Інститут спеціального зв’язку та захисту інформації
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»

ІВАНЧЕНКО С.О.

ОСНОВИ УБЕЗПЕЧЕННЯ ІНФОРМАЦІЇ ВІД ВИТОКУ ТЕХНІЧНИМИ КАНАЛАМИ

Навчальний посібник

*Рекомендовано Вченою радою ІСЗЗІ КПІ ім. Ігоря Сікорського
як навчальний посібник для здобувачів ступеня бакалавр, які навчаються в Інституті
за освітньою програмою Безпека державних інформаційних ресурсів за спеціальністю
F5 Кібербезпека та захист інформації*

Електронне мережне навчальне видання

Київ-2025

УДК 004.056.5
І17

Рецензенти: к.т.н. Гавриленко Олексій Вадимович, заступник начальника управління Департаменту захисту інформації Адміністрації Держспецзвязку.
к.т.н, с.н.с. Зінченко Ярослав Вікторович, начальник Науково-дослідного центру Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».

Відповідальний редактор: Конотопець М.М., к.т.н., доц.

Рекомендовано Методичною комісією «КПІ ім. Ігоря Сікорського»
(протокол № 4 від 05.02.2026)
Ухвалено Вченою радою ІСЗЗІ «КПІ ім. Ігоря Сікорського»
(протокол № 6 від 24.12.2025)

Іванченко С.О.
І 17 Іванченко С.О. Основи убезпечення інформації від витоку технічними каналами: навч. посібник. Київ: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2025. 163 с.

У навчальному посібнику представлено основи щодо убезпечення інформації від витоку технічними каналами. Проводиться теоретичне обґрунтування умов захищеності для найбільш поширених видів джерел: мовних, візуальних та цифрових джерел витоку інформації. В основі обґрунтування покладено забезпечення заданого ризику інформаційної безпеки як загального показника захищеності інформації від її витоку. Захищеність розглядається шляхом забезпечення двох якісних вимог. Це – унеможливлення добування смислового змісту з перехоплених повідомлень та унеможливлення виявлення ознак небезпечного сигналу в технічних каналах витоку. Щодо кожного з шляхів унеможливлення здійснюється обґрунтування окремих показників захищеності в інформаційно-імовірнісному та енергетичному аспектах. Здійснюється коригування показників в залежності від надлишковості джерела, використаних коригуючих кодів, повторів сеансу передачі тощо.

Навчальний посібник розроблено в розрізі завдань сучасних міжнародних стандартів з менеджменту інформаційної безпеки для здобувачів вищої освіти, що вивчають основи убезпечення інформації від витоку технічними каналами за спеціальністю F5 Кібербезпека та захист інформації.

УДК 004.056.5

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ТЗІ – технічний захист інформації;
КТЗІ – комплекс технічного захисту інформації;
КСЗІ – комплексна система захисту інформації;
ОІД – об’єкт інформаційної діяльності;
ІКС – інформаційно-комунікаційна система;
ТКВ – технічний канал витоку інформації;
ІзОД – інформаці з обмеженим доступом;
ОТЗС – основні технічні засоби та системи;
ДТЗС – допоміжні технічні засоби та системи;
ТЗС – технічні засоби та системи;
АЦП – аналого-цифрове перетворення;
ЦАП – цифро-аналогове перетворення.

ВСТУП

Інформація – це не матерія і не енергія. Інформація – це інформація.

Норберт Вінер

Хто володіє інформацією, той володіє світом.

Натан Ротшильд

Робота електронних засобів, якими є всі сучасні засоби та системи обробки та передачі інформації, а також інформаційно-комунікаційні системи (ІКС), постійно супроводжується рядом паразитних ефектів, які сприяють реалізації загрози витоку інформації. Такими ефектами є побічні електромагнітні випромінювання та наведення, просочування небезпечних сигналів у різного характеру відвідні ланцюги, ланцюги заземлення та електроживлення тощо. Означені ефекти можуть утворювати на об’єктах інформаційної діяльності (ОІД) технічні канали витоку (ТКВ) інформації, які є небажаними та вимагають від розпорядника інформації відповідних заходів щодо їх усунення та знешкодження. Вочевидь знешкодження ТКВ має полягати у локалізації чи мінімізації чинників, що утворюють ці канали, та досягнення потрібних нормативних умов щодо інформаційної безпеки [1, 2].

Однак, технологічна складова цієї загрози, тобто ТКВ не може бути усунутою абсолютно. Як відомо, сигнали завдяки їх природі можуть поширюватись в середовищі на досить великі відстані, теоретично навить до нескінченності. На практиці закінченням пробігу хвилі вважається її розсіювання в теплових та інших різного характеру шумах, які постійно перебувають в середовищі поширення [3].

В ТКВ сигнали, що несуть інформацію, як правило мають низький рівень, а тому відстань їх поширення є відносно невеликою та може складати від одиниць до сотень метрів. Зазначені відстані хоча і є невеликими, все таки можуть перевищувати межі ОІД та бути достатніми для перехоплення та створення небезпеки витоку інформації.

Таким чином, завдання захисту інформації від витоку ТКВ в першу чергу полягає в пошуку та обґрунтуванні таких умов в середовищі поширення сигналів, за яких отримання інформації чи корисних відомостей із цих спотворених шумами середовища сигналів в заданій мірі стане неможливим. Як очевидно, цією заданою мірою, що означена загальним показником, є ризик інформаційної безпеки – поєднання імовірності наставання ризику та наслідків, збитків від нього.

В другу чергу завданнями захисту є пошук та обґрунтування методів, засобів та заходів захисту інформації, які б надали можливість забезпечити вище зазначені умови, означені заданим ризиком інформаційної безпеки.

Так, на сьогоднішній день увесь розвинений світ використовує ризик-орієнований підхід щодо управління інформаційною безпекою, який базується на сучасних міжнародних стандартах з менеджменту інформаційної безпеки, наприклад, серії ISO/IEC 2700x та інших стандартів. Згідно з ними, розпорядник інформації визначає допустиму межу ризику, яка в разі атак або інцидентів забезпечуватиме його допустимий максимум понесення збитків [2].

Ризик як рівень допустимих збитків залежить від імовірнісно-інформаційних та енергетичних показників, що кількісно характеризують можливість або неможливість витоку інформації. Ці показники разом із показником ризику становлять певну ієрархічну сукупність показників захищеності інформації в ТКВ, які дозволяють автоматизацію їх обробки та автоматизоване управління безпекою щодо витоку інформації цими каналами. З метою гарантування достовірності захисту зазначені показники мають бути належним чином обґрунтованими та доказово забезпечувати виконання заданого ризику безпеки, дозволяти його аналіз та коригування із застосуванням засобів автоматизації. З цією ж метою показники захищеності вимагають періодичного переогляду, з їх коригуванням та коригуванням вжитих обмежень та припущень, що необхідно здійснювати з розвитком науки й техніки.

Навчальний посібник складається з чотирьох розділів. У посібнику наведено основні засади ризик-орієнтованого підходу щодо убезпечення інформації від витоку технічними каналами; обґрунтовано умови захищеності для найбільш поширених видів джерел, якими є мовні, візуальні та цифрові джерела витоку інформації; наведено показники захищеності інформації від витоку та обґрунтовано їхній зв’язок між собою. Такими показниками є:

– *загальний імовірнісний показник* – імовірність ризику інформаційної безпеки для всіх видів джерел;

– *приватні імовірнісні показники щодо особливостей джерел витоку інформації* – розбірливість та розпізнання, відповідно, для мовних та візуальних джерел. Пропускна здатність ТКВ з імовірністю помилки в каналі або імовірність неможливості виявлення ознак небезпечного сигналу для цифрових джерел витоку інформації. Ці показники є індивідуальними щодо видів інформації та їхніх джерел, мають забезпечувати заданий ризик та є інформаційно-сенсовими за сутністю;

– *приватні енергетичні показники щодо особливостей небезпечних сигналів* – відношення сигнал/завада на вході приймача перехоплення, яке має забезпечувати виконання всіх вище наведених показників,

визначається відносно оптимального прийому як потенційної можливості перехоплення. Цей показник є індивідуальним щодо сигналу, який несе інформацію, та є мірилом для фізичного носія та середовища щодо його поширення.

Здійснюється коригування показників залежно від надлишковості джерела, використаних коригуючих кодів, повторів сеансу передачі тощо.

Навчальний посібник розроблено в розрізі завдань сучасних міжнародних стандартів з менеджменту інформаційної безпеки для курсантів і аспірантів, що вивчають основи убезпечення інформації від витоку технічними каналами за спеціальністю F5 Кібербезпека та захист інформації.

РОЗДІЛ 1. РИЗИК-ОРІЄНТОВАНІ ПОКАЗНИКИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ ВІД ВИТОКУ ТЕХНІЧНИМИ КАНАЛАМИ. ОСОБЛИВОСТІ ДЖЕРЕЛ ВИТОКУ

1.1. Основні джерела витоку інформації, їхні характеристики та ризик-орієнтовані показники захищеності в каналі

Джерела витоку інформації та їхні характеристики. В попередніх дисциплінах здійснено аналіз різновидів технічних каналів витоку інформації, які можуть виникати на об'єктах інформаційної діяльності та від технічних засобів і систем обробки та передачі інформації. Для цього було використано чотири ознаки, які дозволили здійснити розділення цих каналів та подати їх як певну логічну структуру. Це структурне представлення потрібне для того, щоб надати можливість краще зрозуміти сутність та уявити різновиди технічних каналів витоку інформації для виявлення цих каналів на реальних об'єктах. При цьому ознаками, за якими здійснювалося зазначене розділення, є:

1. Фізичні ефекти або процеси, що сприяють витоку інформації та утворенню технічних каналів витоку.
2. Джерела витоку інформації, від яких поширюється інформаційний сигнал.
3. Фізичні середовища та носії небезпечного сигналу в середовищі їх поширення.
4. Способи перехоплення інформації засобами розвідки противника.

Наявність фізичних передумов витоку інформації є загрозою, а тому захист має передбачати усунення цих передумов, а саме ліквідування та знешкодження технічних каналів витоку. Це можна здійснити, наприклад, шляхом застосування навколо об'єкта великих контрольованих територій, з виключенням розташування в їхніх межах будь-яких засобів перехоплення. Так, якщо між джерелом витоку та приймачем перехоплення досить велика відстань (більше ніж сотні метрів та кілометри) і приймач не реагує на інформаційний сигнал, то можна вважати, що технічний канал витоку повністю відсутній.

Однак, на практиці таке ліквідування каналів не завжди можливе. Адже забезпечення великих відстаней може бути лише на вільних місцевостях, в рідконаселених пунктах, де низька щільність розташування об'єктів різного характеру.

У густонаселених пунктах реалізація зазначеного способу часто є складним або ж зовсім неможливим завданням. Причиною цього є зайнятість потрібних територій та їхня приватна власність, завелика вартість корисних будинкових площ, складність та недоцільність їх

придбання та орендування, наприклад, через тимчасовість об’єктів, що вимагають захисту тощо.

Очевидно, що для обмежених контрольованих територій повна ліквідація технічних каналів витоку інформації є неможливою, оскільки приймальні пристрої перехоплення реагуватимуть на сигнал та виявлятимуть деякі його ознаки.

Однак, виявлення ознак небезпечного сигналу – це ще не факт перехоплення інформації. Адже інформація – це не сигнал, а певні відомості, які зменшують наявну невизначеність про стан об’єкта чи суб’єкта. Інформація хоч і не є видом матерії, проте має мірило, її можна охарактеризувати кількісно.

Так, залежно від повноти зазначених ознак, інформація може частково витікати, а частково ні. Як правило, інформація може втрачатися в технічному каналі через спотворення сигналів завадами. Очевидно, що зменшення частки перехопленої інформації приводитиме до зниження ступеня небезпеки щодо її витоку, а збільшення навпаки – до посилення небезпеки та необхідності вжиття відповідних заходів.

Таким чином, можна стверджувати, що в точці імовірного перехоплення можуть знайтися такі енергетичні умови – відношення сигнал/завада – за яких ознаки небезпечного сигналу ще виявлятимуться, але інформація вже не витікатиме.

При цьому, вочевидь, для забезпечення захищеності завжди виникатимуть питання: “А де ж межа, що розділятиме факт витоку та факт не-витоку? Якою має бути норма, що задовольнятиме вимоги та забезпечуватиме інформаційну безпеку?“

Отже для відповіді на поставлені запитання та вирішення відповідних завдань доцільно розглянути технічні канали витоку інформації дещо інакше, ніж як це було зроблено раніше з точки зору фізичних процесів. Оскільки йдеться про захищеність інформації, ці канали потрібно розглянути з точки зору саме цієї захищеності, а точніше її обґрунтування. Також очевидно, що захищеність має бути обґрунтована належним чином, за допомогою кількісних показників, з гарантуванням потрібної достовірності. Водночас обов’язково потрібно врахувати особливості основних джерел витоку інформації.

Основними різновидами таких джерел є:

– джерела мовної інформації;
– джерела візуальної (телевізійної) інформації;
– джерела цифрової інформації (інформаційних даних), що утворюються від основних технічних засобів та систем обробки та передачі інформації.

Охарактеризуємо вказані джерела та їхні особливості.

1. *Характеристики мовних джерел витоку інформації.* До мовної інформації належать звуки, слова та речення. Вони виробляються голосовим апаратом людини або технічними засобами відтворення мовлення та сприймаються людиною, її слуховими органами чуття. Як приймачі також можуть бути й технічні пристрої з мікрофонами, що реалізують статистичну обробку сигналів та надають мовний сигнал в "очищеному" вигляді для покращеного сприйняття людиною.

З точки зору певних (статистичних, суб'єктивно-об'єктивних та ін.) особливостей, що допоможуть обґрунтувати захищеність, канал витоку мовної інформації можна зобразити у вигляді схеми на рис. 1.1.1. На схемі в якості первинного джерела витоку та кінцевого приймача слугують люди – суб'єкти. Середовищем поширення мовного сигналу є певне узагальнене фізичне середовище, яке не враховує його походження, але містить завади – фактори, що заважають проходженню сигналів.

Рис. 1.1.1. Узагальнений канал витоку мовної інформації та схема для обґрунтування захищеності мовної інформації з точки зору статистичних особливостей джерела

Основними характеристиками будь-якого інформаційного сигналу є:

– середній рівень (за потужністю, або за динамічним чи потенційним параметром);

– швидкість зміни;

– динамічний діапазон.

Для мовного сигналу *середній рівень* є величиною плаваючою та залежить від потужності вироблення джерелом сигналу.

Швидкість зміни характеризується частотним спектром. Вважається, що енергія мовного сигналу максимально зосереджена в смузі частот 0,3…3,4 кГц, яка для каналів зв'язку є оптимальною (див. рис. 1.1.2). Слід зазначити, що для каналів витоку вказаний спектр не є повністю вичерпним. Практика показує, що мовний сигнал містить інформативні спектральні складові також за межами вище зазначеної смуги, які в різних середовищах проявляють себе по-різному. Наприклад, при просочуванні цих сигналів у відвідні електричні ланцюги вони мають стійку присутність огинаючої, яка зосереджена в смузі до 30 Гц. Очевидно, що для гарантування захищеності мовних джерел від витоку інформації

технічними каналами є необхідність враховувати всі інформативні спектральні складові, навіть ті, що зосереджені за межами смуги частот 0,3…3,4 кГц. Водночас окремим питанням є технічні можливості очищення мовних сигналів у сумішах із завад та їхнього синтезу за інформативними гармоніками спектра.

