

РЕФЕРАТ

ПЗ: 85 с, 25 рис., 7 табл., 20 джерел

Об'єктом дослідження є інформація, яку необхідно захищати, і яка циркулює у контрольованій зоні режимного приміщення.

Предметом дослідження є Wi-Fi пристрій та персональний комп'ютер, з яких здійснюється виток інформації безконтактним способом.

Мета роботи та завдання дослідження. Метою роботи є дослідження вразливостей у системах бездротової мережі і вразливостей у персональних комп'ютерах.

Методи дослідження. У роботі використані методи розпізнавання людей бездротовими технологіями, методи перехвату паролів користувачів, які використовують бездротову мережу, методи соціальної інженерії і методи запобігання витоку інформації.

Наукова новизна результатів:

1. Вразливості, які присутні у бездротових мережах дозволяють здійснювати спостереження контрольованої зони дистанційно.
2. У бездротових мережах за допомогою соціальної інженерії, можливо здійснити перехоплення конфіденційної інформації.
3. За допомогою соціальної інженерії, користувачі встановлюють на свої персональні комп'ютери троянські програми, що призводить до дистанційного спостереження за дією користувача.

БЕЗДРОВОТА МЕРЕЖА, WI-FI, БРАНДМАУЕР, АНТИВІРУС, МАЙНІНГ, ВІДДАЛЕНИЙ ДОСТУП, WIFIPHISHER, RMS, PROCESS HACKER

ЗМІСТ

Вступ	8
1 Огляд ризиків витоку режимної інформації.....	10
1.1 Основні завдання забезпечення безпеки.....	10
1.2 Етапи створення і забезпечення системи захисту інформації.....	12
1.3 Види конфіденційних даних.....	14
1.4 Загрози конфіденційності інформаційних ресурсів.....	14
1.5 Апаратна і програмна ІБ.....	15
1.6 Канали витоку інформації.....	17
2 Дослідження шляхів виникнення витоку інформації безконтактними методами.....	21
2.1 Спостереження за приміщенням за допомогою RF Capture.....	21
2.1.1 Метод усунення засвічування.....	24
2.1.2 Аналіз параметрів, які відстежують рухи.....	25
2.2 Перехват трафіку через програмне забезпечення Wifiphisher.....	27
2.3 Програми майнінгу.....	31
2.4 Програма прихованого віддаленого доступу RMS.....	33
3 Рекомендації щодо удосконалення методів захисту інформації.....	37
3.1 Оптимізація розповсюджень радіохвиль у режимній зоні.....	37
3.2 Моніторинг систем безпеки у бездротових мережах.....	40
3.3 Удосконалений комплекс заходів з забезпечення безпеки комп'ютера від безконтактних методів проникнення.....	41
3.3.1 Програми оптимізації роботи комп'ютера.....	42
3.3.2 Диспетчер завдань Process Hacker.....	43
3.3.3 Програмні та апаратні брандмауери.....	45
3.3.4 Антивірусні програмні забезпечення.....	47
4 Економічні розрахунки.....	50
4.1 Важливість інформаційної безпеки для підприємств.....	50
4.2 Тенденції та перспективи розвитку ринку засобів та послуг інформаційної безпеки.....	52

4.3	Розрахунок витрат на практичну реалізацію проекту.....	54
4.4	Бальна оцінка економічної ефективності проекту.....	56
5	Охорона праці та безпека у надзвичайних ситуаціях.....	61
5.1	Аналіз потенційних небезпек.....	61
5.2	Заходи по забезпеченню безпеки.....	62
5.3	Заходи по забезпеченню виробничої санітарії та гігієни праці.....	65
5.4	Заходи з пожежної безпеки.....	67
5.5	Заходи по забезпеченню безпеки у надзвичайних ситуаціях.....	69
	Висновок.....	81
	Список використаних джерел.....	83

СПИСОК СКОРОЧЕНЬ

ІБ	– Інформаційна безпека
КС	– Комп’ютерні системи
ОТЗС	– Основні технічні засоби і системи
ДТЗС	– Допоміжні технічні засоби і системи
ЦП	– центральний процесор
DLP	– Data Loss Prevention – Системи запобігання витоку інформації
ID	– Identity Document - унікальна ознака об’єкта
SIEM	– Security information and event management – Інформація про безпеку та керування подіями
MIMO	– Multiple Input Multiple Output – Декілька входів, декілька виходів
MITM	– Man in the middle – людина посередині
HTTP	– Hyper Text Transfer Protocol – протокол передачі гіпертексту
HTTPS	– Hyper Text Transfer Protocol Secure – безпечний протокол передачі гіпертексту
NAT	– Network Address Translation - перетворення мережевих адрес
DHCP	– Dynamic Host Configuration Protocol – протокол динамічної настройки вузла
ISAR	– Техніка зворотного радіолокаційного синтезування апертури
RAT	– Remote Access Toolkit – засіб віддаленого адміністрування
VPN	– Virtual private network – Віртуальна приватна мережа
Wi-Fi	– Wireless Fidelity – Бездротова точність

ВСТУП

З кожним днем посилюється зростання інформаційних і телекомунікаційних технологій. На ряду з удосконаленням обчислювальної техніки і засобів зв'язку, актуальним стає питання про якість і захищеність передаючої інформації. У наш час будь-які листи передаються через комп'ютерну мережу, розрахунки здійснюється через електронний платіж, гігантські масиви даних зберігаються в хмарних сервісах, а число мобільних гаджетів перевищує загальну чисельність населення Землі. З появою нових технологій обмін інформацією стає доступнішим і чим легше передати повідомлення, тим простіше вкрасти його вміст. Сьогодні, коли комп'ютери і стільникові телефони містять численні дані про власника, коли угоди укладаються через електронний документообіг, відсутність захищеності інформації загрожує матеріальними втратами, втратою довіри, збитком репутації, як для окремої особистості, так і для компанії або цілої країни.

Захист інформації – це комплекс технічних, організаційних і правових заходів, які повинні забезпечувати конфіденційність, захист від несанкціонованого доступу, захист від несанкціонованої зміни та забезпечення доступу до інформації.

Тобто, головне завдання інформаційного захисту зберегти такі властивості інформації, як:

- доступність - вказує, що всі авторизовані користувачі повинні мати доступ до конфіденційної інформації;
- цілісність - передбачає забезпечення достовірності і коректного відображення охоронюваних даних, незалежно від того, які системи безпеки і прийоми захисту використовуються в компанії;
- конфіденційність - означає, що доступ до перегляду та редагування даних надається виключно авторизованим користувачам системи захисту.

В режимних приміщеннях при використанні бездротових з'єднань можливе спостереження за об'єктами, які знаходяться в ньому. Можливо здійснювати перехват інформації, яка проходить через бездротові з'єднання.

Проблеми, пов'язані з безпекою передачі інформації при роботі в комп'ютерних мережах, можливо розподілити на п'ять основних типів:

- перехоплення інформації;
- порушення конфіденційності інформації при збереженні її цілісності;
- зміна інформації – справжнє повідомлення повністю замінюється іншим або змінюється його частина і надсилається адресату;
- заміщення або викрадення авторської інформації;
- захоплення повідомлення.

1 ОГЛЯД РИЗИКІВ ВИТОКУ РЕЖИМНОЇ ІНФОРМАЦІЇ

1.1 Основні завдання забезпечення безпеки

Основними задачами забезпечення безпеки є:

- захист інформації за допомогою шифрування і кодування, які є складовими видами криптографічного методу;
- перевірка достовірності даних та автентифікація користувачів;
- своєчасне виявлення порушень цілісності об'єктів даних, створення захисних процедур і безпечного веб-середовища, що запобігає спробі вторгнення зловмисників і знижує потенційний ризик або втрати;
- забезпечення захисту приміщень, в яких відбувається передача конфіденційної інформації;
- забезпечення захисту програмного забезпечення і комп'ютерного обладнання від впровадження в них програмних вірусів і закладок;
- захист від несанкціонованих дій по каналу зв'язку від осіб, що не допущені до засобів шифрування;
- організаційно-технічні заходи, спрямовані на забезпечення схоронності конфіденційних даних та виконання заходів з контролю чи припиненню шкідливих дій при виявленні атаки або вторгнення.

Об'єктом захисту інформації є – інформація, носій інформації, або інформаційний процес, які необхідно захищати відповідно до поставленої мети захисту інформації. За формою подання інформацію можливо класифікувати таким чином: паперові носії, цифрові сигнали, аналогові сигнали, віртуальна форма. До ресурсних об'єктів відносять: апаратне та програмне забезпечення, процедури і процеси обробки інформації. Фізичні об'єкти складаються з: території, приміщень, будівель, технічного спорудження, засобів і каналів зв'язку. Призначені для користувачів об'єкти,

включають в себе: користувачів інформацією, суб'єкти інформації, власників інформації, обслуговуючий персонал.

Інформаційна безпека (ІБ) – це стан інформаційної системи, при якому вона найменш сприйнятлива до втручання і нанесення збитку з боку третіх осіб. Безпека даних також має на увазі управління ризиками, які пов'язані з розголошенням інформації або впливом на апаратні і програмні модулі захисту. Забезпечення безпеки інформації, яка обробляється в організації - це комплекс дій, спрямованих на вирішення проблеми захисту інформаційного середовища в рамках компанії. При цьому інформація не повинна бути обмежена у використанні і динамічному розвитку для уповноважених осіб.

Захист інформаційних ресурсів повинен бути:

1. Постійним (зловмисник, у будь-яку мить може спробувати обійти модулі захисту даних, які його цікавлять).
2. Цільовим (інформація повинна захищатися в рамках певної мети, яку висуває власник даних).
3. Плановим (всі методи захисту повинні відповідати державним стандартам, законам і підзаконним актам, які регулюють питання захисту конфіденційних даних).
4. Активним (заходи для підтримки роботи та вдосконалення системи захисту повинні проводитися регулярно).
5. Комплексним (використання тільки окремих модулів захисту або технічних засобів неприпустимо, також необхідно застосовувати всі види захисту в повній мірі, інакше розроблена система буде позбавлена сенсу і економічного підґрунтя).
6. Універсальним (засоби захисту повинні бути обрані відповідно до існуючих в компанії каналах витоку інформації).
7. Надійним (всі прийоми захисту повинні надійно перекривати можливі шляхи до охоронюваної інформації з боку зловмисника, незалежно від форми представлення даних).

1.2 Етапи створення і забезпечення системи захисту інформації

На практиці створення системи захисту інформації здійснюється в три етапи.

На першому, розробляється базова модель системи, яка буде функціонувати в компанії. Далі визначається, які джерела інформації слід захистити і яка мета отримання доступу до інформації, що захищається.

Метою може бути ознайомлення, зміна, модифікація або знищення даних. Ознайомлення не призводить до руйнування структури даних, а модифікація і знищення призводять до часткової або повної втрати інформації. Далі необхідно передбачити джерело конфіденційної інформації - люди або інформаційні ресурси: документи, флеш-носії, публікації, продукція, комп'ютерні системи, засоби забезпечення трудової діяльності.

Необхідно з'ясувати способи отримання доступу:

- несанкціонований доступ - незаконне використання даних;
- витік - неконтрольоване поширення інформації за межі корпоративної мережі через недоліки технічного каналу системи безпеки;
- розголошення - наслідок впливу людського фактору (користувачі можуть розголошувати інформацію, щоб передати конкурентам, або з необережності).

Другий етап включає розробку системи захисту. Він означає реалізацію всіх обраних способів, засобів і напрямів захисту даних.

Система будується відразу по декільком напрямках захисту, на декількох рівнях, які взаємодіють один з одним для забезпечення надійного контролю інформації.

Правовий рівень забезпечує відповідність державним стандартам у сфері захисту інформації та включає авторське право, укази, патенти і посадові інструкції. Грамотно вибудована система захисту не порушує права користувачів і норми обробки даних.

Організаційний рівень дозволяє створити регламент роботи користувачів з конфіденційною інформацією, підібрати кадри, організувати роботу з документацією і фізичними носіями даних.

Регламент роботи користувачів з конфіденційною інформацією називають правилами розмежування доступу. Правила встановлюються керівництвом компанії спільно зі службою безпеки і постачальником, який впроваджує систему безпеки. Мета - створити умови доступу до інформаційних ресурсів для кожного користувача, наприклад, право на читання, редагування, передачу конфіденційного документа. Правила розмежування доступу розробляються на організаційному рівні і впроваджуються на етапі робіт з технічної складової системи.

Технічний рівень умовно поділяють на фізичний, апаратний, програмний і математичний підрівні.

- фізичний - створення перешкод навколо об'єкта, що захищається: охоронні системи, зашумлення, зміцнення архітектурних конструкцій;
- апаратний - установка технічних засобів: спеціальні комп'ютери, системи контролю співробітників, захисту серверів і корпоративних мереж;
- програмний - установка програмної оболонки системи захисту, впровадження правила розмежування доступу і тестування роботи;
- математичний - впровадження криптографічних і стенографічних методів захисту даних для безпечної передачі по корпоративній або глобальній мережі.

Третій, завершальний етап - це підтримка працездатності системи, регулярний контроль і управління ризиками. Важливо, щоб модуль захисту відрізнявся гнучкістю і дозволяв адміністратору безпеки швидко удосконалювати систему при виявленні нових потенційних загроз. [1]

1.3 Види конфіденційних даних

Конфіденційні дані – це інформація, доступ до якої обмежується відповідно до законів держави і нормами, які компанії встановлюються самостійно.

Особисті конфіденційні дані: персональні дані громадян, право на особисте життя, листування, приховування особистості.

Службові конфіденційні дані: інформація, доступ до якої може обмежити тільки держава (органи державної влади).

Судові конфіденційні дані: таємниця слідства і судочинства.

Комерційні конфіденційні дані: всі види інформації, яка пов'язана з комерцією (прибутком) і доступ до якої обмежується законом або підприємством (секретні розробки, технології виробництва і т.д.).

Професійні конфіденційні дані: дані, пов'язані з діяльністю громадян, наприклад, лікарська, нотаріальна або адвокатська таємниця, розголошення якої переслідується по закону.

1.4 Загрози конфіденційності інформаційних ресурсів

Загроза – це можливі або дійсні спроби заволодіти захищеними інформаційними ресурсами.

Джерелами загрози безпеці конфіденційних даних є компанії-конкуренти, зловмисники, органи управління. Мета будь-якої загрози полягає в тому, щоб вплинути на цілісність, повноту і доступність даних.

Загрози бувають внутрішніми або зовнішніми. Зовнішні загрози є спробами отримати доступ до даних ззовні і супроводжуються зломом серверів, мереж, облікових записів працівників і зчитуванням інформації з технічних каналів витоку (акустичне зчитування за допомогою жучків, камер,

наведення на апаратні засоби, отримання віброакустичної інформації з вікон і архітектурних конструкцій).

Внутрішні загрози мають на увазі неправомірні дії персоналу, робочого відділу або управління фірми. В результаті користувач системи, який працює з конфіденційною інформацією, може видати інформацію стороннім. На практиці така загроза зустрічається частіше за інших. Працівник може роками «зливати» конкурентам секретні дані. Це легко реалізується, адже дії авторизованого користувача адміністратор безпеки не кваліфікує як загрозу.

Спроба несанкціонованого доступу може відбуватися декількома шляхами:

- через співробітників, які можуть передавати конфіденційні дані стороннім, забирати фізичні носії або отримувати доступ до охоронюваної інформації через друковані документи;
- за допомогою програмного забезпечення зловмисники здійснюють атаки, які спрямовані на крадіжку пар «логін-пароль», перехоплення криптографічних ключів для розшифровки даних, несанкціонованого копіювання інформації;
- за допомогою апаратних компонентів автоматизованої системи, наприклад, впровадження прослуховуючих пристроїв або застосування апаратних технологій зчитування інформації на відстані (поза контрольованою зоною).

1.5 Апаратна і програмна ІБ

Всі сучасні операційні системи оснащені вбудованими модулями захисту даних на програмному рівні. MAC OS, Windows, Linux, iOS відмінно справляються із завданням шифрування даних на диску і в процесі передачі на інші пристрої. Однак для створення ефективної роботи з конфіденційною інформацією важливо використовувати додаткові модулі захисту.

Призначені для користувача ОС не захищають інформацію в момент передачі по мережі, а системи захисту дозволяють контролювати інформаційні потоки, які циркулюють по корпоративній мережі, і зберігання даних на серверах.

Апаратно-програмний модуль захисту прийнято розділяти на групи, кожна з яких виконує функцію захисту чутливої інформації:

- рівень ідентифікації - це комплексна система розпізнавання користувачів, яка може використовувати стандартну або багаторівневу аутентифікацію, біометрії (розпізнавання особи, сканування відбитка пальця, запис голосу і інші прийоми);
- рівень шифрування забезпечує обмін ключами між відправником і отримувачем і шифрує / дешифрує всі дані системи.

Захисту потребують як основні технічні засоби і системи (ОТЗС), задіяні в роботі з захищеними даними, так і допоміжні технічні засоби і системи (ДТЗС), а також заздалегідь певні приміщення.

Організаційний захист інформації складається в зведенні правил, складених на основі правових актів, покликаних запобігти неправомірному заволодінню конфіденційними даними.

Організаційний метод забезпечення інформаційної безпеки має наступні складові:

- створення режиму охорони інформації;
- розробка правил взаємовідносин між співробітниками;
- регламентація роботи з документами;
- правила використання технічних засобів в рамках існуючого правового поля;
- аналітична робота з оцінки загроз інформаційній безпеці.

Захист інформаційної інфраструктури від несанкціонованого доступу забезпечується регламентацією доступу суб'єктів (працівників) до об'єктів (носіїв даних і каналам їх передачі). Організаційний метод забезпечення інформаційної безпеки не має на увазі використання технічного

інструментарію. Така інформаційна безпека часто складається, наприклад, у видаленні ОТЗС за периметр території, що охороняється на максимально можливу відстань.

Застосування технічного обладнання і різних програм для забезпечення інформаційної безпеки, включаючи системи управління базами даних, прикладне ПЗ, різні шифрувальники, DLP-системи і SIEM-системи, що виключають виток даних через комп'ютерну мережу, вже належить до технічного методу забезпечення інформаційного захисту. Обидва методи взаємодоповнювані і називаються організаційно-технічними (наприклад, проведення спеціальних перевірок технічних засобів і приміщень на предмет виявлення сторонніх пристроїв, призначених для фіксування і передачі інформації). Організаційно-технічні заходи в обов'язковому порядку повинні відповідати правовим методам забезпечення інформаційної безпеки, запропонованим нормативними документами.

Політика інформаційної безпеки розробляється з урахуванням існування безлічі підсистем, включаючи:

- підсистему надання доступу;
- підсистему реєстрації та обліку;
- підсистему щодо забезпечення безпеки за рахунок використання шифрів.

Головні правила успішної системи інформаційної безпеки:

- перманентність дії встановлених правил;
- повнота заходів, що вживаються;
- комплексність;
- узгодженість;
- результативність.

