та підтримка СМЗІ в робочий стан;

4) встановлює критерії, за якими оцінюватиметься значущість ризику;

5) було затверджено керівництвом.

ПРИМІТКА: Для цілей цього міжнародного стандарту політика щодо СМЗІ розглядається як розширена версія політики у сфері захисту інформації. Обидві ці політики можна описати в одному документі.

c) Визначити підхід до оцінки ризику організації.

1) Визначити методологію оцінки ризику, яка підходить для СМЗІ, а також відповідає встановленим діловим вимогам захисту інформації, законодавчим та нормативним вимогам.

2) Розробити критерії прийняття ризиків та визначити прийнятні рівні ризику. Вибрана методологія оцінки ризику має гарантувати, що оцінки ризику дають порівняні та відтворювані результати.

d) Виявити ризики.

1) Виявити активи в рамках області додатка СМЗІ, а також власників цих активів.

2) Виявити загрози для цих активів.

3) Виявити вразливі місця, які можна використовувати загрозами.

4) Виявити негативні впливи на втрати конфіденційності, цілісності та доступності можуть надати активи.

e) Проаналізувати ризик та оцінити значущість ризику.

1) Оцінити ділові негативні впливи на організацію, які можуть бути результатом збоїв у захисті, беручи до уваги наслідки втрати конфіденційності, цілісності чи доступності активів.

2) Оцінити реалістичну ймовірність випадків порушення захисту, переважаючих загроз і вразливих місць, що відбуваються у світлі, і негативні впливи, пов'язані з цими активами, а також реалізовані на поточний момент засобу управління.

3) Оцінити рівні ризику.

4) Визначити, чи є ризики прийнятними чи вимагають обробки з використанням критеріїв прийняття ризику.

f) Виявити та оцінити можливості для обробки ризиків.

Можливі дії включають:

1) застосування відповідних засобів управління;

2) свідоме та об'єктивне прийняття ризиків, за умови, що вони чітко відповідають політиці організації та задовольняють критеріям для прийняття ризиків;

3) уникнення ризику;

4) передача пов'язаних ділових ризиків іншим сторонам, наприклад, страховикам, постачальникам.

g) Вибрати цілі управління та засоби управління для обробки ризику.

Цілі управління та засоби управління повинні бути обрані та реалізовані, з метою задовольнити вимоги, виявлені процесом оцінки ризиків та обробки ризиків Цей вибір повинен враховувати критерії прийняття ризиків, а також законодавчі, нормативні та договірні вимоги. Вибір цілей керування та засобів керування з Додатка А має бути частиною цього процесу; вони повинні вибиратися як відповідні для того, щоб охопити виявлені вимоги. Списки цілей управління та засобів управління, не є вичерпними, також можна вибрати додаткові цілі управління та засоби управління.

h) Отримати затвердження керівництва пропонованого залишкового ризику.

i) Отримати дозвіл керівництва на реалізацію та роботу СМЗІ.

j) Підготувати Заяву про застосування.

Повинна бути підготовлена заява про застосовність, яка включає себе таке:

1) цілі управління та засоби управління, а також причини їхнього вибору;

2) цілі управління та засоби управління, що реалізуються на даний момент;

3) виключення будь-яких цілей управління та засобів управління, а також обґрунтування для їх виключення.

6.2.2 Реалізувати та експлуатувати СМЗІ

Організація має зробити таке.

a) Сформулювати план обробки ризиків, у якому було б визначено відповідні дії з менеджменту, ресурси, відповідальність та пріоритети для управління ризиками захисту безпеки.

b) Реалізувати план обробки ризиків для того, щоб досягти певних цілей управління, що включає в себе облік фінансування та розподілу ролей та відповідальності.

c) Реалізувати засоби управління, з метою досягти цілей управління.

d) Визначити, як вимірювати результативність вибраних засобів управління або групи засобів управління, а також визначити, як ці вимірювання належить використовувати для оцінки результативності управління так, щоб видати порівняні та відтворювані результати.