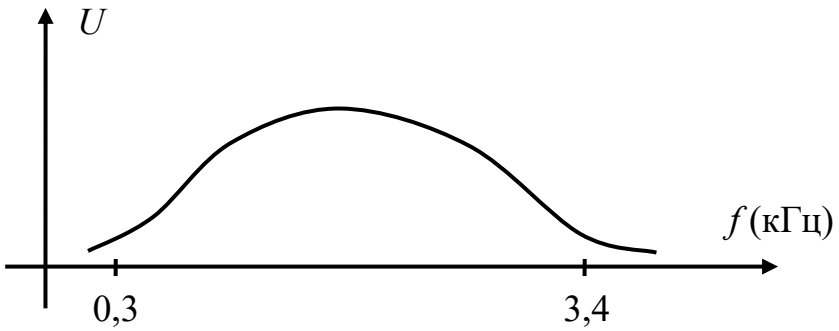


Рис. 1.1.2. Графічне зображення спектра мовного сигналу

Динамічним діапазоном вважається відношення максимальної потужності сигналу до її мінімуму. Під час телефонних розмов він складає приблизно 30 – 40 дБ.

2. *Характеристики джерел візуальної інформації.* До візуальної інформації зараховують тексти, картини та інші зображення різного характеру, які сприймаються органами зору людини. Одним з основних різновидів цих джерел є телевізійна інформація, яка є послідовністю картинок, що змінюються та сприймається людським оком як рух об’єктів на зображеннях. При цьому, вочевидь, інтервал затримки картинки має бути не більшим ніж час реакції зорового апарату разом із нервовою системою людини щодо сприйняття. Вважається, що для того, щоб людина спостерігала рух предмета без блимання та з комфортом, частота кадрів повинна бути не меншою ніж 24 кадри за секунду.

Для обґрунтування захищеності, технічний канал витоку візуальної інформації можна зобразити у вигляді схеми, як показано на рис. 1.1.3. На відміну від каналів витоку мовної інформації, первинним джерелом тут є об’єкт, його зовнішній вигляд, зображення. Приймачем, як і для попередніх каналів є суб’єкт – зоровий апарат людини. Щодо джерел витоку візуальної інформації, як правило, найбільш актуальними є технічні засоби та системи, що обробляють та передають цей вид інформації. А тому середовищем поширення сигналів у технічному каналі є середовище, що оточує ці засоби та системи. Адже саме вони формують сигнали, що несуть зображення, з використанням чи без використання різних виглядів модуляції.

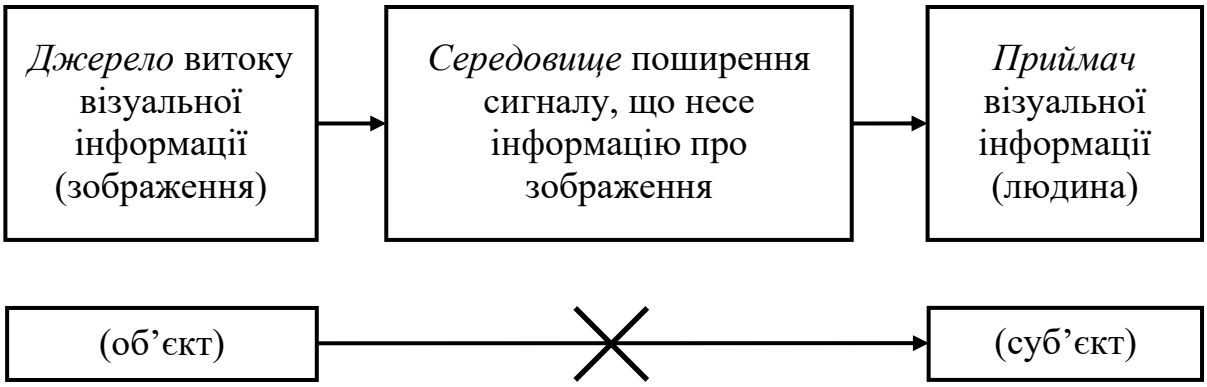


Рис. 1.1.3. Узагальнений канал витоку візуальної інформації та схема для обґрунтування захищеності візуальної інформації з точки зору статистичних особливостей джерела

Джерела витоку візуальної інформації, що не використовують для обробки та передачі технічні засоби та системи, також підлягають захисту. Однак, їхній захист зводиться до приховування, маскування або дезінформування. Як правило, ці заходи носять переважно організаційний характер та не використовують технічних засобів.

Прикладом зазначеного може бути:

– зберігання документів в зачинених та опечатаних сейфах, оскільки текст документа сприймається візуально. Робота з ними в спеціально виділених приміщеннях, де виключається можливість підглядування;

– зачохління техніки з метою приховування її зовнішнього виду при транспортуванні;

– будівництво та створення зайвих споруд з метою дезінформування.

Середній рівень сигналу, як і для мовного, є величиною плаваючою та залежить від часу доби або потужності джерела.

Щодо охарактеризування *швидкості зміни* сигналів, що несуть інформацію про зображення, є декілька точок зору:

1. Зображення мають статичний характер та представляють собою певну панораму – одночасне представляється інформації в повному об'ємі.

2. За фізичною сутністю зображення є певною комбінацію розташованих на площині точок певного кольору з певною інтенсивністю, які утворені або випромінюванням або перевипромінюванням (ефект люмінесценції) світлової енергії. Відповідно, світіння характеризується *частотним спектром у світловому діапазоні частот* $10^{12} \div 10^{15}$ Гц.

3. Під час подання та передачі зображень технічними засобами можуть бути використані різні сигнали та способи їх модуляції. Ці сигнали

(модульовані та немодульовані) мають власну *швидкість зміни* та характеризуються власним частотним спектром.

4. Телевізійна інформація має динамічний характер, як послідовність картинок, що швидко змінюються. У формуванні телевізійної інформації практично завжди беруть участь технічні засоби. Тому в її спектрі частот окрім енергії кожного зображення, як це було зазначено в попередньому пункті, з'явиться спектральна складова, що відповідає за швидкість зміни зображення. Вважається, що для телебачення повна зміна зображень здійснюється не швидше, ніж 2-3 рази за секунду. Це, в свою чергу, дозволяє вважати телевізійний сигнал періодичним та використовувати її в знаходженні умов захищеності.

Аналіз згинаючої відеосигналу показав, що *динамічний діапазон* телевізійних сигналів сягає до 40 дБ. Спектр телевізійної інформації, на прикладі одного з перших започаткованих "чорно-білих" стандартів, складає 0,015 ÷ 6,5 МГц. Щодо зазначеного стандарту спектр сигналу має характер лінійчатого спектра та має вигляд, як показано на рис. 1.1.4.

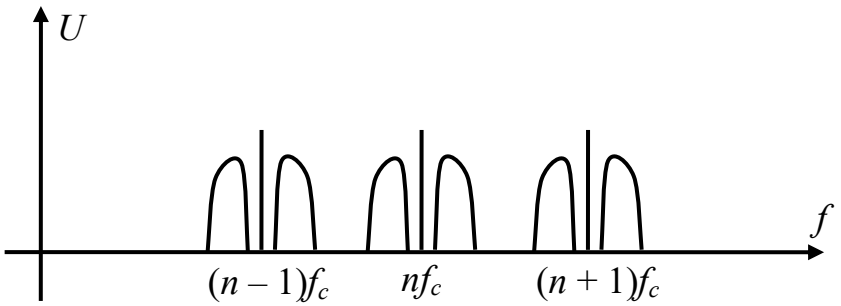


Рис. 1.1.4. Спектр частот телевізійного сигналу на прикладі "чорно-білого" стандарту

3. *Характеристики джерел цифрової інформації.* До цифрових джерел інформації зараховують джерела послідовностей дискретних даних, які в технічних засобах та, відповідно, в середовищі технічного каналу витоку мають вигляд певних неперервних реалізацій. Прикладами таких реалізацій є відеоімпульси з різноманітними формами: однополярними, різнополярними, ортогональними тощо. У якості реалізацій дискретних даних можуть виступати ті радіоімпульси, які, як правило, використовуються для низькошвидкісних даних (наприклад, телеграфних – до 300 імпульсів на хвилину) з використанням певних видів модуляції. За своєю природою дискретні дані виробляються та, відповідно, випромінюються в середовище каналів витоку виключно цифровими технічними засобами та системами, переважна більшість яких – це сучасні технічні засоби та системи. Цифрова інформація може передаватися за допомогою одного або декількох електричних ланцюгів у вигляді послідовного або паралельного кодів.

Для обґрунтування захищеності технічний канал витоку цифрової інформації можна зобразити у вигляді схеми, як показано на рис. 1.1.5. На відміну від попередніх каналів витоку, джерелом та приймачем інформації тут є об’єкти, в ролі яких завжди виступають технічні засоби та системи: як джерело – ті, що обробляють та передають цей вид інформації; як приймач – ті, що перехоплюють небезпечні сигнали та добувають із них інформацію.

Середовище поширення цифрової інформації може мати подвійну сутність.

1. Фізичне середовище – це середовище, що оточує технічні засоби та системи обробки та передачі інформації, та в якому поширюються реалізації даних за посередництва фізичних носіїв. Прикладами таких носіїв можуть бути: електромагнітне поле, електричні струми у відвідних ланцюгах тощо.

2. Математичне середовище – це середовище імовірнісних переходів даних як математичних об’єктів. Математичне середовище є апроксимацією фізичного середовища. Прикладом такого середовища може бути дискретний симетричний канал без пам’яті.

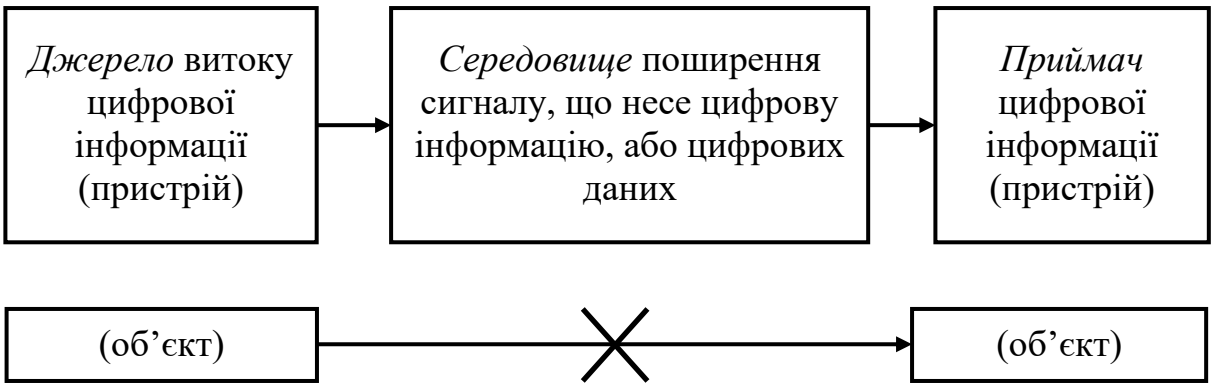


Рис. 1.1.5. Узагальнений канал витоку цифрової інформації та схема для обґрунтування захищеності цифрової інформації з точки зору статистичних особливостей джерела

Середній рівень сигналу, як і для мовного, є величиною плаваючою та, як для інших джерел, залежить від потужності джерела, виду модуляції та балансу знаків, що передаються. При реалізації технічних засобів з метою економії енергетичних затрат має місце тенденція спрямування середнього рівня сигналу до нуля. Наприклад, для різнополярних сигналів, що реалізують двійковий алфавіт даних, при балансі знаків від’ємні імпульси компенсуватимуть позитивні, тому в середньому потужність буде близькою до нуля.

Мають місце й інші способи подання даних, які забезпечують розподіл енергії в постійній смузі за спектром частот. Наприклад, фазова, біімпульсна модуляція та інші її гібриди.

Слід зазначити, що приймачем цифрової інформації є також технічний засіб або система обробки перехоплених повідомлень, які за своєю сутністю мають відповідати сучасному розвитку науки та техніки світу. Вони мають можливість реалізувати будь-який алгоритм статистичної обробки сумішей сигналу та завади, що надасть максимальний ефект перехоплення. По суті, перехоплення визначається максимальними технічними та технологічними можливостями світової науки, які постійно зростають та визначають його потенційні можливості.

Щодо *швидкості зміни сигналів*, важливу роль відіграє частота такту слідування даних, їхня форма реалізації та тривалість імпульсу, що задані технічним засобом обробки та передачі – джерелом витоку інформації. Так, наприклад, для однополярного сигналу з періодичністю T та тривалістю τ (див. рис. 1.1.6) спектр шляхом перетворення в ряд Фур'є набуде вигляду як показано на рис. 1.1.7.

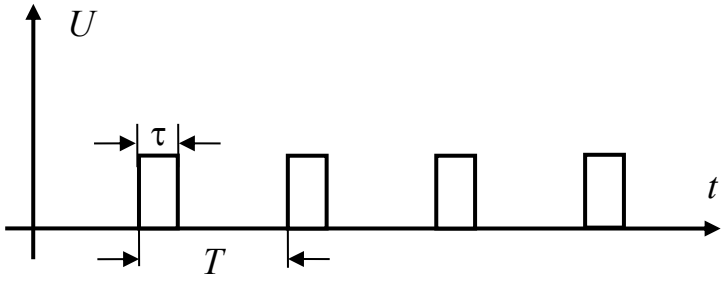


Рис. 1.1.6. Приклад часового подання періодичного відеосигналу

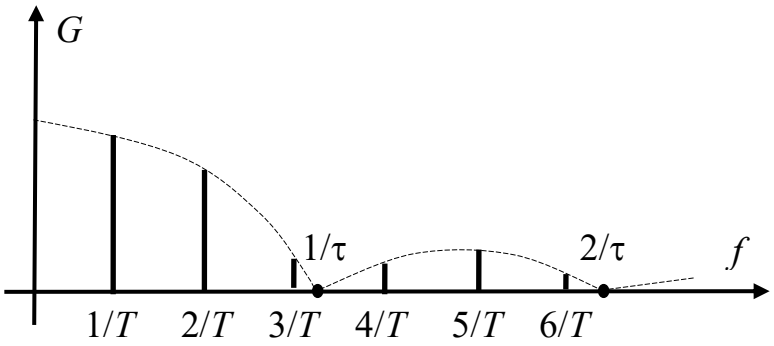


Рис. 1.1.7. Приклад подання частотного спектру періодичного відеосигналу

Динамічний діапазон цифрового сигналу (відношення його максимальної потужності до мінімальної) залежить від способів подання

дискретних даних неперервними реалізаціями та є величиною стабільною. Наприклад, якщо для подання даних використані різнополярні реалізації, то в кожному такті потужність буде незмінною, а тому динамічний діапазон складатиме 0 дБ. Для інших же способів подання цей діапазон може бути відмінним від нуля.

Таким чином, з'ясовано основні характеристики сучасних джерел, від яких утворюються технічні канали витоку інформації. Як такі було взято: джерела мовної інформації, джерела візуальної (телевізійної) інформації та джерела цифрової (в минулому телеграфної та телекодової) інформації. Було показано їхню сутність з точки зору захищеності, що впливає на захищеність цих джерел в технічних каналах витоку інформації.

В наступному питанні визначимо статистичні показники, що впливають на захищеність цих джерел в технічних каналах витоку, та які можливо нормувати з метою досягнення вимог із захищеності інформації від витоку технічними каналами.

Ризик інформаційної безпеки та ризик-орієнтовані показники захищеності джерел витоку інформації. Одним із показників інформаційної безпеки, що визначені міжнародними стандартами серії ISO/IEC 27000, є ризик безпеки.

Під *ризиком інформаційної безпеки* (information security risk) будемо розуміти потенційну можливість того, що *уразливість* буде використана для створення *загрози активу* чи групі активів, що призводить до збитків для організації чи держави.

Уразливість – це слабке місце активу, або заходів та засобів контролю й управління, яке може бути використано *загрозою*.

Загроза – це можлива причина небажаного *інциденту*, який може нанести збитки системі, організації або державі.

Актив – це будь-що, що має цінність для організації, держави.

