Лабораторна робота №14

ДОСЛІДЖЕННЯ МЕТОДІВ, ЗАСОБІВ ТА ТЕХНОЛОГІЙ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Мета – провести дослідження щодо технічного захисту інформації у визначеному призначенні. Провести аналіз об'єкту захисту, виявити канали витоку інформації та визначити засоби захисту інформації.

ТЕОЕРЕТИЧНІ ВІДОМОСТІ

1. Загальні теоретичні відомості

Одним з напрямків захисту інформації в інформаційних системах є технічний захист інформації (ТЗІ). У свою чергу, питання ТЗІ розбиваються на два великих класи завдань: захист інформації від несанкціонованого доступу (НСД) і захисту інформації від витоку технічними каналами. Під НСД звичайно мається на увазі доступ до інформації, що порушує встановлену в інформаційній системі політику розмежування доступу. Під технічними каналами розглядаються канали сторонніх електромагнітних випромінювань і наведень (ПЕМІН), акустичні канали, оптичні канали й ін.

Захист від НСД може здійснюватися в різних складових інформаційної системи:

- прикладне й системне ПЗ;
- апаратна частина серверів і робочих станцій;
- комунікаційне устаткування й канали зв'язку;
- периметр інформаційної системи.

Для захисту інформації на рівні прикладного й системного ПЗ використовуються:

- системи розмежування доступу до інформації;
- системи ідентифікації й аутентифікації;
- системи аудиту й моніторингу;
- системи антивірусного захисту.

Для захисту інформації на рівні апаратного забезпечення використовуються:

- апаратні ключі;
- системи сигналізації;
- засоби блокування пристроїв і інтерфейсів вводу-виводу інформації.

У комунікаційних системах використовуються наступні засоби мереженого захисту інформації:

- міжмережеві екрани (Firewall) – для блокування атак із зовнішнього середовища (Cisco PIX Firewall, Symantec Enterprise FirewallTM, Contivity Secure Gateway і Alteon Switched Firewall від компанії Nortel Networks). Вони управляють проходженням мереженого трафіка відповідно до правил (policies) безпеки. Як правило, міжмережеві екрани встановлюються на вході мережі й розділяють внутрішні (частки) і зовнішні (загального доступу) мережі;

- системи виявлення вторгнень (IDS - Intrusion Detection System) – для виявлення спроб несанкціонованого доступу як ззовні, так і усередині мережі, захисту від атак типу "відмова в обслуговуванні" (Cisco Secure IDS, Intruder Alert і NetProwler від компанії Symantec). Використовуючи спеціальні механізми, системи виявлення вторгнень здатні запобігати шкідливим діям, що дозволяє значно знизити час простою в результаті атаки й витрати на підтримку працездатності мережі;
- засоби створення віртуальних приватних мереж (VPN - Virtual Private Network) – для організації захищених каналів передачі даних через незахищене середовище (Symantec Enterprise VPN, Cisco IOS VPN, Cisco VPN concentrator). Віртуальні приватні мережі забезпечують прозоре для користувача з'єднання локальних мереж, зберігаючи при цьому конфіденційність і цілісність інформації шляхом її динамічного шифрування;
- засоби аналізу захищеності – для аналізу захищеності корпоративної мережі й виявлення можливих каналів реалізації погроз інформації (Symantec Enterprise Security Manager, Symantec NetRecon). Їхнє застосування дозволяє запобігти можливим атакам на корпоративну мережу, оптимізувати витрати на захист інформації й контролювати поточний стан захищеності мережі.

Для захисту периметра інформаційної системи створюються:

- системи охоронної й пожежної сигналізації;
- системи цифрового відеоспостереження;
- системи контролю й керування доступом (СККД).

Захист інформації від її витоку технічними каналами зв'язку забезпечується наступними засобами й заходами:

- використанням екранованого кабелю й прокладкою проводів і кабелів в екранованих конструкціях;
- установкою на лініях зв'язку високочастотних фільтрів;
- побудовою екранованих приміщень ("капсул");
- використанням екранованого устаткування;
- установкою активних систем зашумлення.

