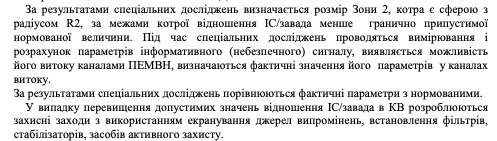
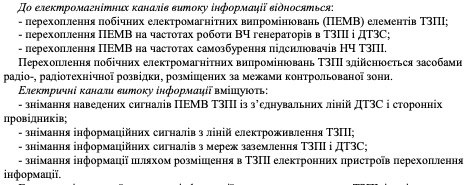
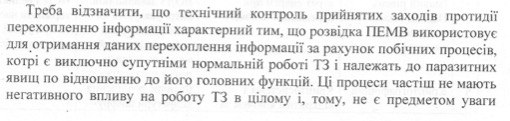
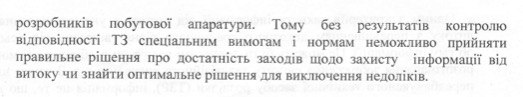
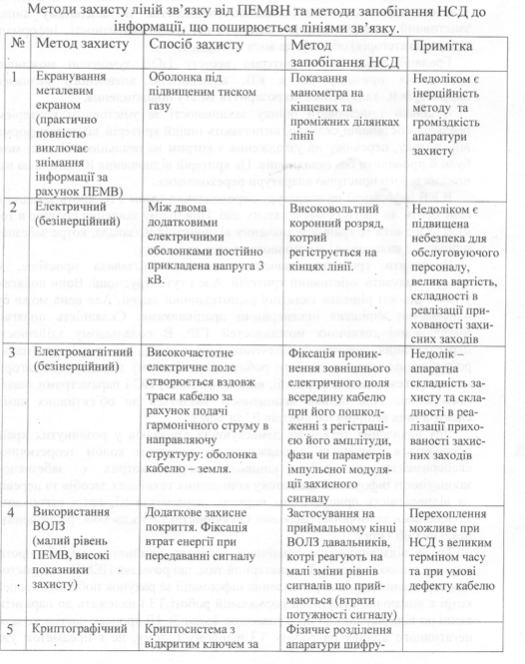
1. ПЕМВН













Методи захисту інформації від витоку по каналу побічних електромагнітних випромінювань та наведень (ПЕМВН) поділяють на ***пасивні*** та ***активні***. ***Пасивні методи захисту*** дозволяють зменшити рівень інформаційної цінності, або рівень випромінювання випромінюючого інформаційного сигналу ПЕМВН. ***Активні методи захисту*** полягають у створенні завад в каналах ПЕМВН, які ускладнюють приймання корисної інформації з перехоплених зловмисником сигналів.

***Пасивні методи захисту.***

Розрізняють три групи пасивних методів захисту:

● екранування;

● зменшення рівня випромінювань та наведень;

● зменшення рівня інформативної цінності сигналів.

Методи ***екранування електромагнітного випромінювання*** є найбільш ефективними методами захисту інформації від ПЕМВН. Вони полягають у розміщенні елементів інформаційної системи, яки створюють електричні, магнітні чи електромагнітні поля в просторово замкнених конструкціях. Способи екранування залежать від особливостей полів, яки виникають в технічних елементах інформаційної системи при проходженні в них електричного струму.

Екранування здійснюється на рівні елементів схем, блоків, засобів, кабельних ліній, приміщень. У залежності від рівня екранування у якості екранів використовуються заземлені металеві, або з металізованим покриттям корпуса, конструкції з листової сталі, металеві сітки та інше.

Методи ***зменшення рівня випромінювань та наведень ПЕМВН*** базуються на удосконаленні електричних схем, використанні оптичних каналів зв’язку, удосконаленні конструкцій, використанні фільтрів, використанні гальванічних розв’язок у схемах живлення та інших.

Методи ***зменшення рівня інформативної цінності сигналів ПЕМВН*** базуються на спеціальних схемних рішеннях та кодуванні інформації. Спеціальні схемні рішення можуть полягати у заміні послідовних кодів на паралельні, збільшенні довжини регістрів та інше.

***Активні методи захисту***

Активні методи захисту інформації від ПЕМВН базуються на використанні маскуючих випадкових завад. Такі завади створюють електронні генератори завад.

Розрізняють ***просторовий та лінійний типи завад***. ***Просторові завади*** виставляють шляхом випромінювання електромагнітних сигналів завад в простір за допомоги антен. ***Лінійні завади*** створюються генераторами завад, яки приєднуються до струмопровідних ліній. Електричні завади в струмопровідних лініях ускладнюють роботу зловмисників.