Інцидент інформаційної безпеки (information security incident) – одна чи декілька небажаних подій інформаційної безпеки, які зі значним ступенем імовірності призводять до компрометації операцій будь-якої діяльності та створюють загрози для інформаційної безпеки.

Кількісно ризик можна виразити формулою:

$$R = p_R W \,, \tag{1.1.1}$$

де p_R – імовірність ризику (реалізації загрози); W – повна вартість активу.

Слід зазначити, що імовірність ризику p_R визначається рядом різноманітних факторів, серед яких основними є фізичні, яких не можна позбутися повністю, а можливо лише частково ліквідувати або мінімізувати. Тому для нормування рекомендацій щодо показників захищеності інформації від витоку гранично допустима імовірність ризику

$p_{R\text{гр.д.}}$ є беззаперечно невід'ємною нормою. Відносно неї можна здійснити розрахунок усіх інших показників захищеності, зокрема й енергетичних, для всього різноманіття джерел з врахуванням їх особливостей.

Таким чином, початковими даними для убезпечення інформації від витоку технічними каналами мають бути:

1. *Якісна вимога* з безпеки інформації щодо її витоку технічними каналами. Наприклад, унеможливлення добування смислового змісту з перехопленого повідомлення.

2. *Допустима імовірність ризику* – імовірність витоку інформації технічними каналами. По суті ця імовірність є гранично допустимою імовірністю невиконання заданої якісної вимоги, що визначає безпеку.

Розглянемо деякі підходи, які можна застосувати для обґрунтування захищеності розглянутих вище основних джерел витоку інформації.

Мовна інформація – виникає в результаті мовлення, яке формується людиною. Під час видихання створюється повітряний тиск (потік елементарних частинок повітря), який приводить голосові зв'язки до коливання та вироблення основного голосового тону. Ротова порожнина є резонатором. Рухи губ, щелепи та язика роблять цей резонатор змінної форми та перетворюють повітряний потік, що видихається.

Так, якщо під час вимови одного звуку, що відповідає літері алфавіту, використовується звучання основного тону, і ротова порожнина, набувши певної форми, не змінює її, то це промовляються голосні звуки. Не складно зазначене уявити, промовляючи літери "а", "о", "у" і т. п.

Якщо ж під час озвучення літери алфавіту ротовий резонатор набуває певної форми та змінює її, тобто вимова пов'язана з рухом губ, щелепи або язика, то це промовляються приголосні звуки: з використанням основного тону – дзвінкі, без його використання – глухі. Прикладом зазначеного є звучання літер по парах "б" "п", "в" "ф", "ж" "ш" і т. п. Наявні й звуки, що не мають глухих пар, наприклад, літера "р", а також комбінації літер – "дж" "дз" тощо.

Отже, як очевидно, мовлення є процесом суб'єктивного формування звуків, що використовує різного характеру модуляцію та фільтрацію. При цьому також очевидно, що хоча основна енергія і зосереджена в смузі частот 0,3 ÷ 3,4 кГц, все ж статистика мовлення матиме великий діапазон параметрів та різний розподіл інформативності по частоті. У зв'язку з цим, обґрунтування умов захищеності мовної інформації від витоку технічними каналами (статистичних та енергетичних) доцільно здійснювати відносно суб'єктивно-оптимального прийому, тобто відносно найкращого способу прийому, елементом якого та кінцеве рішення в якому ухвалює людина.

Це субоптимальний прийом, щодо якого для обґрунтування захищеності мовної інформації та нормування кількісних показників захищеності може бути використаний наступний їх ланцюг, як показано на

рис. 1.1.8. За заданою імовірністю ризику можна знайти потрібну розбірливість, за потрібною розбірливістю – гранично допустиме відношення сигнал/завада.

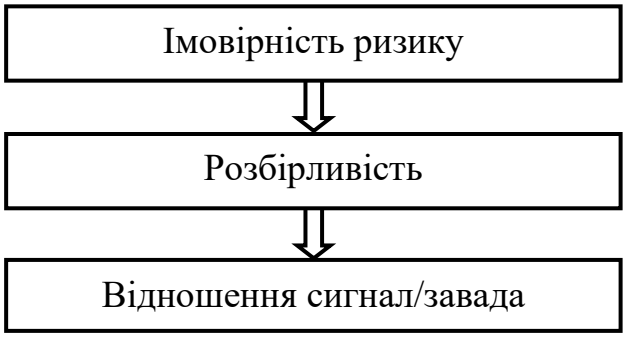


Рис. 1.1.8. Ланцюг показників захищеності мовної інформації від витоку технічними каналами

Візуальна інформація являє собою зображення, яке може бачити людина. За допомогою світла людина власним зоровим апаратом сприймає навколишній світ та його зображення на картинці. Завдяки різниці інтенсивності цього світла людина бачить геометричні обриси предметів, завдяки частоті – кольори цих предметів.

Сприйняття зоровою (нервовою) системою здійснюється шляхом швидкого періодичного сканування панорами комбінацій кольорів та їх інтенсивності, які є інформативними та несуть візуальну інформацію. Оскільки частота такого сканування складає до 16 разів за секунду, то перші зразки кіноапаратів німого кіно, створені у 1896 році винахідником кінематографа Люм'єром, були налаштовані на цю ж частоту кадрів. З одного боку це було пов'язано з економією фотоплівки, з іншого – зі звичайністю сприйняття людським оком зміни картинок як об'єкту, що рухається.

Пізніше, в 1926 році, з появою звукового кіно, консорціум американських кінокомпаній підвищив цю частоту до 24 кадрів за секунду та визначив її як стандарт для систем звукового кінематографа тих часів.

Слід зазначити, що телевізійна швидкість 24 кадри за секунду не є оптимальною з точки зору людського сприйняття. Практика показала, що ця частота призводить до швидкої фізіологічної втоми та погіршення зору людини. Тому сучасні відеопристрої працюють з більшою частотою ніж 24 кадри за секунду. Як правило, вона складає 60 ÷ 100 Гц.

Отже, як очевидно, візуальна інформація є процесом об'єктивного формування та суб'єктивного сприйняття. Водночас також очевидно, що зображення можуть мати різний характер деталізації, що виражатиметься розподілом інформативності за інтенсивністю та частотою. Тому, як і для мовної інформації, незалежно від видів модуляції сигналів та технологій їх

очищення від завад статистика візуальної інформації характеризується великим діапазоном параметрів. У зв'язку з цим, обґрунтування умов захищеності цього виду інформації від витоку технічними каналами (статистичних та енергетичних) доцільно здійснювати, як і для мовних джерел, відносно субоптимального прийому – найкращого способу прийому, елементом якого та кінцеве рішення в якому **ухвалює людина-суб'єкт.**

Щодо субоптимального прийому обґрунтування захищеності візуальної та телевізійної інформації, що виражається у нормуванні кількісних показників захищеності, може бути використаний наступний їх ланцюг (див. рис. 1.1.9). За заданою імовірністю ризику можна знайти потрібне розпізнання, а за потрібним розпізнанням – гранично допустиме відношення сигнал/завада.

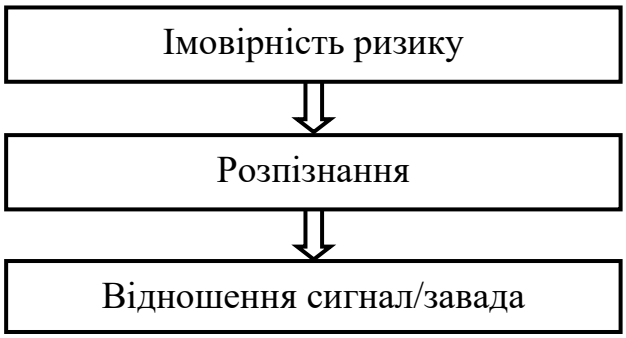


Рис. 1.1.9. Ланцюг показників захищеності візуальної (телевізійної) інформації від витоку технічними каналами

Цифрова інформація – це спосіб уніфікованого подання всіх видів інформації, що використовує сучасна цифрова техніка. Це ті види інформації, які раніше класифікувалися як телеграфні та телекодові сигнали, що призначалися для передачі текстів та широко використовувалися у 80-х роках минулого сторіччя.

Зараз переважно всі сучасні інформаційні, комунікаційні та інформаційно-комунікаційні системи (ІКС) є цифровими. На відміну від техніки старого парку, вони є автоматизованими та самокерованими. Сучасні ІКС самостійно керують режимами власної роботи, маршрутизацією потоків та їхнім часовим об'єднанням та роз'єднанням. Шляхом використання завадостійких кодів та повторів на сеанс передачі, вони коригують якість каналів комунікацій тощо.

Крім того потоки в ІКС можуть містити дані об'єктивного чи суб'єктивного походження, утворені аналого-цифровим перетворенням повідомлень від аналогових первинних джерел. Вочевидь, для обґрунтування захищеності інформації від витоку технічними каналами

врахування особливостей цих джерел за деякими незначними винятками є складним, а то й недоцільним.

Тому є сенс вважати цифрову інформацію послідовністю цифрових даних об'єктивного походження. Оскільки цифрове подання інформації викликане технічною особливістю сучасних засобів обробки та передачі інформації, то приймачем в каналі витоку має бути об'єкт – технічний пристрій.

У зв'язку з цим, обґрунтування умов захищеності цього виду інформації, на відміну від попередніх джерел, доцільно здійснювати відносно оптимального прийому як найкращого способу перехоплення. При цьому, для нормування кількісних показників захищеності може бути використаний такий їх ланцюг (див. рис. 1.1.10). За заданою імовірністю ризику можна знайти потрібну пропускну здатність каналу, а за пропускною спроможністю – гранично допустимі імовірність помилки в каналі та відношення сигнал/завада. Оскільки цифровий потік може мати коректувальну надлишковість для виправлення помилок в каналі комунікацій та власну надлишковість природного походження, яка також може сприяти виправленню помилок під час прийому, то гранична імовірність помилки вимагає відповідного коригування, що також показано на рис. 1.1.10.

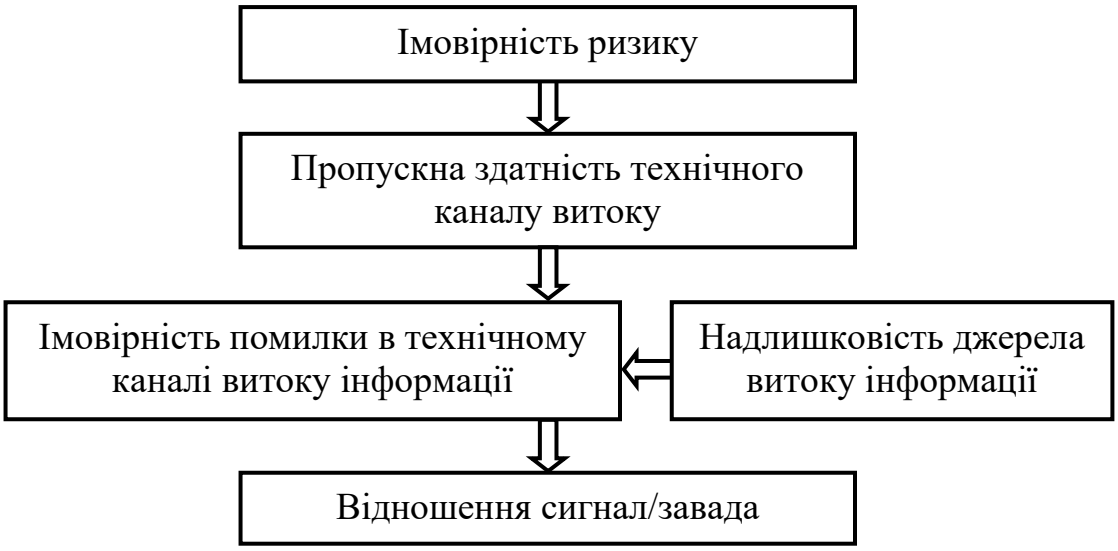


Рис. 1.1.10. Ланцюг показників захищеності цифрової інформації від витоку технічними каналами

Таким чином, розкрито сутність ризик-орієнтованих підходів щодо обґрунтування захищеності основних джерел витоку інформації, що мають місце у виробничій діяльності людства. З'ясовано показники захищеності цих джерел, які знаходяться в певному структурованому зв'язку. Ці показники дозволяють нормування відношення сигнал/завада за

допустимою імовірністю ризику, яка регламентована міжнародними стандартами з інформаційної безпеки серії ISO/IEC 27000, та досягнення вимог із захищеності інформації від витоку технічними каналами.

Контрольні питання:

1. Основні джерела витоку інформації.
2. Характеристики мовних джерел витоку інформації.
3. Схема каналу витоку для обґрунтування захищеності мовних джерел.
4. Характеристики джерел витоку візуальної інформації.
5. Схема каналу витоку для обґрунтування захищеності візуальної інформації.
6. Характеристики джерел витоку цифрової інформації.
7. Схема каналу витоку для обґрунтування захищеності цифрової інформації.
8. Поняття ризику та імовірності ризику інформаційної безпеки національної безпеки.
9. Ризик та ризик-орієнтовані показники захищеності мовних джерел витоку інформації
10. Ризик та ризик-орієнтовані показники захищеності візуальних джерел витоку інформації
11. Ризик та ризик-орієнтовані показники захищеності цифрових джерел витоку інформації

1.2. Особливості джерел витоку сигналів, їхніх фізичних носіїв, середовищ та шляхів поширення з точки зору убезпечення інформації від витоку технічними каналами

Особливості інформаційних сигналів, їхніх фізичних носіїв, середовищ та шляхів поширення з точки зору убезпечення інформації від витоку технічними каналами для мовних джерел. Як зазначалось раніше, одним з найпоширеніших джерел витоку інформації є мовне джерело. Адже мовлення є головним засобом для спілкування між людьми. Людина з народження фізіологічно наділена голосовим мовоутворювальним та слуховим мовосприймальним апаратами, за допомогою яких вона може і говорити, і слухати.

В аспекті вироблення звуку до мовоутворювального апарату належать:

– грудна клітина з легенями, від якої здійснюється напір повітря;

– голосові зв’язки, які під дією цього напору формують основний тон голосу людини;

– ротова порожнина (піднебіння, язик, зуби та губи), яка виступає в ролі резонатора для формування звуків, що відповідають літерам алфавіту різних мов: української, англійської, китайської тощо.

Так, різниця в розмірах та формах голосових зв’язок визначає різницю голосів людини, наприклад, голосів чоловіка чи жінки, дитини чи дорослої людини. Різниця в розмірах та формах ротової порожнини визначає різницю мовленнєвих вимов звуків-літер алфавітів мов і не тільки. Аналіз показав, що люди з різних місцевостей по різному можуть вимовляти одні й ті ж звуки, чим показують свою належність до того чи іншого народу. Крім цього, є частими випадками, коли діти, народжені від батьків певної народності, що мають походження з іншої місцевості, під час дорослішання мають особливості вимовляння не тієї місцевості, де вони виховувались, а місцевості власних батьків.

В аспекті приймання звуку слуховий апарат – це:

– зовнішнє вухо;
– середнє вухо;
– внутрішнє вухо.

В аспекті ж синтезу, сприйняття та накопичення інформації в обох випадках виступає головний мозок, який відповідає за функцію мислення людини. Саме головний мозок виробляє та приймає інформацію, на основі чого людина здійснює розумову діяльність: аналізує, міркує, розрізняє, ухвалює рішення тощо. Саме ця інформація, яка озвучується за допомогою голосового апарату людини та сприймається її слуховим апаратам, також може цікавити й зловмисника, який ніяк інакше як так само, за допомогою власного фізіологічного слухового апарату може прийняти цю інформацію при перехопленні. При цьому, як очевидно, інформацією виступає не звук, а різниця між звуками мовлення – літерами алфавіту. Звук же, поширюючись у просторі, є лише фізичним носієм, який може містити, а може й не містити інформацію.

