***Лекція №9***

***Тема №1: Захист мовної інформації***

**Захист мовної інформації** – діяльність, спрямована на запобігання витоку інформації, яка циркулює у вигляді акустичних хвиль (голосу людини).

Якщо інформація існує у вигляди акустичних хвиль, які створюються за допомогою голосового апарату людини, вона називається **мовною**.

**Мовний сигнал** – складний фізичний процес, пов'язаний зі зміною акустичних параметрів, які містять інформацію про зміст повідомлення. Мовний сигнал створюється голосовим апаратом людини і являє собою обурення повітряного середовища у вигляді хвиль стиснення і розтягнення (акустичні коливання). Енергія мовного сигналу зосереджена в діапазоні 300 - 4000 Гц.

Під впливом акустичних коливань в огороджувальних будівельних конструкціях та інженерних комунікаціях приміщення, в якому знаходиться джерело мовного сигналу, виникають вібраційні коливання.

Таким чином, у своєму первісному вигляді мовний сигнал в приміщенні присутній у вигляді акустичних і вібраційних коливань. Різного роду перетворювачі акустичних і вібраційних коливань є вторинними джерелами.

До них відносяться:

* *гучномовці;*
* *телефони;*
* *мікрофони;*
* *акселерометри тощо*.

Залежно від середовища поширення сигналів і способів їх перехоплення технічні канали витоку мовної інформації можна розділити на: *акустичні, вібраційні (віброакутсичні), акустоелектричні, оптоелектронні і параметричні.*

Інженерно-технічна споруда, яка за функціональним призначенням передбачає обіг інформації з обмеженим доступом (будівлі, приміщення, транспортні засоби тощо) називається **об’єктом інформаційної діяльності** (скорочено – ОІД).

Для захисту мовної інформації від витоку технічними каналами на об’єктах інформаційної діяльності, де циркулює інформація з обмеженим доступом, створюється комплекс технічного захисту інформації (скорочено – КТЗІ або комплекс ТЗІ), якій являє собою сукупність організаційних, інженерних і технічних заходів та засобів,

Акустичні канали витоку інформації можна класифікувати наступним чином:

1. ***Акустичні*** - за рахунок поширення акустичних коливань у вільному повітряному просторі (переговори на відкритому просторі, відкриті двері, вікна, вентиляційні канали);
2. ***Вібраційні*** - за рахунок впливу звукових коливань на елементи і конструкції будівель, викликаючи вібрації (огороджувальні конструкції (стіни, стелі, підлоги, вікна, двері, короба вентиляційних систем тощо), інженерні комунікації (труби водопостачання, опалення, кондиціонування тощо));
3. ***Оптико-електронні (лазерні канали) канали*** - за рахунок приймання та демодуляції відбитого від вібруючих під дією акустичного сигналу поверхонь приміщень (шибок, дзеркал тощо) випромінювання;
4. ***Акустоелектричні*** - за рахунок впливу звукових коливань на ДТЗС (за рахунок зміни параметрів (ємність, індуктивність, опір) під дією акустичного поля, створюваного джерелом мовного сигналу та виникнення електрорушійної сили (ЕРС), або до модуляції струмів, що протікають по цим елементам, за рахунок «мікрофонного ефекту», за рахунок використання «високочастотного електромагнітного нав'язування»);
5. ***Параметричні*** - за рахунок впливу звукових коливань на ОТЗ і ДТЗС (за рахунок паразитної модуляції інформаційним сигналом випромінювань гетеродинів радіоприймальних і телевізійних пристроїв, які перебувають у приміщеннях, де ведуться конфіденційні переговори, за рахунок утворення вторинних радіохвиль, при «при високочастотному опроміненні» приміщення, де встановлені закладні пристрої, що мають елементи, параметри яких змінюються під дією мовного сигналу);
6. ***Через закладні пристрої*** - канали витоку акустичної іфнормації, канали витоку видової інформації\*.

\* під час виявлення закладних пристроїв, як правило, здійснюється комплекс робіт із захисту від витоку мовної та видової інформації, а також радіомаяків (для рухомих об’єктів).

\*\* відповідно до ТР ТЗІ - ПЕМВН-95 (Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань та наводок), затверджених наказом Державної служби України з питань технічного захисту інформації від 09 червня 1995 р. № 25, акустоелектричний та параметричний канали витоку інформації об'єднані і називаються каналами побічних електромагнітних випромінювань та наводок.

