Завдання №5

1. Об’єкти захисту інформації (ЗІ) та технічні канали її витоку;

2. Захист каналів зв’язку;

3. Пасивні та активні методи ЗІ;

4. Принципи витоку інформації по телефонних каналах зв’язку.

1)Технічний канал витоку інформації – сукупність джерел небезпечного сигналу, середовища поширення небезпечного сигналу та засобу технічної розвідки

Об’єктами захисту інформації є – інформаційні ресурси, котрі несуть відомості, що можуть відноситись до державної таємниці та конфіденційної інформації;

-тзпі;

-дтзс;

-Виділені приміщення;

За фізичним принципом технічні канали витоку інформації можуть бути класифіковані за групами:

- акустичні (включаючи акустоперетворювальні);

- візуально-оптичні (фотографування);

- електромагнітні (а також з розподілом на електричні і магнітні окремо);

- матеріальні (папір, фото.).

3) Технічні заходи – це заходи з захисту інформації, котрі передбачають використання спеціальних технічних засобів, а також реалізацію технічних рішень.

ТЗІ поділяється на методи ативного (підвищення рівня завад) та пасивного (зниження рівня небезпечних сигналів) (захисту інформації та спецдослідження

До технічних заходів з використанням пасивних засобів відносяться:

-контроль та обмеження доступу на об’єкти ТЗПІ та виділені приміщення (встановлення на об’єктах ТЗПІ та у виділених приміщеннях технічних засобів та систем обмеження і контролю доступу).

- екранування;

-зниження потужності випромінювань і наведень;

- зниження інформативності сигналів.

-локалізація випромінювання( екранування ТЗПІ , заземлення ТЗПІ ,звукоізолювання)

Залежно від типу створюваного електромагнітного поля розрізняють наступні види екранування:

• екранування електричного поля (електростатичне);

• екранування магнітного поля (магнітостатичне);

• екранування електромагнітного поля.

До активних методів

-просторове зашумлення( зашумлення з використанням генераторів шуму або створення прицільних завад ,створення акустичних і вібраційних завад

-лінійне зашумлення

-знешкодження закладних пристроїв.

При локальному просторовому зашумленні використовуються прицільні перешкоди. Антена перебуває поруч із елементом, що захищається. Об'єктове просторове зашумлення здійснюється, як правило, декількома генераторами зі своїми антенами, що дозволяє створювати перешкоди у всіх діапазонах побічних електромагнітних випромінювань усіх випромінюючих пристроїв об'єкта.

Просторове зашумлення повинне забезпечувати неможливість виділення побічних випромінювань на тлі створюваних перешкод у всіх діапазонах випромінювання й, разом з тим, рівень створюваних перешкод не повинен перевищувати санітарних норм і норм по електромагнітній сумісності радіоелектронної апаратури.

4) Методи:

-акустичні телефонні закладки для передавання інформації по телефонних лініях зв’язку на підвищених частотах

-акустичні телефонні закладки типу “електронне вухо” для передавання інформації пр телефонній лінії “телефону-наглядачу” на низькій частоті.

-безпосереднє підключення до лінії ( найпростіший спосіб)

-прослуховування приміщення за допомогою вч нав’язування телефонного апарату, коли він стає модулятором сигналу

-зворотнє перетворювання

- якщо при пошкодженні кабеля зберігається відстань в 1 м, то кінці кабеля стають

конденсатором і можна буде прослухувати зв'язок (тому кабель треба класти в шкаф\_)

2) Канал — частина [комунікаційної системи](https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D1%83%D0%BD%D1%96%D0%BA%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D0%B0" \o "Комунікаційна мережа), яка зв'язує між собою [джерело та приймач](https://uk.wikipedia.org/wiki/%D0%9A%D1%96%D0%BD%D1%86%D0%B5%D0%B2%D0%B5_%D1%83%D1%81%D1%82%D0%B0%D1%82%D0%BA%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F_%D0%BB%D1%96%D0%BD%D1%96%D1%97_%D0%B7%D0%B2%27%D1%8F%D0%B7%D0%BA%D1%83) повідомлень. В каналах зв’язку мають місце як природні, так і штучні перешкоди і впливи. Для боротьби з природними завадами використовують методи завадостійкого кодування з детектуванням та виправленням помилок. Боротьба зі штучними впливами здійснюється різними методами, зокрема шифруванням даних, а також застосуванням квантових принципів, чутливих до несанкціонованого доступу. Квантові методи у криптографії знаходяться у стадії активного розвитку. Однією з актуальних задач квантової криптографіє є збільшення швидкодії квантових каналів зв’язку.