Звук спільно з інформацією, яку він несе, називають *мовним* (*мовленнєвим*) *повідомленням*. Як правило, мовні повідомлення є надлишковими та можуть нести різну кількість інформації, яку окрім цього можуть розділяти ще й на корисну та некорисну.

Комунікація, яка відбувається між людьми за допомогою звуку, що циркулює між голосовим та слуховим апаратами, може здійснюватися як безпосередньо через повітря, так і з використанням технічних засобів. Відповідно, і технічні канали витоку інформації від мовних джерел можуть утворюватись: як шляхом поширення механічних коливань без будь-яких перетворень, так і шляхом складних комбінацій, наприклад, з технічних засобів оброки та передачі інформації; як в аналоговому вигляді побічних

електромагнітних випромінювань та наведень, так і в цифровому вигляді, якщо технічний засіб здійснює аналого-цифрове перетворення (АЦП); як з частотною так і з часовою модуляцією тощо.

Шляхи витоку мовної інформації на об’єкті інформаційної діяльності (ОІД) та через технічний засіб чи систему (ТЗС) обробки та передачі інформації або інформаційно-комунікаційну систему (ІКС) зручно показати схематично за допомогою рис. 1.2.1 та рис. 1.2.2.

Як видно з рис. 1.2.1 та рис. 1.2.2, канали витоку інформації від мовних джерел з точки зору їх убезпечення мають такі особливості:

– в будь-якому разі кінцевим приймачем мовної інформації є людина, а тому головним показником захищеності є гранично допустима розбірливість слів, складів чи звуків, за якої людиною, а точніше її слуховим апаратом та мозком інформація вже не сприймається. Гранично допустиму розбірливість можна поставити у відповідність до заданого ризику безпеки, який визначений вимогою власника інформації та має бути обов’язково забезпеченим;

– середовище поширення мовної інформації, з якого можливе перехоплення, є фізичним середовищем з завадами. Саме середовище може дозволити чи не дозволити прийом інформації, забезпечуючи такий дозвільний показник, як відношення сигнал/завада. Очевидно, що гранично допустима розбірливість має забезпечуватися певним гранично допустимим відношенням сигнал/завада;

– в різних каналах витоку сигнал, що несе мовну інформацію, може мати різну форму з різним спектром частот (з переносом по частоті та без переносу, з модуляцією та без неї, в аналоговому та цифровому вигляді), а тому зазначене гранично допустиме відношення сигнал/завада при забезпеченні однієї і тієї ж розбірливості в різних каналах матиме різне значення та залежатиме від особливостей перетворення та передачі мовних сигналів;

– зв'язок розбірливості з відношенням сигнал/завада може мати різний ланцюг показників захищеності, а тому захист інформації від витоку технічними каналами може бути забезпечений шляхом впливу на кожен з них. Зниження рівня сигналу та підвищення рівня завад в ТКВ є традиційними універсальними способами, що лежать в основі пасивних та активних систем захисту;

– перебування мовної інформації в цифровому вигляді для її захисту від витоку технічними каналами може додатково дозволити застосування математичних методів, що випливатимуть на зростання, наприклад, імовірності помилки при перехопленні.

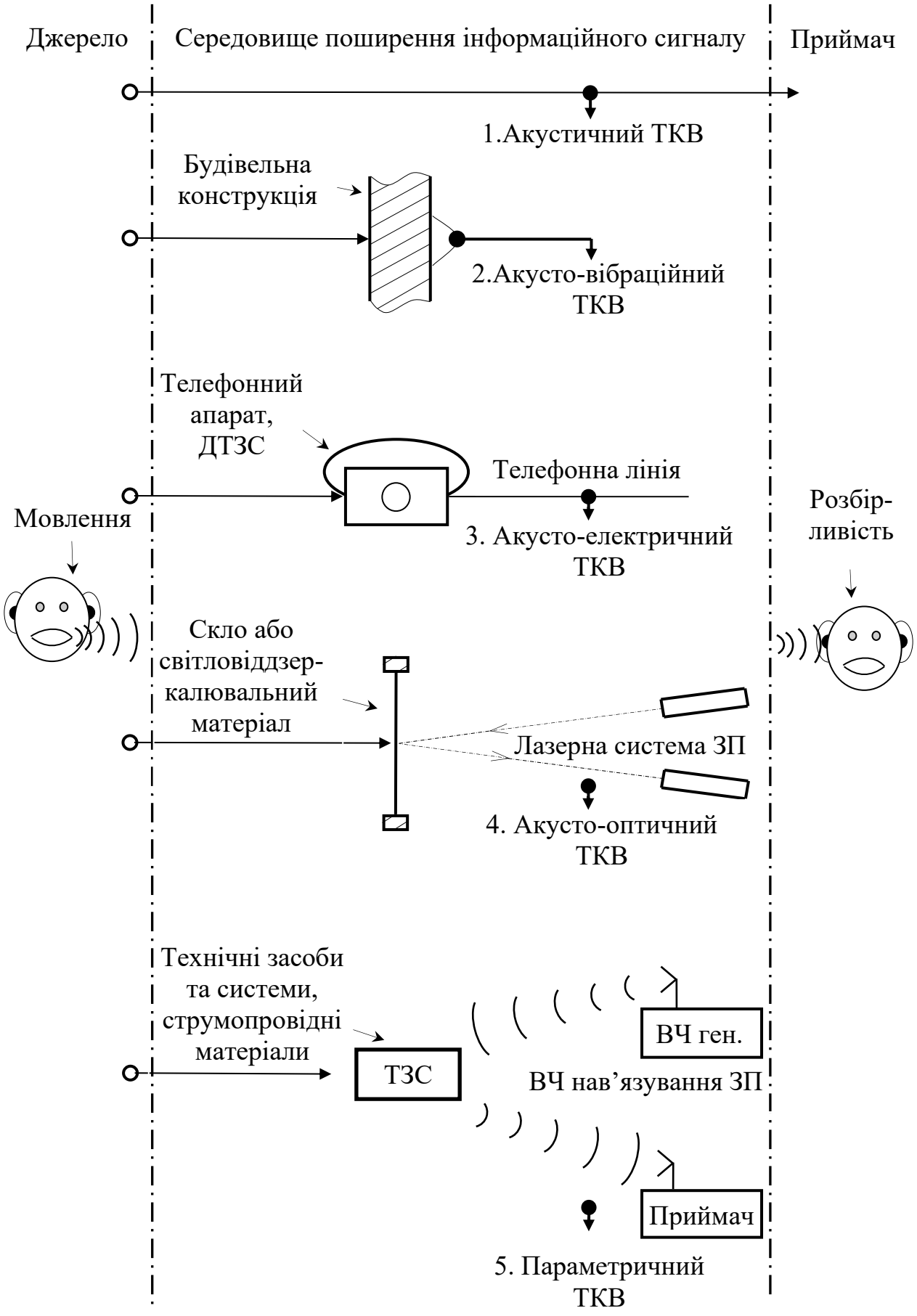


Рис. 1.2.1. Шляхи витоку мовної інформації на ОІД від акустичних джерел

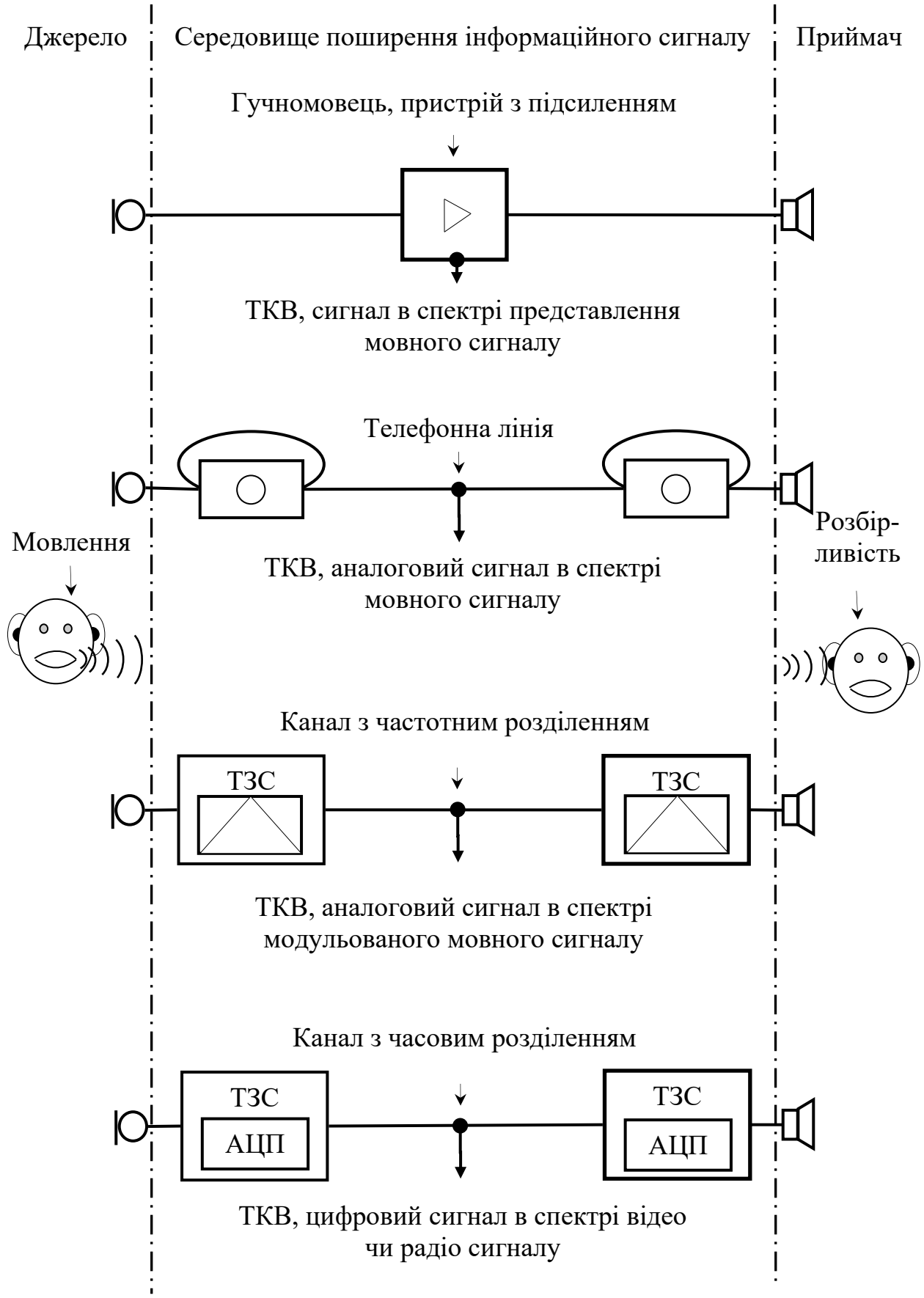


Рис. 1.2.2. Шляхи витоку мовної інформації через ІКС, ТЗС. Електричні та електромагнітні ТКВ мовної інформації

Таким чином, проведено огляд особливостей інформаційних сигналів, їхніх фізичних носіїв, середовищ та шляхів поширення з точки зору убезпечення інформації від витоку технічними каналами для мовних джерел. Визначено основні ризик-орієнтовані підходи щодо убезпечення інформації та показники, які характеризують захищеність мовної інформації від витоку та можуть бути використаними як нормативні.

Особливості інформаційних сигналів, їхніх фізичних носіїв, середовищ та шляхів поширення з точки зору убезпечення технічних каналів витоку для джерел візуальної інформації. В комунікації людства, а ще більше у сприйнятті світу, важливу роль відіграє візуальна інформація.

На відміну від мовної інформації, яку виробляє людина та, відповідно, має суб'єктивне походження, візуальну інформацію можна розглянути в трьох таких аспектах:

– візуальна інформація – це об'єктивна інформація про предмет, про його зовнішній вигляд у непорушному стані або в стані руху;

– візуальна інформація – це зображення, яке утворюється за допомогою світла та ефекту люмінесценції – відбиття світла поверхнею матеріальних предметів. Зображення предметів також може утворюватися через випромінювання їхнього власного тепла. Саме завдяки такому випромінюванню деякі тварини та птахи без освітлення бачать оточуючі предмети, а також у темряві вільно орієнтуються на місцевості та в просторі. Саме перетворення цього тепла у видиме світло покладено в основу принципу роботи приладів нічного бачення;

– візуальна інформація – це те, що може сприймати людина за допомогою власного органу зору, бачити та аналізувати зовнішній вид предметів в усій їхній красі з кольоровим забарвленням, відтінками тощо.

Таким чином, джерелом візуальної інформації є предмети та їхнє зображення, а носієм – звичайне світло або тепло. Світло, що освітлює предмети та дозволяє їх бачити людиною, може мати природне та штучне походження:

– світло природного походження – це зазвичай денне біле світло, вироблене Сонцем. Це може бути світло, вироблене або віддзеркалене іншими небесними тілами: місяцем, зірками тощо. До світла природного походження можна також віднести короткочасні блискавки, які утворюються під час грозових дощів, стихійне горіння матеріалів, що схильні до окислення, інші природні катаклізми, що супроводжуються в тією чи іншою мірою світінням;

– світло штучного походження – це світло, керовано вироблене з використанням призначених для цього пристроїв: електричних ламп та світлодіодів. Світло можуть виробляти й не призначені для цього пристрої, але робота яких супроводжується світінням. Це, насамперед, нагрівальні та

інші прилади, що використовують нитку розжарення. Це зварювальні апарати тощо.

Комунікації, що здійснюються через візуальне інформування, можуть відбуватися як шляхом безпосереднього бачення предметів та спостереження за ними, так і за допомогою механічних чи електронних засобів фотозйомки та відеозйомки, як з обробкою та передаванням на відстань візуальної інформації сучасними ІКС, так і без цих обробок та передавань.

Відповідно, технічні канали витоку інформації від візуальних джерел можуть утворюватись: як шляхом поширення світла (тепла) за умови прямої видимості, так і шляхом різного характеру та різної складності перетворень, наприклад, як в аналоговому так і в цифровому вигляді побічних електромагнітних випромінювань та наведень, як з частотною так і з часовою модуляцією тощо.

Схематично шляхи витоку візуальної інформації на ОІД та через ІКС зручно показати за допомогою рис. 1.2.3 та рис. 1.2.4.