e) Здійснювати підготовку та програми підвищення обізнаності.

f) Здійснювати управління експлуатацією СМЗІ.

g) Керувати ресурсами для СМЗІ.

h) Впровадити процедури та інші засоби управління, здатні надати можливість швидкого виявлення події в системі захисту інформації та реакції на інциденти у системі захисту інформації

6.2.3 Постійно контролювати та аналізувати СМЗІ

Організація має зробити таке.

a) Виконувати процедури постійного контролю та аналізу, а також інші засоби управління для того, щоб:

1) швидко виявляти помилки у результатах обробки;

2) швидко виявляти вживані та успішні порушення захисту та інциденти;

3) дати керівництву можливість визначати, чи здійснюються види діяльності із захисту, призначені людям або які здійснюються інформаційною технологією, як очікувалося;

4) допомагати виявляти події в системі захисту інформації та тем самим запобігати інцидентам у системі захисту інформації шляхом використання індикаторів;

5) Визначати, чи були дії, вжиті для вирішення проблеми з порушенням захисту, результативними.

b) Робити регулярний аналіз результативності СМЗІ (включаючи відповідність політиці та цілям СМЗІ, а також аналіз засобів управління захистом), беручи до уваги результати аудитів захисту, інциденти, результати вимірювань результативності, пропозиції та зворотну реакцію усіх зацікавлених сторін.

c) Вимірювати результативність засобів управління для того, щоб перевірити, що вимоги захисту були задоволені.

d) Аналізувати оцінки ризику через заплановані інтервали та аналізувати залишкові ризики та певні прийнятні рівні ризику, беручи до уваги зміни у наступному:

1) організація;

2) технологія;

3) ділові цілі та процеси;

4) виявлені небезпеки;

5) результативність реалізованих засобів управління;

6) зовнішні події, такі як зміни до законодавчої або нормативно-правовому середовищі, змінені договірні зобов'язання, а також зміни у соціальному кліматі.

e) Проводити внутрішні аудити СМЗІ через заплановані інтервали.

f) Регулярно здійснювати аналіз СМЗІ з боку керівництва з метою гарантувати, що сфера застосування залишається адекватною, і виявляються покращення у процесі СМЗІ.

g) Оновлювати плани захисту, щоб врахувати дані, отримані в ході діяльності з постійного контролю та аналізу.

h) Записувати дії та події, які могли б негативно вплинути на результативність чи якість роботи СМЗІ.

6.2.4 Підтримувати у робочому стані та покращувати СМЗІ

Організація має регулярно робити таке.

a) Впроваджувати виявлені покращення у СМЗІ.

b) Здійснювати належні коригувальні та запобіжні дії. Застосовувати уроки з досвіду захисту інших організацій, і навіть з досвіду самої організації.

c) Повідомляти про всі дії та покращення всім зацікавленим сторонам з рівнем детальності, відповідним обставинам та, за значимістю, узгоджувати подальші дії.

d) Гарантувати, що покращення досягають передбачуваних цілей.

РОЗДІЛ 6.
ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ ПТК БЕЗДРОТОВОГО ЗВ’ЯЗКУ

Для захисту найрозповсюдженішого пристрою в повсякденному житті, а саме мобільного телефону, запропоновано використовувати скремблер рис1

рис.1.

Скремблер (аудіо-скремблер) — програмне забезпечення або апаратний прилад, який виконує обробка і шифрування сигналу таким чином, що він може бути прийнятим тільки приймачем, що оснащений відповідним дешифратором.

Завдяки ньому підслуховування розмови, що ведеться по вашому телефону, стає повністю неможливим, незалежно від методики перехоплення. Маються на увазі будь-які методи, включаючи такі, як контроль оператора», пасивне перехоплення в зоні телефону, активне перехоплення з перемиканням телефону на «хибну» базу тощо.