1.6 Канали витоку інформації

Під загрозою безпеки інформації в комп'ютерній системі (КС) визначають подію або дію, яка може викликати зміну функціонування КС, пов'язану з порушенням захищеності оброблюваної в ній інформації. До однієї з цих загроз відносять витік інформації по технічним каналам зв'язку, під яким розуміється неконтрольоване поширення інформативного сигналу від його джерела через фізичне середовище до технічного засобу, який здійснює прийом інформації. При передачі інформації можливо її перехоплення, тобто неправомірне отримання інформації з використанням технічного засобу, який здійснює виявлення, прийом і обробку інформативних сигналів. [2]

В результаті перехоплення інформації можливо неправомірне ознайомлення з інформацією або неправомірний запис інформації на носій. Особливості технічних каналів витоку інформації визначаються фізичною природою інформаційних сигналів і характеристиками середовища їх поширення.

Серед поширених причин витоку інформації виділяють наступне:

- недостатня охорона даних (організацією або довіреною особою);
- якщо неправильно поводитися з пристроями, які зберігають інформацію (з технічних причин).

Все це відбувається при супутніх умовах, які допускають виникнення ситуації витоку:

- некомпетентність співробітників, які займаються захистом даних, їх нерозуміння важливості процесу і недбале ставлення до інформації в цілому;
- використання неліцензійних продуктів або тих продуктів, які не пройшли атестацію програм щодо захисту інформації клієнтів і збереження їх конфіденційності;
- постійна зміна роботи співробітників, які займаються захистом персональних даних.

Причину у витоку інформації найчастіше покладається саме на співробітників фірм і підприємств, а також на їх керівництво. Від будь-якого зловмисника можливо захиститися при бажанні і компетентності працівників.

Основами для передачі інформації будь-якого виду служать системи зв'язку. Найпростіші системи складаються з носія інформації, приймача, одержувача інформації, а також каналу передачі. Будь-який сигнал можливо передати наступним чином:

- світлові промені;
- електромагнітний спосіб передачі;
- звукові хвилювання;
- матеріали і речовини.

Кожен канал передачі інформації має ряд характеристик:

- місцезнаходження початку і кінця;
- форма передачі інформації;
- складові, або структура каналу;
- швидкість, обсяги відправлення та отримання даних;
- вид каналу і спосіб передачі (як перетворюється сигнал);
- пропускна здатність ланцюга;
- ємність каналу.

Ці системи і канали використовуються для передачі інформації. Але бувають випадки, коли канал виникає в іншому місці, він не явний і тому називається каналом витоку інформації. Канал з'являється незалежно від джерела інформації та способу її передачі.

Технічний канал витоку інформації - це фізичний шлях сигналу від джерела передачі інформації до приймального пристрою зловмисника. Сам процес односторонній, і з його допомогою людина несанкціоновано отримує приховані відомості або особисту інформацію, яку можливо зафіксувати.

Технічні канали витоку інформації поділяються на контактні та безконтактні канали витоку інформації.

Контактні канали витоку інформації існують при прямому контакті злоумисника з каналом передачі.

Безконтактні каналу витоку інформації можливо здійснити при відсутності фізичного втручання у канали передачі інформації. Такими каналами можуть бути:

- бездротові мережі (Wi-Fi, Bluetooth, AirDrop та інші);
- програмні віруси, які встановлюються на персональних комп'ютерах;
- дистанційне прослуховування приміщень за допомогою направлених мікрофонів та інші.

2 ДОСЛІДЖЕННЯ ШЛЯХІВ ВИНИКНЕННЯ ВИТОКУ ІНФОРМАЦІЇ БЕЗКОНТАКТНИМИ МЕТОДАМИ

2.1 Спостереження за приміщенням за допомогою RF Capture

RF Capture - це технологія, яка за допомогою Wi-Fi пристрою дозволяє дистанційно відстежувати рухомі предмети і людей, які знаходяться за стіною і закритими дверима, а також оцінювати їх зріст і масу.

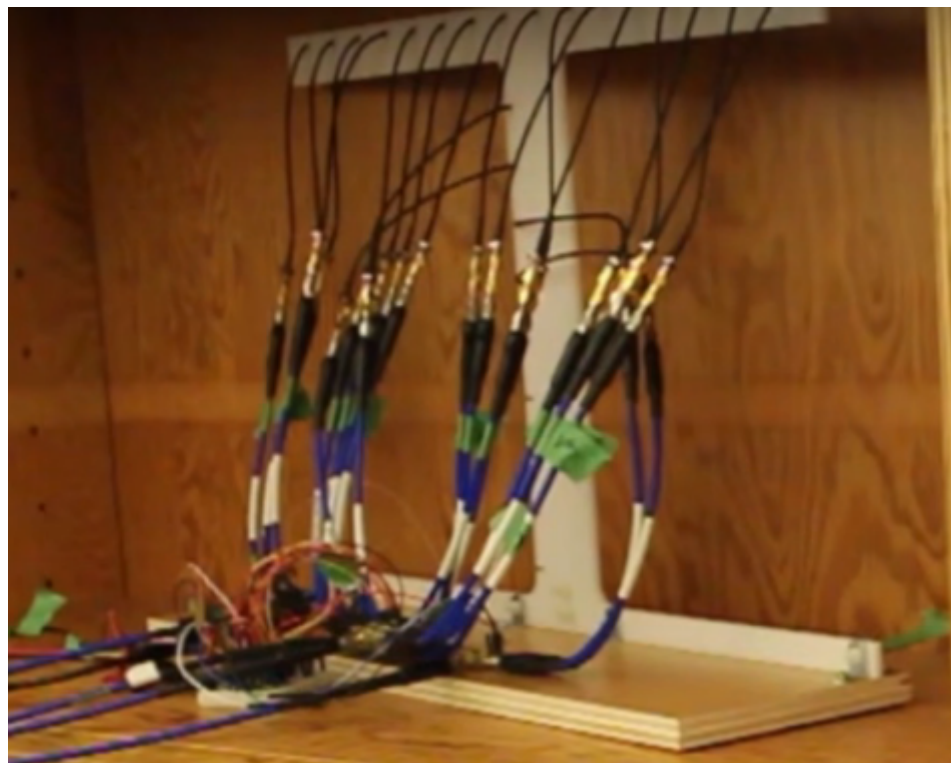


Рисунок 2.1 – Пристрій RF Capture

Відбитий радіосигнал, що надійшов в Wi-Fi-приймач, аналізується за допомогою особливого алгоритму. Це дозволяє зробити висновок, що та чи інша людина стоїть, сидить або рухається за стіною (по варіаціям в його силі і іншим параметрам) [3].

RF Capture по суті є MIMO-пристроєм з трьома спрямованими антенами: дві антени використовуються для передачі сигналу в протифазі і

одна використовується для прийому. Пристрій включає два основних компоненти [4]:

- перший компонент усуває засвічування (flash), яке відбивається від нерухомих предметів сигналу, виконуючи гасіння хвиль (MIMO nulling), що дозволяє після програмної фільтрації враховувати тільки ті радіохвилі, які відбилися від рухомих об'єктів;
- другий компонент відстежує об'єкт, що рухається, розглядаючи сам об'єкт як масив антен, використовуючи техніку зворотного радіолокаційного синтезування апертури.

RF Capture може бути використаний в одному з двох режимів, в залежності від вибору користувача. У режимі 1 він може бути використаний для відображення і відстеження рухомих об'єктів за стіною. У режимі 2, діє як інтерфейс передачі жестів через стіни.

Радіохвилі низькочастотного діапазону не дозволяють отримати на екрані деталізоване зображення, що сканує образ. Разом з тим, можливості програмних алгоритмів RF-Capture дозволяють виділити конкретну людину з декількох, які перебувають в тому ж приміщенні. Для цієї мети потрібно попереднє введення в базу даних ряду індивідуальних метричних характеристик, таких як зріст і контури тіла, що виконують роль своєрідного ідентифікатора. За результатами експерименту система RF-Capture дозволила з точністю до 95,7% ідентифікувати конкретну людину з 5-ти присутніх у тій же кімнаті і з точністю 88,2% при збільшенні їх числа до 15. На відстані "об'єкта" по ту сторону стіни в 3 м, рухомі фрагменти тіла розпізнаються з точністю 99,13%, на відстані в 8 м - з точністю 76,4%. [5]

Технологія працює досить просто – по-особливому модифікований передавач Wi-Fi "бомбардує" стіну. Частина породжених їм хвиль відбивається від людей і предметів, розташованих за стіною, і потрапляє назад, в розташований поруч приймача сигналу. Ці хвилі аналізуються за допомогою спеціального алгоритму, "натасканого" на розпізнавання силуетів, схожих за формою на тіло людини або окремі частини тіла [6].

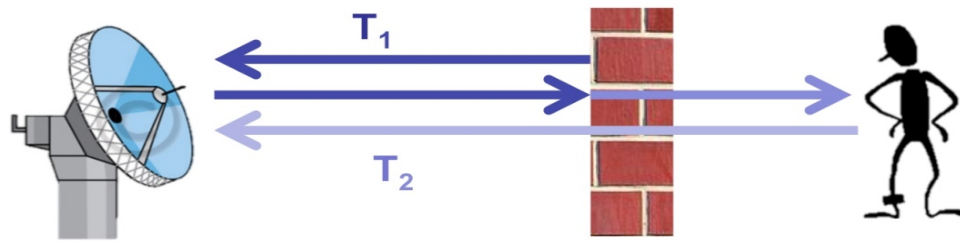


Рисунок 2.2 – Спосіб спостереження через стіну

Спостереження через стіну аналогічно принципу дії радара або гідролокатора. Сигнал проходить крізь неметалеві елементи стіни, відбивається від об'єктів і людей та повертається до приймача, несучи інформацію про те, що знаходиться за стіною.

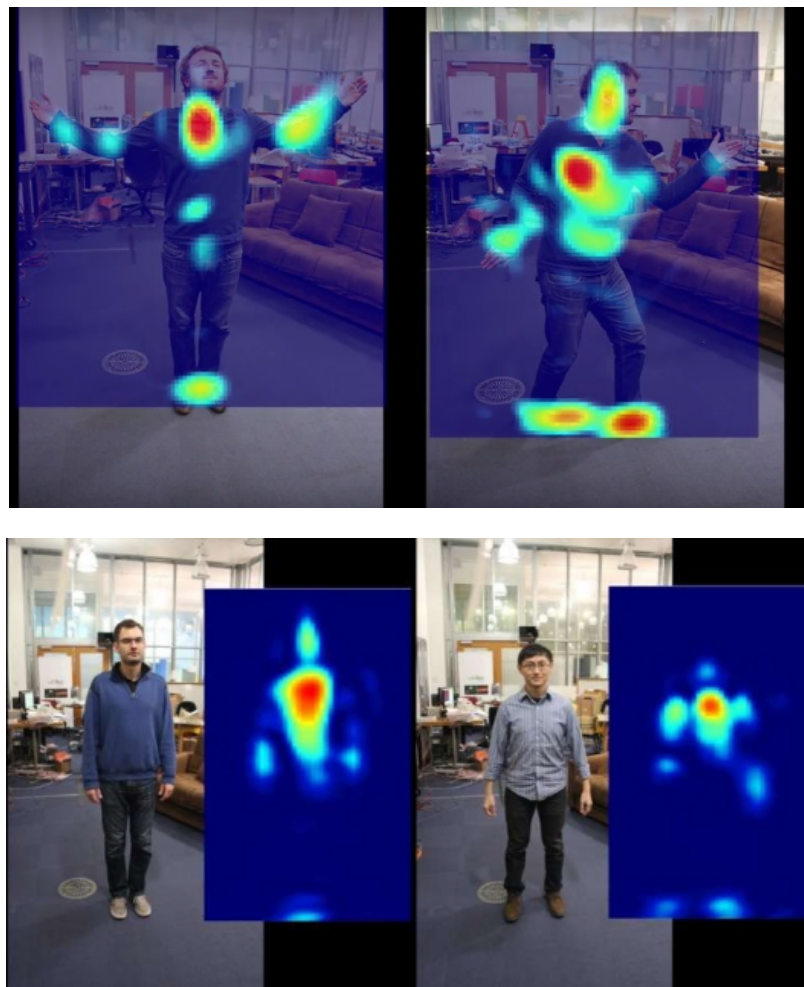


Рисунок 2.3 – Силуети людей, отриманих RF Capture

2.1.1 Метод усунення засвічування

Створення пристрою, який зможе відстежити рухомі об'єкти складне, тому що потужність сигналу після подвійного проходження стіни скорочується в три-п'ять разів. Ще більш складним завданням є обробка відображень сигналів від самої стіни, які набагато сильніше, ніж відображення від об'єктів за стіною. Обробка відбитих від стіни сигналів може зайняти аналогово-цифровий перетворювач, не дозволяючи йому обробляти сигнали, відбиті від об'єктів за стіною. Це явище називається ефект засвічування (flash effect). [7]

Для виключення ефекту засвічування технологія RF Capture посиляє сигнал через кілька антен, щоб відбиття від нерухомих об'єктів не надходили на приймач. Пристрій RF Capture має дві передавальні антени і одну приймаючу і працює в два етапи. На першому етапі пристрій вимірює сигнали від двох передавальних антен, що надходять на приймач. На другому етапі вимірювання сигналів від передавальних антен з першого етапу використовуються для обнулення сигналу. Так як бездротові сигнали (включаючи відображені) складаються лінійно, то тільки відбиті від об'єктів, що рухаються сигнали реєструються на другому етапі. Після цього у технології розвинули механізм обнулення шляхом введення ітераційного занулення, яке дозволяє усунути залишкове засвічування і слабкі відображення від нерухомих об'єктів за стіною [8].

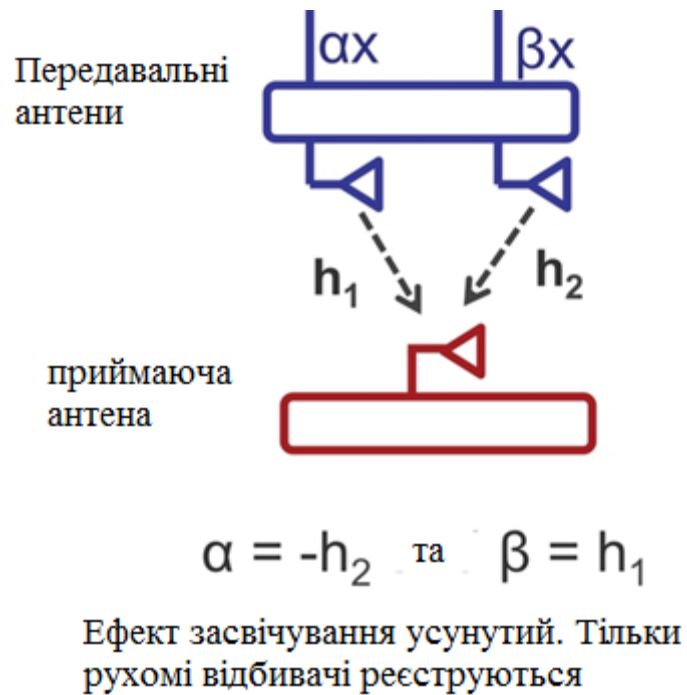


Рисунок 2.4 – Усунення ефекту засвічування

2.1.2 Аналіз параметрів, які відстежують рухи

RF Capture відстежує рухи об'єктів за допомогою техніки зворотного радіолокаційного синтезування апертури (ISAR). [9] Техніка працює наступним чином: коли об'єкт переміщується, він відображає сигнал з різних точок простору, що дозволяє думати про нього, як про рухому антену. Пристрій захоплює тимчасову послідовність значень відбитого сигналу і розглядає їх послідовність просторових міток. Використовуючи стандартну антену, RF Capture здатний визначити відносний кут руху людини по відношенню до пристрою [10].

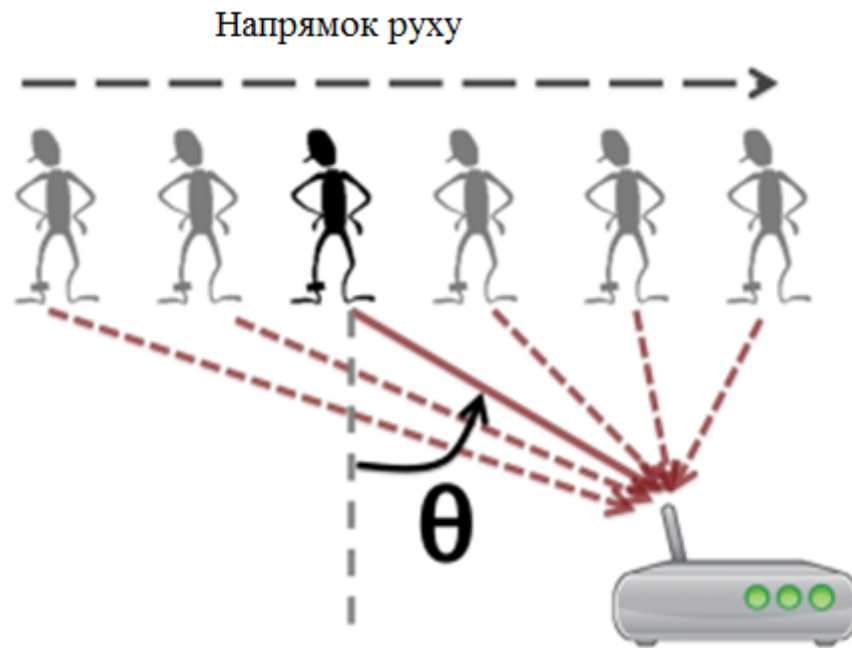


Рисунок 2.5 – Відстеження руху

Завдяки даній технології розширюється вибір засобів захищеного приміщення. Пристроєм Wi-Fi можливо поєднувати 2 функції: як доступ в інтернет, так і контроль за виділеним приміщенням і можливо своєчасно виявити проникнення людей на територію, що охороняється.

Такі системи можливо застосовувати в різних сферах. Перш за все – у військовій промисловості, щоб бачити супротивника крізь стіну. При проведенні рятувальних операцій, щоб знаходити людей в самих важкодоступних місцях. RF Capture використовуватимуть правоохоронні органи при спостереженні за злочинцями. З точки зору захисту інформації, цю технологію можливо поєднувати з діючими системами виявлення проникнення зломисників на контрольовану зону. Але зломисники можуть також використовувати цю технологію, для відстеження присутності і переміщення людей у контрольованій зоні. [11]

2.2 Перехват трафіку через програмне забезпечення Wifiphisher

Програма Wifiphisher працює у дистрибутиві Kali Linux і використовує набір програм Aircrack-ng, яка призначена для виявлення бездротових мереж, перехоплення переданого через бездротові мережі трафіку, а також аудиту WEP і WPA / WPA2-PSK ключів.

Дистрибутив Kali Linux розроблений для тестування безпеки, відновлення даних і виявлення атак. Однак, при певних умовах зловмисники можуть його використовувати для перехоплення Wi-Fi трафіку.