Основною одиницею прийому-передачі даних на канальному рівні є символи або блоки символів. Найпростішим символом передачі даних є біт. Сучасні телекомунікаційні системи використовують більші символи, що містять від 2 до 64 біт і більше. Головна мета боротьби з природними перешкодами в каналі зв'язку - це підвищення достовірності інформації що передається, тобто обмеження ймовірності прийому помилкового символу. Для цього застосовують т.зв. надлишкове кодування, при якому на передавальній стороні змістовні блоки символів відображаються в розширені блоки передачі, аналіз яких на приймальній стороні каналу дозволяє виявити або виправити помилки певних типів. Для захисту інформації в каналі зв'язку від несанкціонованого доступу типу «прослуховування» використовують різні методи криптографії (шифрування даних): заміна (підстановка) символів, перестановка, аналітичні перетворення шифрованих даних та інші. Поширений метод шифрування - це заміна переданих символів на символи з того ж самого алфавіту, здійснювана по секретним таблицям шифрування. На основі цього методу можна побудувати алгоритм, який в принципі не піддається дешифруванню при відсутності таблиці шифрування. Для цього достатньо, щоб множина символів підстановки утворювала випадкову послідовність довжиною не менше переданого повідомлення (з однаковою ймовірністю всіх символів підстановки і незалежністю між будь-якою парою символів підстановки). Обмеження такого методу шифруванняобумовлені технічними можливостями створення, обміну та зберігання таблиць шифрування великих розмірів. Підвищення швидкості передачі і зменшення енергії на одиницю інформації в оптичних каналах обумовлює появу квантових ефектів, пов'язаних з нечіткою ідентифікацією прийнятих символів. З точки зору детектора сигналу, один і той символ (наприклад, один біт), що генерується на передавальній стороні каналу, може перебувати в двох станах (нуль і одиниця). При цьому відносні частоти появи нулів і одиниць наближаються до можливостям їх появи. Однак при однаковій фізичній швидкості передавання символів, збільшення надмірності переданих блоків символів призводить до зниження кількості корисної інформації. При цьому зменшується ймовірність помилок; це, в свою чергу, дозволяє збільшити фізичну швидкість передачі. В результаті взаємного впливу цих факторів може бути досягнуто загальне підвищення ефективності передавання корисної інформації.

Захист інформації, що оброблюється ТЗПІ, здійснюється з використанням пасивних та

активних методів та засобів.

Пасивні методи захисту направлені на:

-ослаблення інформаційних сигналів ТЗПІ на межі зони що контролюється до рівнів,

унеможливлюючих їх виділення засобами розвідки на шумовому фоні;

-ослаблення наведень побічних електромагнітних випромінювань ТЗПІ на сторонні

провідники та з’єднувальні лінії ДТЗС, що виходять за межі зони що контролюється

до рівнів, унеможливлюючих їх виділення засобами розвідки на шумовому фоні;

-виключення (ослаблення) просочування інформаційних сигналів ТЗПІ до мереж

живлення що виходять за межі зони що контролюється до рівнів, унеможливлюючих

їх виділення засобами розвідки на шумовому фоні;

Активні методи захисту спрямовані на:

-створення просторових маскуючих електромагнітних завад з ціллю зменшення

відношення сигнал/завада на межі зони що контролюється до рівнів,

унеможливлюючих їх виділення засобами розвідки на шумовому фоні;

-створення маскуючих електромагнітних завад у сторонніх провідниках та

з’єднувальних лініях ДТЗС з ціллю зменшення відношення сигнал/завада на межі зони

що контролюється до рівнів, унеможливлюючих їх виділення засобами розвідки на

шумовому фоні;