Для перевірки приміщень на закладні пристрої запропоновано прости та дієвий варіант. А саме зйомка фото, або відео зі спалахом що покаже наявність лінз у приміщенні та так званий ефект червоного ока рис2.

Рис.2.

Щоб перевірити та оцінити звукоізоляцію в приміщенні запропоновано завантажити в мобільний телефон програми для виміру акустичного шуму. Наприклад Sound Meter для ОС Android IOS. Приклад інтерфейсу додатку Sound Meter можна побачити на рис3

Якщо використати СДР кабель та кабель до порту телефону за допомогою програми SDR Touch, інтерфейс якої ми бачимо на рис4 можна відшукати зловмисні сигнал в діапазоні 25-1700 мгц а також знайти сигнали в діапазонах Wi-FI, Bluetooth, тощо.

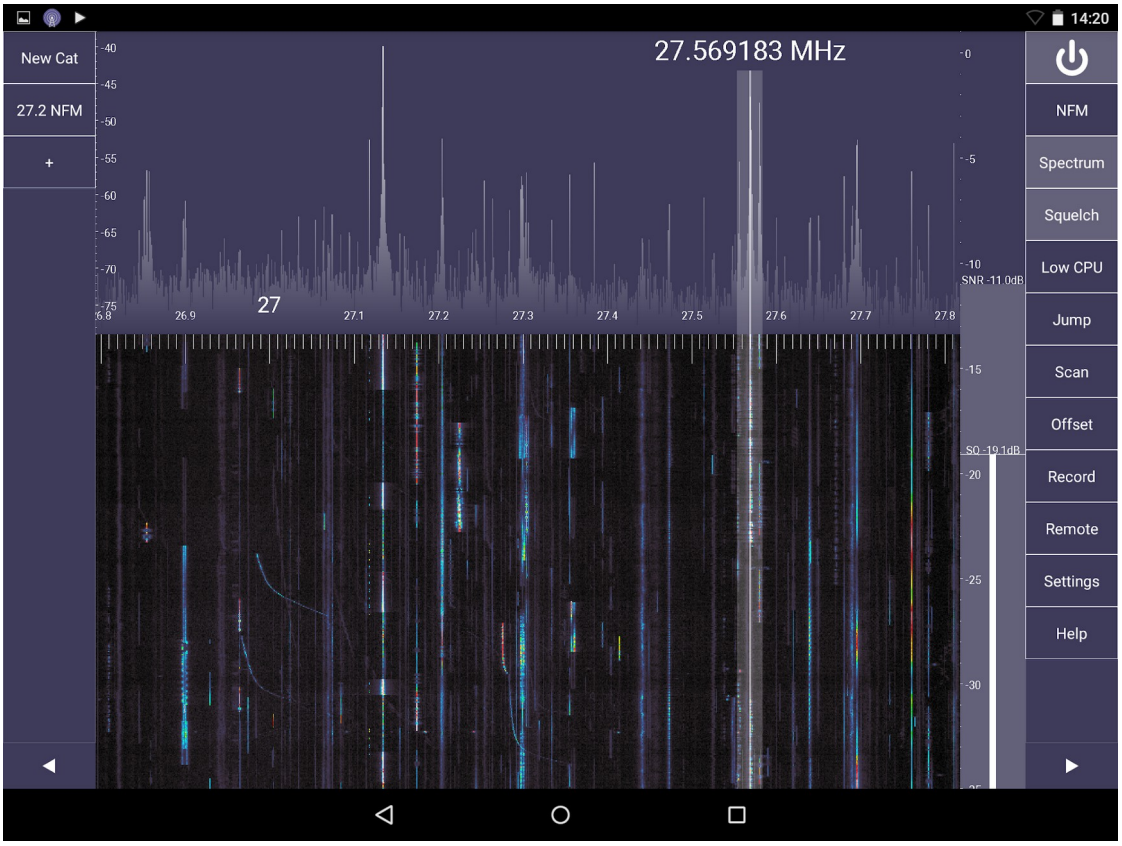


Рис.4.