Для цієї мети був розроблений інструмент у вигляді програми Wifiphisher з відкритим вихідним кодом, яка може бути використана для автоматизації фішингових атак зі збору облікових даних користувачів. На відміну від інших методів злому Wi-Fi паролів, у даній програмі застосовується соціальна інженерія. Таким чином, можливо збирати різні секретні фрази, паролі та інше. [12]

Для реалізації атаки за допомогою Wifiphisher використовує три етапи:

Етап 1. Жертва повинна відключитися від активної Wi-Fi мережі. Для цього Wifiphisher постійно пригнічує всі пристрої, підключені до даного мережі доступу, розсилаючи пакети «deauth» (припинити аутентифікацію) клієнтам від точки доступу Wi-Fi і до точки доступу Wi-Fi від клієнта, а також по ширококомовним адресами.

На цьому етапі жертва втрачає можливість підключитися до Wi-Fi пристрою внаслідок постійного надходження пакету «deauth».

У налаштуваннях телефону Wi-Fi пристрою у момент сканування з'являється дві мережі з однаковою назвою. Підключитися до активної мережі у користувача не буде можливим, через наслідок постійної де-аутентифікації, тому користувач спробує підключитися до ворожої мережі з аналогічною назвою.

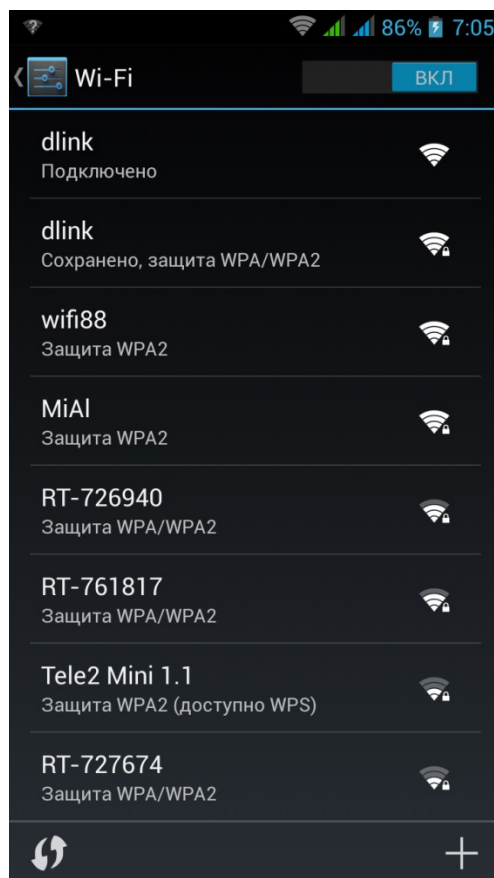


Рисунок 2.6 – Сканування Wi-Fi мереж із двома однаковими назвами, активної та ворожої Wi-Fi мережами

Етап 2. Жертва повинна підключитися до ворожої Wi-Fi мережі.

На цьому етапі Wifiphisher копіює настройки активної Wi-Fi точки доступу. Потім створюється ворожа Wi-Fi мережа, змодельована на прикладі справжньої. Також копіюється адреса сервера NAT / DHCP, який буде перенаправляти потрібні порти з нашого комп'ютера до створеної Wi-Fi мережі. В результаті, через постійне скидання з'єднання, клієнти починають підключатися до ворожої точки доступу Wi-Fi (але це відбувається не повністю автоматично: користувачеві потрібно підтвердити дію у налаштуваннях). Після цього, з'єднанні клієнти стають жертвою атаки MITM (атака «людина посередині»).

Етап 3. Далі жертві відправляється сторінка з налаштуваннями конфігурації маршрутизатора. Wifiphisher використовує мінімальний ресурс веб-сервера, який реагує на будь-які запити HTTP і HTTPS. Як тільки жертва

запитує сторінку з інтернету, Wifiphisher відправляє сторінку із запитом ввести облікові дані. Наприклад, можливо запросити ввести пароль WPA через налаштування програмного оновлення маршрутизатора.

Режими сценаріїв перехвату трафіку Wifiphisher представлені на рисунку 2.7.

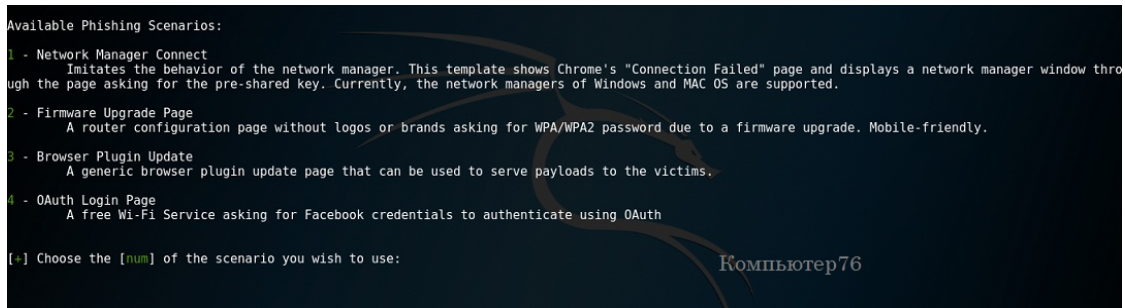


Рисунок 2.7 – Сценарії перехвату інформації через Wifiphisher

У першому сценарії імітується поведінка менеджера мережі. Цей шаблон показує сторінку «Не вдалося з'єднати» та відображає вікно керування мережею через сторінку, що вимагає ввести пароль до мережі.

У другому сценарії пропонується сторінка оновлення прошивки маршрутизатора. Wifiphisher при копіюванні налаштувань активної точки доступу ідентифікує виробника маршрутизатора. Тому користувач при будь-якому запиті у мережі інтернет надходить «справжня» сторінка з оновлення прошивки, де користувач бачить логотип та ліцензійні права скопійовані з офіційного сайту виробника маршрутизатора та необхідність погодитись з правами та ввести свій пароль від точки доступу. Користувач вважає цю сторінку справжньою і він вводить все як написано. Якщо він спробує закрити цю сторінку і зробити запит на інший інтернет ресурс, йому знову буде надісланий запит на введення паролю.

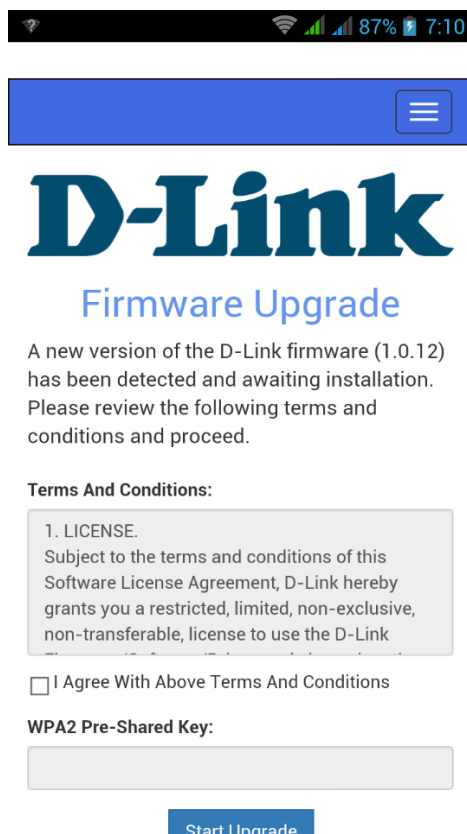


Рисунок 2.8 – Необхідність оновити налаштування у маршрутизаторі та ввести пароль від точки доступу

Третій сценарій передбачає оновленням будь-якого плагіна до браузеру, наприклад Adobe Flash Player. Насправді жертві підсувається шкідливий виконавчий файл - ідеальний варіант розміщення на комп'ютері жертви троянського коня.

І четвертий сценарій, коли жертва бачить на екрані сторінку аутентифікації від Facebook з проханням підтвердити логін і пароль для безкоштовного використання цієї точкою доступу. Після введення, пишеться помилка і що неправильно введена інформація, а зломисник перехоплює введену інформацію.

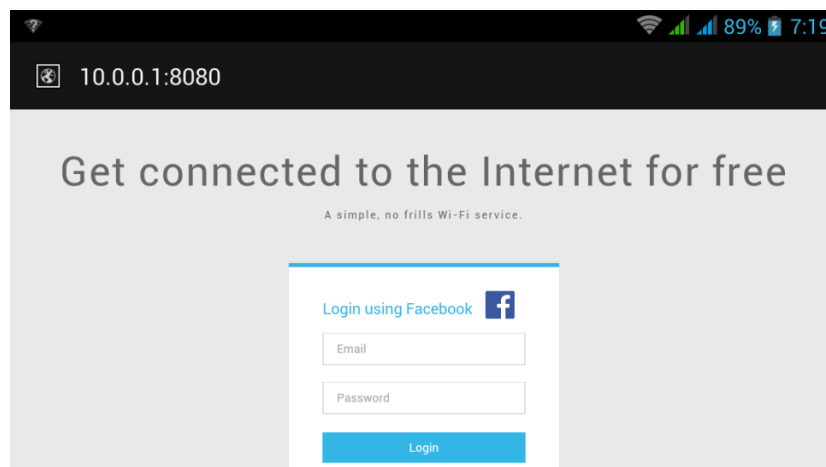


Рисунок 2.9 – Фішингова сторінка аутентифікації Facebook

Це стандартні сценарії, які пропонуються. Сценарії атаки можливо і самотійно задати в налаштуваннях програмного забезпечення Wifiphisher.

На цьому етапі можливо не тільки запросити користувача ввести пароль від Wi-Fi мережі, а можливо і «імітувати» роботу інтернету, і всі дії у мережі будуть проходити через зловмисника і таким чином можливо отримати практично будь-яку інформацію про користувача, а саме пароль від Wi-Fi, дані про банківську картку, особисту інформацію та будь-яку іншу інформацію.

Завдяки даній програмі можливо здійснити атаку на будь-яку Wi-Fi мережу, тому при приведених вище випадках, необхідно не підключатись до ворожої мережі, а шукати зловмисника.

2.3 Програми майнінгу

Майнінг – це діяльність по створенню нових структур для забезпечення функціонування криптовалютних платформ. Для видобутку криптовалюти можливо не тільки використання власного комп'ютера, але і безлічі чужих машин. Наприклад, у магазині Google Play знайшли додаток під назвою Vilny.net, що працює як VPN-сервіс, проте в той же час використовує ресурси смартфонів, щоб майніти криптовалюту Monero [13].

Програми прихованого майнінгу поширені і в модифікаціях встановлення операційної системи Windows. Після встановлення виконується скрипт, який протидіє будь-яким процесам захисту від шкідливих програм. Також програма майнінгу володіє механізмом самознищення. Якщо програма аналізатор сканує даний каталог, вона видаляє кожен файл під встановленим каталогом і знищує сліди перебування програми майнінгу. [14]

На сьогоднішній день прихований майнінг може зробити будь-який користувач. Для цього досить лише завантажити готову програму, написати номер свого електронного гаманця і все. Програма модифікована так, що вона не відрізняється від троянського вірусу: вона може поширюватися в мережі, копіювати сама себе на зовнішній накопичувач, приховувати свої процеси в диспетчері завдань і використовувати комп'ютер коли ним ніхто не користується. [15]

На сьогоднішній день скриті майнінги роблять двох типів: майнери з малим навантаженням на ЦП та майнери з великим навантаженням на ЦП. Різниця в них полягає у навантаженні на ЦП та відео карту. Програми майнери на сьогодні працюють наступним чином:

- якщо користувач на даний момент не користується комп'ютером більше 5 хвилин, то навантаження майнера може сягати 100 відсотків від усієї потужності комп'ютера;
- якщо користувач на даний момент не користується комп'ютером менше 5 хвилин, то навантаження майнера може сягати 50 відсотків від усієї потужності комп'ютера;
- якщо користувач на даний момент користується комп'ютером, то навантаження майнера може сягати до 25 відсотків від усієї потужності комп'ютера.

Таке навантаження не дає можливість простому користувачу запідозрити, що з його системою щось не ладне.

Для прихованого видобутку криптовалюти не потрібно зламувати комп'ютер і встановлювати троян. Поки у користувача в браузері відкрита сторінка з шкідливим скриптом, процесор буде непомітно майніти. [16]

Ви можете і не помітити великої різниці, якщо у вас досить потужна техніка. Це важлива умова для збереження прихованої роботи майнера.

Ці програми необхідно знищувати, тому що розробники програм майнінгу можуть модифікувати її за певну суму, та можливо здійснювати знімання інформації про всі дії користувача. При видаленні необхідно перевірити, що дана програма була видалена повністю, тому що вона може після видалення і перевантаження комп'ютеру, заново завантажитись і знову працювати.

2.4 Програма прихованого віддаленого доступу RMS

RMS - це програма для віддаленого доступу комп'ютером, схожа на RAT. У прихованій версії RMS на відміну від ліцензійної версії, прихована версія не відображає, що до комп'ютера хтось підключений, прибрані всі банери і ознаки наявності програми RMS.

Для початку необхідно створити файл Regedit (файл реєстру), який буде використовуватися для автозавантаження і відправки ID комп'ютера на пошту, в цьому випадку нам допоможе програма TheGenSet.

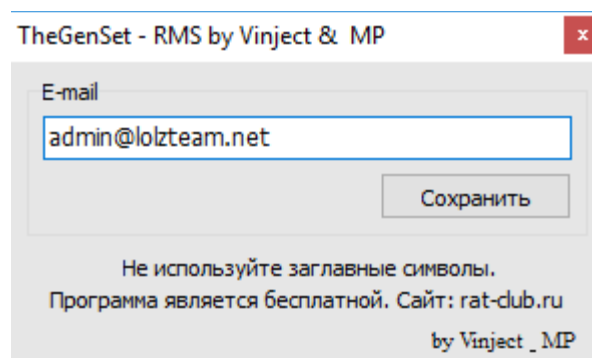


Рисунок 2.10 – Інтерфейс програми TheGenSet

У текстове поле необхідно ввести свій E-mail, також потрібно пам'ятати, що введена електронна адреса може бути розкрита і жертва зможе побачити електронну адресу творця шкідливої програми. Після введення електронної адреси необхідно натиснути на кнопку зберегти, файл regedit збережеться в папку C:\set. Його треба перемістити в папку RMS, де знаходяться модифіковані файли RMS.

Далі необхідно вибрати файли з папки, де знаходиться модифіковані файли та створити архів. Під час створення, необхідно обрати «Створити SFX-архів» та «Створити неперервний архів», як зображено на рисунку 2.4.2. Також необхідно вибрати вкладку «Додатково» і обираємо де саме буде встановлено шкідливу програму, наприклад «C:\Program Files (x86)\Windows Media Player».

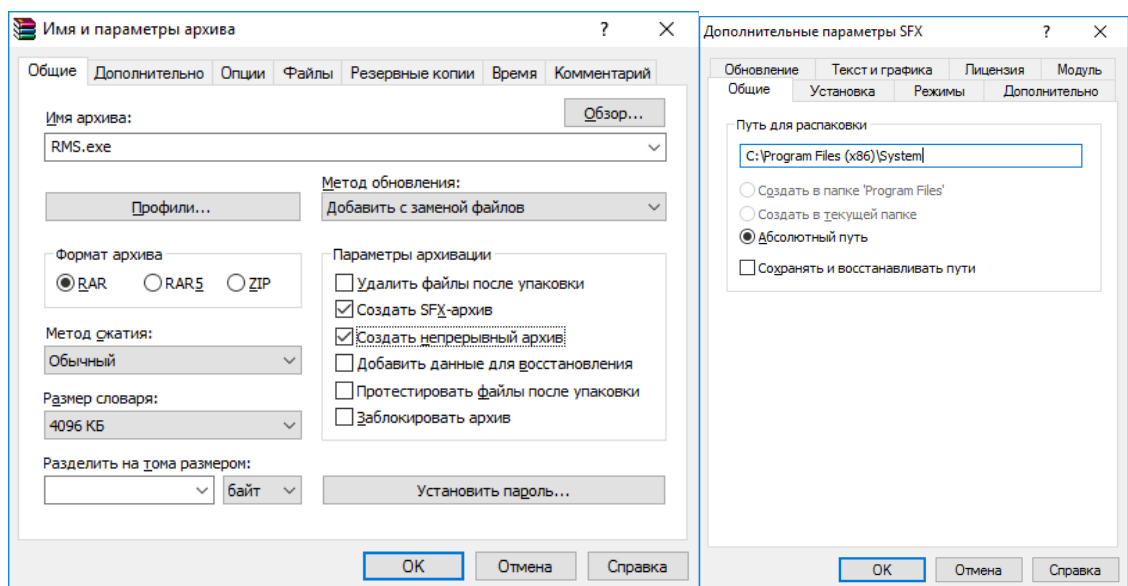


Рисунок 2.11 – Налаштування з створення шкідливої програми RMS

Для того щоб жертва не побачила встановлення програми, необхідно у вкладці "Установка", виконати після розпакування «install.vbs», у вкладці "Режими" обрати «приховати все», у вкладці "Оновлення" в розділі "Режим оновлення" обрати «витягти і оновити файли» в розділі "Режим перезапису" обрати «Переписувати всі файли без запиту».

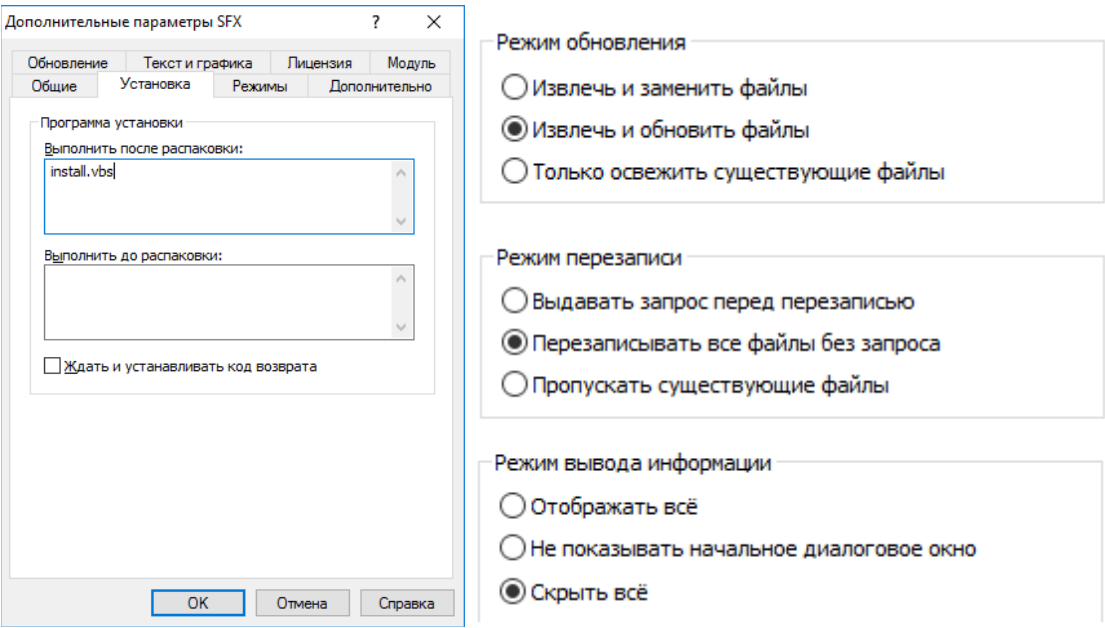


Рисунок 2.12 – Налаштування запуску шкідливої програми RMS

Далі необхідно відіслати цей файл жертві і переконати її запуснути шкідливий файл. Через декілька хвилин на пошту надійте лист, з ID комп'ютера та паролем для входу. З цього моменту можливо здійснювати повний контроль над жертвою.