З рис. 1.2.3 та рис. 1.2.4 видно, що канали витоку візуальної інформації, аналогічно, як і канали витоку інформації від мовних джерел, з точки зору їх убезпечення мають такі особливості (див. рис. 1.2.1. та рис. 1.2.2):

– кінцевим приймачем візуальної інформації є людина, а тому її головним показником захищеності є гранично допустиме розпізнання зображень чи то фото-, чи то відео-, за якої візуальна інформація людиною вже не сприймаються та зображення не розпізнаються. Гранично допустиме розпізнання можна поставити у відповідність ризику безпеки, який визначений вимогою власника інформації та має бути обов’язково забезпеченим;

– середовище поширення візуальної інформації, з якого можливе перехоплення, є фізичним середовищем із завадами. Аналогічно, як і для мовної інформації, гранично допустиме розпізнання має забезпечуватись певним гранично допустимим відношенням сигнал/завада;

– в різних каналах витоку сигнал, що несе візуальну інформацію, може мати різну форму подання цієї інформації в часі та з різним спектром частот (з переносом по частоті та без переносу, з модуляцією та без неї, в аналоговому та цифровому вигляді). Тому, як і для мовних джерел витоку інформації, зазначене гранично допустиме відношення сигнал/завада при забезпеченні одного і того ж розпізнання в різних каналах матиме різне значення та залежатиме від способів перетворення та передачі сигналів подання фото- та відеозображень;

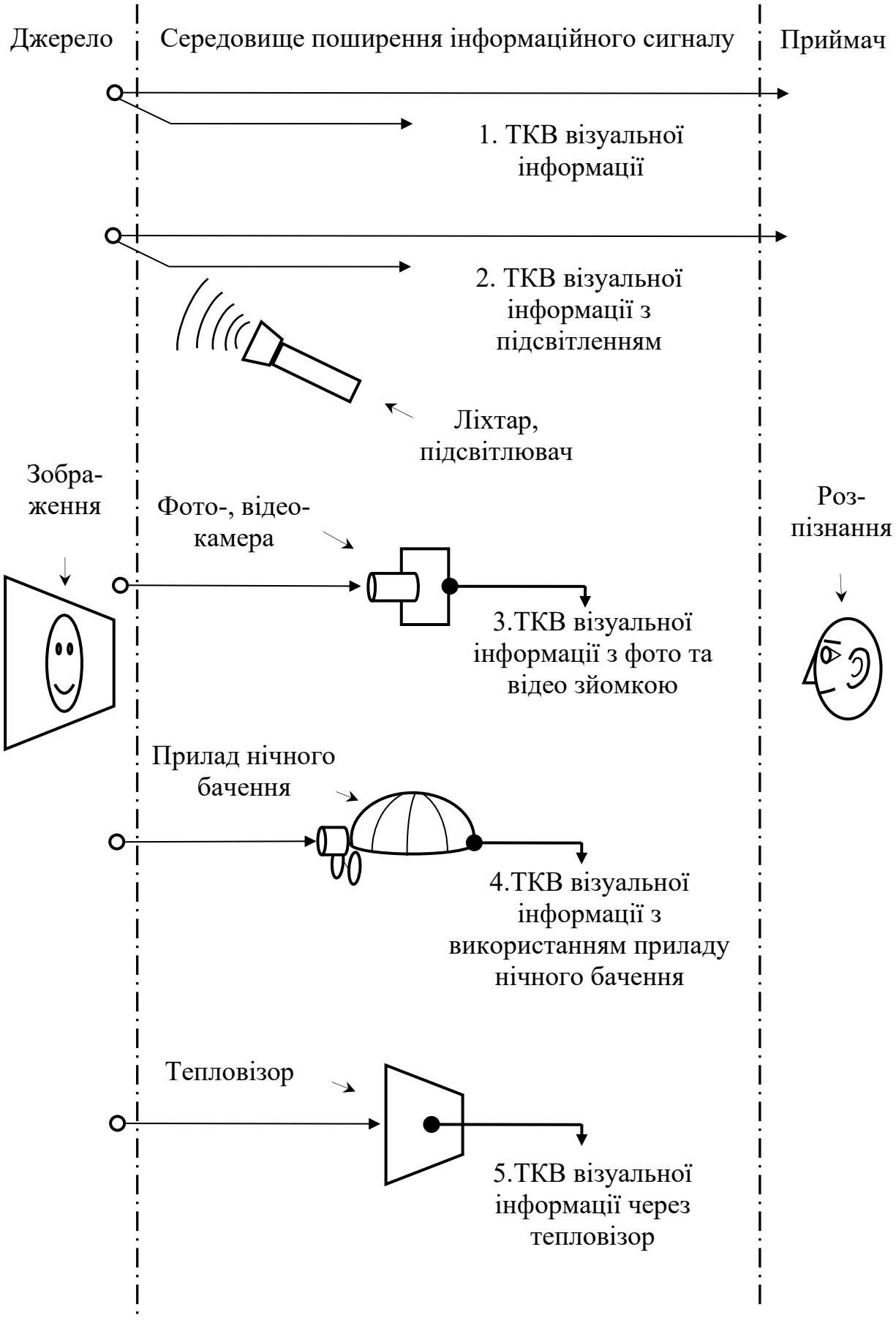


Рис. 1.2.3. Шляхи витоку візуальної інформації у вигляді зображень на ОІД

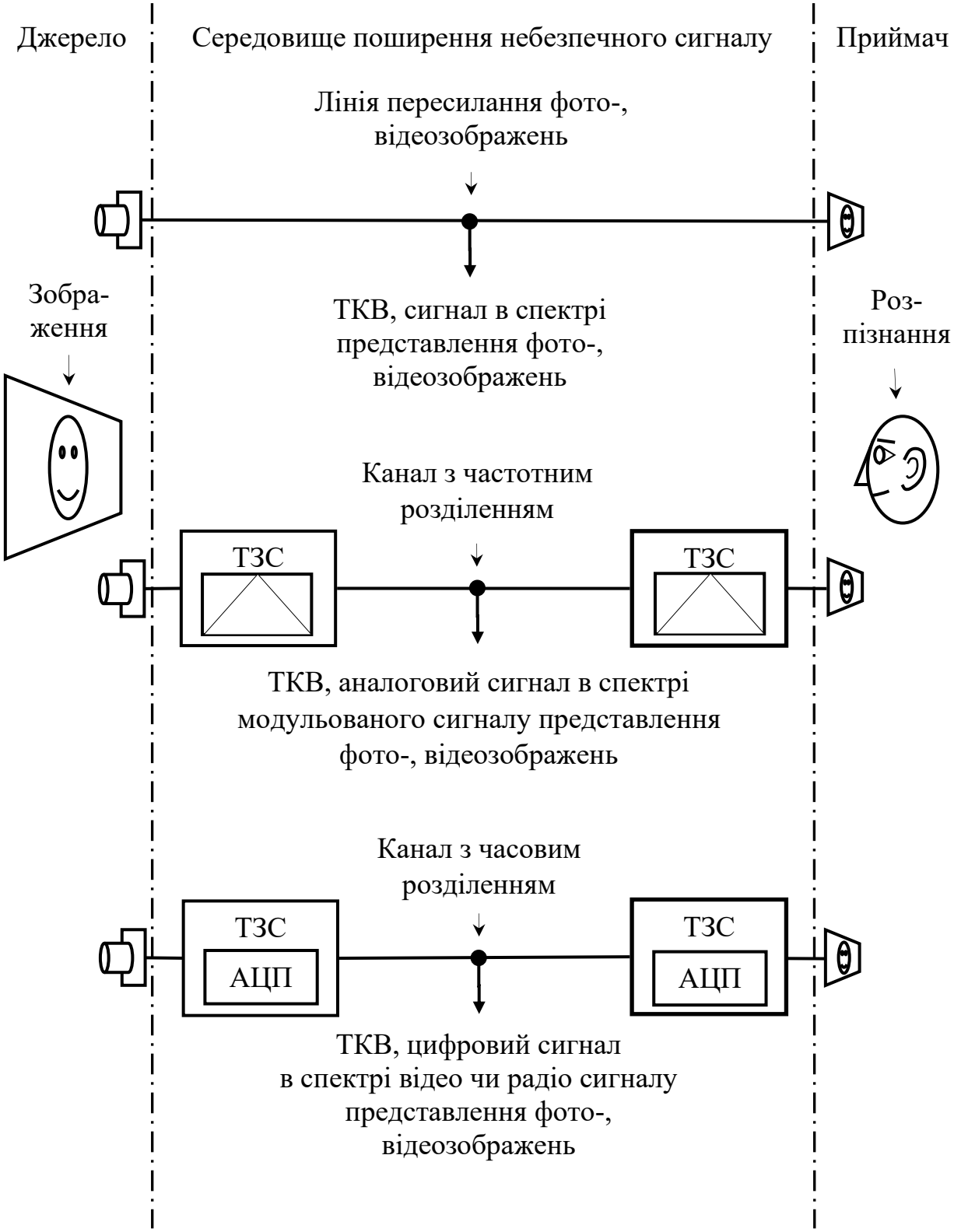


Рис. 1.2.4. Шляхи витоку візуальної інформації через ІКС, ТЗС. Електричні та електромагнітні ТКВ візуальної інформації

– зв'язок розпізнання з відношенням сигнал/завада може мати різний ланцюг показників захищеності, а тому, так само як і для мовних джерел, захист візуальної інформації від витоку може бути забезпечений шляхом впливу на кожен з них;

– перебування візуальної інформації в цифровому вигляді для її захисту може також, як і для мовних чи інших джерел витоку, дозволити застосування математичних методів захисту, наприклад, випадкового кодування.

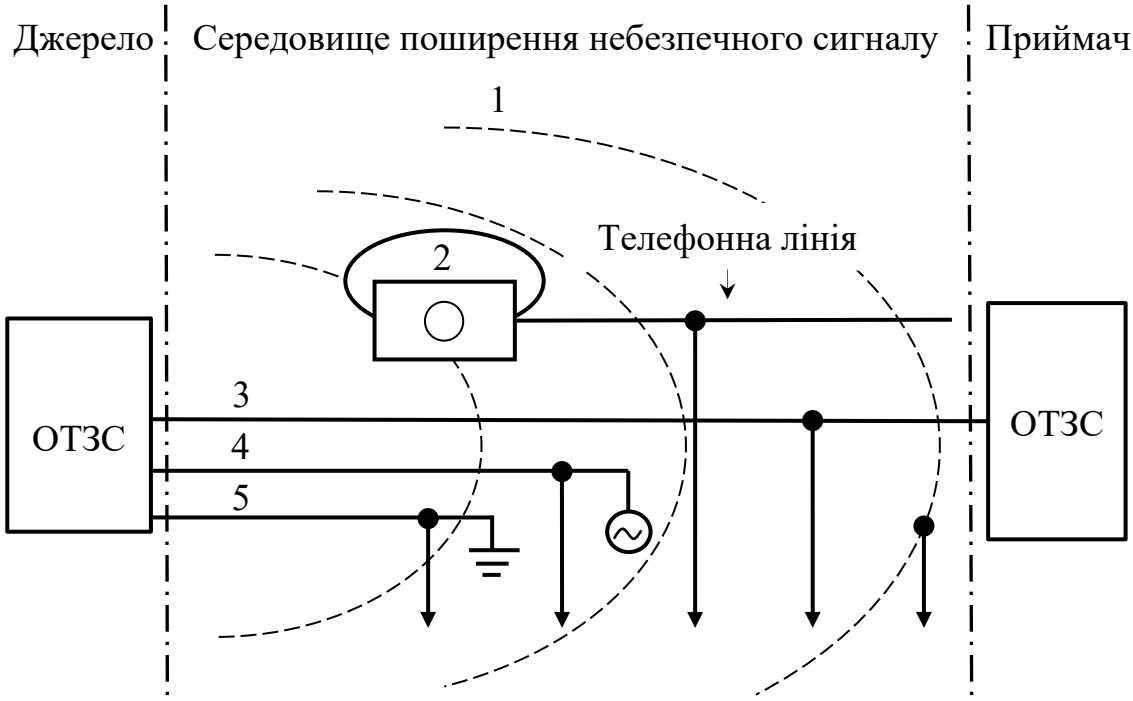
Таким чином, проведено огляд особливостей інформаційних сигналів, їхніх фізичних носіїв, середовищ та шляхів поширення з точки зору убезпечення технічних каналів витоку для джерел візуальної інформації. Визначено основні ризик-орієнтовані підходи щодо убезпечення цієї інформації та показники, які характеризують захищеність візуальної інформації від витоку технічними каналами та можуть бути використаними як нормативні.

Особливості інформаційних сигналів, їхніх фізичних носіїв, середовищ та шляхів поширення з точки зору убезпечення інформації від витоку технічними каналами для цифрових джерел інформації. Технічні канали витоку від цифрових джерел інформації поряд з іншими каналами, що виникають від джерел мовної та візуальної інформації, мають суттєву особливість. Це полягає в наступному (див. рис. 1.2.5):

– цифровим джерелом витоку є завжди основні технічні засоби та системи (ОТЗС) обробки та передачі інформації, які переважно електронні та зазвичай належать до ІКС. Тому технічними каналами витоку інформації є всі ті канали (електромагнітні, електричні через допоміжні технічні засоби, пристрої заземлення, мережі електропостачання тощо), що можуть виникати від технічних засобів під час їхньої роботи;

– приймачем цього виду фізичного носія та інформації, як і джерело, завжди є технічний засіб, до якого вже не можна застосувати такі показники захищеності, як розбірливість та розпізнання, за винятком окремих випадків, коли сигналом є оцифровані мова чи зображення;

– середовище поширення візуальної інформації, з якого можливе перехоплення, як і для каналів витоку мовної та візуальної інформації, є фізичним середовищем з завадами. Однак, на відміну від зазначених каналів головним показником захищеності може бути вже не статистичні розбірливість та розпізнання, а імовірнісні. Це або пропускна здатність каналу, яка характеризує кількість інформації, що в середньому може пройти через канал, або імовірність неможливості виявлення ознак небезпечного сигналу, яка характеризує кількість (частину) даних, що в середньому втратилися в каналі витоку. Гранично допустимі значення цих показників мають бути забезпеченими певними гранично допустимими відношеннями сигнал/завада;



Електромагнітні та електричні ТКВ цифрової інформації

Позначення:
1) побічні електромагнітні випромінювання основних технічних засобів і систем (ОТЗС),
2) наведення електромагнітних випромінювань на допоміжні технічні засоби та системи (ДТЗС),
3) лінія (канал) з'єднання,
4) ланцюг живлення,
5) пристрій заземлення.

Рис.1.2.5. Шляхи витоку інформації від цифрових джерел (ІКС, ТЗС). Електричні та електромагнітні ТКВ цифрової інформації

– цифрові дані для поширення в неперервному середовищі можуть мати різні форми реалізацій (різнополярні, однополярні, ортогональні тощо). Тому зазначене гранично допустиме відношення сигнал/завада при забезпеченні одних і тих самих пропускної здатності каналу та імовірності неможливості виявлення ознак небезпечного сигналу в каналі для різних реалізацій може мати різне значення;

– пропускна здатність каналу та імовірність неможливості виявлення ознак небезпечного сигналу в каналі як показники захищеності цифрової інформації від витоку технічними каналами дозволяють застосування математичних методів перетворення, наприклад випадкового

кодування. Це кодування може зменшувати пропускну здатність та підвищувати імовірність неможливості виявлення ознак небезпечного сигналу при фіксованому відношенні сигнал/завада.

Таким чином, проведено огляд інформаційних сигналів, їхніх фізичних носіїв, середовищ та шляхів поширення з точки зору убезпечення інформації від витоку технічними каналами для цифрових джерел інформації. Визначено основні ризик-орієнтовані підходи щодо убезпечення цієї інформації та показники, які характеризують захищеність цифрової інформації від витоку технічними каналами та можуть бути використаними як нормативні.

Таким чином, проведено огляд особливостей витоку сигналів, їхніх фізичних носіїв, середовищ та шляхів поширення з точки зору убезпечення інформації від витоку технічними каналами для мовних, візуальних та цифрових джерел. Визначено основні ризик-орієнтовані підходи щодо убезпечення інформації та показники, які характеризують захищеність цієї інформації від витоку технічними каналами та можуть бути використаними як нормативні.

Захищеність зазначених джерел витоку інформації, яка визначатиметься граничними значеннями на показники захищеності цих джерел, вимагає проведення окремих обґрунтувань зав’язків між цими показниками та ризиком інформаційної безпеки. Знаходженню цих зав’язків присвячені наступні розділи дисципліни.

Контрольні питання:

1. Особливості інформаційних сигналів, їхніх фізичних носіїв, середовищ та шляхів поширення з точки зору убезпечення інформації від витоку технічними каналами на ОІД для мовних акустичних джерел.
2. Особливості інформаційних сигналів, їхніх фізичних носіїв, середовищ та шляхів поширення через інформаційно-комунікаційні системи та інші електронні технічні засоби та системи для мовних джерел.
3. Особливості інформаційних сигналів, їхніх фізичних носіїв, середовищ та шляхів поширення з точки зору убезпечення інформації від витоку технічними каналами для візуальної інформації (зображень).
4. Особливості інформаційних сигналів, їхніх фізичних носіїв, середовищ та шляхів поширення через інформаційно-комунікаційні системи та інші електронні технічні засоби та системи для візуальних джерел інформації.
5. Особливості енергетичних показників захищеності цифрових джерел витоку інформації – інформаційно-комунікаційних систем та інших електронних технічних засобів та систем.