При проведенні робіт із технічного захисту інформації одночасно, з використанням одних і тих же приладів, методик та спеціалістів можуть здійснюватися заходи із захисту декількох каналів витоку інформації. Так, при проведенні робіт із захисту інформації від витоку акустичним каналом можуть проводитися роботи із захисту інформації від витоку віброакустичним і оптоелектронним каналами. Аналогічним чином здійснюються роботи із захисту інформації від витоку акустоелектричним та параметричним каналами побічних електромагнітних випромінювань та наводок (канали побічних електромагнітних випромінювань та наводок).

Виходячи з цього види роботи з технічного захисту інформації доцільно проводити за наступними напрямками:

1. ***Захист інформації від витоку акустичним, віброакустичним та оптоелектронним каналами;***
2. ***Захист інформації від витоку акустоелектричними та параметричними каналами;***
3. ***Захист інформації від витоку через закладні пристрої.***

Для захисту мовної інформації з обмеженим доступом від витоку технічними каналами на об’єктах інформаційної діяльності створюється комплекс ТЗІ. Комплекс ТЗІ складається з наступних заходів та засобів, призначених для захисту інформації:

* ***організаційних;***
* ***інженерних;***
* ***технічних.***

Результатом проведення всіх вищеперерахованих заходів є випробування та атестація.

***Випробування комплексу ТЗІ*** – сукупність аналітичних, експериментальних та вимірювальних робіт, які проводяться з метою визначення повноти виконання вимог щодо захисту від витоку інформації з обмеженим доступом технічними каналами, а також перевірки (контролю) повноти та достатності реалізованих заходів із захисту інформації на об'єктах інформаційної діяльності.

***Атестація*** – це, визначення відповідності виконаних робіт зі створення комплексу ТЗІ на об'єкті інформаційної діяльності вимогам нормативних документів з питань ТЗІ.

Під час проведення робіт із захисту інформації від витоку технічними каналами здійснюються наступні етапи:

***1. Категоріювання об’єкта інформаційної діяльності.***

Категоріювання об’єкта інформаційної діяльності або іншими словами встановлення категорії об’єкта - це встановлення класифікаційної характеристики важливості об’єкта, за якою визначається необхідний рівень захисту інформації, що обробляється технічними засобами та/або озвучується на цьому об’єкті.

***2. Обстеження ОІД.***

Обстеження необхідно для підготовки вихідних даних для формування вимог щодо створення комплексу ТЗІ.

Під час обстеження з’ясовуються:

* умови функціонування ОІД, архітектурно-будівельні особливості та особливості розташування його на місцевості відносно меж контрольованої зони (КЗ);
* наявність і порядок роботи технічних засобів, що оброблятимуть ІзОД, та технічних засобів, які не використовують безпосередньо для її оброблення, визначають місця їх розташування на ОІД та їх особливості;
* розташування інженерних комунікацій та металоконструкцій, наявність транзитних, незадіяних кабелів, що виходять за межі КЗ тощо.

***3. Попередні інструментальні дослідження щодо захищеності мовної інформації від витоку технічними каналами.***

Попередні інструментальні дослідження щодо захищеності мовної інформації проводяться з метою оцінки захищеності мовної інформації з обмеженим доступом від витоку технічними каналами без використання засобів активного захисту.

Результати обстеження та попередніх інструментальних досліджень аналізуються і використовуються при визначенні загроз для інформації з обмеженим доступом та обґрунтуванні необхідності впровадження організаційних, інженерних і технічних заходів захисту від витоку ІзОД технічними каналами, у т.ч. прийняття рішення про необхідність встановлення засобів захисту інформації та мінімально необхідну її кількість і склад.

***4. Визначення загроз для інформації з обмеженим доступом.***

Визначення загроз для інформації з обмеженим доступом здійснюється на основі відомостей, викладених в акті категоріювання, акті обстеження ОІД, протоколах попередніх інструментальних досліджень, будівельних схемах, кресленнях тощо.

Можливі загрози для інформації з обмеженим доступом відображаються у Моделі загроз для інформації, яка циркулює на ОІД.

***5. Формулювання технічних вимог до комплексу ТЗІ.***

Формулювання технічних вимог до комплексу ТЗІ здійснюється в технічному завданні на створення комплексу ТЗІ (далі – ТЗ). ТЗ повинне містити наступні вимоги:

* ***загальні вимоги;***
* ***вимоги щодо стійкості до зовнішніх впливів;***
* ***вимоги з безпеки експлуатації;***
* ***вимоги до метрологічного забезпечення;***
* ***вимоги щодо забезпечення охорони державної таємниці;***
* ***вимоги щодо технічного забезпечення виконання робіт;***
* ***вимоги щодо забезпечення безпеки при виконанні робіт;***
* ***вимоги до документації.***

***6. Проведення монтажних/демонтажних робіт, пуско-наладка засобів захисту інформації.***

На цьому етапі здійснюється монтаж технічних засобів захисту інформації, необхідних для забезпечення вимог технічного завдання, а також демонтаж систем, транзитних, незадіяних (повітряних, настінних, зовнішніх та закладених в каналізацію) кабелів, контурів та інших комунікацій застосування яких не обґрунтовано службовою чи виробничою необхідністю.