2. Защита каналов связи

Защита линии связи, выходящих за пределы охраняемых помещений или за пределы всего объекта, представляет собой очень серьезную проблему, так как эти линии чаще всего оказываются бесконтрольными, и к ним могут подключаться различные средства съема информации. Экранирование информационных линий связи между устройствами технических средств передачи информации (ТСПИ) имеет целью, главным образом, защиты линий от наводок, создаваемых линиями связи в окружающем пространстве. Наиболее экономичным способом экранирования является групповое размещение информационных кабелей в экранирующем изолированном коробе. Когда такой короб отсутствует, приходится экранировать отдельные линии связи. Для защиты линий связи от наводок необходимо разместить линию в экранирующую оплетку или фольгу, заземленную в одном месте, чтобы избежать протекания по экрану токов, вызванных неэквипотенциальностью точек заземления. Для защиты линий связи от наводок необходимо минимизировать площадь контура, образованного прямым и обратным проводом линии. Если линия представляет собой одиночный провод, а возвратный ток течет по некоторой заземляющей поверхности, то необходимо максимально приблизить провод к поверхности. Если линия образована двумя проводами, имеет большую протяженность, то ее необходимо скрутить, образовав бифиляры (витую пару). Линии, выполненные из экранированного провода или коаксиального кабеля, по оплетке которого протекает возвратный ток, также должны отвечать требованиям минимизации площади контура линии. Наилучшую защиту одновременно от изменений напряженности электрического и магнитного полей обеспечивают информационные линии связи типа экранированного бифиляра, трифиляра (трех скрученных вместе проводов, из которых один используется в качестве электрического экрана), триаксиального кабеля (изолированного коаксиального кабеля, помещенного в электрический экран), экранированного плоского кабеля (плоского многопроводного кабеля, покрытого с одной или с обеих сторон медной фольгой). Для уменьшения магнитной и электрической связи между проводами необходимо сделать следующее: • уменьшить напряжение источника сигнала или тока; • уменьшить площадь петли; • максимально разнести цепи; • передавать сигналы постоянным током или на низких частотах; • использовать провод в магнитном экране с высокой проницаемостью; • включить в цепь дифференциальный усилитель. Рассмотрим несколько схем защиты от излучения (рис. 16.5). Цепь, показанная на рис. 16.5, а, имеет большую петлю, образованную “прямым” проводом и “землей”. Эта цепь подвергается, прежде всего, магнитному влиянию. Экран заземлен на одном конце и не защищает от магнитного влияния. Переходное затухание для этой схемы примем

равным 0 дБ для сравнения с затуханием, обеспечиваемым схемами, представленными на рис. 16.5, б–и. Схема, представленная на рис. 16.5, б, практически не уменьшает магнитную связь, поскольку обратный провод заземлен с обоих концов, и в этом смысле она аналогична предыдущей схеме (рис. 16.5, а). Степень улучшения соизмерима с погрешностью расчета (измерения) и составляет порядка –2–4 дБ. Следующая схема (рис. 16.5, в) отличается от первой схемы (рис. 16.5, а), наличием обратного провода (коаксиального экрана), однако экранирование магнитного поля ухудшено, так как цепь заземлена на обоих концах, в результате чего с “землей” образуется петля большей площади. Схема, представленная на рис. 16.5, г, позволяет существенно повысить защищенность цепи (–49 дБ) благодаря скрутке проводов. В этом случае (по сравнению со схемой, приведенной на рис. 16.5, б) петли нет, поскольку правый конец цепи не заземлен. Дальнейшее повышение защищенности достигается применением схемы, представленной на рис. 16.5, д, коаксиальная цепь которой обеспечивает лучшее магнитное экранирование, чем скрученная пара (рис. 16.5, г). Площадь петли схемы (рис. 16.5, д), не больше, чем в схеме на рис. 16.5, г, так как продольная ось экрана коаксиального кабеля совпадает с его центральным проводом. Схема, приведенная на рис. 16.5, е, позволяет повысить защищенность цепи благодаря тому, что скрученная пара заземлена лишь на одном конце. Следующая схема (рис. 16.5, ж), имеет ту же защищенность: эффект заземления экрана на одном и том же конце тот же, что и при заземлении на обоих концах, поскольку длина цепи и экрана существенно меньше рабочей длины волны. Причины улучшения защищенности схемы, представленной на рис. 16.5, з, по сравнению со схемой, представленной на рис. 16.5, ж, физически объяснить трудно. Возможно, причиной является уменьшение площади эквивалентной петли. Более понятна схема со скруткой, показанная на рис. 16.5, и, которая позволяет дополнительно уменьшить магнитную связь. Кроме того, при этом уменьшается и электрическая связь.

Для защиты информации, передаваемой АО каналам связи, применяется комплекс методов и средств защиты, позволяющих блокировать возможные угрозы безопасности информации.

Наиболее надежным и универсальным методом защиты информации в каналах связи является шифрование.

Шифрование на абонентском уровне позволяет защитить рабочую информацию от утраты конфиденциальности и навязывания ложной информации.

Линейное шифрование позволяет, кроме того, защитить служебную информацию. Не имея доступа к служебной информации, злоумышленник не может фиксировать факт передачи между конкретными абонентами сети, изменить адресную часть сообщения с целью его переадресации.

Противодействие ложным соединениям абонентов (процессов) обеспечивается применением целого ряда процедур взаимного подтверждения подлинности абонентов или процессов. Против удаления, явного искажения, переупорядочивания, передачи дублей сообщений используется механизм квитирования, нумерации сообщений или использования информации о времени отправки сообщения. Эти служебные данные должны быть зашифрованы.

Интенсивность обмена может быть скрыта путем добавления к рабочему трафику обмена специальными сообщениями.

Попыткам блокировки коммуникационной подсистемы путем интенсивной передачи злоумышленником сообщений или распространения вредительских программ типа с «червь», в подсистеме управления РКС должны быть созданы распределенные механизмы контроля интенсивности обмена и блокирования доступа в сеть абонентов при исчерпании ими лимита активности или в случае угрожающего возрастания трафика. Для блокирования угроз физического воздействия на каналы связи (нарушение линий связи или постановка помех в радиоканалах) необходимо иметь дублирующие каналы с возможностью автоматического перехода на их использование.