РОЗДІЛ 2. КІЛЬКІСНІ ПОКАЗНИКИ ТА ПРОПУСКНА ЗДАТНІСТЬ ДЛЯ УБЕЗПЕЧЕННЯ ІНФОРМАЦІЇ ВІД ВИТОКУ ТЕХНІЧНИМИ КАНАЛАМИ

2.1. Дискретне джерело як опис джерела витоку та кількість інформації на його виході

Кількість інформації на виході дискретного джерела, його ентропія, продуктивність та надлишковість. Під *інформацією* будемо розуміти сукупність відомостей про будь-що (стан матеріальної системи, або її елементів, стан суспільства, явища природи тощо), які можуть бути об’єктами зберігання, передачі та перетворення.

Дуже часто поняття інформації ототожнюють з її формою існування, хоча по суті вони означають не одне і те ж. Існування інформації, її передача, обробка та зберігання здійснюється через повідомлення, дані або сигнали (див. рис. 2.1.1). Говорять, що повідомлення, дані та сигнал містять, або несуть в собі інформацію.

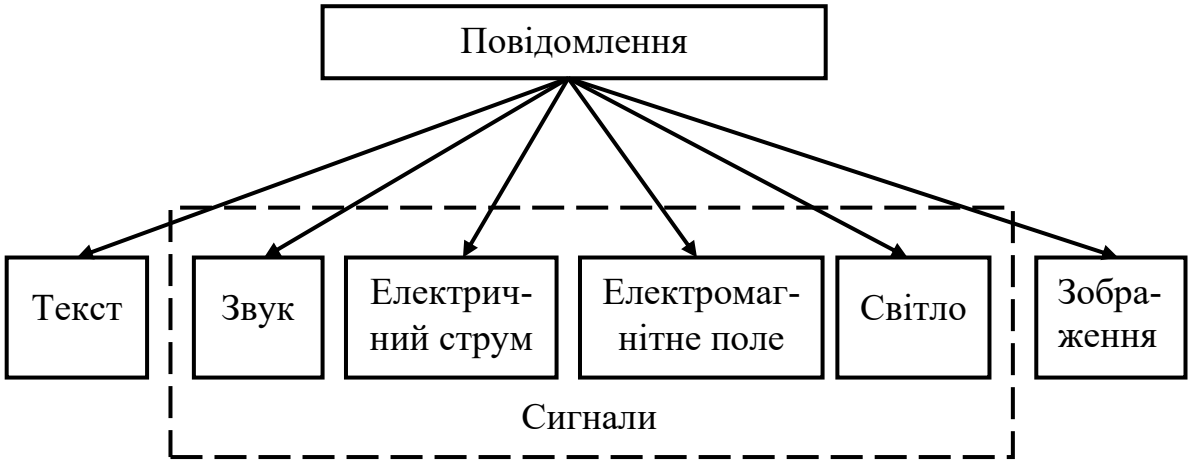


Рис.2.1.1. Способи подання повідомлень

Повідомлення – це загальна форма подання інформації. Повідомленням, як правило, вважають інформацію, якою повідомляють, яку передають та отримують (див. рис. 2.1.1). Наприклад, в давні часи це була передача якихось предметів з викарбуваними знаками, листівок з текстом тощо. Пізніше, з появою відповідної техніки зв’язку (телефонного, телеграфного, передачі даних) інформацію почали передавати за допомогою сигналів, з використанням фізичних процесів та властивостей їх розповсюдження в різних середовищах: ефірі, струмопровідних лініях тощо. Як приклад, це – поширення коливань електромагнітних полів, акустичні хвилі, світло тощо. Властивості полів зберігати пропорційність

значень амплітуд та форми зміни миттєвих значень при поширенні їхніх коливань в просторі дозволяють передавати інформацію на великі відстані.

Сучасні інформаційні та комунікаційні системи використовують цифрову форму подання інформації – дані, або послідовність символів знаків. На теперішній час дані не тільки передаються каналами зв'язку, за допомогою даних інформація в сучасній техніці може досить ефективно оброблятися та зберігатись у великих обсягах.

Інформація або повідомлення зазвичай утворюються відповідними джерелами. Джерела інформації розділяють на дискретні та неперервні.

Якщо джерело виробляє послідовність знаків, літер, символів або інших дискретних елементів, то таке джерело називають дискретним джерелом. Якщо ж джерелом формуються безперервні сигнали, тобто сигнали, які в часі приймають значення на безперервній множині, називають неперервними джерелами.

Розглянемо сутність кількісної міри інформації на виході дискретного джерела, його ентропію, продуктивність та надлишковість.

Нехай дискретне джерело інформації виробляє деяке повідомлення, для простоти – послідовність двійкових символів $X^n_k = (x_1, x_2, x_3, \ldots, x_n)$ довжиною n, де $x = \{0, 1\}$, $k = 1, 2, 3, \ldots, 2^n$ (див. рис. 2.1.2). Індекс k означає номер комбінації символів із всіх можливих 2^n комбінацій.

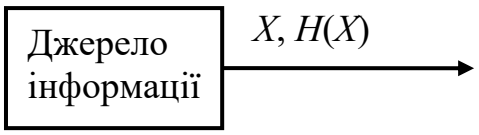


Рис.2.1.2. Джерело інформації

Наприклад:

Для послідовності довжиною 3 може бути 8 комбінацій, де $k = 1 \div 8$:

$$X^3_1 = (0, 0, 1);$$

$$X^3_2 = (0, 1, 0);$$

$$X^3_3 = (0, 1, 1);$$

$$X^3_4 = (1, 0, 0);$$

$$X^3_5 = (1, 0, 1);$$

$$X^3_6 = (1, 1, 0);$$

$$X^3_7 = (1, 1, 1);$$

$$X^3_8 = (0, 0, 0).$$

Кількісна міра інформації повинна відповідати інтуїтивним уявленням та задовольняти наступні властивості:

1. Якщо джерело виробляє вже відоме повідомлення (або, як приклад, періодичну послідовність), то таке повідомлення в собі не повинно містити інформації, оскільки при цьому не додається ніяких відомостей. Поява на виході джерела такої послідовності однозначно визначена і тому її імовірність буде рівною одиниці.

2. Якщо джерело виробляє повідомлення про майже відому подію, але уточнюються деякі невідомі деталі, то очевидно, що воно буде містити певну інформацію, хоча можливо й незначну. При цьому імовірність даної послідовності знаків буде близькою, але не рівною одиниці.

3. Якщо джерело виробляє повідомлення про малоймовірну подію, тобто подію, яка є сенсацією, то вона несе в собі багато інформації.

Таким чином, міра інформації повинна відображати ступінь новизни, оригінальності, несподіваності повідомлення та бути функцією імовірності його появи.

Так, якщо дискретне джерело виробляє повідомлення X^n_k з імовірністю $p(X^n_k)$, то кількість інформації:

$$i(X^n_k) = i(p(X^n_k)).$$

Вище вказані властивості можуть бути виражені математично, як вимоги до введеної функції:

1) $i(X^n_k) = 0$, якщо $p(X^n_k) = 1$;

2) $i(p(X^n_k))$ – неперервна функція, що диференціюється від аргументу $p(X^n_k)$;

3) $i(X^n_k, X^m_j) = i(X^n_k) + i(X^m_j)$, де $i(X^n_k, X^m_j)$ – кількість інформації в парі повідомлень X^n_k, X^m_j, якщо вони незалежні (умова адитивності).

Функцією, що задовольняє ці вимоги, є логарифмічна функція:

$$i(X^n_k) = \log_a \frac{1}{p(X^n_k)}, \qquad (2.1.1)$$

де a – довільне число $a > 1$, яке є основою логарифма і визначає систему виміру кількості інформації.

На практиці зручно користуватися $a = 2$, при цьому одиницею виміру інформації є так звана двійкова одиниця, або всім знайомий “біт”, який є скороченням англійських слів *binary unit*. Число a може бути і будь-яким іншим більшим одиниці, але при цьому система виміру буде відповідною.

Отже формула (2.1.1) означає власну кількість інформації, що несе в собі вся послідовність X^n_k і є функцією від випадкової величини – її імовірності.

Якщо всі вироблені послідовності X^n_k будуть рівноймовірними, то

$$i(X^n_k) = \log_a 2^n = n \log_a 2.$$

При цьому слід зазначити, що при $a = 2$ кількість інформації $i(X^n_k)$ співпадає з кількістю розрядів послідовності X^n_k.

Для охарактеризування джерела знайдемо цю величину в середньому.

Так, середня кількість інформації, що припадає на один символ послідовності X^n_k , знаходиться шляхом ділення на її довжину:

$$i(x) = \frac{1}{n}\log_a \frac{1}{p(X^n_k)}. \qquad (2.1.2)$$

Середньою ж кількістю інформації на один символ послідовності за всіма реалізаціями X^n_k для всіх значень k ($k = 1, 2, 3,\ldots, 2^n$) є математичне сподівання функції (2.1.2):

$$H(X) = M\left\{\frac{1}{n}\log_a \frac{1}{p(X^n_k)}\right\} = \lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^{2^n} p(X^n_k)\log_a \frac{1}{p(X^n_k)}. \qquad (2.1.3)$$

Формула (2.1.3) є визначенням так названої *ентропії*, під якою розуміють середню кількість інформації, що припадає на один символ нескінченно довгого повідомлення (послідовності) за всіма її можливими реалізаціями. Ентропія вимірюється в бітах.

Говорять, що *інформація* є невизначеністю, а *ентропія* – мірою невизначеності.

Інколи, окрім як ентропією, джерело інформації характеризують продуктивністю, збитковістю.

Під *продуктивністю* розуміють характеристику джерела (процесу формування повідомлення), яка виражається як середня кількість інформації, що вироблена за одиницю часу нескінченно довгого повідомлення за всіма можливими його реалізаціями. Вона має одиницю виміру [біт/с] та виражається формулою:

$$H'(X) = F_т H(X),$$

де $F_т$ – частота надходження імпульсів джерела.

Під *надлишковістю* розуміють величину, яка характеризує джерело з точки зору його неінформативності.

Надлишковість буває абсолютною та відносною.

Абсолютна надлишковість визначається як величина, якої не вистачає до максимуму ентропії джерела та виражається формулою:

$$\rho = H_{\max} - H(X).$$

Якщо ентропія виражена в бітах, то:

$$\rho = 1 - H(X).$$

Відносна надлишковість являє собою нормовану абсолютну збитковість по максимуму ентропії джерела та виражається формулою:

$$\rho' = \frac{H_{\max} - H(X)}{H_{\max}}.$$

Таким чином, проведено огляд дискретного джерела як опису джерела витоку інформації. Обґрунтовано кількісну міру інформації на його виході. Розкрито сутність ентропії, продуктивності та абсолютної і відносної надлишковостей дискретного джерела з довільним розподілом. Отримано співвідношення щодо їх оцінювання.

Ентропія, продуктивність та надлишковість двійкового джерела з бернуллієвським розподілом. Найпростішим різновидом дискретного джерела інформації є *дискретне джерело без пам'яті з бернуллієвським розподілом або бернуллієвське джерело*. Під цим джерелом будемо розуміти таке дискретне джерело, для якого поява кожного наступного символа не залежить від передісторії всіх попередніх.

Визначимо його розподіл ймовірностей.

Нехай дискретне джерело інформації виробляє повідомлення, для простоти – послідовність двійкових символів $X^n_k = (x_1, x_2, x_3,\ldots, x_n)$, де $n \to \infty$ (див. рис. 2.1.2).

Тоді умова незалежності може бути вираженою так:

$$p(x_i = 1) = p(x_i = 1 / x_1, x_2, x_3, ..., x_{i-1})$$

та

$$p(x_i = 0) = p(x_i = 0 / x_1, x_2, x_3, ..., x_{i-1}).$$

де $p(x_i = 1)$ та $p(x_i = 0)$ – безумовні імовірності того, що довільно взятий, але фіксований символ x_i, що формується джерелом, приймає значення "1", або "0"; $p(x_i = 1 / x_1, x_2, x_3,\ldots, x_{i-1})$ та $p(x_i = 0 / x_1, x_2, x_3,\ldots, x_{i-1})$ – умовні імовірності символу x_i за умови всієї передісторії.

Різновидом дискретного джерела без пам'яті є джерело з бернуллієвським розподілом ймовірностей – *бернуллієвське дискретне джерело*, для якого імовірності однойменних символів рівні між собою за всіма i. Відповідно сума ймовірностей різнойменних символів, як повна група, складає одиницю. Для бернуллієвського джерела двійкових символів розподіл ймовірностей має вигляд:

$$p(x = 1) = p_x; \quad p(x = 0) = 1 - p_x = q_x \qquad (2.1.4).$$

Розглянемо деякі властивості бернуллііївського розподілу, а саме, для знаходження ентропії джерела, виразимо імовірність $p(X^n_k)$ через введені позначення (2.1.4).

Вочевидь, імовірність послідовності $X^n_k = (x_1, x_2, x_3,\ldots, x_n)$ дорівнює добутку ймовірностей її символів:

$$p(X^n_{k,b}) = p_x^b(1 - p_x)^{n-b}, \qquad (2.1.5)$$

де b – вага послідовності X^n_k, яка означає кількість одиниць в ній; $X^n_{k,b}$ – послідовність X^n_k з вагою b.

Оскільки у визначенні імовірності послідовності $X^n_{k,b}$ індекс k не бере участі, то надалі в записі $X^n_{k,b}$ даний індекс опускатимемо – X^n_b.

Наприклад:

Імовірність послідовності X^7_4 = (1, 0, 0, 1, 1, 0, 1) довжиною 7 та вагою 4 дорівнює:

$$p(1,0,0,1,1,0,1) = p_x^4(1 - p_x)^3,$$

а для X^7_2 = (1, 0, 0, 0, 0, 0, 1) –

$$p(1,0,0,0,0,0,1) = p_x^2(1 - p_x)^5.$$

Знайдемо ентропію, продуктивність та надлишковість для бернуллііївського дискретного джерела.

Для знаходження шуканої ентропії скористаємося формулою для загального випадку, яка має вигляд:

$$H(X) = \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{2^n} p(X^n_k) \log_2 \frac{1}{p(X^n_k)}. \qquad (2.1.6)$$

В даній формулі бернуллііївський розподіл дає право імовірності $p(X^n_k)$ замінити співвідношеннями (2.1.5), які визначаються імовірністю p_x та вагою b. При цьому знайдуться такі комбінації X^n_k, які матимуть одну вагу b, а тому їх імовірності будуть рівними.

В свою чергу кількість комбінацій $X^n_{k,b}$ однієї ваги визначається кількістю перестановок b одиниць в послідовності довжиною n:

$$C_n^b = \frac{n!}{b!(n-b)!} = \frac{n(n-1)(n-2)\ldots(n-(b-1))}{1\times 2\times 3\times\ldots\times b}. \qquad (2.1.7)$$

Наприклад:

Послідовність $X^4_{k,2}$ з вагою $b = 2$ має

$$C_4^2 = \frac{4\times 3}{2} = 6$$

комбінацій, а саме:

$$X^4_{1,2} = (0, 0, 1, 1);$$
$$X^4_{2,2} = (0, 1, 0, 1);$$
$$X^4_{3,2} = (1, 0, 0, 1);$$
$$X^4_{4,2} = (0, 1, 1, 0);$$
$$X^4_{5,2} = (1, 0, 1, 0);$$
$$X^4_{6,2} = (1, 1, 0, 0).$$

З врахуванням (2.1.5) та (2.1.7) ентропія (2.1.6) матиме вигляд:

$$H(X) = \lim_{n\to\infty} \frac{1}{n} \sum_{b=0}^{n} C_n^b p_x^b (1 - p_x)^{n-b} \log_2 \frac{1}{p_x^b (1 - p_x)^{n-b}}. \qquad (2.1.8)$$

У формулі (2.1.8) зазначимо, що сума здійснюється не за індексом k, а за вагою b з коефіцієнтами C^k_n.