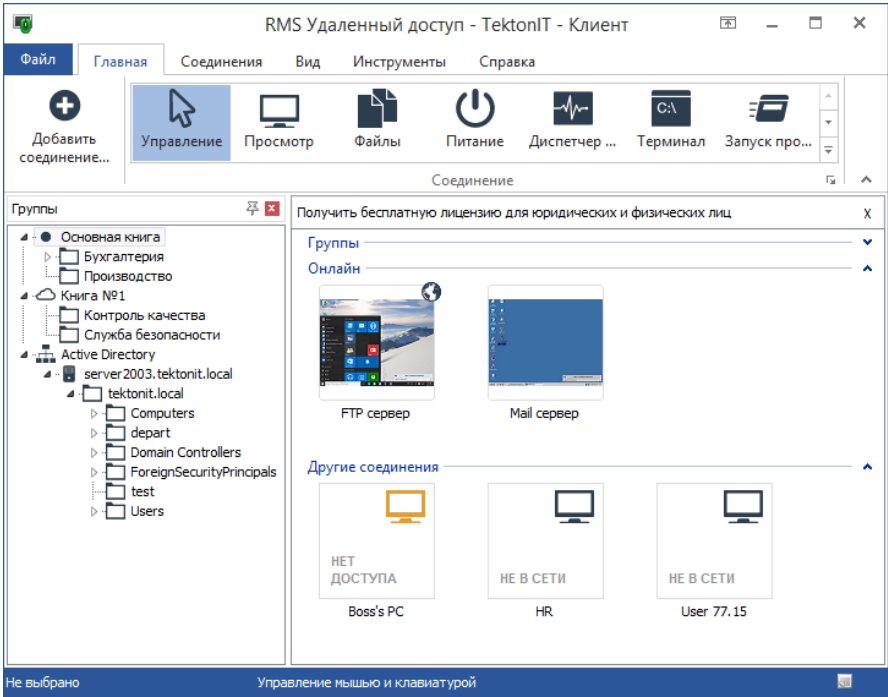


Рисунок 2.13 – Інтерфейс програми RMS

Дана програма має свої особливості, що антивірусні програми та аналізатори не розпізнають її як шкідливу. Лише після аналізу цієї програми експертами антивірусних компаній, цю програму антивіруси визнають як шкідливу програму. Ніщо не заважає створити цю програму творцю знову і антивіруси знову не зможуть ідентифікувати її як шкідливу. Якщо програма вже була встановлена на комп'ютер жертви, її антивірус не зможе вимкнути, тому що програма виконується системою з найвищими правами.

Тому необхідно перед завантажувати програмні забезпечення тільки з офіційних джерел. Це дає хоча б якусь гарантію того, що програма, яку встановлюють, не модифікована додатковими програмами віддаленого доступу.

3 РЕКОМЕНДАЦІЇ ЩОДО УДОСКОНАЛЕННЯ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

3.1 Оптимізація розповсюдження радіохвиль у режимній зоні

Перед визначенням режимної зони слід визначити зону дії бездротової мережі. Усі бездротові мережі досить сильно піддаються впливу перешкод, а на шляху поширення бездротового сигналу можуть зустрічатися стіни та інші об'єкти, і після чергового такої перешкоди електромагнітна хвиля може посилювати свій сигнал або навпаки послаблювати сигнал. На сьогоднішній день цифрові технології дають можливість візуалізувати все що завгодно, і навіть те, як поширюються невидимі людському оку сигнали Wi-Fi-діапазону.



Рисунок 3.1 – Розповсюдження радіохвиль у середині будівлі

Рисунок вище зроблений в програмі Acrylic Wi-Fi (для ОС Windows), що дозволяє будувати теплові карти з використанням даних з Google Map, але і для мобільних пристроїв існують не менш ефективні програмні продукти. Більшість інструментів для аналізу Wi-Fi покриття на базі операційної системи Windows пропонують велику кількість функціональних можливостей.

Коли є інструмент, що дозволяє візуально показати рівень сигналу відразу на карті місцевості, це набагато полегшує сприйняття картини мережі в цілому. Такі інструменти дозволяють відразу завантажувати план будівлі, а пройшовшись по ньому з включеним Wi-Fi приймачем можливо отримати теплові карти радіо покриття:

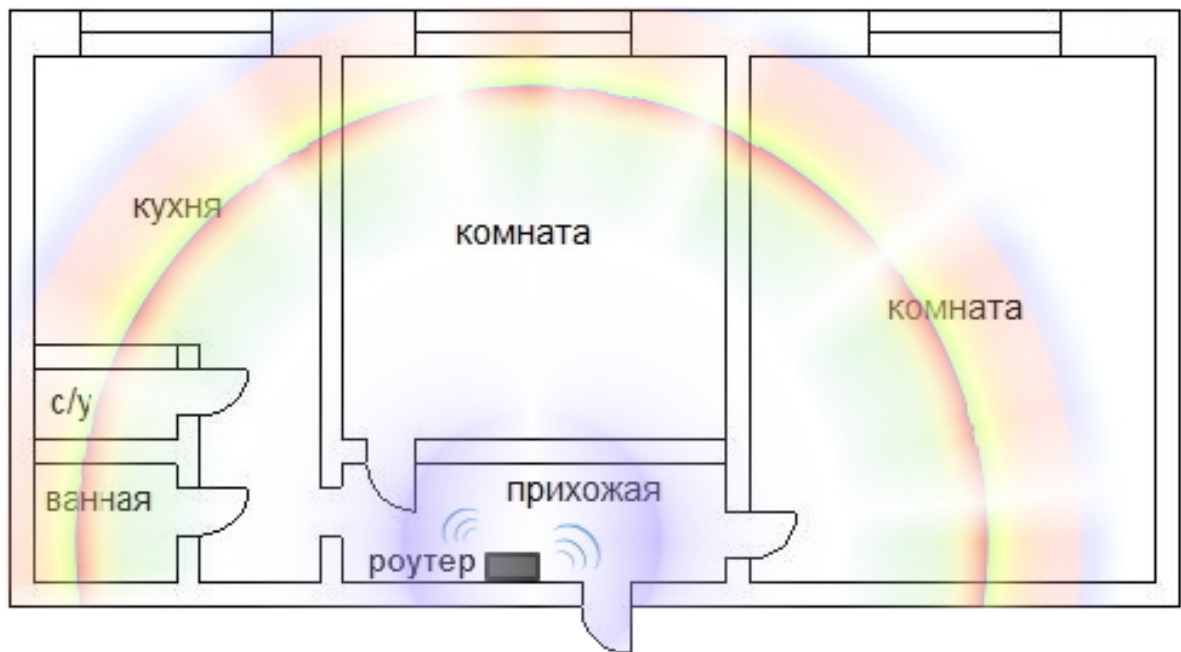


Рисунок 3.2 – Карта поширення радіохвиль у приміщенні

На розповсюдження радіохвиль впливають наступні властивості Wi-Fi сигналу:

- поглинання (кожна стіна або перекриття "відбирає" у сигналу деяку кількість ефективності);
- довжина хвилі (з теоретичної точки зору, чим більше довжина хвилі, тим більше проникаюча здатність сигналу. Відповідно, Wi-Fi в діапазоні 2,4 ГГц має велику проникаючу здатність, ніж в діапазоні 5 ГГц. В реальних умовах виконання цього правила дуже тісно залежить від того, через перешкоду якої структури і складу проходить сигнал. Також, якщо у приміщенні присутні додаткові металеві конструкції, це додатково

ускладнює поширення радіохвиль від джерела випромінення і до кордону поширення контрольованої зони).

Таблиця 3.1 – Розповсюдження радіохвиль через перешкоди

Перешкода	Додаткові втрати при проходженні (dB)	Відсоток ефективного відстані *, %
Відкритий простір	0	100
Нетонізоване вікно (відсутній металізоване покриття)	3	70
Вікно з металізованим покриттям (тонуванням)	5-8	50
Дерев'яна стіна	10	30
Стіна 15,2 см (міжкімнатна)	15-20	15
Стіна 30,5 см (несуща)	20-25	10
Бетонна підлога або стеля	15-25	10-15
Цільне залізобетонне перекриття	20-25	10

Для того щоб здійснити затухання радіохвиль на межі контрольованої зони у стіни потрібно вбудувати цільне залізобетонне перекриття з металевою решіткою. А в місцях, де немає стін потрібно застосовувати Wi-Fi глушилки, наприклад Wi-Fi Jammer.

Wi-Fi Jammer – це гаджет, який призначений для відключення бездротових пристроїв від бездротової мережі.

На відміну від справжніх глушилок, які перебивають сигнал радіопередавача своїм сильнішим сигналом, деаутентифікатор працює на програмному рівні. Він реалізує атаку типу «відмова в обслуговуванні», відправляючи на роутер фрейм деаутентифікації від імені підключених до

мережі пристроїв. Оскільки цей фрейм ніяк не шифрується, глушилки досить дізнатися MAC-адреси пристроїв, проаналізував трафік в мережі.

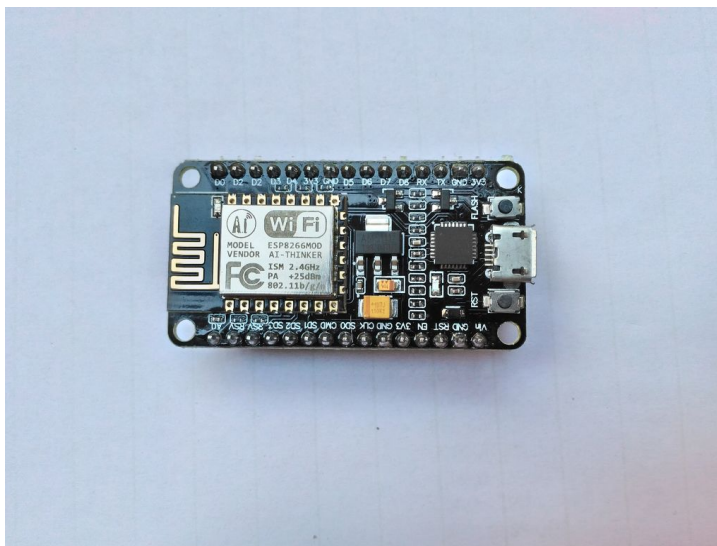


Рисунок 3.3 – Wi-Fi глушилка

Але варто пам'ятати, що відповідно до ст. 361 закону України заборонено використання технічних засобів для глушіння мобільного зв'язку або бездротових мереж.

3.2 Моніторинг систем безпеки у бездротових мережах

Практика показує, що більшість користувачів забувають про захист своєї домашньої мережі відразу після встановлення пароля для бездротової мережі Wi-Fi. Однак, варто пам'ятати, що це далеко не все, що необхідно зробити, щоб ваша бездротова мережа була дійсно безпечною і виключити можливість несанкціонованого доступу.

Недавні дослідження промислової групи "Wi-Fi Alliance" показали, що одна третина від опитаних користувачів бездротових мереж хоча б раз в житті намагалися отримати доступ до чужої бездротової мережі. А зростання частки користувачів смартфонів, які оснащені останніми модулями бездротового зв'язку і простота злому Wi-Fi мережі може тільки погіршити ситуацію.

Тому необхідно використовувати наступне:

- необхідно використовувати тільки WPA2 шифрування (більшість побутових маршрутизаторів цей режим підтримують, проте старі маршрутизатори працюють тільки з WEP алгоритмом, а він набагато більш вразливий. Також, тут варто пам'ятати, що потрібно застосовувати складні паролі. Вони не повинні бути осмисленими словами або словосполученнями, інакше їх легко можливо зламати методом перебору по словнику);
- налаштуйте доступ за MAC адресами (якщо до вашої Wi-Fi підключається тільки обмежене число пристроїв, наприклад, декілька ноутбуків і кілька смартфонів або планшетів, розумніше буде дізнатися їх MAC адреси, і дозволити доступ тільки їм. Цей метод незручний, так як для того, щоб підключити до мережі новий пристрій, необхідно входити у налаштування маршрутизатора та додавати його у білий список роутера. Безумовно, це не дасть 100% захисту від злому, але завдасть незручності зловмиснику);
- зробити вашу бездротову мережу скритою (це ускладнює підключення до цієї мережі, тому що користувачу необхідно ввести крім паролю ще й назву мережі).

Але усі ці методи не дають жодної гарантії захисту бездротової мережі від Wifiphisher. При атаці, потрібно за допомогою програмного аналізатора рівня сигналу Wi-Fi мережі, наприклад «Wi-Fi Analyzer», знайти зловмисника та затримати його до прибуття групи швидкого реагування. Але в жодному разі не потрібно підключатися до створеної мережі, тому що це може призвести до фатальних наслідків.

3.3 Удосконалений комплекс заходів з забезпечення безпеки комп'ютера від безконтактних методів проникнення

Комплекс заходів безпеки комп'ютера повинен здійснювати захист системи постійно. Він повинен у себе включати:

- програми з оптимізації роботи комп'ютера;
- програми, які показують активні процеси у системі;
- програмні та апаратні брандмауери;
- антивірусні програмні забезпечення.

3.3.1 Програми оптимізації роботи комп'ютера

Через деякий час навіть найпотужніші комп'ютери починають повільно працювати. Це відбувається через переповнення оперативної і постійної пам'яті, через помилки в реєстрі, через програми майнінгу та інших шкідливих програм. Тому необхідно проводити аналіз комп'ютера на помилки. Програма CCleaner здійснює аналіз реєстру на помилки, видаляє невикористовуванні файли та відображає зміни в списку автозавантаження. Шкідливі програми у більшості випадків здійснюють запуск своєї програми через додавання її до списку автозавантаження.

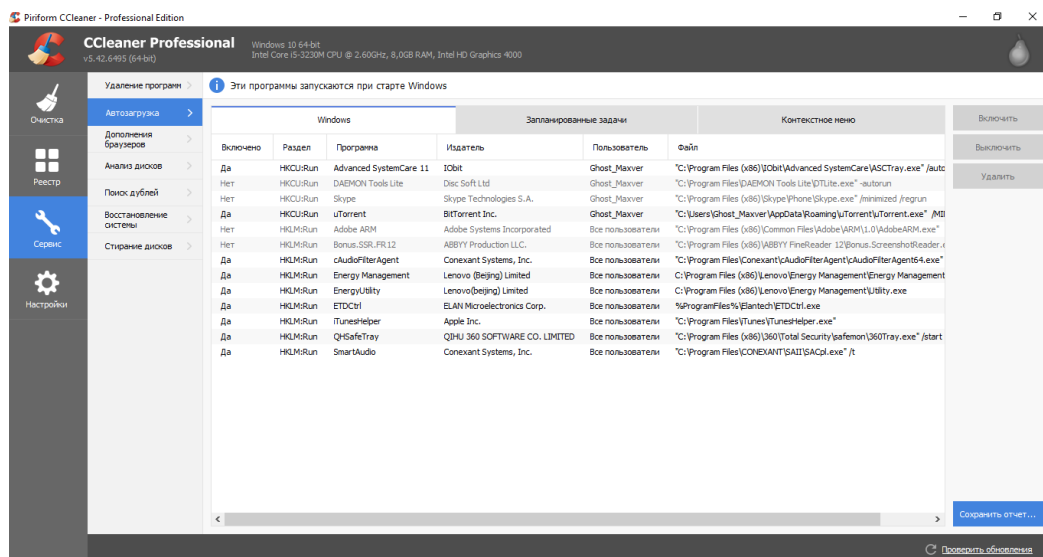


Рисунок 3.4 – Список програм автозавантаження при запуску Windows

Якщо ви виявили підозрілу програму у цьому списку, необхідно знайти де встановлена ця програма. Потрібно провести аналіз, що саме виконує ця програма і чи користується цією програмою користувач. Цю програму також необхідно перевірити антивірусною програмою. Ця програма також може маскуватися під системний ресурс, тому слід перевірити назву підозрілого процесу та місця де встановлена ця програма і місця де встановлена ця системна програма.

Якщо ви виявили, що ця програма призводить до уповільнення роботи комп'ютера, спробуйте вимкнути тимчасово доступ до інтернету. Якщо навантаження на комп'ютер зникло, це може означати, що ця програма працює з мережею інтернет. Це означає, що шкідлива програма слідкує за діями користувача, передає чи збирає інформацію або майнить криптовалюту. Цю програму слід перед видаленням зупинити у диспетчері завдань. Після цього видалити усі файли з місця, де встановлена ця програма, а також видалити її з списку автозавантаження.

3.3.2 Диспетчер завдань Process Hacker

Для захисту комп'ютера від шкідливих програм необхідно використовувати постійний аналіз за роботою комп'ютера. Для цієї мети необхідно використовувати програми, які аналізують активні процеси у системі. Програма Process Hacker дозволяє це програма, яка допомагає користувачу переглядати та здійснювати контроль за процесами та їх потоками, модулями і пам'яттю їх комп'ютерів.

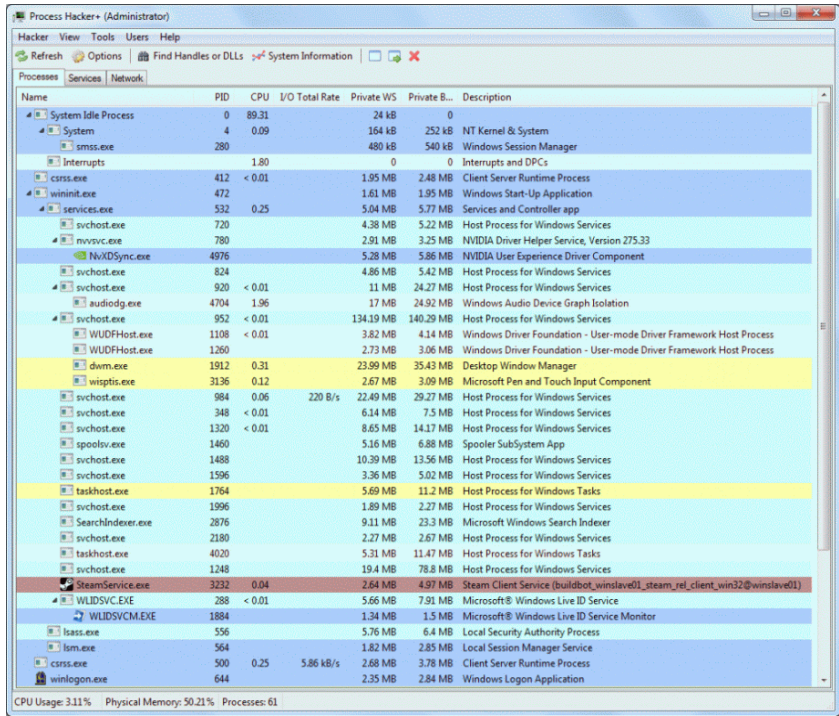


Рисунок 3.5 – Сканування активних процесів у системі

Програма здійснює вибірку процесів на кольори. Це дає можливість користувачу одразу привертати увагу на підозрілі процеси.