Необхідно провести дослідження приміщення в якому проводяться переговори і робота з документами в твердому і електронному вигляді, дати оцінку захищеності об'єкту від витоку інформації по технічних каналах і сформувати рекомендації по захисту інформації на об'єкті.

2. Просторова і структурна моделі приміщення переговорів

Під кімнатою, приміщенням розуміється службове приміщення, у якому ведуться розмови (переговори) конфіденційного характеру, рис.14.1.

Тут мова йде про службові приміщення, у яких відсутні які-небудь технічні засоби обробки (передачі) конфіденційної інформації. До таких

приміщень ставляться, насамперед, кімнати для переговорів на фірмах, де ведуться ділові переговори, що містять конфіденційну інформацію.

Слід зазначити, що переговірні кімнати використаються всі частіше і на сьогодні вони є практично невід'ємним атрибутом фірми. Тому буде цікаво розглянути питання забезпечення безпеки інформації у виділених приміщеннях, маючи на увазі, насамперед, кімнати для ведення переговорів.

По-перше, необхідно зрозуміти основну мету і завдання захисту, тому що правильне з'ясування мети і завдань захисту визначить надалі состав комплексу проведених заходів, їхня вартість і ефективність захисту в цілому.

Оскільки при роботі обробляється інформація, що носить конфіденційний характер (відомості про осіб, факти, події і інше, таке, що стосується фінансової діяльності підприємства), то можна зробити висновок про незаперечну необхідність побудови системи захисту даного приміщення.

Клас захищеності автоматизованої системи від несанкціонованого доступу до інформації згідно керівному документу Державної технічної комісії при Президенті України «Класифікація автоматизованих систем і вимог по захисту інформації»: 3Б.