Спростимо співвідношення (2.1.8).

З урахуванням властивостей логарифма його можна записати у вигляді:

$$H(X) = p_x \log_2 \frac{1}{p_x} \lim_{n\to\infty} \left(\sum_{b=0}^{n} \frac{b}{n} \frac{n!}{b!(n-b)!} p_x^{b-1} (1-p_x)^{n-b} \right) +$$

$$+(1-p_x) \log_2 \frac{1}{1-p_x} \lim_{n\to\infty} \left(\sum_{b=0}^{n} \frac{n-b}{n} \frac{n!}{b!(n-b)!} p_x^{b} (1-p_x)^{n-b-1} \right). \qquad (2.1.9)$$

Розглянемо множник першої складової:

$$\sum_{b=0}^{n} \frac{b}{n} \frac{n!}{b!(n-b)!} p_x^{b-1} (1-p_x)^{n-b} = \sum_{b=1}^{n} \frac{(n-1)!}{(b-1)!((n-1)-(b-1))!} \times$$

$$\times p_x^{b-1} (1-p_x)^{(n-1)-(b-1)} = \sum_{b=1}^{n} C_{n-1}^{b-1} p_x^{b-1} (1-p_x)^{(n-1)-(b-1)} = 1. \qquad (2.1.10)$$

В останньому складова суми з $b = 0$ виключена, оскільки вона дорівнюватиме 0, а рівність одиниці випливає з правила розкладання степеня суми в поліном:

$$(c+d)^n = \sum_{b=0}^{n} C_n^b c^b d^{n-b}.$$

Якщо прирівняти $c = p_x$ та $b = 1\text{-}p_x$, то впевнимося в стверджуваному:

$$\sum_{b=1}^{n} C_{n-1}^{b-1} p_x^{b-1} (1 - p_x)^{(n-1)-(b-1)} = (p_x + 1 - p_x)^{n-1} = (1)^{n-1} = 1.$$

Аналогічно можна показати, що і подібний множник другої складової в співвідношенні (2.1.9) буде рівним одиниці.

$$\sum_{b=0}^{n}\frac{n-b}{n}\frac{n!}{b!(n-b)!}p_x^b(1\text{-}p_x)^{n-b-1}=\sum_{b=0}^{n-1}\frac{(n-1)!}{b!((n-1)-b)!}\times$$

$$\times p_x^b(1\text{-}p_x)^{(n-1)-b}=\sum_{b=0}^{n-1}C_{n-1}^b p_x^b(1\text{-}p_x)^{(n-1)-b}=1. \qquad (2.1.11)$$

З врахуванням (2.1.10) та (2.1.11) співвідношення ентропії для бернуллііївського джерела (2.1.9) матиме вигляд:

$$H(X)=p_x\log_2\frac{1}{p_x}+(1-p_x)\log_2\frac{1}{1-p_x}=h(p_x). \qquad (2.1.12)$$

З останнього випливає, що ентропія джерела, яка розглядається, не залежить від довжини виробленої послідовності та визначається ентропійною функцією $h(p_x)$.

Продуктивність та надлишковості дискретного джерела без пам'яті визначаються відповідно за формулами:

$$H'(X)=F_{\text{т}}\left[p_x\log_2\frac{1}{p_x}+(1-p_x)\log_2\frac{1}{1-p_x}\right], \text{[біт/с]} \qquad (2.1.13)$$

$$\rho=1+p_x\log_2 p_x+(1-p_x)\log_2(1-p_x), \quad \text{[біт]} \qquad (2.1.14)$$

$$\rho'=1+p_x\log_2 p_x+(1-p_x)\log_2(1-p_x). \qquad (2.1.15)$$

Таким чином, розглянуто окремий випадок дискретного джерела, а саме джерела без пам'яті, що має бернуллііївський розподіл, як спрощеного опису джерела витоку інформації. Отримано співвідношення щодо оцінювання ентропії, продуктивності та абсолютної і відносної надлишковостей дискретного джерела з бернуллііївськи розподілом.

Таким чином, проведено огляд дискретного джерела як опису джерела витоку інформації. Обґрунтовано кількісну міру інформації на його виході. Розкрито сутність ентропії, продуктивності та абсолютної і відносної надлишковостей дискретного джерела з довільним розподілом. Отримано співвідношення щодо їх оцінювання.

Розглянуто окремий випадок дискретного джерела, а саме джерела без пам'яті, що має бернуллііївський розподіл. Отримано співвідношення щодо оцінювання його ентропії, продуктивності та абсолютної і відносної надлишковостей. Співвідношення є відносно нескладними та можуть бути використаними на практиці для оцінювання кількісних показників інформації на виході дискретних джерел.

Контрольні питання:

1. Дискретне джерело. Опис повідомлення на виході дискретного джерела.
2. Інтуїтивні уявлення та властивості, яким має відповідати міра інформації на виході джерела. Математична функція, що задовольняє ці уявлення та властивості. Одиниці виміру кількості інформації.
3. Середня кількість інформації на виході джерела. Ентропія, продуктивність та надлишковість дискретного джерела.
4. Бернуллііївське джерело. Бернуллііївський розподіл імовірностей на виході джерела.
5. Ентропія, продуктивність та надлишковість бернуллііївського джерела.

2.2. Дискретний канал як опис каналу витоку та кількість інформації, що проходить через дискретний канал

Кількість взаємної інформації в дискретному каналі. Під *дискретним каналом* будемо розуміти канал, для якого вхід та вихід можна описати дискретними даними (див. рис. 2.2.1).

Розглянемо вказаний канал.

Вважається, що канал заданий, якщо описано його (1) вхід, (2) вихід та (3) перехідні процеси як показано в табл. 2.2.1.

$$I(X;\ Y) = I(Y;\ X)$$

Рис. 2.2.1. Схема дискретного каналу

Для простоти розглянемо дискретний, двійковий канал.

Нехай на вхід каналу потрапляє деяка послідовність X^n_k довжини n, з імовірністю $P(X^n_k)$, де k – номер комбінації (k = 1, 2,…, 2^n). Імовірність $P(X^n_k)$ – є апріорною імовірністю, яка характеризує шанси противника на її відгадування до того, як вона передаватиметься по каналу.

В каналі під впливом завад послідовність X^n_k перетворюється в деяку двійкову послідовність Y^n_l тієї ж довжини, де l – номер комбінації (l = 1, 2,…, 2^n). Завада носить випадковий характер, тому це перетворення справедливо охарактеризувати умовною імовірністю $P(Y^n_l/X^n_k)$, яка є

мірою, що визначає можливість переходу послідовностей X^n_k в Y^n_l (див. табл. 2.2.1).

Таблиця 2.2.1

Опис дискретного каналу

№ з/п	Найме-нування	Опис
1	Вхід каналу	Вхідна послідовність: $X^n_k = (x_1, x_2, x_3,\ldots, x_n)$, де $x = \{0, 1\}$, $k = 1, 2, 3,\ldots, 2^n$, n – довжина. Розподіл імовірностей: $X^n_k \leftrightarrow P(X^n_k)$.
2	Вихід каналу	Вихідна послідовність: $Y^n_l = (y_1, y_2, y_3,\ldots, y_n)$, де $y = \{0, 1\}$, $l = 1, 2, 3,\ldots, 2^n$.
3	Перехідні процеси в каналі	Розподіл імовірностей переходів для всіх пар: $(X^n_k \rightarrow Y^n_l) \leftrightarrow P(Y^n_l/X^n_k)$.

Після отримання на виході каналу повідомлення Y^n_l завданням приймача є визначення повідомлення X^n_k, що надійшло в канал. Для цього на прийомі необхідно провести статистичний аналіз та визначити всі можливі умовні імовірності $P(X^n_k/Y^n_l)$. $P(X^n_k/Y^n_l)$ є апостеріорною імовірністю, яка означає можливість існування на вході каналу послідовності X^n_k, якщо на виході з'явилась – Y^n_l.

Знайдемо кількість взаємної інформації між входом та виходом каналу – інформації, що виробилась джерелом X з ентропією $H(X)$ та пройшла через канал на його вихід Y.

Ця міра повинна задовольняти наступні умови:

1) якщо повідомлення на виході каналу не збільшило знання про повідомлення, що передавалося:

$$P(X^n_k/Y^n_l) = P(X^n_k),$$

то інформація зовсім не пройшла через канал;

2) якщо повідомлення на виході каналу однозначно визначає повідомлення на вході каналу:

$$P(X^n_k/Y^n_l) = 1,\ k = l,$$

$$P(X^n_k/Y^n_l) = 0,\ k \neq l,$$

то інформація повністю пройшла через канал;

3) якщо отримання послідовності на виході каналу змінює статистику повідомлення на вході каналу:

$$P(X^n_k/Y^n_l) \neq P(X^n_k),$$

то інформація частково пройшла через канал, а частково втратилася.

Таким чином, кількість інформації, що пройшла через канал є функцією від зміни апостеріорної імовірності $P(X^n_k/Y^n_l)$ відносно апріорної – $P(X^n_k)$. Ця функція має вигляд:

$$i(X^n_k;Y^n_l) = \log \frac{p(X^n_k / Y^n_l)}{p(X^n_k)} . \qquad (2.2.1)$$

Функція (2.2.1) повністю відображає наші інтуїтивні уявлення про кількість інформації, яка проходить через дискретний канал. Нескладно в цьому впевнитися, якщо проаналізувати вище вказані умови.

Покажемо, що кількість взаємної інформації між входом і виходом каналу не залежить від того, відносно чого її оцінюють: входу чи виходу.

Для цього в правій частині співвідношення (2.2.1) помножимо числівник та знаменник на $P(Y^n_l)$:

$$i(X^n_k;Y^n_l) = \log \frac{p(X^n_k / Y^n_l)p(Y^n_l)}{p(X^n_k)p(Y^n_l)} =$$

$$= \log \frac{p(X^n_k, Y^n_l)}{p(X^n_k)p(Y^n_l)} = \log \frac{p(Y^n_l / X^n_k)p(X^n_k)}{p(Y^n_l)p(X^n_k)} =$$

$$= \log \frac{p(Y^n_l / X^n_k)}{p(Y^n_l)} = i(Y^n_l;X^n_k) \qquad (2.2.2)$$

В перетвореннях співвідношення (2.2.3) використана формула для повної імовірності:

$$p(X^n_k)p(Y^n_l / X^n_k) = p(X^n_k, Y^n_l) =$$

$$= p(Y^n_l, X^n_k) = p(Y^n_l)p(X^n_k / Y^n_l) \ . \qquad (2.2.3)$$

Щоб охарактеризувати канал, необхідно знайти кількість взаємної інформації в середньому за всіма реалізаціями X^n_k та Y^n_l, яка виражатиметься через математичне сподівання:

$$I(X;Y) = M\left\{\frac{1}{n} i(X^n_k;Y^n_l)\right\} =$$

$$= \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{2^n} \sum_{l=1}^{2^n} p(X^n_k, Y^n_l) \log \frac{p(X^n_k, Y^n_l)}{p(X^n_k)p(Y^n_l)} . \qquad (2.2.4)$$

Співвідношення (2.2.4) можна спростити та виразити через безумовні та умовні ентропії, скориставшись формулою (2.2.2) та (2.2.3):

$$I(X;Y)=\lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^{2^n}\sum_{l=1}^{2^n}p(X_k^n)p(Y_l^n/X_k^n)\log\frac{p(X_k^n/Y_l^n)}{p(X_k^n)}=$$

$$=\lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^{2^n}\sum_{l=1}^{2^n}p(X_k^n)p(Y_l^n/X_k^n)\log\frac{1}{p(X_k^n)}-$$

$$-\lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^{2^n}\sum_{l=1}^{2^n}p(X_k^n)p(Y_l^n/X_k^n)\log\frac{1}{p(X_k^n/Y_l^n)}=$$

$$=\lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^{2^n}p(X_k^n)\log\frac{1}{p(X_k^n)}-$$

$$-\lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^{2^n}\sum_{l=1}^{2^n}p(X_k^n,Y_l^n)\log\frac{1}{p(X_k^n/Y_l^n)}. \qquad (2.2.5)$$

Вочевидь перша складова у співвідношенні (2.2.5) є ентропією джерела – $H(X)$, яку називають безумовною ентропією.

$$H(X)=\lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^{2^n}p(X_k^n)\log\frac{1}{p(X_k^n)}. \qquad (2.2.6)$$

Другу складову називають умовною ентропією, яка виражається формулою:

$$H(X/Y)=\lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^{2^n}\sum_{l=1}^{2^n}p(X_k^n,Y_l^n)\log\frac{1}{p(X_k^n/Y_l^n)}. \qquad (2.2.7)$$

Умовна ентропія (2.2.7) означає невизначеність вхідної послідовності X^n_k, за умови якщо на виході отримана послідовність Y^n_l.

Аналогічним чином співвідношення (2.2.4) можна перетворити та виразити через безумовну та умовну ентропії відносно виходу каналу:

$$I(X;Y)=\lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^{2^n}\sum_{l=1}^{2^n}p(Y_l^n)p(X_k^n/Y_l^n)\log\frac{p(Y_l^n/X_k^n)}{p(Y_l^n)}=$$

$$=\lim_{n\to\infty}\frac{1}{n}\sum_{l=1}^{2^n}\sum_{k=1}^{2^n}p(Y_l^n)p(X_k^n/Y_l^n)\log\frac{1}{p(Y_l^n)}-$$

$$-\lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^{2^n}\sum_{l=1}^{2^n}p(Y_l^n)p(X_k^n/Y_l^n)\log\frac{1}{p(Y_l^n/X_k^n)}=$$

$$= \lim_{n\to\infty} \frac{1}{n} \sum_{l=1}^{2^n} p(Y_l^n) \log \frac{1}{p(Y_l^n)} -$$

$$- \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{2^n} \sum_{l=1}^{2^n} p(Y_l^n, X_k^n) \log \frac{1}{p(Y_l^n / X_k^n)}. \quad (2.2.8)$$

При перетвореннях було використано формулу повної імовірності:

$$p(Y_l^n) = \sum_{k=1}^{2^n} p(Y_l^n, X_k^n) = \sum_{k=1}^{2^n} p(X_k^n) p(Y_l^n / X_k^n). \quad (2.2.9)$$

У формулі взаємної інформації (2.2.9) перша складова є безумовною ентропією виходу каналу *Y*, а друга – умовною ентропією виходу каналу *Y* відносно входу *X*. Відповідно ці ентропії мають співвідношення:

$$H(Y) = \lim_{n\to\infty} \frac{1}{n} \sum_{l=1}^{2^n} p(Y_l^n) \log \frac{1}{p(Y_l^n)}, \quad (2.4.10)$$

$$H(Y / X) = \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{2^n} \sum_{l=1}^{2^n} p(Y_l^n, X_k^n) \log \frac{1}{p(Y_l^n / X_k^n)}. \quad (2.2.11)$$

Отже, взаємна інформація в каналі виражається через безумовні та умовні ентропії:

$$I(X;Y) = H(X) - H(X/Y) = H(Y) - H(Y/X) = I(Y;X). \quad (2.2.12)$$

Таким чином, проведено огляд дискретного каналу як опису каналу витоку інформації. Обґрунтовано кількісну міру інформації, що проходить через дискретний канал. Розкрито сутність взаємної інформації та отримано її співвідношення через відношення апостеріорної та апріорної ентропій.

Введено поняття безумовних та умовних ентропій. Отримані співвідношення відносно входу та відносно виходу каналу через безумовні та умовні ентропії.