А за допомогою динаміку підключеного до виходу телефону та СДР в парі з конвектором нЧ можна перевірити приміщення на акустоелектрику и акустогенерацію рис5

Рис.5.

РОЗДІЛ 7.
СТВОРЕННЯ СИСТЕМИ КОМПЛЕКСА РАДІОМОНІТОРИНГУ РДЖ

Базова модифікація	Вартість, грн	Лінк
Портативна система Divoom Iris-02 USB Green	510	https://kvshop.com.ua/ru/akusticheskie-sistemy/divoom/divoom-iris-02-usb-green/
Портативна кімнатна антена MS2 FFX	90	https://cs1130680.uaprom.net/ua/p240468381-portativnaya-komnatnaya-antenna.html
USB трійник хаб	300	https://rozetka.com.ua/frime_fh_20041/p289769513/
Смартфон	2000	https://rozetka.com.ua/alcatel_5033d_2laluaf/p246767797/
Антенний комутатор	100	https://www.olx.ua/d/uk/obyavlenie/pit-adm7280-antennyy-kommutator-s-vneshney-sinhronizatsiey-IDPUR6J.html
RTL SDR приймач, тюнер SDR+DAB+FM+HDTV+DVB-T на чіпі rtl2832u r828d	1800	https://www.olx.ua/d/uk/obyavlenie/rtl-sdr-priemnik-tyuner-sdr-dab-fm-hdtv-dvb-t-na-chipe-rtl2832u-r828d-IDHjjNd.html
ВСЬОГО	**4800**	

Комплекс радіомоніторингу РДЖ в складі:

-SDR USB приймач,
-комутаційний модуль,
-антена дипольна активна,
-антена дипольна пасивна.
-антена штирьова
-програмне забезпечення,
-інструкція по експлуатації