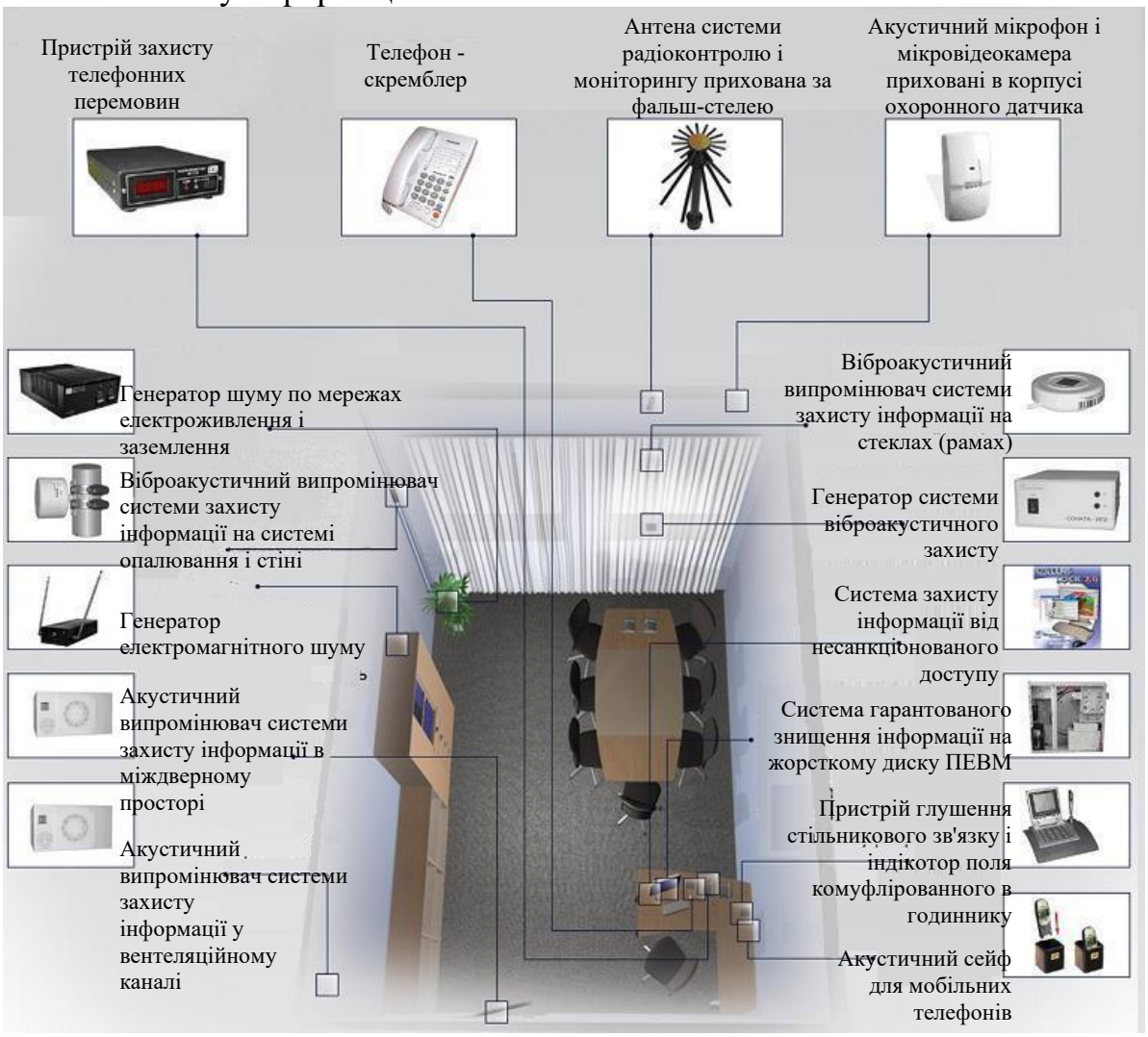

Рисунок 14.1. – Схема комплексу рішень по захисту кімнат переговорів, кабінетів керівників, службових приміщень від просочування конфіденційної інформації по технічних каналах

Виділене приміщення знаходиться на четвертому поверсі будівлі. Схема комплексу рішень по захисту кімнат переговорів, кабінетів керівників, службових приміщень від просочування конфіденційної інформації по технічних каналах представлений на рисунку 1. Розміри приміщення: висота 3,5 метра, ширина 6 метрів, довжина 9 метрів. Приміщення знаходиться в межах контрольованої зони, відстань до межі якої не менше 40 метрів. Приміщення має одне вікно, яке виходить на внутрішню частину території. Двері виходять в коридор, в якому можуть знаходитися як працівники самої організації, так і сторонні люди.

Меблі кімнати складаються з двох столів (один стіл керівника, один стіл для переговорів), восьми стільців. Так само в приміщенні знаходиться шафа, три полки під документи, сейф та прилади захисту інформації, таблиця 14.1.

Таблиця 14.1 - Перелік меблів і побутових приладів, встановлених в кабінеті

Найменування	Кількість, шт.	Обліковий номер
Стіл робочий	1	006
Стіл для нарад	1	007
Стільці	8	008-015
Комп’ютер	1	016
Шафа	1	017
Полка для документів	3	018-020
Сейф	1	021

Всі стіни виконані з червоної цеглини загальною товщиною 200 мм лівої і правої стін і 400 мм стіна, що виходить в коридор і на вулицю. Всі три стіни обштукатурені і пофарбовані з обох боків. Приміщення обладнане двома батареями опалення радіаторного типу. Притока води по батареях здійснюється з приміщення, розташованого над контрольованим приміщенням, а стік з батарей здійснюється по трубах в приміщення за стіною №2. Зліва від входу за стіною №1 знаходиться допоміжне приміщення, яке є власністю організації, але доступ в нього мають сторонні люди. За стіною №2 знаходиться праворуч від входу приміщення №404. Це приміщення, так само як і попереднє, належить організації. Там знаходиться аудиторія.

Двері в приміщенні звукоізольовані, подвійні із зазором більше 200 мм, габарити 1500×2300 мм.