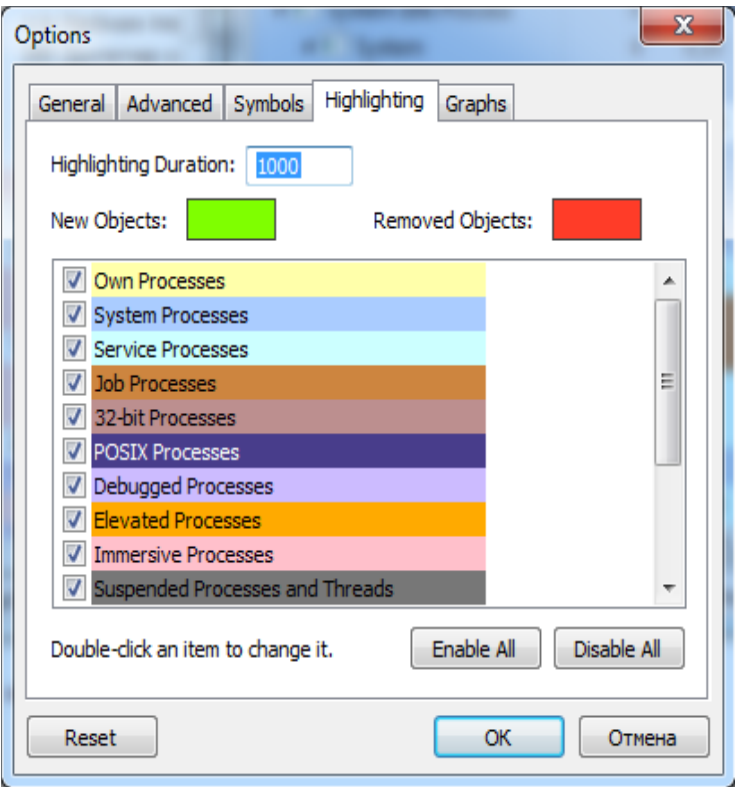


Рисунок 3.6 – Відображення процесів у системі до певних категорій

Підозрілі процеси відображаються фіолетовим та червоним кольором. Програма дозволяє показувати ієрархію запуску цього процесу. Також якщо цей процес після запуску програми, швидко закривається, необхідно відстежити «батьків» цього процесу. Це дає можливість проаналізувати кожен процес, який запускає підозрілий процес.

За ієрархією процесів, які запускають підозрілий процес, необхідно проаналізувати кожен процес за місцем, де він здійснює свій запуск. Якщо це шкідливий процес, його необхідно видалити.

Перед вимкненням процесу, потрібно зайти у директорію, де встановлена програма, вимкнути процес, далі видалити усі файли з директорії. Після видалення, бажано, запустити програму оптимізації системи та провести сканування реєстру на помилки і видалити їх.

3.3.3 Програмні та апаратні брандмауери

Насамперед необхідно визначити, що таке програмний та апаратний брандмауер. Апаратний брандмауер – це пристрій виконаний окремим корпусом, у середині якого є свій окремий комп'ютер та операційна система, який підключається до мережі. Програмний брандмауер – це набір рішень, реалізований програмним продуктом.

Як правило, програмний брандмауер встановлюється на кожен комп'ютер, який входить у внутрішню мережу, а апаратний брандмауер забезпечує захист не окремого комп'ютера, а всієї мережі відразу.

Недоліком апаратних брандмауерів є те що, як правило, у всіх цих пристроїв є кнопка скидання, натиснувши яку можливо повернути параметри за замовчуванням. Для натискання цієї кнопки не потрібно володіти якоюсь особливою кваліфікацією. А ось, щоб змінити параметри програмного брандмауера, потрібно, як мінімум, отримати права адміністратора. Натиснувши одну кнопку, незадоволений співробітник може негативно

вплинути на безпечність всього підприємства. Тому при використанні апаратних рішень потрібно, пам'ятати про це. [17]

Щоб перевірити брандмауер на захищеність існують різноманітні тести на захищеність. Головне завдання брандмауеру – це здійснення захисту системи від зовнішніх загроз. Для цього необхідно бути впевненим, що усі відкриті порти у системі закриті. Для перевірки брандмауерів на захищеність застосовують сканування зовні за допомогою програми Zenmap.

Брандмауер Comodo Firewall – це програмний брандмауер, який дозволить зберегти комп'ютер від віддаленого доступу, майнінгу та інших загроз. Перед тестування необхідно його налаштувати. Для цього необхідно увійти у налаштування і перейти до розширених налаштувань і обрати «COMODO - Proactive Security». Також необхідно:

- увімкнути фільтрацію IPv6-трафіку;
- увімкнути фільтрацію loopback-трафіку (наприклад, 127.x.x.x, :: 1);
- блокувати фрагментований IP трафік;
- включити захист від ARP-спуфинга.

Після цих налаштувань, скануємо комп'ютер з зовні і отримуємо наступні результати:

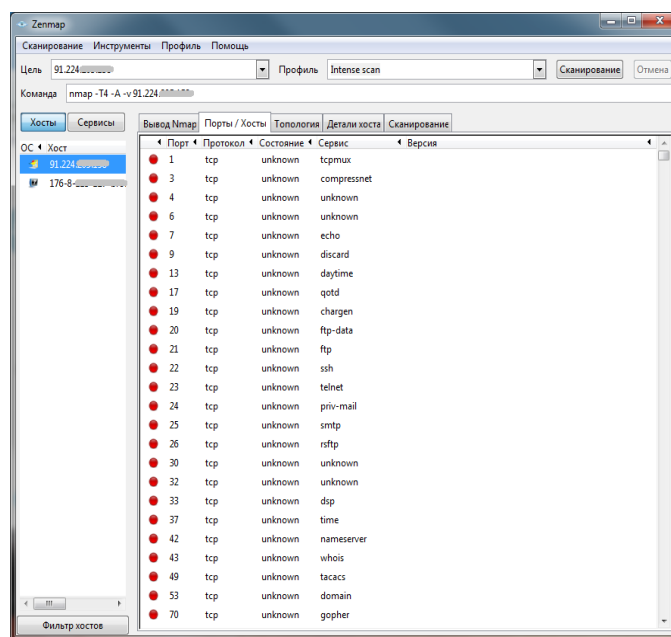


Рисунок 3.7 – Відкриті порти відсутні

Таким чином, комп'ютер був захищений від зовнішніх загроз та при спробі відкрити будь-який порт користувачу з правами адміністратора буде надіслано запит на відкриття порту. Якщо користувач з правами адміністратора дає доступ на відкриття, програма записує у свій журнал ці записи і цього запиту в подальшому не буде. Звичайному користувачу буде надіслано запит, що його спроба зробити це була відхилена.

3.3.4 Антивірусні програмні забезпечення

З поняттям «комп'ютерний вірус» знайомі всі власники комп'ютерів. Вірус – це шкідлива програма, мета якої – завдати якомога більшої шкоди комп'ютеру користувача або викрасти його особисті дані.

З усіх шкідливих програм найбільш відомі трояни. Зазвичай трояни маскують під відомі програми, щоб користувач запустив вірус, нічого не підозрюючи. У результаті троян завдає величезної шкоди комп'ютеру, наприклад, якщо у його функціях є майнити криптовалюту, а після виявлення її як трояну і спроби видалити, деякі види таких програм здатні повністю видаляти особисті файли користувача, без можливості відновлення. Також під видом троянів можливе розповсюдження шкідливої програми віддаленого доступу, наприклад RMS.

Основне завдання антивірусів – пошук і видалення вірусів, а також запобігання їх проникненню на комп'ютер користувача. Крім цього, антивіруси здатні сканувати інтернет сайти на наявність шкідливих програм, а також блокувати спливаючі рекламні оголошення.

Часто шкідливі програми пошкоджують різні знімні носії. Антивірусних програм дійсно дуже багато, але користувачі так і не визначилися з кращою, оскільки у кожної програми є як переваги, так і недоліки. Наприклад, деякі антивіруси недостатньо добре справляються з вірусами, інші коштують дуже дорого. Тому вибирати антивірус необхідно, вивчивши всі пропозиції на ринку. Кожен користувач вибирає найбільш

зручну для себе програму. Є певні критерії, за якими необхідно вибирати антивірус.

Критерії антивірусних програм:

- антивірус повинен перевіряти всі файли користувача на наявність шкідливих програм (також він повинен перевіряти файли, які завантажують користувач, щоб вірус не потрапив на ПК);
- функція самозахисту (справа в тому, що досить багато вірусів просто блокують роботу антивірусу, тому дуже важливо, щоб він міг сам себе захистити від атак);
- оновлення баз даних вірусів (антивірусна база - це список відомих шкідливих програм, а з огляду на те, що нові віруси з'являються майже кожен день, антивірус повинен знати про них, щоб успішно з ними боротися);
- скільки ресурсів споживає антивірус (деякі програми недостатньо оптимізовані, тому сильно навантажують систему, через що і не користуються особливою популярністю у користувачів, навіть незважаючи на їх здатності боротися з вірусами);

Антивірус 360 Total Security – комплексний антивірусний захист з 5 антивірусними модулями:

- Bitdefender;
- Avira;
- QVMII;
- хмарний двигун 360 Cloud;
- відновлює двигун System Repair.

Після встановлення даного антивірусу необхідно включити модуль Bitdefender та Avira. Для цього необхідно увійти у налаштування і включити наступне:

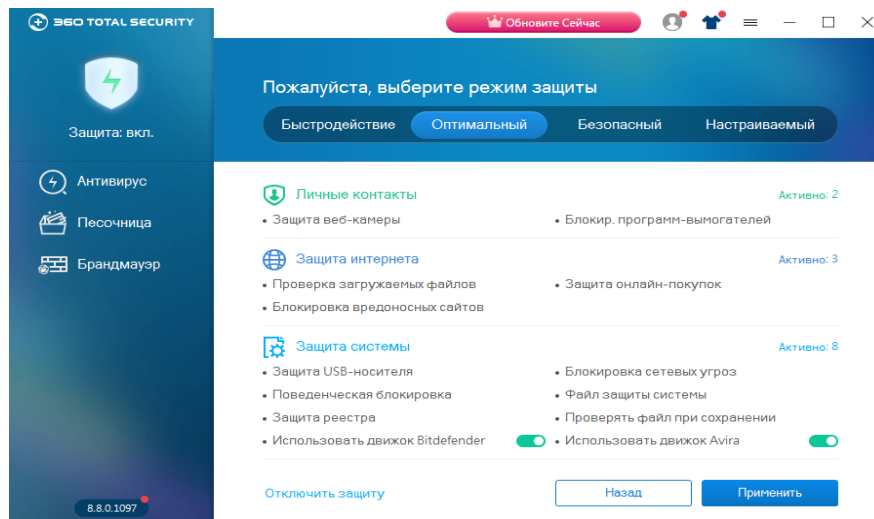


Рисунок 3.8 – Налаштування антивірусу 360 Total Security

Таким чином, якщо використовувати усі програмні забезпечення у комплексі, а також проводити постійний моніторинг за системою – комп'ютерна мережа буде максимально захищена від шкідливих програм.

4 ЕКОНОМІЧНІ РОЗРАХУНКИ

4.1 Важливість інформаційної безпеки для підприємств

Вибухове зростання кількості даних і інформації, що зберігаються в цифровій формі, не послаблюється. За оцінками багатьох аналітиків щодня в світі створюється понад мільярди файлів. У міру зростання обсягів даних, з якими оперують користувачі інформаційних систем, зростають труднощі успішного ведення бізнесу. Однією з найважливіших завдань для успішного функціонування підприємства є забезпечення збереження даних в мережі.

З даними може статися багато неприємностей, такі як віруси, збої устаткування або природні катастрофи. Саме через вихід з ладу систем зберігання інформації відбуваються простої серверів корпоративних мереж. А робота сервера мережі підприємства в режимі очікування може принести великий збиток компанії. Тому в разі надзвичайної ситуації, при якій дані можуть бути загублені, необхідно мати можливості їх швидкого відновлення.

Діяльність будь-якої комерційної організації спрямована в першу чергу на отримання прибутку. На досягненні цієї основної мети сфокусовані основні бізнес-процеси організації (наприклад, виробництво, продаж, логістика). Також існує ряд підтримуючих процесів, до яких відносяться, в тому числі, інформаційні технології та інформаційна безпека (ІБ), спрямовані на забезпечення інфраструктури для функціонування основних процесів. Керівництво практично будь-якої організації зацікавлене в тому, щоб процеси всередині організації були підконтрольні, функціонували так, як були задумані, а кількість помилок або зловмисних дій з боку співробітників, бізнес-партнерів, а також інших сторін, залучених в бізнес-процеси, було мінімальним.

Тобто, повинен ініціювати процес, спрямований на отримання достатнього ступеня впевненості в досягненні операційних цілей,

достовірності фінансової і управлінської звітності, а також відповідності вимогам законодавства, тобто процес внутрішнього контролю.

Роль, яку відіграють заходи і засоби інформаційної безпеки в процесі внутрішнього контролю, не потрібно недооцінювати. Такі аспекти, як розмежування повноважень в інформаційних системах у відповідності з посадовими обов'язками користувачів цих систем, функціональність, що не дозволяє здійснювати певні транзакції (наприклад, перевищують певний ліміт) без затвердження відповідальних осіб, перевірка цілісності даних при передачі між системами та інші подібні засоби контролю, мають пряме відношення до інформаційної безпеки, оскільки безпосередньо впливають на забезпечення конфіденційності, цілісності та доступності даних в рамках бізнес-процесів компанії.

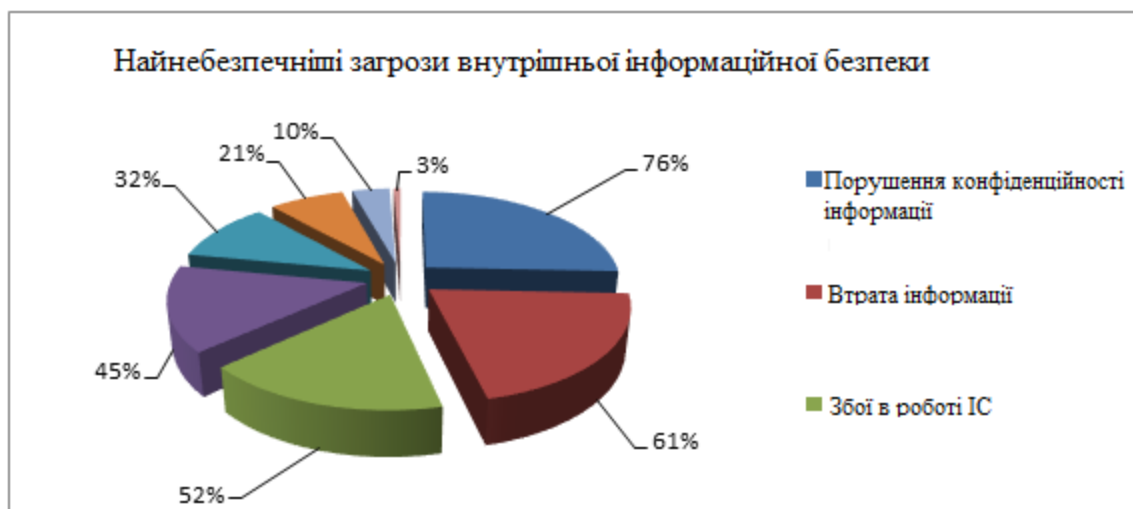


Рисунок 4.1 – Найнебезпечніші внутрішні інформаційні загрози

На рисунку 4.1 зображені найнебезпечніші внутрішні інформаційні загрози, які можуть виникнути на підприємстві. Досліджені в дипломній роботі методи захисту запобігають інформаційним загрозам і всіляким видам втрат.

4.2 Тенденції та перспективи розвитку ринку засобів та послуг інформаційної безпеки

Розвиток телекомунікацій та інтернету призводить до появи негативних наслідків, таких як збільшення загроз і атак на інформацію. Темпи розвитку і появи нових загроз інформаційної безпеки випереджають темпи розвитку засобів і послуг захисту інформації.

Засоби і послуги захисту інформації постійно розвивається з появою нових загроз і видів атак, тому що, кіберзлочини завдають величезної шкоди світовій економіці. Компанії постійно на ринку продукції представляють нові вирішення актуальних проблем інформаційної безпеки.

Ринок включає в себе споживачів і постачальників засобів і послуг, комплексних рішень, страхувальників ризиків, пов'язаних з інформаційною безпекою. Дану структуру ринку можливо представити у вигляді рисунка 4.2.

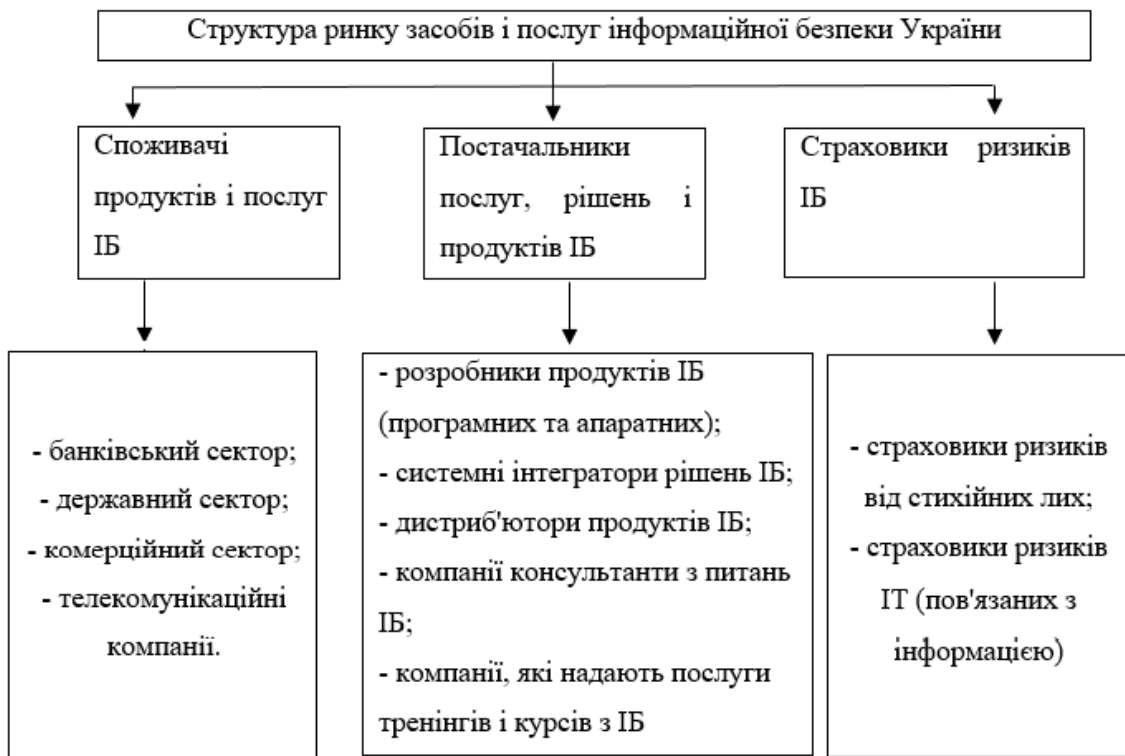


Рисунок 4.2 – Структура ринку засобів і послуг інформаційної безпеки України

Ринок не обмежується цими учасниками, але вони є найбільш важливими. Споживачами засобів і послуг захисту інформації є практично всі підприємства, які функціонують в різних галузях, що приділяють увагу безпеці ведення свого бізнесу.