Також підібрані антени

Пасивна дипольна - ТВ-антена X-Digital PIN 170

Активна дипольна - ТВ антена EuroSky ES-001

Штирьова антена - Портативна кімнатна антена MS2 FFX

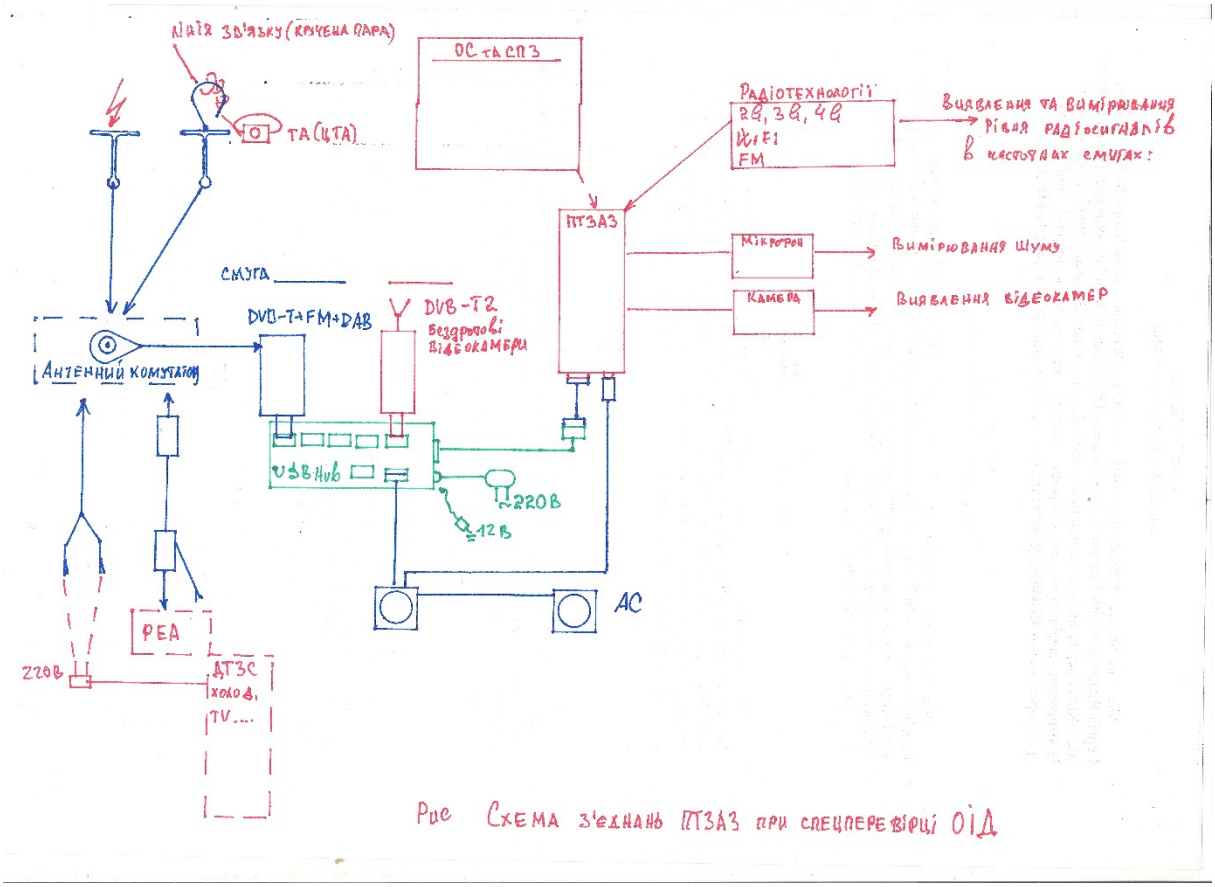
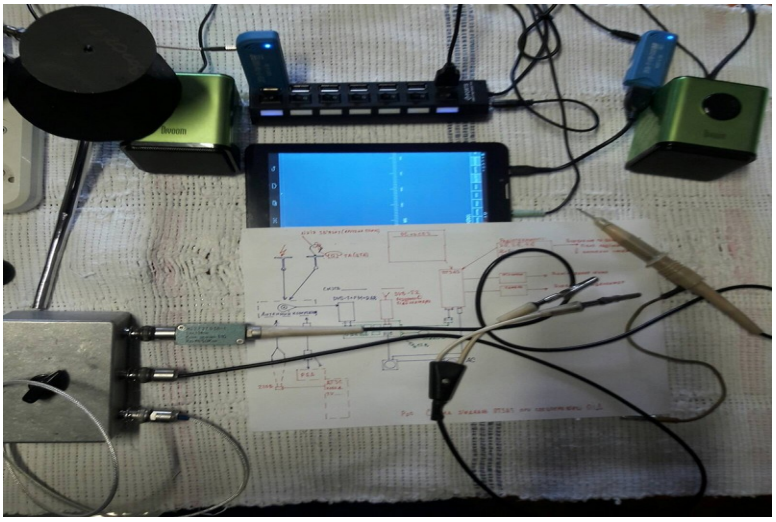
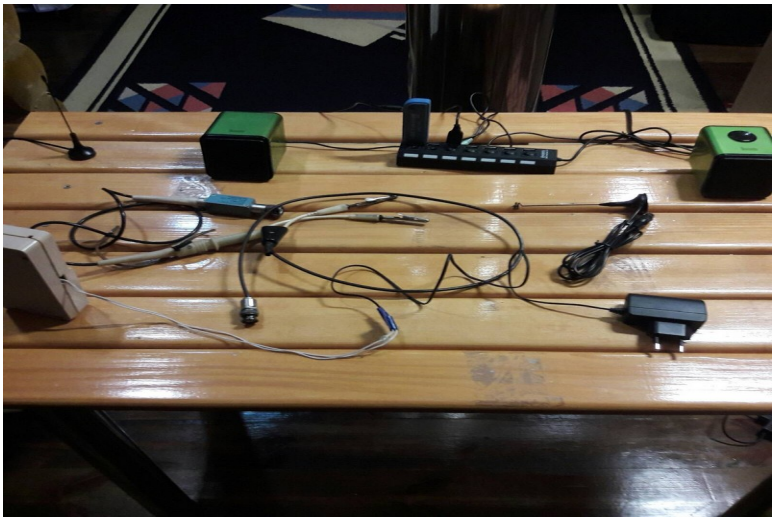