Вікно має подвійне скління, при цьому відстань між шибками дорівнює 57 мм, товщина скла 5 мм. Розмір отвору: 2200×1200 мм. Візуальному огляду виділеного приміщення ззовні (через вікно) перешкоджають жалюзі.

Перекриття – стеля і підлога виконані з бетонних плит з круглими порожнечами, 220 мм. На підлозі постелений паркет. Оскільки будівля чотириповерхова, то над стелею приміщення, що захищається, горище, вхід в який закритий на замок. Приміщення під підлогою є аудиторія.

Отвір припливної вентиляції знаходиться відразу при вході (зліва від дверей), а другий отвір в кінці цієї ж стіни (також ліворуч від дверей). Діаметр отвору складає 20 сантиметрів.

У мережу електроживлення подається напруга 220 В з постійною промисловою частотою 50 Герц. Офіс, що захищається, обладнаний дванадцятьма розетками.

Проаналізувавши приведені вище початкові дані, вивчивши теоретичні, аналітичні матеріали, а так само нормативні і керівні документи в даній області захисту інформації, потрібно скласти план проведення робіт на об'єкті, визначити склад заходів і їх послідовність, виробити вимоги до спеціальних технічних засобів, які використовуватимуться для дослідження об'єкту. Далі потрібно привести результати обстеження об'єкту, на їх підставі зробити висновки про захищеність досліджуваного приміщення і сформувати рекомендації по захисту.

В ході обстеження приміщення потрібно перевірити всю радіоелектронну апаратуру, предмети меблів і інтер'єру, що несуть конструкції, системи комунікації на наявність закладених пристроїв (ЗП). Провести дану перевірку слід в два етапи:

– візуальний огляд;
– пошук ЗП з використанням спеціального устаткування.

Для захисту від несанкціонованого доступу співробітників фірми і сторонніх осіб в неробочий час, приміщення обладнане дверима із замком і охоронною сигналізацією. Так само пожежна і охоронна сигналізації виведені на пульт чергового. Черговий знаходитися при вході в будівлю. Пульт чергового обладнаний світловою і звуковою індикацією, і у разі спрацьовування сигналізації спалахує відповідна лампа і подається звуковий сигнал високих частот.

Основна мета забезпечення безпеки конфіденційної інформації в переговірних кімнатах - виключити доступ до її змісту при проведенні переговорів (розмов), рис.14.2.

.

Рисунок 14.2 – Завдання забезпечення безпеки конфіденційної інформації в кімнаті для переговорів

Першорядними завданнями забезпечення безпеки інформації (рисунок 14.2.) є:

– захист інформації від витоку по акустичному каналі (АК);
– захист інформації від витоку по віброакустичному каналу (ВАК);
– захист інформації від витоку за рахунок електроакустичного перетворення (ЕАП);
– захист інформації від витоку за рахунок високочастотного нав'язування (ВЧН);
– захист інформації від витоку по оптичному каналі (ОК).

Усвідомивши основну мету і завдання захисту інформації, можна перейти до розробки моделі погроз для конфіденційної інформації, що мають місце при веденні переговорів (розмов). Моделі погроз доцільно розробляти, погодившись із завданнями захисту.

Модель погроз для інформації через акустичний канал витоку

Несанкціонований доступ до конфіденційної інформації з акустичного каналу витоку (рисунок 14.3.) може здійснюватися:

Рисунок 14.3 – Несанкціонований доступ до конфіденційної інформації з акустичного каналу витоку

Модель погроз для інформації через віброакустичний канал витоку Несанкціонований доступ до вмісту переговорів (розмов) зловмисниками

може бути також здійснений (рисунок 14.4.) за допомогою стетоскопів і гідроакустичних датчиків.

Рисунок 14.4 – Несанкціонований доступ до вмісту переговорів

За допомогою стетоскопів можливе прослуховування переговорів через стіни товщиною до 1 м 20 см (залежно від матеріалу).

