Для захисту інформації, переданої по каналах зв'язку, застосовується комплекс методів і засобів захисту, що дозволяють блокувати можливі загрози безпеки інформації.Найбільш надійним і універсальним методом захисту інформації в каналах зв'язку є шифрування.Шифрування на абонентському рівні дозволяє захистити робочу інформацію від втрати конфіденційності та нав'язування хибної інформації.Лінійне шифрування дозволяє, крім того, захистити службову інформацію. Не маючи доступу до службової інформації, зловмисник не може фіксувати факт передачі між конкретними абонентами мережі, змінити адресну частину повідомлення з метою його переадресації.Протидія неправдивим з'єднанням абонентів (процесів) забезпечується застосуванням цілого ряду процедур взаємного підтвердження автентичності абонентів або процесів. Проти видалення, явного спотворення, переупорядочивания, передачі дублів повідомлень використовується механізм квітірованія, нумерації повідомлень або використання інформації про час відправки повідомлення. Ці службові дані повинні бути зашифровані.

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

-  ослаблення наведень побічних електромагнітних випромінювань на сторонні провідники та з лінії, що виходять за межі зони що контролюється

-  виключення (ослаблення) просочування інформаційних сигналів до мереж живлення що виходять за межі зони що контролюється щоб не можна було виділити з шумів

Активні методи захисту спрямовані на:

- створення маскуючих електромагнітних завад з ціллю зменшення відношення сигнал/завада на межі зони

- створення маскуючих електромагнітних завад у сторонніх провідниках та з’єднувальних лініях з ціллю зменшення відношення сигнал/завада на межі зони