Рис.1.





На базі запропонованих в Таблиці 1. компонентів була створена схема з’єднань рис.1 при спецперевірці ОІД, та за цією схемою створена відповідна система захисту інформації програмно технічного комплексу бездротового зв’язку.

ВИСНОВКИ

Проведений аналіз можливостей ПТКБЗ, можливих каналів витоку інформації в місцях його використання дав змогу розробити модель загроз, оцінити ризики та на підставі цього визначити основні технічні вимоги (далі ТВ) до системи захисту ПТКБЗ.

Розроблений варіант реалізації ТВ дає змогу забезпечити безпечний обмін конфіденційною інформацією з перевірених об’єктів інформаційної діяльності, за допомогою загальнодоступних програмних та апаратних засобів.

Основною перевагою запропонованої системи захисту ПТКБЗ є простота її використання, суттєво нижча вартість та достатність забезпечувати захист конфіденційної інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ленков С.В., Перегудов Д.А., Хорошко В.А. Методи та засоби захисту інформації / Под ред. В.А. Хорошко. – К.: Арий, Несанкціоноване отримання інформації ,2010. – 464 с.

2. Коженевський С.Р. Термінологічний довідник з питань захисту інформації / Коженевський С.Р., Кузнецов Г.В., Хорошко В.О., Чирков Д.В.. – К.: ДУІКТ, 2007. – 382 с.

3. Поляков М.Г., Фомичова Л.Я., Сушко С.О., Математичні основи теоретичної електротехніки: Навчальний посібник -Дн.: НГА України, 2001. –210с.

4. Довбня С.Я., Наталенко П.П. Основи використання, адміністрування та забезпечення захисту інформації в автоматизованих системах: Навчальний посібник. – К.: ТОВ «Софтлайн ІТ», 2017. – 164 с.

5.1. Оцінка захищеності інформації, Створення та атестація комплексів технічного захисту інформації на об’єктах інформаційної діяльності Сил спеціальних операції України: Методичні рекомендації/ Довбня С.Я.. – К.: ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «ДЕПС СОЛЮШЕНЗ» 2020. – 120 с.

6. Довбня С.Я.. Методи (моделі) розробки комплексів технічного захисту інформації на об’єктах інформаційної діяльності та радіоелектронної техніки: Навчальний посібник. – К.: ДП «Український центр «Безпека», 2019. – 95 с.

7. Довбня С.Я.. Підготовка користувачів та адміністраторів ЗАТК "Персонал-Командування" з технічного захисту інформації: Навчальний посібник. – К.: ТОВ «Софтлайн ІТ», 2018. – 280 с.

8. Андріанов В. В. Забезпечення інформаційної безпеки бізнесу / В. В. Андріанов, С. Л. Зефіров, В. Б. Голованов. - М.: ЦІПСіР, 2016. - 373 с

9. Конахович Г.Ф. та інші. Захист інформації в телекомунікаційних системах: Навчальний посібник. – К.: НАУ, 2009.-380 с.

10. Гулак Г.М. та інші. Основи криптографічного захисту інформації.-К.: ІММ НАНУ, 2011.-200 с.

11. Основи інформаційної безпеки. Лужецький В.А., Кожухівський А.Д., Войтович О.П. Навчальний посібник. – Вінниця: ВНТУ, 2009. – 268 с.

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