Якщо, неможливо або недоцільно захищати інформацію пасивними заходами захисту (див. розділ «Захист інформації від витоку акустичним, віброакустичним та оптоелектронним каналами») використовуються активні засоби захисту інформації.
Результати монтажних робіт засобів захисту інформації відображаються у відповідному акті.

***7. Атестація ОІД***

7.1. Складання Програми і методик випробувань.

7.2. Проведення робіт з виявлення закладних пристроїв.

7.3. Проведення робіт з контролю захищеності мовної інформації від витоку за рахунок акустоелектромагнітних та акустоелектричних перетворень в допоміжних технічних засобах і системах.

7.4. Проведення робіт з контролю захищеності мовної інформації від витоку акустичним і віброакустичним каналами на об’єкті інформаційної діяльності.
7.5 Висновки за результатами випробувань. Акт атестації ОІД.

Основні характеристики ОІД відображаються в Паспорті на комплекс технічного захисту інформації.

***Тема №2: Види пристроїв для прослуховування***

 [***Жучок для прослушки***](https://ssbb.ua/poshuk-i-vyyavlennya-proslyshky/poshuk-zakladnykh-ustrojstv/kak-obnaruzhit-zhuchki-dlya-proslushki/) - це електронний пристрій, за допомогою якого можна негласно отримати інформацію, або іншими словами це мікрофон з радіо передавачем, який може передавати звук з приміщення, в яке його непомітно, приховано встановили на великі відстані на радіо приймальний пристрій.

**Пристрої для прослуховування можна розділити на наступні види:**

* GSM жучки;
* Радіо-жучки;
* Міні-диктофони;
* Приховані відеокамери;
* Лазерна прослушка.

GSM-жучок це універсальне і сучасний пристрій нового покоління, яке має більший радіус дії і має об'ємний акумулятор, який дозволить Цей пристрій працювати в режимі очікування від 7 до 10 днів, а в режимі прослуховування від 2 до 4 годин. Основною функцією даного виду жучка для прослушки є моніторинг онлайн, тобто Ви можете чути, що відбувається прямо зараз, "в прямому ефірі". Також GSM-жучок може приймати сигнал на великій відстані - Ви можете перебувати в іншому місті або навіть країні, і все одно зможете контролювати ситуацію. Деякі моделі можуть дзвонити Вам самі при виникненні голосу.

Радіо жучок - це мініатюрне подслушіающее пристрій, яке випромінює сигнал на певну відстань. Залежно від потужності передавача воно може бути від декількох десятків метрів до сотень метрів. Радіо жучок віщає в діапазоні FM частот, так що його можна зловити на звичайному приймачі. Правда, варто брати до уваги, що найкраще використовувати приймач з навушниками, наприклад, телефон з гарнітурою. Тоді найкраще можна буде підібрати потрібну частоту.

У міні-диктофонах запис ведеться на вбудовану (постійну або змінну) пам'ять. Дане підслуховуючий пристрій володіє малими розмірами, а запасу батареї вистачає на 40, 90 і більше годин. Переваги міні-диктофонів - можна прослухати зроблений запис, а також даний пристрій практично не випромінює електромагнітні хвилі. А недоліком є те, що розмову не можна прослуховувати "в прямому ефірі".

Приховані відеокамери - це міні камера останнього покоління, яка поєднує в собі мініатюрний розмір, надміцний металевий корпус і чудову якість відеозапису з циклічністю. Вони не помітні для зловмисників, а значить, ті будуть вести себе, не підозрюючи про спостереження. Існують автономні шпигунські відеокамери, які вже йдуть вбудовані в різні предмети, наприклад, в іграшки або пожежні датчики. Такі типи камер можуть знімати відеоматеріал із записом на карту пам'яті, яку і згодом зможете переглянути на комп'ютері.

Лазерна прослушка - це пристрій прихованого спостереження, що використовує лазерний промінь для того, щоб фіксувати звукові вібрації в віддалених об'єктах. Ця технологія може бути використана для прослушки з мінімальним ризиком виявлення. Лазерний промінь наводиться на поверхню віконного скла або на іншу плоску поверхню, яка перебувала під впливом звуку. Вібрації цієї поверхні змінюють кут відображення променя, і рух лазерної точки повернутого променя фіксується і трансформується в аудіо-сигнал.