2) 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 шифрування Комп’ютерні мережеві технології 74 обумовлені 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. Властивості каналу зв'язку з квантовими ефектами визначаються матрицею ймовірностей

Pi,k = p(i,k), де i - значення переданого символу, j - значення прийнятого символу.

Ця матриця є чутливою до змін фізичних властивостей каналу, наприклад, при несанкціонованому доступі до каналу матриця зміниться в тій чи іншій мірі. Дана матриця є унікальною характеристикою каналу зв'язку, яка може бути досліджена в метрологічному експерименті, а далі використана для детектування сигналів та виявлення несанкціонованого доступу. Квантові методи у криптографії поки що знаходяться у стадії активного розвитку. Однією з основних проблем у квантовій криптографії є підвищення швидкості передачі даних на великі відстані.

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

активних методів та засобів.

Пасивні методи захисту направлені на:

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

унеможливлюючих їх виділення засобами розвідки на шумовому фоні;

2)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;

3)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:

3)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;

4)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;

1) Під технічними каналами розглядаються канали побічних електромагнітних випромінювань і наводок -**ПЕМВН.** Захист інформації від витоку за рахунок ПЕМВН ‑ це комплекс заходів, що виключає або суттєво знижує вірогідність витоку інформації з обмеженим доступом за межи контрольованої зони.

Усі методи захисту від ПЕМВН можна розділити на пасивні й активні.Пасивні методи забезпечують зменшення рівня небезпечного (інформативного) сигналу або зниження його інформативності.

Активні методи захисту спрямовані на створення електромагнітних завад, що утрудняють приймання й виділення корисної інформації з перехоплених порушником сигналів.

Пасивні методи захисту від ПЕМВН можуть бути розбиті на три групи:

• екранування;

• зниження потужності випромінювань і наведень;

• зниження інформативності сигналів.

Екранування є одним з найефективніших методів захисту від електромагнітних випромінювань. Під екрануванням розуміється розміщення елементів автоматизованої системи, що створюють електричні, магнітні й електромагнітні поля, у просторово замкнених конструкціях. Способи екранування залежать від особливостей полів, що створюються елементами системи при протіканні в них електричного струму.

Залежно від типу створюваного електромагнітного поля розрізняють наступні види екранування:

• екранування електричного поля (електростатичне);

• екранування магнітного поля (магнітостатичне);

• екранування електромагнітного поля.

Екранування дозволяє не тільки захистити обладнання автоматизованих систем від випромінювання власних небезпечних сигналів, а й зменшити ризик небажаного впливу зовнішніх електромагнітних та акустичних полів.

До групи, що забезпечує зниження потужності випромінювань і наведень, ставляться наступні методи:

• зміна електричних схем пристроїв;

• використання оптичних інтерфейсів – оптичних перетворювачів сигналів;

• зміна конструкції пристроїв;

• використання фільтрів;

• гальванічні розв'язки в системі електроживлення.

Зменшення потужності побічних випромінювань шляхом змін електричних схем передбачає використання електро- і радіоелементів з меншим випромінюванням, уникнення регулярності повторень в інформаційних сигналах, зміна форми (крутизни фронтів) сигналів, запобігання виникненню паразитної генерації.

Ефективним напрямом подолання ПЕМВН є використання оптичних каналів зв'язку. Волоконно-оптичні кабелі успішно використовуються для передачі інформації на великі відстані, практично не маючі (у разі правильної прокладки) каналів витоку. Вони забезпечують високу швидкість передачі й не піддані впливу електромагнітних перешкод. Крім того, передачу інформації в межах одного приміщення, навіть великих розмірів, можна здійснювати за допомогою бездротових систем, що використовують випромінювання в інфрачервоному діапазоні.

Використання фільтрів є одним з основних способів захисту від ПЕМВН. Фільтри є пристроями на основі різних електричних компонентів, які встановлюються або усередині пристроїв та систем для усунення поширення й можливого посилення наведених побічних електромагнітних сигналів, або на виході у напряму ліній зв'язку, сигналізації та електроживлення. Фільтри розраховуються таким чином, щоб вони забезпечували зниження сигналів у діапазоні побічних наведень до безпечного рівня й не вносили істотних викривлень корисного сигналу.

Повністю виключається влучення побічних наведених сигналів у зовнішній ланцюг електроживлення у разі використання джерел живлення, у яких реалізована гальванічна розв'язка між первинним та вторинним ланцюгами.

Зниження інформативності сигналів ПЕМВН, що утрудняє їхнє використання при перехопленні, реалізується шляхом застосування:

• спеціальних схемних рішень;

• кодування інформації.

У якості прикладів зниження інформативності сигналів можна привести такі, як заміна послідовного коду оброблення інформації паралельним, збільшення розрядності паралельних кодів, зміна черговості розгорнення рядків на моніторі тощо. Ці заходи утрудняють процес одержання інформації з перехопленого зловмисником сигналу.

Активні методи захисту від ПЕМВН передбачають застосування електромагнітних генераторів випадкових або псевдовипадкових шумів, які маскують небезпечний сигнал.

**Використовується просторове й лінійне зашумлення.**

Просторове зашумлення здійснюється за рахунок випромінювання за допомогою антен електромагнітних сигналів у простір. Застосовується локальне просторове зашумлення для захисту конкретного елемента системи й об'єктове просторове зашумлення для захисту від побічних електромагнітних випромінювань усього об'єкта.

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.

При використанні лінійного зашумлення генератори прицільних перешкод підключаються до струмопровідних ліній для створення в них електричних перешкод, які не дозволяють зловмисникам виділяти наведені сигнали.