В основному в Україні використовуються іноземні товари інформаційної безпеки - це виробники антивірусного програмного забезпечення, засоби захисту від несанкціонованого доступу, засоби криптографічного захисту та обладнання для захисту периметра, відеоспостереження та інформаційних мереж. На Українському ринку постачальниками в сфері інформаційної безпеки є - 4 провідних компанії, на які припадає близько 70% всіх поставок.

Лідером ринку за обсягами поставок є Electronic Resource Company (ERC) - партнерська мережа компанії охоплює понад 1700 споживачів. Друге місце займає група компаній МУК з більш ніж 900 партнерами. Третє місце ділять група компаній МТІ (з майже п'ятьма сотнями партнерів по всій Україні) і «Мега-трейд» (партнерська мережа дистриб'ютора охоплює кілька сотень компаній). Слід зазначити, також, що саме ці компанії займають велику частку в поставках у корпоративний сегмент. Структура розподілу поставок між цими компаніями з корпоративного та призначеному для користувача сегментах представлена на рисунках 4.3 і 4.4



Рисунок 4.3 – Поставки в корпоративний сегмент

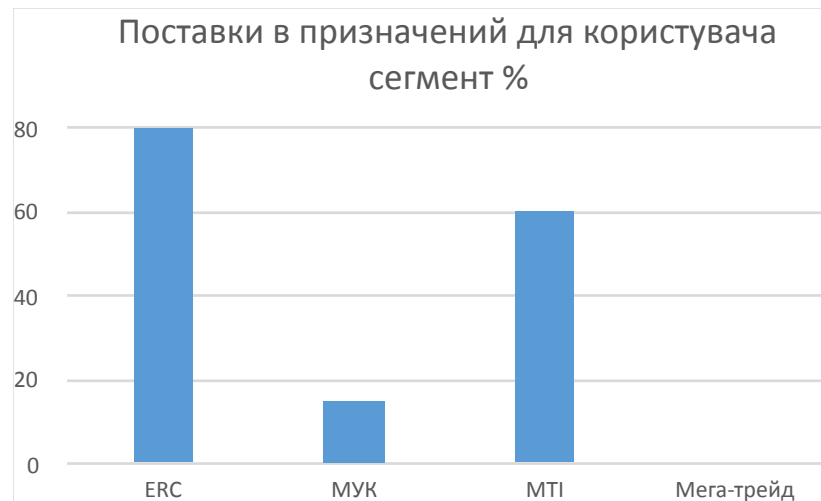


Рисунок 4.4 – Поставки в призначений для користувача сегмент

Аналіз по структурі ринку показує, що в даний час здійснюється поступове зростання. Однак, це зростання недостатнє порівняно з іншими країнами. За окремими напрямками спостерігається позитивна тенденція. Відбувається постійне вдосконалення обладнання, призначеного для забезпечення захисту інформації, але з удосконаленням збільшується ціна на нього. На території України в основному використовується зарубіжне виробництво і на українському ринку компанії виробники безпосередньо не працюють, а використовують дистриб'юторів. [18]

4.3 Розрахунок витрат на практичну реалізацію проекту

Особливістю даного проекту є те, що для його реалізації не потрібно буде закуповувати велику кількість нового обладнання. Вся новизна полягає в аналізі вразливостей операційних систем і удосконаленні роботи існуючого пристрою Wi-Fi.

Застосувавши пропозиції захисту, які описуються в попередніх розділах можливо запобігти витоку інформації на різноманітних підприємствах. Це в свою чергу запобіжить різноманітним втратам, в тому числі і фінансовим.

Таким чином для кошторису витрат на реалізацію проекту необхідно врахувати амортизацію ПК. За статистикою, середній термін служби персональних комп'ютерів та Wi-Fi маршрутизатора становить - 5 років. Амортизація обладнання розраховується за формулою :

$$A_M = \frac{A_{\text{обладнання}}}{T_{\text{експл}}} \quad (4.1)$$

де A_M – амортизація обладнання, грн;

$A_{\text{обладнання}}$ – загальна вартість обладнання, грн;

$T_{\text{експл}}$ – термін експлуатації обладнання, роки.

Дані вартості обладнання подано в таблиці 4.1

Таблиця 4.1 – Витрати на обладнання, грн

Обладнання	Wi-Fi Маршрутизатор	Високопродуктивні ПК
Модель	TP-LINK TL-WR841N	Acer Aspire C24-865(DQ.BBUME.004)
Кількість	1	2
Ціна за одиницю, грн	550	26 500
Доставка, грн (1% від вартості всього обладнання)	5.5	530
Установка, грн (всього обладнання)	100	2000
Налаштування, грн (всього обладнання)	300	2000
Амортизація, грн (всіх ПК)	110	10600
Разом, грн	1065,5	41630
Всього, грн	-	42695,5

У центрі безпеки компанії повинен знаходитися фахівець, який буде забезпечувати внутрішню і зовнішню безпеку. Його завданням буде

відстеження та запобігання будь-яких спроб крадіжки інформації. Слід найняти двох фахівців: системного адміністратора і спеціаліста в галузі захисту інформації, тому що системний адміністратор забезпечує безпеку в денний час, в нічний - захист забезпечує система. В разі виникнення загроз проникнення спрацьовує сигналізація і виїжджає група швидкого реагування на чолі з інженером щодо захисту інформації. У теоретичному розрахунку вказується зарплата за 3 місяці.

У теоретичному розрахунку вказується зарплата за 3 місяці. 22% загального фонду складають соціальні відрахування.

Таблиця 4.2 – Заробітна плата співробітників (за 3 місяці)

№ п/п	Посада	Основна заробітна плата (за 1 місяць), грн.	Додаткова оплата (за 1 місяць), грн.
1	Спеціаліст з захисту інформації	20000	4000
2	Системний адміністратор	10000	2000
Фонд оплати праці (Σ за 3 місяця), грн.	108000		
Соціальні відрахування (22% от Σ)	23760		
Всього	131760		

$$Z_{\text{загальна} - \Sigma} = Z_{\text{обладнання}} + \Phi_{\text{от}} \quad (4.2)$$

де $Z_{\text{загальна} - \Sigma}$ - загальна сума витрат на реалізацію проекту, грн;

$Z_{\text{обладнання}}$ - загальна сума витрат на обладнання, грн;

$\Phi_{от}$ - заробітна плата співробітників (за 3 місяці), грн.

Розрахуємо загальну суму витрат на реалізацію проекту:

$$З_{загальна_ \Sigma} = 42695,5 + 131760 = 174455,5 \text{ грн}$$

4.4 Бальна оцінка економічної ефективності проекту

Бальна оцінка проводиться за такими важливими показниками:

- важливість розробки K_1 ;
- можливість використання результатів розробки K_2 ;
- теоретична значущість і рівень новизни дослідження K_3 ;
- складність розробки K_4 .

Шкала для оцінки важливості розробки, оцінки можливості використання результатів розробки, оцінки рівня новизни, оцінки складності розробки наведені в таблицях 4.3, 4.4, 4.5, 4.6.

Таблиця 4.3 – Шкала для оцінки важливості розробки K_1

№ п/п	Показник	Бали
1	Ініціативна робота, що не є частиною комплексної програми, або завданням відомчих органів	1
2	Робота, виконувана за договором про науково-технічну допомогу	3
3	Робота представляє частину відомчої програми	5
4	Робота представляє частину відомчої комплексної програми	7
5	Робота представляє частину міжнародної комплексної програми	8

Для даної роботи коефіцієнт важливості розробки K_1 дорівнює 3.

Таблиця 4.4 – Шкала оцінки можливості використання результатів розробки K_2

№ п/п	Показник	Бали
1	У даному підрозділі	1
2	У даній організації	3
3	У багатьох організаціях	5
4	У масштабах країни	8

Для даної роботи коефіцієнт можливості використання результатів розробки K_2 дорівнює 5.

Таблиця 4.5 – Шкала оцінки теоретичної значимості й рівня новизни дослідження K_3

№ п/п	Показник	Бали
1	Аналіз, узагальнення й класифікація відомої інформації. Подібні результати були відомі в досліджуваній області	2
2	Одержання нової інформації, що доповнює знання про сутність досліджуваних процесів, не відомі в досліджуваній області	3
3	Одержання нової інформації, що змінює уявлення про сутність досліджуваних процесів, не відомої раніше	5
4	Створення нових теорій, методик	6
5	Одержання інформації, що сприяє формуванню напрямків, не відомих раніше	8

Для даної роботи коефіцієнт теоретичної значущості і рівня новизни дослідження K_3 дорівнює 3

Таблиця 4.6 – Шкала оцінки показників складності дослідження K_4

№ п/п	Показник	Бали
1	Робота виконується одним підрозділом, витрати менш 10000 грн.	1
2	Робота виконується одним підрозділом, витрати 10000-50000 грн.	3
3	Робота виконується одним підрозділом, витрати 50000-100000 грн.	5
4	Робота виконується за участю багатьох підрозділів, витрати 100000-500000 грн.	7
5	Робота виконується декількома організаціями, витрати понад 500000 грн.	8

Для даної роботи коефіцієнт складності розробки K_4 дорівнює 7.

Загальна оцінка встановлюється за добутком коефіцієнтів:

$$Pc = K_1 \cdot K_2 \cdot K_3 \cdot K_4 \quad (4.3)$$

де K_1 – коефіцієнт важливості розробки; K_2 – коефіцієнт можливості використання результатів розробки; K_3 – коефіцієнт теоретичної значущості і рівня новизни дослідження; K_4 – коефіцієнт складності розробки.

$$Pc = K_1 \cdot K_2 \cdot K_3 \cdot K_4 = 3 \cdot 5 \cdot 3 \cdot 3 = 135$$

Питомий ефект на кожний бал - 2 000 грн.

Загальний ефект від розробки складає:

$$A_{\text{заг_еф}} = Pc \cdot 2000 \cdot K_1 \cdot K_2 \cdot K_3 \cdot K_4 \quad (4.4)$$

де $A_{\text{заг_еф}}$ - загальний ефект від розробки, грн;

K_1 - коефіцієнт важливості розробки;

K_2 - коефіцієнт можливості використання результатів розробки;

K_3 - коефіцієнт теоретичної значущості і рівня новизни дослідження;

K_4 - коефіцієнт складності розробки.

$$A_{\text{заг_еф}} = Пс2000 \cdot K_1 \cdot K_2 \cdot K_3 \cdot K_4 = 2000 \cdot 5 \cdot 3 \cdot 3 \cdot 3 = 270000 \text{ грн.}$$

Економічна ефективність від реалізації дипломного проекту визначається за допомогою коефіцієнта ефективності, що характеризує частку загального ефекту від розробки, що приходить на одну грн. витрат (собівартості НДР):

$$K_e = \frac{A_{\text{заг_еф}}}{\sum_{\text{загальна}} 3} \quad (4.5)$$

де K_e - коефіцієнт ефективності;

$A_{\text{заг_еф}}$ - загальний ефект від розробки, грн;

$\sum_{\text{загальна}} 3$ - загальна сума витрат на реалізацію проекту, грн.

Розрахуємо коефіцієнт ефективності:

$$K_e = \frac{A_{\text{заг_еф}}}{\sum_{\text{загальна}} 3} = \frac{270000}{174455,5} = 1,55$$

Висновок: Таким чином, проект має перспективу розвитку і в подальшому може використовуватися компаніями для збереження конфіденційної інформації від витоку її безконтактним способом.

Технологія Wi-Fi зможе поєднувати дві функції, як доступ до інтернету, так і спостереження за виділеним приміщенням, застосування

брандмауерів збережуть комп'ютерну мережу від видаленого доступу, а постійний моніторинг в автоматичному режимі у диспетчері завдань вчасно виявить програми майнінгу і збереже цінну інформацію від конкурентів та зацікавлених осіб.

Використання цих технологій у сукупності допоможе зберегти цінну інформацію у доступності, цілісності і конфіденційності.

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА У НАДЗВИЧАЙНИХ СИТУАЦІЯХ

Тема дипломного проекту «Дослідження вразливостей об'єктів від деяких видів безконтактного проникнення» передбачає роботу працівника з захисту інформації, який здійснює контроль безпеки програмного забезпечення.

Для виконання спеціалістом безпосередніх трудових обов'язків, робоче місце повинно бути забезпечено таким обладнанням: робочим столом та комп'ютерним кріслом, персональним комп'ютером (ПК), електронними та периферійними пристроями, засобами зв'язку, шафою для зберігання документів, різноманітним офісним приладдям. Приміщення обладнане системою опалення, кондиціонером, зволожувачем повітря, пожежною сигналізацією та переносним вогнегасником.

5.1 Аналіз потенційних небезпек

Розглянемо наступні потенційні небезпеки:

1. Ураження електричним струмом через несправність електрообладнання, підвищене значення напруги в електричному ланцюзі або недотримання вимог безпеки при його експлуатації, що може призвести до травми або летального наслідку.
2. Ураження статичним струмом, призводить до отримання неприємних відчуттів людиною та до виходу з ладу приладів.
3. Негативний вплив електромагнітних, в тому числі і рентгенівських випромінювань при використанні моніторів персональних комп'ютерів з електронно-променевою трубкою, що призводить до погіршення зору, зниження імунітету.
4. Механічні травми – виникають через нераціональну організованість робочого місця, захащеність приміщення.

5. Кістково-м'язові порушення, у зв'язку з тривалим статичним напруженням м'язів спини, шиї, рук і ніг, що призводить до ушкодження опорно-рухового апарату.

6. Монотонність праці – виникає внаслідок одноманітного повторення робочих операцій. Небезпека монотонності полягає в зниженні уваги до процесу виробництва, швидкої стомлюваності і зниженні інтересу до трудового процесу, що впливає на безпеку праці в цілому.

7. Негативні відносини у колективі в наслідок постійних емоційних зривів, які призводять до підвищених емоційних навантажень.

8. Нервово-психічні навантаження внаслідок специфіки виконуваних робіт, котрі призводять до захворювань загального характеру.

9. Недостатнє освітлення виробничих приміщень і робочих місць, у зв'язку з несправністю, або хибного вибору освітлювальних приладів, що призводить до погіршення зору.

10. Потрапляння в легені і на слизові оболонки пилу, через підвищену запиленість повітря робочої зони, що провокує появу алергічних захворювань органів зору та дихання.

11. Вірогідність виникнення пожежі у зв'язку із несправністю електричного обладнання, недотриманням, або порушенням правил протипожежної безпеки обслуговуючим персоналом.

12. Неправильні дії персоналу в умовах надзвичайних ситуацій, які призводять до паніки та загибелі людей.

5.2 Заходи по забезпеченню безпеки

Під час проектування систем електропостачання, монтажу силового електрообладнання та електричного освітлення будівель та приміщень для ЕОМ необхідно дотримуватись вимог ПВЕ, ПТЕ, ПБЕ, СН 357-77 «Инструкция по проектированию силового осветительного оборудования

промышленных предприятий», затверджених Держбудом, ГОСТ 12.1.006, ГОСТ 12.1.030 «ССБТ. Электробезопасность. Защитное заземление, зануление», ГОСТ 12.1.019 «ССБТ. Электробезопасность. Общие требования и номенклатура видов защиты», ГОСТ 12.1.045, ВСН 59-88 Держкомархітектури «Электрооборудование жилых и общественных зданий. Нормы проектирования», Правил пожежної безпеки в Україні, цих Правил, а також розділів СНіП, що стосуються штучного освітлення та електротехнічних пристроїв, та вимог нормативно-технічної та експлуатаційної документації заводу-виробника ЕОМ. Для виключення ураження електричним струмом передбачено:

- організаційні заходи: проведення навчання з правил електробезпеки, перевірка знань та атестація персоналу на кваліфікаційну групу з електробезпеки, згідно НПАОП 0.00-4.12-05 «Типове положення про порядок проведення навчання і перевірки знань з питань охорони праці»;
- технічні заходи: встановлення аварійного резервного вимикачу, який може повністю вимкнути електричне живлення приміщення, окрім освітлення, використовується підключення до мережі пристроїв за допомогою справних штепсельних з'єднань і електророзеток заводського виготовлення; проведено електромережу штепсельних розеток для живлення пристроїв уздовж стін приміщення, по підлозі поряд за стінами приміщення, в металевих трубах і гнучких металевих рукавах з відводами відповідно до затвердженого плану розміщення обладнання та технічних характеристик обладнання; відповідність усіх пристроїв вимогам чинних в Україні стандартів нормативних актів з охорони праці, а також пристрої закордонного виробництва додатково відповідають вимогам національних стандартів держав – виробників і мають відповідну позначку на корпусі, в паспорті або іншій експлуатаційній документації; використання захисного заземлення та занулення згідно «Правил устрою електроустановок» («ПУЕ»).

Для виключення ураження статичним струмом та впливу електромагнітного поля застосовуються:

- організаційні заходи: проведення навчання з правил електробезпеки, перевірка знань та атестація персоналу на кваліфікаційну групу з електробезпеки, згідно НПАОП 0.00-4.12-05 «Типове положення про порядок проведення навчання і перевірки знань з питань охорони праці»;
- технічні заходи: екранування джерела статичного навантаження, згідно з ГОСТ 12.4.124-83 «Засоби захисту від статичної електрики. Загальні технічні вимоги»; використання покриття технологічних підлог з одношарового полівінілхлоридного антистатичного лінолеуму, для зниження величини виникаючих зарядів статичної електрики в робочому приміщенні; загальне і місцеве періодичне зволоження повітря.

Для запобігання механічних травм необхідна раціональна організація робочих місць та дотримання техніки безпеки.

Для запобігання кістково-м'язових порушень у зв'язку з тривалим статичним напруженням м'язів спини, ший, рук і ніг необхідно виконувати фізичні вправи 2-3 рази протягом робочого часу.