Залежно від виду каналу передачі інформації від самого вібродатчика стетоскопи підрозділяються на:

- провідні (провідний канал передачі);
- радіо - (канал передачі по радіо);
- інфрачервоні (інфрачервоний канал передачі).

Не виключена можливість використання і гідроакустичних датчиків, що дозволяють прослуховувати розмови в приміщеннях, використовуючи труби водопостачання і опалення. Правда, випадки застосування таких пристроїв на практиці дуже рідкі.

Модель погроз для інформації за рахунок електроакустичного перетворення і гетеродинного встаткування

Витік конфіденційної інформації при веденні переговорів (розмов) можлива через вплив звукових коливань на елементи електричної схеми деяких технічних засобів обробки інформації, що одержали в літературі назва "Допоміжні засоби".

До допоміжних засобів ставляться ті, які особистої участі в обробці конфіденційної інформації не приймають, але можуть бути причиною її витоку. Доступ до змісту переговорів (розмов) може бути здійснений на значному видаленні від приміщення, що становить у деяких випадках сотні метрів, залежно від виду каналу витоку (рисунок 14.5.).

Рисунок 14.5 – Доступ до конфіденційної інформації в залежності від виду каналу витоку

Подібні канали витоку існують при наявності в приміщеннях телефонних апаратів з дисковим номеронабирачем, телевізорів, електричних годин, підключених до системи годинофікації, приймачів і т.д.

Причому у випадку з телефонними апаратами і електричними годинниками витік інформації здійснюється за рахунок перетворення звукових коливань в електричний сигнал, що потім поширюється по провідних лініях (телефонним або по проводам системи годинофікації). Доступ до конфіденційної інформації може здійснюватися шляхом підключення до цих ліній.

Що стосується телевізорів і приймачів, то витік конфіденційної інформації відбувається тут за рахунок наявних у них гетеродинів (генераторів частоти). Причина витоку - модуляція звуковим коливанням при веденні розмови несучої частоти гетеродина, просочування її в систему з наступним випромінюванням у вигляді електромагнітного поля.

Модель погроз для інформації з оптичного каналу і за рахунок високочастотного нав'язування

Якщо переговори ведуться в кімнаті, вікна якої не обладнані шторами або жалюзі, то в цьому випадку в зловмисника є можливість за допомогою оптичних приладів з більшим посиленням (біноклів, підзорних труб) переглядати приміщення. Сутність прослуховування переговорів за допомогою високочастотного нав'язування складається в підключенні до телефонної лінії генератора частоти і наступного прийому "відбитого" від телефонного апарата промодельованого розмовою, що ведеться в кімнаті, сигналу.

Таким чином, аналіз погроз для конфіденційної інформації, які мають місце при веденні переговорів (розмов) показує, що якщо не прийняти мір захисту, те можливий доступ зловмисників до її змісту.

3. Рекомендації із захисту

Перш ніж перейти до мір захисту, можна обрисувати загалом модель зловмисника.

Передбачуваний зловмисник – це люди добре підготовлені, знаючі всі канали витоку інформації в кімнатах для ведення переговорів, що професійно володіє способами і засобами добування відомостей, що містять конфіденційну інформацію. Тому необхідно розробити і реалізувати комплекс заходів, що забезпечують надійний захист під час ведення переговорів (розмов).