Для запобігання перевтоми робітників під час виконання монотонної роботи, необхідно чергувати її з іншими видами діяльності, які мають більш динамічний характер та слугують відволікаючим фактором для робітника. З метою запобігання перевтоми від виконання монотонної роботи також необхідно робити перерви у роботі – кожні дві години по 15 хвилин. [19]

Для оптимізації відносин у колективі проводяться тренінги з залучанням психологів на теми: «Адаптація у новому колективі», «Поведінка в суспільстві».

З метою зниження нервово-емоційного напруження, стомлення зорового аналізатора, поліпшення мозкового кровообігу, подолання несприятливих наслідків гіподинамії, запобігання втоми, передбачені перерви

у роботі – 15 хвилин кожні дві години, а також спеціально обладнане приміщення – кімната відпочинку.

5.3 Заходи по забезпеченню виробничої санітарії та гігієни праці

Для запобігання несприятливого впливу на людину шкідливих факторів, які супроводжують роботу з відео терміналами і персональними електронно-обчислювальними машинами, розроблений ряд санітарно-гігієнічних вимог.

Заходи з виробничої санітарії та гігієни праці спрямовані на запобігання або зменшення впливу на персонал шкідливих виробничих факторів. Вони забезпечують на робочих місцях нормальні умови повітряного середовища, необхідну освітленість, усувають вплив шуму, випромінювань та інших шкідливих виробничих чинників.

Організація робочого місця користувача відео терміналу та ЕОМ повинна забезпечувати відповідність усіх елементів робочого місця та їх розташування ергономічним вимогам ГОСТ 12.2.032 «ССБТ. Рабочее место при выполнении работ сидя. Общие эргономические требования», характеру та особливостям трудової діяльності. Площа, виділена для одного робочого місця з відео терміналом або персональною ЕОМ, повинна складати не менше 6 м² , а обсяг – не менше 20 м³ . Робочі місця з відео терміналами відносно світлових прорізів повинні розміщуватися так, щоб природне світло падало збоку, переважно зліва.

У офісному приміщенні, згідно ДБН В.2.5-28-2006 «Інженерне обладнання будинків і споруд. Природне і штучне освітлення» передбачене природне та штучне освітлення. Природне освітлення здійснено через світлові прорізи, які забезпечують коефіцієнт природної освітленості (КПО) не нижче 1,5%. Для захисту від прямих сонячних променів, які створюють

прямі та відбиті відблиски на поверхні екранів і клавіатури, передбачено сонцезахисні пристрої, на вікнах встановлені жалюзі або штори.

В зоні, де відбувається робота з документами освітленість становить 300-500 лк.

Для забезпечення нормованих значень освітлення в приміщеннях з відео терміналами ЕОМ загального та персонального користування необхідно очищати віконне скло та світильники не рідше ніж 2 рази на рік, та своєчасно, проводити заміну ламп, що перегоріли.

Метеорологічні умови в приміщенні офісу – температура повітря, відносна вологість повітря й швидкість його переміщення відповідають встановленим санітарно-гігієнічним вимогам ДСН 3.3.6.042-99 «Державні санітарні норми мікроклімату виробничих приміщень» і ГОСТ 12.1.005-88 (1991) «ССБТ. Общие санитарно-гигиенические требования к воздуху рабочей зоны». Роботи в офісному приміщенні, належать до категорії Іб - легка робота, тому передбачені наступні оптимальні значення параметрів мікроклімату: - у холодний період року: температура 21-23°C; відносна вологість: 40-60%; швидкість переміщення повітря: 0,1 м/с; - у теплий період року: температура 22-24°C; відносна вологість: 40-60%; швидкість переміщення повітря: 0,2 м/с. Забезпечення таких параметрів мікроклімату досягається оснащенням приміщень пристроями кондиціонування, вентиляції та дезодорації повітря, системами опалювання.

З метою усунення сухого повітря, в офісі встановлено ультразвуковий зволожувач повітря Bonesco Air-O-Swiss U650, що має два режиму роботи: «холодний пар» та «теплий пар», має систему дезінфікування води шляхом нагріву до 80°C, змінні наповнювачі для картриджу, 8 годинний таймер, функція підтримки оптимального рівня вологості відносно температури.

Необхідний повітрообмін в приміщенні визначається за формулою:

$$L = \frac{Q}{C \cdot \gamma \cdot (t - t_{np})}, \text{ м}^3 / \text{час} \quad (5.1)$$

де Q – сумарна кількість теплоти, що утворюється в приміщенні, кДж / год;

C – питома теплоємність повітря, що дорівнює $C = 1$ кДж / (кг °С);

γ - щільність зовнішнього повітря, що дорівнює $= 353/((273+t_{\text{пр}}))$, кг / м³;

t – температура повітря, що видаляється °С;

$t_{\text{пр}}$ – температура припливного повітря, °С;

Вхідні дані: $Q = 7300$ кДж / год; $t = 32^\circ \text{C}$; $t_{\text{пр}} = 19^\circ \text{C}$.

Розрахуємо необхідний повітрообмін в приміщенні:

$$L = \frac{7300}{1 \cdot 1,209 \cdot (32 - 19)} = 464,5 \text{ м}^3 / \text{год}$$

5.4 Заходи з пожежної безпеки

Горінням називається складний фізикохімічний процес взаємодії горючої речовини та окислювача, який супроводжується виділенням тепла та випромінюванням світла. Процес горіння призводить до пожежі. Пожежа – неконтрольоване горіння поза спеціальним вогнищем, що розповсюджується в часі і просторі.

Забезпечення пожежної безпеки є важливою частиною політики будь якої установи. Пожежна безпека регламентується державними стандартами НАПБ А.01.001-2014 «Правила пожежної безпеки в Україні».

При прийомі на роботу з працівниками проводиться інструктаж з техніки пожежної безпеки, періодично здійснюються перевірки приміщень на предмет дотримання норм пожежної безпеки, а також періодично з працівниками проводять навчання, щодо правильності їх дій при пожежі.

Залежно від агрегатного стану й особливостей горіння різних горючих речовин й матеріалів пожежі за ДБН В.1.1.7 2002 «Пожежна безпека об'єктів будівництва» поділяються на відповідні класи та підкласи:

- клас А – горіння твердих горючих речовин, переважно органічного походження, горіння яких супроводжується тлінням (деревина, текстиль, папір):

A1 — горіння, яке супроводжується тлінням;

A2 — яке не супроводжується тлінням.

- клас В – горіння рідких речовин або твердих речовин, які розтоплюються:

B1 — які розчинні у воді;

B2 — нерозчинні у воді;

- клас С – горіння газоподібних речовин;

- клас D – горіння металів та їх сплавів:

D1 — легкі метали;

D2 — лужні і лужноземельні метали;

D3 — металомісткі сполуки.

Крім цих чотирьох класів Правилами пожежної безпеки в Україні введено ще один додатковий п'ятий клас (Е) прийнятий для позначення пожеж, пов'язаних з горінням електроустановок:

- клас Е – пожежі пов'язані з горінням електроустановок.

Відповідно до стандартів безпеки НАПББ.03.002-2007 «Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою» та ДБН В.1.1.7-2002 «Пожежна безпека об'єктів будівництва» приміщення кабінету офісу відноситься до категорії Д, а саме: негорючі рідини і матеріали у холодному стані, а за класами робочих зон з вибухової та пожежної небезпеки – до класу А (пожежі твердих речовин) та класу Е (пожежі, пов'язані з горінням електроустановок).

Основними причинами пожежі можуть бути:

- коротке замикання електропроводки;
- несправність комп'ютерної техніки та іншого електрообладнання.

Для відводу надлишкової теплоти від персонального комп'ютера служать системи вентиляції та кондиціонування повітря. При цьому можливе оплавлення ізоляції сполучних проводів, їх оголення, і, як наслідок, коротке замикання, яке супроводжується іскрінням.

У відділі передбачені заходи як щодо попередження виникнення пожежі, так і щодо успішної евакуації людей та матеріальних цінностей, у випадку її виникнення.

Площа відділу складає 24 м². і згідно рекомендаціям щодо оснащення приміщень переносними вогнегасниками оснащена наступними засобами протипожежної безпеки:

- вуглекислотний вогнегасник ВВК-5 місткістю 5л;
- система автоматичного спринклерного пожежогасіння;
- пожежна сигналізація комбінованого типу що реагує на зміну температури та дим.

На стіні перед виходом з приміщення відділу є план та схема евакуації внаслідок виникненні пожежі, а також тривожна кнопка виклику пожежної служби.

5.5 Заходи по забезпеченню безпеки у надзвичайних ситуаціях

Евакуація проводиться за рішенням Кабінету Міністрів України і здійснюється органами виконавчої влади. Рішення на проведення екстреної евакуації можуть прийняти начальники цивільного захисту об'єкта, району, міста. Підготовча й організаційна робота з проведення евакуації покладається на штаби цивільного захисту і евакуаційні органи.

Одержавши розпорядження про проведення евакуації, штаби ЦЗ об'єктів народного господарства разом з евакуаційними комісіями:

- уточнюють чисельність робітників, службовців і членів їхніх родин, що підлягають розосередженню й евакуації, номери залізничних ешелонів, автомобільних колон і пішохідних маршрутів, виділених об'єкту за планом; терміни прибуття на збірний евакуаційний пункт;
- оповіщають і організовують збір робітників, службовців і членів їхніх родин;
- надають допомогу збірні евакуаційні пункти (ЗЕП) відносно реєстрації і посадки тих, кого евакуюють, на транспорт, а також у формуванні і відправленні піших колон;
- допомагають місцевим органам у районах розосередження й евакуації розміщувати прибуваюче населення.

Начальники ЗЕП з одержанням розпорядження про початок проведення евакуаційних заходів:

- приводять ЗЕП у готовність до прийому евакуйованих;
- встановлюють зв'язок з начальниками станцій, портів, пристаней і пунктів посадки, а також зі штабами ЦЗ об'єктів, приписаних до даного ЗЕП;
- уточнюють порядок відправлення робітників та службовців підприємств, установ і організацій, номери виділених залізничних ешелонів (автоколон, суден), час їхньої подачі і відправлення, номери пішохідних маршрутів, склад піших колон і вихідні пункти.

В міру прибуття населення начальники ЗЕП разом із представниками штабів ЦЗ об'єктів і Житлово-експлуатаційна контор здійснюють його прийом і реєстрацію, розподіляють по вагонах (автомобілях, кораблях), формують піші колони, інформують штаб ЦЗ й евакуаційну комісію міста про хід евакуації.

Про початок евакуації населення оповіщається через підприємства, навчальні заклади, домоуправління й органи міліції.

Ідучи на ЗЕП, кожен повинен узяти із собою паспорт, військовий квиток, документи про освіту, трудову книжку чи пенсійне посвідчення, свідоцтво про народження дітей, необхідний запас продуктів (на 2—3 дні),

білизну, постіль та інші необхідні речі з урахуванням тривалого перебування в заміській зоні.

Дітям дошкільного віку необхідно покласти в кишені чи пришити до одягу записки із зазначенням прізвища, імені, по батькові і місця проживання чи роботи батьків.

Перед виходом з квартири необхідно відключити електроживлення, закрити вікна і кватирки, перекрити вентиля в системі опалення і водопостачання, відключити газ, зачинити квартиру, здати ключі представнику домоуправління.

На ЗЕП ті, кого евакуюють, проходять реєстрацію, групуються по вагонах залізничного ешелону або по автомашинах автоколони і у призначений час виводяться до пунктів посадки на транспорт.

Транспортне забезпечення розосередження й евакуації включає: вивезення населення, установ і організацій у райони евакуації, вивезення матеріальних цінностей; перевезення робочих змін з районів евакуації в місто на підприємства і назад.

Штаб ЦЗ об'єкта одержує від вищестоящого штабу виписку із плану евакуаційних заходів, в котрій зазначено, які транспортні засоби виділяються об'єкту, їх місткість, час подачі, місце посадки, час відправлення, місце і час висадки.

Перевезення автотранспортом плануються й організовуються начальником автотранспортної служби міста, який розробляє план перевезень, узгоджує його з начальником ЦЗ міста і доводить до виконавців розпорядження.

Для перевезення людей виділяються автобуси, легкові та вантажні автомашини, у тому числі і самоскиди; вантажні автомашини і самоскиди обладнуються сидіннями.

З одержанням розпорядження про початок розосередження й евакуації автоколони прибувають на ЗЕП і подаються для посадки людей. По закінченні посадки виходять на свої маршрути і доставляють людей у

призначені пункти висадки, потім повертаються на ЗЕП для виконання наступних рейсів. Управління автотранспортними перевезеннями на маршруті здійснюється диспетчерськими пунктами, які організовуються по одному на кожному маршруті.

Матеріальне забезпечення включає, головним чином, постачання евакуйованого населення продовольством і предметами першої необхідності. Організація його покладається на заступника начальника об'єкта з матеріально-технічного забезпечення, що спільно зі службами ЦЗ міського та сільського районів підготовляє необхідні умови для постачання матеріальними засобами робітників та службовців об'єкта і членів їх родин у заміській зоні, а також організовує харчування працюючої зміни на об'єкті.

Забезпечення продовольством та предметами першої необхідності у заміській зоні організовується через місцеві торгові організації, мережі громадського харчування і побутового обслуговування.

Міські підприємства торгівлі, громадського харчування і побутового обслуговування одночасно з розосередженням і евакуацією населення вивозяться в заміську зону і використовуються для розширення і збільшення пропускної здатності сільських мереж.

На пішохідних маршрутах для забезпечення евакуйованих слід передбачати організацію рухомих пунктів харчування і водопостачання, а в зимовий час — і пунктів обігріву.

Постачання питною водою у заміській зоні здійснюється в основному з артезіанських колодязів, шахтних, трубчастих та інших закритих джерел.

Медичне обслуговування евакуйованого населення здійснюється через існуючу мережу лікарень, поліклінік і медпунктів сільської місцевості, розширювану за рахунок міських лікувальних установ, що вивозяться. Для збільшення персоналу лікарень і поліклінік залучаються лікарі й інші медпрацівники з числа евакуйованих.

На період проведення евакуаційних перевезень населення медична служба ЦЗ виділяє на пункти збору і посадки медичний персонал. Для

надання медичної допомоги в дорозі на кожен залізничний ешелон, автоколону чи пішу колону виділяються медпрацівники, переважно з числа евакуйованих; у ППЕ й у пунктах висадки медичними службами сільських районів створюються медпункти.

На підприємствах, що продовжують виробничу діяльність у місті, медичне обслуговування працюючих змін організовується начальниками медичних служб об'єктів. Лікарська допомога забезпечується медичними установами, що залишаються в місті, стаціонарне лікування проводиться в лікарнях заміської зони.

Інженерне забезпечення розосередження й евакуації включає: забезпечення утримання і ремонту доріг, бруківки дорожніх споруд, устаткування пунктів посадки і висадки, колонних шляхів на пішохідних маршрутах, побудову пішохідних переходів на водних перешкодах, обладнання укриттів для населення на шляхах евакуації й у районах розміщення. Відповідальність за стан колонних шляхів і доріг покладається на начальника ЦЗ, по території якого вони проходять.

Захисні споруди призначені для захисту людей від наслідків аварій (катастроф) і стихійних лих, а також від уражальної дії зброї масового знищення і звичайних засобів ураження та впливу другорядних чинників ядерного вибуху.

Захисні споруди розрізняють:

- за призначенням - для захисту населення, розміщення органів управління (командного пункту, пункту управління, вузла зв'язку) і медичних закладів;
- за місцем знаходження - вбудовані, відокремлені, метрополітен, у гірських виробках;
- за терміном будівництва - зведені завчасно, швидко зведені;
- за захисними властивостями - найпростіші укриття (щілини відкриті і перекриті), протирадіаційні укриття (ПРУ) і сховища.

У системі захисту населення особливе значення мають найпростіші укриття типу щілин. Це найбільш масові захисні споруди, що можуть бути збудовані населенням у найкоротший термін. Щілини будують відкритими і перекритими. Відкрита щілина зменшує ймовірність ураження ударною хвилею (в 1,2-2 рази), світловим випромінюванням і проникаючою радіацією.

Перекрита щілина захищає: від світлового випромінювання - повністю, від ударної хвилі - у 1,5-3 рази, від проникаючої радіації і радіоактивного випромінювання - у 200-300 разів, а також надійно захищає від осколкових і кулькових бомб, від запалювальних засобів.

Відкрита щілина - це зигзагоподібна траншея з кількох прямолінійних ділянок довжиною до 15 м. Глибина її - 1,8 - 2,0 м; ширина: зверху - 1,1-1,3 м, на дні - 0,8 м. Будівництво щілини починається з розмітки і трасування, тобто визначення її плану на місцевості. Копають спочатку на ширину дна. В міру заглиблення поступово підрівнюють крутизну, доводячи до потрібних параметрів. Стінки (крутизну) щілини укріплюють дошками, жердинами, очеретом, іншими наявними матеріалами.

Коли є час і в разі потреби, щілину перекривають колодами, шпалами або малогабаритними залізобетонними плитами. Зверху покриття влаштовують шар гідроізоляції з толю, руберойду, хлорвінілової плівки або утрамбовують шар глини і насипають шар ґрунту товщиною 50-60 см. У перекритій щілині роблять вхід з однієї або двох сторін з дверима і тамбуром. Для вентиляції встановлюють витяжну коробку.

Нормальна місткість щілини - 10-15 чоловік.

Протирадіаційними укриттями називаються негерметичні захисні споруди, що забезпечують захист людей в умовах надзвичайних ситуацій. До протирадіаційним укриттям можна віднести не тільки спеціально побудовані споруди, а й будівлі господарського призначення (погреби, підпілля, овочесховища), пристосовані під укриття, і звичайні житлові будівлі.

Захисні властивості укриттів визначаються коефіцієнтом послаблення радіації, що залежить від товщини огорожувальних конструкцій,

властивостей матеріалу, з якого виготовлені конструкції, а також від енергії гамма-випромінювання. Наприклад, підвали дерев'яних будинків послаблюють радіацію в 7-12 разів, а кам'яних - у 200-300 разів.

У протирадіаційних укриттях, розрахованому на 50 чоловік і більше, повинно бути не менше двох виходів розміром 80x180 см, причому бажано, щоб вони були розташовані в протилежних кінцях укриття під кутом 90° один до одного. Для підсилення захисних властивостей у приміщенні забивають вікна і зайві двері, насипають шар ґрунту на перекриття і роблять, якщо треба, ґрунтову підсипку ззовні біля стін, що виступають вище поверхні землі.

Для герметизації приміщень ретельно замурують тріщини, щілини, отвори у стінах і стелі, біля вікон і дверей, припасовують двері, оббивають їх повстю, ущільнюють дверні рами валиком з повсті або з іншої м'якої тканини. Укриття, що вміщує до 30 чоловік, провітрюється природною вентиляцією через припливний і витяжний короби. Для створення тяги витяжний короб встановлюють на 1,5-2 м вище припливного. На зовнішньому виводі вентиляційного короба роблять дашок, а в припливному коробі - щільно підігнані засуви.