1. Особливо важливий вибір місця для переговірної кімнати. Її доцільно розмістити по можливості на верхніх поверхах. Бажано, щоб кімната для переговорів не мала вікон або ж вони виходили у двір.
2. У кімнаті для переговорів не повинне бути телевізорів, приймачів, ксероксів, електричних годин, системи годонофікації, телефонних апаратів.
3. Вхід у переговірну кімнату повинен бути обладнаний тамбуром, а внутрішня сторона тамбура оббита звукоізоляційним матеріалом. Необхідно пам'ятати, що незначна щілина (одиниці міліметрів) багаторазово знижує звукоізоляцію.
4. При наявності в кімнаті для переговорів вентиляційних каналів потрібно подбати, щоб вони були обладнані спеціальними ґратами, що дозволяють закривати отвір вентиляційного каналу при веденні переговорів і відкривати його, коли переговори не ведуться.
5. Якщо в переговірній є вікна, то повинні бути вжиті наступні заходи обережності:
   - Проводити переговори при закритих кватирках.
   - На вікнах повинні бути штори або жалюзі.
   - Шибки повинні бути обладнані вібродатчиками.
6. При наявності в переговірної телефонного апарата повинні бути вжиті наступні заходи захисту. У телефонних апаратах з дисковим номеронабирачем вимагає захисту дзвінковий ланцюг. Тому доцільно використати фільтр "Корунд-М", що забезпечує загасання сигналу витоку порядку 80 дБ. Для захисту від високочастотного нав'язування рекомендується підключити паралельно мікрофону (для будь-яких телефонних апаратів) конденсатор ємністю С = 0,01 - 0,05 мкФ. На практиці можуть зустрічатися і більше складні схеми захисту дзвінкового і мікрофонного ланцюга телефонних апаратів.
7. Для захисту від провідних мікрофонів, що використають для передачі інформації мережа електроживлення в 220 В, рекомендується використати генератор типу " Соната-С1", що має гарні тактико-технічні характеристики і ефективно виконує функції захисту.
8. Для захисту переговірних від спеціальних технічних засобів добре скористатися генератором віброакустичного шуму "Соната-АВ" і генератором радіоперешкод "Барикада-1". Генератор віброакустичного шуму "Соната-АВ" захищає від:

- безпосереднього підслуховування в умовах поганої звукоізоляції;
- застосування радіо і провідних мікрофонів, установлених у порожнинах стін, надстельному просторі, у вентиляційних проходах і т.д.;
- використання стетоскопів, установлених на стінах, стелях, підлогах, трубах водо і теплопостачання і т.д.;
- застосування лазерних і інших типів спрямованих мікрофонів.

Генератор радіошуму "Барикада-1" забезпечує захист переговорів від всіх радіозакладок, створюючи в крапці прийому зловмисником перевищуючого рівня перешкоди над рівнем випромінюваного радіозакладкой сигналу.

Важливий також контроль над станом безпеки конфіденційної інформації в переговірних кімнатах, що здійснюється при періодичному проведенні спецобстежень і атестацій. По закінченні складається акт спецобстеження і атестат відповідності.

Таким чином, запропоновані нами рекомендації дозволять забезпечити безпека переговорів, проведених у спеціально виділені для цієї мети приміщеннях.

ЗАВДАННЯ ДО ВИКОНАННЯ

1.3.Провести дослідження приміщення з метою оформлення опитувального листа.

Необхідно захистити мовну інформацію в приміщенні, призначеному для проведення конфіденційних переговорів. Забезпечити аудіо-відео протоколізацію переговорів, що проводяться в приміщенні.

Загальні відомості про приміщення.

Призначення приміщення:
Міра конфіденційності (секретності) інформації, що заявляється:
Поверх:
Площа (кв. м), висота стель (м):
Перекриття (потовк, пів), товщина (мм):
Стінні перегородки:
Стіни зовнішні:
Вікна:
Двері:
Опис суміжних приміщень:
Система електроживлення (освітлення):
Система заземлення:
Системи сигналізації (тип):_
Система вентиляції (тип):
Система опалення:

Телефонні лінії:
Інші дротяні лінії:
Засоби зв'язку:
Оргтехніка:
Побутова техніка:
Спеціальні технічні засоби захисту інформації:
Опис обстановки довкола об'єкту:

1.4.Описати та представити склад та опис виявлених функціональних каналів витоку інформації.
1.5.Визначити можливості порушника по перехопленню мовної інформації.
1.6. На підставі проведеного аналізу представити вимоги до системи захисту інформації.
1.7. Представити опис трьох засобів зняття інформації.
1.8. Представити опис трьох засобів для захисту приміщення від витоку мовної інформації.
1.9. Оформити звіт на надіслати на пошту викладачу.