У пристосованих під укриття приміщеннях встановлюють бачки з водою з розрахунку 3-4 л на одну людину на добу, а в туалеті - виносну тару або влаштовують люфт-клозет з вигрібною ямою. Крім того, в укритті встановлюють лавки для відпочинку, стелажі для продуктів харчування. Освітлення - від електромережі або переносними електричними ліхтарями.

Сховище є найбільш надійним захистом від усіх уражальних чинників: високих температур і шкідливих газів у зонах пожеж, вибухонебезпечних, радіоактивних і сильнодіючих отруйних речовин, обвалів і уламків зруйнованих будинків і споруд тощо, а також засобів масового ураження і звичайних засобів ураження. Воно обладнане комплексом інженерних споруд, що забезпечують необхідні умови життєдіяльності протягом певного часу.

За місцем знаходження сховища бувають вбудованими (у підвалах будинків) і відокремленими (поза будинками), їх споруджують заздалегідь, у мирний час, але можуть будувати і в період загрози нападу або під час воєнних дій (швидко зведені).

За місткістю розрізняють малі сховища (150. -300 чол.), середні (300-600 чол.) і великі (понад 600 чол.).

Сховища мають фільтровентиляційні установки промислового виготовлення. ФВУ очищає зовнішнє повітря, розподіляє його по відсіках і створює у захисному приміщенні надлишковий тиск, що перешкоджає проникненню зараженого повітря через тріщини і щілини.

В усіх сховищах передбачаються два режими вентиляції:

- чистої, коли зовнішнє повітря очищається від пилу;
- фільтровентиляції, коли воно проходить крізь поглинальні фільтри, де очищається від радіоактивного пилу, отруйних речовин, СДОР і бактеріологічних засобів.

Система водопостачання забезпечує людей водою для життя і гігієнічних потреб від зовнішньої водопровідної мережі. На той випадок, коли водопровід перестане діяти, передбачено аварійний запас води або її джерело. Кожна захисна споруда має систему каналізації для відводу фекальних стоків. Санвузол влаштовують у приміщенні, ізольованому перегородками від секцій сховища, обов'язково з витяжкою.

Система опалення сховища працює від опалювальної мережі будинку, під яким воно знаходиться. Освітлюється сховище від міської електромережі, в аварійних випадках - від автономної електростанції, а якщо її немає - від акумуляторів або ліхтарями.

Запас продуктів харчування робиться з розрахунку не менше ніж на дві доби для кожної людини у сховищі.

Медичне обслуговування здійснюють санітарні пости і медпункти об'єктів народного господарства.

Населення укривається у захисних спорудах за сигналами ЦО. Заходити до них потрібно організовано, швидко і без паніки. У сховищі зручніше розміщуватися групами - з тих, хто разом працює або мешкає в одному будинку. В кожній групі призначають старшого. Тих, хто з дітьми, розміщують в окремих відсіках або у спеціально відведених місцях. Літніх і хворих намагаються влаштувати ближче до вентиляційних труб.

У сховище (укриття) потрібно приходити зі своїми засобами індивідуального захисту органів дихання, продуктами харчування і документами. Не дозволяється приносити з собою речі громіздкі, з сильним запахом, легкозаймисті, приводити тварин. У сховищі забороняється ходити без потреби, шуміти, курити, виходити назовні без дозволу коменданта. Всі у сховищі зобов'язані виконувати розпорядження чергового по сховищу, надавати посильну допомогу хворим, інвалідам.

Ще перебуваючи в зоні ураження або відразу після виходу з неї, потрібно здійснити часткову санітарну обробку, щоб видалити небезпечні речовини з відкритих ділянок шкіри, із взуття, одягу, протигаза.

При зараженні радіоактивними речовинами насамперед потрібно: обтрусити, вибити одяг; протерти вологою ганчіркою взуття; помити відкриті частини рук і шиї; протерти лицьову частину протигаза і зняти його (чи респіратор, протипилову тканинну маску, ватно-марлеву пов'язку); вимити обличчя, прополоскати рот і горло.

Якщо води мало, відкриті ділянки тіла і протигаз протирають зволоженим тампоном, причому лише в одному напрямку. Взимку з цією метою можна використати незаражений сніг. Обробку проводять протягом першої години після зараження у самій зоні і повторюють після виходу з неї.

При зараженні краплиннорідкими ОР для часткової санітарної обробки застосовують індивідуальний протихімічний пакет (ППП-8). Спочатку обробляють відкриті ділянки шкіри, а потім заражені частини одягу і взуття. Якщо немає ППП, усе ретельно промивають теплою водою з милом.

При зараженні бактеріологічними засобами, не знімаючи протигаза (ПТМ, ватно-марлевої пов'язки), обтрушують одяг, обмітають взуття, розчином з ІПП обробляють відкриті ділянки тіла. Якщо пакета немає, використовують дезінфікуючі розчини і воду з милом.

Часткова санітарна обробка не забезпечує повного знезараження і не гарантує людям захисту від ураження. Тому за найменшої можливості проводять повну санітарну обробку.

При повній санітарній обробці усе тіло обмивають теплою водою з милом і мочалкою, обов'язково міняють білизну і верхній одяг. Проводиться на стаціонарних пунктах, у банях і душових павільйонах або на спеціальних майданчиках для миття і пунктах спеціальної обробки. Влітку повну санітарну обробку можна здійснити біля незаражених проточних водоймищ.

Пункти санітарної обробки мають три відділення: для роздягання, для миття і для одягання. Крім того, може бути відділення для знезараження одягу. Особи, які прибули для санітарної обробки, у роздягальні знімають верхній одяг, засоби захисту (крім протигаза), білизну, проходять медичний огляд, дозиметричний контроль. Одяг, заражений радіоактивними речовинами вище допустимої норми, а також отруйними речовинами і бактеріологічними засобами, складають у гумові мішки і відправляють на станцію знезараження одягу.

Перед входом до відділення миття уражені знімають протигаз і обробляють слизисті оболонки 2-процентним розчином питної соди. Якщо відбулося зараження отруйними речовинами типу зарин, то перш ніж зняти протигаз, проводять контроль приладами хімічної розвідки. Одержавши мило і мочалку, уражені заходять у відділення миття. Особливо ретельно треба вимити голову, шию, руки. Температура води має бути 38-40°C.

При зараженні бактеріологічними засобами перед входом у роздягальню одяг зрошують 0,5-процентним розчином монохлораміну. Біля входу у відділення миття руки і шию обробляють 2-процентним розчином монохлораміну, знімають протигаз, одержують мило та мочалку і переходять

у відділення миття. Після виходу з нього проводять повторний медичний огляд і дозиметричний контроль. Якщо радіоактивне зараження вище допустимого, проводять повторну санітарну обробку.

У відділенні одягання кожний, хто пройшов обробку, одержує одяг (свій знезаражений або із запасного фонду) й одягається.

Якщо упорядкованого пункту санітарної обробки немає, то її здійснюють у банях, душових, обладнаних таким чином, щоб потік людей рухався лише в одному напрямі.

Майданчики санітарної обробки поблизу джерела води ділять на брудну і чисту половини. Між ними розміщують дезінфекційні автомобілі з душем. Для відведення води копають канали і поглинальні колодязі. У теплу пору року санітарну обробку можна проводити на відкритому повітрі. Коли холодно, ставлять намети.

Дезактивація - видалення (змивання, змитання) радіоактивних речовин із заражених ділянок місцевості, споруд, техніки, різних предметів. Залежно від обстановки може проводитися частково або в повному обсязі. При частковій дезактивації знезаражуються тільки деякі ділянки місцевості, основні деталі обладнання, одяг, взуття, засоби індивідуального захисту, тобто все, із чим безпосередньо стикаються люди. [20]

Звичайний і захисний одяг і взуття обмітають, витрушують, вибивають і чистять, протирають клоччям, змоченим водою або дезактивувальними розчинами, миють щітками під сильним струменем води. До дезактивувальних речовин належать усі пральні порошки і пасти (ОП-7, ОП-10), що застосовуються у вигляді водних розчинів. Якщо їх немає, можна користуватися господарським милом.

Дегазація - руйнування (нейтралізація) або видалення отруйних речовин з різних предметів, техніки, споруд і місцевості. Дегазація, як часткова, так і повна, здійснюється трьома способами: хімічним, фізико-хімічним, механічним. Хімічний спосіб полягає у дії на отруйних речовин дегазувальної речовини, внаслідок чого утворюються нетоксичні сполуки.

При фізико-хімічному способі отруйних речовин видаляють із заражених об'єктів, розчиняючи, випарюючи або сорбуючи (поглинаючи) їх. Механічний спосіб - це видалення ОР, що знаходиться на поверхні (наприклад, знімають заражений шар ґрунту або засипають його ґрунтом, шлаком).

Основні способи дегазації одягу і взуття - провітрювання, вимочування у воді, кип'ятіння, прання, обробка пароповітряно-аміачною сумішшю. Бавовняні і гумові вироби кип'ятять і перуть. Якщо у воду додати соду, пральний порошок або мило, руйнування отруйних речовин проходить значно швидше. Обробку пароповітряно-аміачною сумішшю застосовують для всіх видів одягу, взуття, хутряних виробів і засобів захисту шкіри.

Дезінфекція - знищення хвороботворних мікроорганізмів і руйнування токсинів на місцевості, спорудах, техніці, різних предметах. Проводиться двома способами - хімічним і фізичним.

Хімічний спосіб - це застосування дезінфікуючих речовин, що знищують хвороботворні мікроби і токсини.

При фізичному способі хвороботворні мікроби гинуть під дією високих температур.

Для дезінфекції території, різних об'єктів, предметів домашнього вжитку використовують хлорне вапно, моно-хлораміни, дихлораміни, їдкий натр у розчинах від 0,2 до 10%.

Приміщення, меблі і речі обробляють 3-5-процентним розчином фенолу (карболовою кислотою). 1-10-про-центним водним розчином формаліну або його парами дезінфікують приміщення, одяг, м'які речі; розчином лізолу - взуття, гумові і шкіряні вироби; розчином гашеного вапна - будинки, склади, транспорт, туалети, дороги, подвір'я та інші території.

Одяг і взуття кладуть у камери, куди подаються гаряче повітря, пароповітряна і пароформалінова суміші.

ВИСНОВОК

У даній роботі були досліджені вразливості бездротових мереж. Доведено, що за допомогою технології RF-Capture розширюється вибір засобів захищеного приміщення. Пристроєм Wi-Fi можливо поєднувати 2 функції: як доступ в інтернет, так і контроль за виділеним приміщенням і можливо своєчасно виявити проникнення людей на територію, що охороняється.

Такі системи можливо застосовувати в різних сферах. Перш за все – у військовій промисловості, щоб бачити супротивника крізь стіну. При проведенні рятувальних операцій, щоб знаходити людей в самих важкодоступних місцях. RF Capture використовуватимуть правоохоронні органи при спостереженні за злочинцями. З точки зору захисту інформації, цю технологію можливо поєднувати з діючими системами виявлення проникнення злоумисників на контрольовану зону.

Звернуто увагу на те, що за допомогою Wifiphisher можливо отримати практично будь-яку інформацію про користувача, а саме: пароль від Wi-Fi, дані про банківську картку, особисту інформацію та будь-яку іншу інформацію. З точки зору захисту інформації, не потрібно з'єднуватись з бездротовими мережами з однаковими назвами, особливо, якщо вона без паролем аутентифікації при з'єднанні з точкою доступу.

Досліджено вразливості у програмному забезпеченні, а саме програми майнінгу та шкідливого програмного забезпечення RMS.

Якщо програму майнінгу модифікувати, то можливе знімання інформації про всі дії користувача. Тому, для захисту інформації, слід обов'язково знищувати програми майнінгу.

Для того, щоб не потрапила шкідлива програма RMS на персональний комп'ютер необхідно завантажувати програмні забезпечення тільки з офіційних джерел. Це дає хоча б якусь гарантію того, що програма, яку

встановлюють, не модифікована додатковими програмами віддаленого доступу або майнінгу.

Розроблено рекомендації щодо удосконалення методів захисту інформації. А саме, наведено рекомендації щодо оптимізації розповсюдження радіохвиль у режимній зоні. Наведено удосконалений комплекс заходів з забезпечення безпеки комп'ютеру від безконтактних методів проникнення. При використанні усіх програм у комплексі, а також постійному моніторингу завдань у системі, можливо виявити шкідливі програмні забезпечення.

Досліджено економічні розрахунки впровадження цього проекту. Цей проект має перспективу розвитку, і, в подальшому, може використовуватися компаніями для збереження конфіденційної інформації від витоку її безконтактним способом.

Також проведені дослідження потенційних небезпек, що можуть загрожувати співробітникам, які обслуговують моніторинг. Викладені правила щодо забезпечення техніки безпеки, з виробничої санітарії і гігієни праці, пожежної безпеки, яких повинен дотримуватися весь персонал при роботі. Для цього ж офісу розрахований необхідний повітрообмін в приміщенні. Так само були розібрані вимоги щодо забезпечення безпеки в надзвичайних ситуаціях.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Богуш В.М., Юдин О.К., Інформаційна безпека держави. – К.: «МК-Прес», 2005. – 432 с.
2. Основы информационной безопасности. Учебное пособие для вузов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая линия – Телеком, 2006. – 544 с.
3. Wi-Vi: как видеть сквозь стены и отслеживать перемещения людей по сигналу Wi-Fi. – Режим доступа: <https://www.computerra.ru/183630/wi-vi-see-through-the-wall/>
4. Обычный Wi-Fi роутер поможет видеть сквозь стены. – Режим доступа: <https://nplus1.ru/news/2017/05/08/wi-fi-through-the-walls>
5. RF-Capture: Capturing the Human Figure Through a Wall. – Режим доступа: <http://rfcapture.csail.mit.edu>
6. Лізунов, С.І. Спостереження за виділеним приміщенням за допомогою пристрою RF Capture / С.І. Лізунов, М.П. Верещака // Матеріали Всеукраїнського науково-практичного семінару "Використання сучасних інформаційних технологій в діяльності Національної поліції України". 25 листопада 2016 року - Дніпро: Державний університет внутрішніх справ - 2016 – С. 86-87.
7. Лизунов, С.И. Наблюдение за выделенным помещением с помощью Wi-Fi / С.И. Лизунов, М.П. Верещака // Тиждень науки: щорічна наук.-практ. конф. викладачів, науковців, молодих учених і аспірантів: збірник тез доповідей в 5 томах. 18-22 квітня 2016 року – Запоріжжя: Запорізький національний технічний університет - 2016. – Т. 1. – С. 318.
8. Лізунов, С.І. Контроль за об'єктами безконтактним методом / С.І. Лізунов, М.П. Верещака // IX Міжнародна науково-практична конференція: збірник тез доповідей. 03–05 жовтня 2018 року – Запоріжжя: Запорізький національний технічний університет - 2018. – С. 221-222.

9. VLASIC, D., ADELSBERGER, R., VANNUCCI, G., BARNWELL, J., GROSS, M., MATUSIK, W., AND POPOVIĆ, J. 2007. Practical motion capture in everyday surroundings. In ACM Transactions on Graphics (TOG), vol. 26, ACM, P. 35.
10. APPLEBY, R., AND ANDERTON, R. N. 2007. Millimeter-wave and submillimeter-wave imaging for security and surveillance. Proceedings of the IEEE. Режим доступу: <https://ieeexplore.ieee.org/document/4337827>
11. GANAPATHI, V., PLAGEMANN, C., KOLLER, D., AND THRUN, S. 2010. Real time motion capture using a single time-of-flight camera. In IEEE CVPR. Режим доступу: <https://www.semanticscholar.org/paper/Real-time-motion-capture-using-a-single-camera-Ganapathi-Plagemann>
12. Верещака, М. П. Тестирование Wi-Fi сетей с помощью kali linux / М. П. Верещака, С. И. Лизунов Тижень науки: щорічна наук.-практ. конф. викладачів, науковців, молодих учених і аспірантів, 18-21 квітня 2017 р.: збірник тез – Запоріжжя, 2017. – С. 598.
13. Скрытый майнинг: найти и уничтожить [Електронний ресурс]. – Режим доступу: <https://bitnovosti.com/2017/08/16/skritiy-mayning-nayti-unichtojit/>
14. Лізунов, С.І. Прихований майнінг та захист від нього / С.І. Лізунов, М.П. Верещака // Тижень науки. Тези доповідей науково-практичної конференції, Запоріжжя, 16–20 квітня 2018 р. [Електронний ресурс] / Редкол. : В. В. Наумик (відпов. ред.) Електрон. дані. – Запоріжжя : ЗНТУ, 2018. – 1 електрон. опт. диск (DVD-ROM); 12 см. – Назва з тит. екрана, с. 910-911.
15. В украинском приложении VPN нашли майнинговый вирус – Режим доступу: <http://mignews.com.ua/society/19587813>
16. Как обезопасить себя от скрытого майнинга криптовалют [Електронний ресурс]. – Режим доступу: <https://tjournal.ru/59579-kak-obezopasit-sebya-ot-skrytogo-mayninga-kriptovalyut>
17. Лізунов, С.І. Аналіз брандмауерів на захищеність / С.І. Лізунов, М.П. Верещака // Матеріали Всеукраїнського науково-

практичного семінару "Використання сучасних інформаційних технологій в діяльності Національної поліції України". 24 листопада 2017 року - Дніпро: Державний університет внутрішніх справ, 2017. – С. 80-81.

18. Методичні вказівки до виконання економічного розділу дипломних та магістерських проектів для студентів спеціальності 7.05090301, 8.05090301 «Інформаційні мережі зв'язку» всіх форм навчання. / Укладачі: Бобровникова Р.Г., Круглікова В.В. – Запоріжжя: ЗНТУ, 2012 – 18 С.

19. Методичні вказівки до практичної роботи «Визначення повітрооб-міну у виробничих та адміністративних приміщеннях» з дисципліни «Охоро-на праці в галузі» для студентів всіх форм навчання / Укл. О.Л. Скуйбіда – Запоріжжя: ЗНТУ, 2011. – 18 с.

20. Методичні вказівки до виконання розділу «Охорона праці та безпека у надзвичайних ситуаціях» у дипломних проектах (роботах) студентів спеціальностей 7(8).05090101 «Радіотехніка», 7(8).05090301 «Інформаційні мережі зв'язку», 7(8).05080101 «Мікро- та наноелектронні прилади і при-строї», 7.18010010 «Якість, стандартизація та сертифікація», 7(8).05090201 «Радіoeлектронні апарати та засоби», 7(8).05090203 «Інтелектуальні техно-логії мікросистемної радіoeлектронної техніки», 7(8).17010201 «Системи те-хнічного захисту інформації, автоматизація її обробки», 7(8).17010101 «Безпека інформаційних і комунікаційних систем» усіх форм навчання / Укл.: О.В. Коробко, А.Є. Островська – Запоріжжя: ЗНТУ, 2014. – 22 с.