Кількість взаємної інформації в дискретному симетричному каналі без пам'яті. Під дискретним симетричним каналом (ДСК) без пам'яті будемо розуміти канал, для якого перехідний процес для будь-якого елемента послідовності, що передається, не залежить від попередніх переходів та статистичних властивостей джерела повідомлень, а також має бернуллііївський розподіл ймовірностей.

Для вказаного каналу, якщо імовірність відсутності помилки передачі позначити як *q*, то імовірність наявності помилки (спотворення вхідних символів) виражаються формулою:

$$p = \frac{1-q}{a-1},$$

де a – об'єм алфавіту вхідної послідовності.

Для двійкового симетричного каналу без пам'яті (a = 2) імовірність помилки:

$$p = 1 - q.$$

ДСК без пам'яті є адитивним каналом (див. рис. 2.2.2):

$$y = x \oplus e, \tag{2.2.13}$$

де e – помилка, на яку відрізняється вихідний символ від вхідного; $\oplus$ – операція додавання за модулем 2.

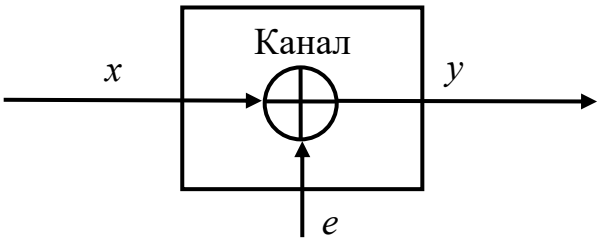


Рис. 2.2.2. Схема дискретного адитивного каналу

Для простоти розглянемо двійковий ДСК без пам'яті (a = 2), для якого вхідні, вихідні символи та символи помилки двійкові:

$$x = \{0, 1\}, y = \{0, 1\}, e = \{0, 1\},$$

Його зручно зобразити у вигляді графу станів (див. рис. 2.2.3).

На графі станів ДСК без пам'яті імовірності переходів матимуть наступні значення (див. рис. 2.2.3):

$$\left.\begin{aligned} p(y=1/x=1) = q = 1-p \\ p(y=0/x=0) = q = 1-p \end{aligned}\right\} \text{ при відсутній помилці в каналі},$$

$$\left.\begin{aligned} p(y=1/x=0) = p \\ p(y=0/x=1) = p \end{aligned}\right\} \text{ при наявності помилки в каналі}. \tag{2.2.14}$$

Як відомо, канал вважається заданим, якщо описані його вхід, вихід та перехідні процеси. Задамо дискретний симетричний канал без пам'яті.

Нехай на вхід дискретного симетричного каналу без пам'яті надходить послідовність від бернуллііївського джерела з параметром – p. Тоді вказаний канал можна описати, як показано в табл. 2.2.2.

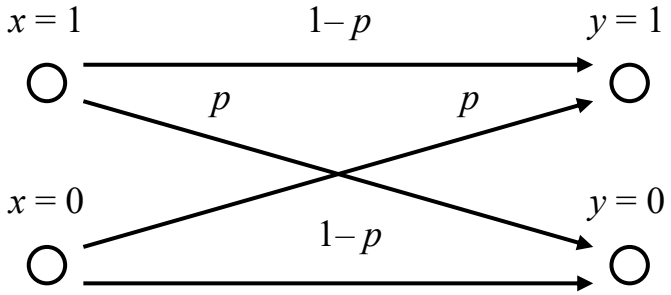


Рис. 2.2.3. Граф станів дискретного симетричного каналу без пам’яті

Таблиця 2.2.2

Опис дискретного симетричного каналу без пам’яті

№ з/п	Найме-нування	Опис
1	Вхід каналу	Вхідна послідовність: $x = \{0, 1\}$. Розподіл імовірностей: $p(x = 1) = p_x$, $p(x = 0) = 1 - p_x$
2	Вихід каналу	Вихідна послідовність: $y = \{0, 1\}$.
3	Перехідні процеси в каналі	Розподіл імовірностей переходів $(x \to y) \leftrightarrow p(y/x)$: $p(y = 1 / x = 1) = 1 - p$, $p(y = 1 / x = 0) = p$, $p(y = 0 / x = 0) = 1 - p$, $p(y = 0 / x = 1) = p$.

Для оцінювання взаємної інформації для ДСК без пам’яті скористаємося загальною формулою:

$$I(X;Y) = H(X) - H(X/Y) = H(Y) - H(Y/X) \qquad (2.2.15)$$

та знайдемо потрібні для цього складові: $H(X)$, $H(X/Y)$, $H(Y)$, $H(Y/X)$.

– Безумовна ентропія $H(X)$:

$$H(X) = \sum_x p(x)\log_2 \frac{1}{p(x)} =$$

$$= -p_x \log_2 p_x - (1 - p_x)\log_2(1 - p_x) = h(p_x). \qquad (2.2.16)$$

Праву частину виразу (2.2.16) отримано виходячи з того, що вхід послідовність каналу X має бернуллііївський розподіл ймовірностей:

$$p(x = 1) = p_x$$

та

$$p(x = 0) = 1 - p_x.$$

– Умовна ентропія $H(X/Y)$:

$$H(X/Y) = \sum_x \sum_y p(x,y)\log_2 \frac{1}{p(x/y)} =$$

$$= p_{x,y}(0,0)\log_2 \frac{1}{p_{x/y}(0/0)} + p_{x,y}(1,0)\log_2 \frac{1}{p_{x/y}(1/0)} +$$

$$+ p_{x,y}(0,1)\log_2 \frac{1}{p_{x/y}(0/1)} + p_{x,y}(1,1)\log_2 \frac{1}{p_{x/y}(1/1)}, \qquad (2.2.17)$$

Виразимо потрібні імовірності через початкові дані: p_x та p:

$$p(x,y) = p(x)p(y/x) \qquad p(y/x) = \ldots$$

$$p_{x,y}(0,0) = p_x(0)p_{y/x}(0/0) = (1-p_x)(1-\text{p}) \qquad p_{y/x}(0/0) = 1-p$$

$$p_{x,y}(1,0) = p_x(1)p_{y/x}(0/1) = p_x p \qquad p_{y/x}(1/0) = p$$

$$p_{x,y}(0,1) = p_x(0)p_{y/x}(1/0) = (1-p_x)p \qquad p_{y/x}(0/1) = p$$

$$p_{x,y}(1,1) = p_x(1)p_{y/x}(1/1) = p_x(1-p) \qquad p_{y/x}(1/1) = 1-p$$

$$p(x/y) = \frac{p(x,y)}{p(y)} = \frac{p(x,y)}{\sum_x p(x,y)}$$

$$p_{x/y}(0/0) = \frac{p_{x,y}(0,0)}{p_y(0)} = \frac{(1-p_x)(1-p)}{(1-p_x)(1-p)+p_x p}$$

$$p_{x/y}(1/0) = \frac{p_{x,y}(1,0)}{p_y(0)} = \frac{p_x p}{(1-p_x)(1-p)+p_x p}$$

$$p_{x/y}(0/1) = \frac{p_{x,y}(0,1)}{p_y(1)} = \frac{(1-p_x)p}{(1-p_x)p+p_x(1-p)}$$

$$p_{x/y}(1/1) = \frac{p_{x,y}(1,1)}{p_y(1)} = \frac{p_x(1-p)}{(1-p_x)p+p_x(1-p)}$$

$$p(y) = \sum_x p(x,y)$$

$$\begin{aligned} p_y(0) &= (1-p_x)(1-p)+p_x p \\ p_y(1) &= (1-p_x)p+p_x(1-p) \end{aligned}.$$

– Безумовна ентропія $H(Y)$:

$$H(Y) = \sum_{y} p(y)\log_2 \frac{1}{p(y)} =$$

$$= -p_y(1)\log_2 p_y(1) - p_y(0)\log_2 p_y(0)\,. \qquad (2.2.18)$$

Виразимо потрібні імовірності, як і в попередньому випадку, через початкові дані: p_x та p:

$$p(y) = \sum_{x} p(x,y)$$

$$p_y(0) = (1 - p_x)(1 - p) + p_x p$$

$$p_y(1) = (1 - p_x)p + p_x(1 - p)$$

Не важко показати, що вихід каналу Y також має бернуллііївський розподіл, перевіривши, що сума ймовірностей $p_y(1)$ та $p_y(0)$ дасть одиницю:

$$p_y(0) + p_y(1) =$$

$$= (1 - p_x)(1 - p) + p_x p + (1 - p_x)p + p_x(1 - p) =$$

$$= (1 - p_x)(1 - p + p) + p_x(1 - p + p) = \qquad .$$

$$= 1 - p_x + p_x = 1$$

Якщо внести позначення $p(y = 1) = p_y$ та $p(y = 0) = 1 - p_y$, то ентропія виходу каналу Y виражатиметься за допомогою ентропійної функції:

$$H(Y) = -p_y \log_2 p_y - (1 - p_y)\log_2(1 - p_y) = h(p_y)\,, \qquad (2.2.19)$$

де $h(p_x)$ – ентропійна функція.

– Умовна ентропія $H(Y / X)$:

$$H(Y/X) = \sum_{x} \sum_{y} p(x,y)\log_2 \frac{1}{p(y/x)} =$$

$$= p_{x,y}(0,0)\log_2 \frac{1}{p_{y/x}(0/0)} + p_{x,y}(1,0)\log_2 \frac{1}{p_{y/x}(0/1)} +$$

$$+ p_{x,y}(0,1)\log_2 \frac{1}{p_{y/x}(1/0)} + p_{x,y}(1,1)\log_2 \frac{1}{p_{y/x}(1/1)}\,. \qquad (2.2.20)$$

Виразимо потрібні імовірності, як і в попередніх випадках, через початкові дані: p_x та p:

$$p(x,y) = p(x)p(y/x) \qquad p(y/x) = \ldots$$

$$p_{x,y}(0,0) = p_x(0)p_{y/x}(0/0) = (1-p_x)(1-\mathrm{p}) \qquad p_{y/x}(0/0) = 1-p$$

$$p_{x,y}(1,0) = p_x(1)p_{y/x}(0/1) = p_x p \qquad p_{y/x}(1/0) = p$$

$$p_{x,y}(0,1) = p_x(0)p_{y/x}(1/0) = (1-p_x)p \qquad p_{y/x}(0/1) = p$$

$$p_{x,y}(1,1) = p_x(1)p_{y/x}(1/1) = p_x(1-p) \qquad p_{y/x}(1/1) = 1-p$$

Підставивши отримані співвідношення в співвідношення для шуканої ентропії, отримаємо:

$$H(Y/X) = (1-p_x)(1-p)\log_2\frac{1}{1-p} + p_x p\log_2\frac{1}{p} +$$

$$+(1-p_x)p\log_2\frac{1}{p} + p_x(1-p)\log_2\frac{1}{(1-p)} =$$

$$= -p\log_2 p - (1-p)\log_2(1-p) = h(p). \qquad (1.2.21)$$

Вочевидно умовна ентропія $H(Y/X)$ є ентропією джерела помилок та може бути знайденою через ентропійну функцію $h(p)$. Якщо ймовірностям p_x та p присвоїти конкретні значення, то можна знайти кількість інформації, що витікає через даний канал.

Таким чином, розглянуто окремий випадок дискретного каналу, а саме дискретного симетричного каналу без пам'яті як спрощеного опису каналу витоку інформації. Отримано співвідношення щодо оцінювання взаємної інформації в цьому каналі, зокрема й відносно входу та відносно виходу каналу через безумовні та умовні ентропії.

Таким чином, проведено огляд дискретного каналу як опису каналу витоку інформації. Обґрунтовано кількісну міру інформації, що проходить через дискретний канал. Розкрито сутність взаємної інформації та отримано її співвідношення через відношення апостеріорної та апріорної ентропій. Введено поняття безумовних та умовних ентропій. Отримані співвідношення відносно входу та відносно виходу каналу через безумовні та умовні ентропії.

Розглянуто окремий випадок дискретного каналу, а саме дискретного симетричного каналу без пам'яті. Отримано співвідношення щодо оцінювання взаємної інформації в цьому каналі, зокрема й відносно входу та відносно виходу каналу через безумовні та умовні ентропії. Співвідношення є відносно нескладними та можуть бути використаними на практиці для оцінювання взаємної інформації в каналі.

Контрольні питання:

1. Дискретний канал та його опис. Повідомлення на вході та на виході каналу.
2. Інтуїтивні уявлення та властивості, яким має відповідати міра інформації, що проходить через канал. Апріорна та апостеріорна імовірності повідомлень в каналі. Математична функція, що задовольняє ці уявлення та властивості.
3. Середня кількість взаємної інформації між входом та виходом каналу. Безумовні та умовні ентропії.
4. Дискретний симетричний канал та його опис. Представлення каналу у вигляді графу станів.
5. Кількість взаємної інформації у дискретному симетричному каналі. Безумовні та умовні ентропії у дискретному симетричному каналі.

2.3. Неперервне джерело як опис джерела витоку та кількість інформації на його виході

Неперервне джерело та неперервні процеси. Означення стаціонарних та ергодичних процесів. Інформаційний сигнал, а також процес його формування, що здійснюється джерелом інформації є випадковими процесами. Якщо джерело інформації вмикати на деякий тривалий час багато разів підряд, то щоразу на його виході з'являтиметься деякий сигнал, який за кожним включенням, як правило, буде різним та непередбаченим. Також якщо спостерігати за джерелом інформації деякий час та аналізувати характер формування інформаційного сигналу, то це також не дозволить спрогнозувати сигнал, що вироблятиметься в наступному.

Різниця між реалізованими сигналами дозволяє переносити інформацію. Однак всю інформацію у виробленому сигналі можна поділити на корисну та некорисну для отримувача. Так, наприклад, в сигналі людського мовлення окрім звуків, що відповідають буквам алфавіту, присутня інформація про особливості людини, що промовляє, а саме про її стать, настрій та інше. Якщо промовою передавати будь-які відомості, то при слуханні цієї промови корисною інформацією будуть звуки, з яких можна складати речення та записувати текст.

Так всі сигнали, що виробляє джерело інформації, можна об'єднати в підмножини за схожістю чи за ознакою відповідності сигналам корисної інформації та поставити їм у відповідність деякі реалізації сигналів: $S_1(t)$, $S_2(t)$, $S_3(t)$,..., $S_r(t)$,..., де r – номер реалізації (див. рис. 2.3.1). Вказані реалізації являють собою реалізації випадкового процесу, а їх множина

(кінцева чи нескінченна), на якій задано розподіл ймовірностей – *ансамбль реалізацій випадкового процесу*. В свою чергу кожна реалізація має конкретний опис та являє собою функцію часу.

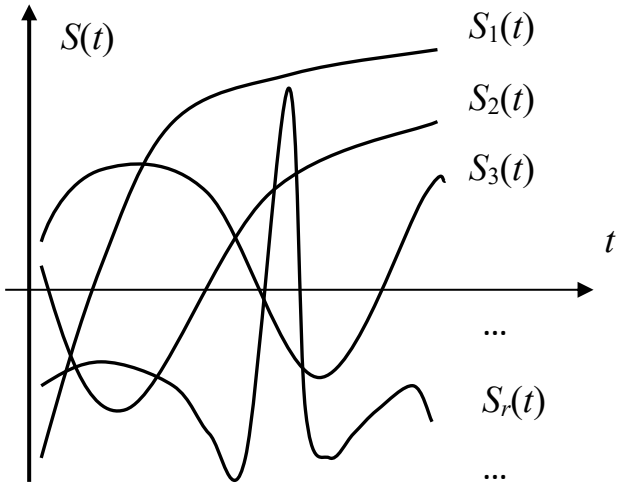


Рис. 2.3.1. Реалізації інформаційних сигналів

З точки зору неперервності або дискретності, сигнали можна розділити за трьома типами:

1) дискретні сигнали – сигнали, що приймають дискретні значення в дискретні відліки часу (див. рис. 2.3.2.а);

2) неперервні сигнали з дискретним часом – сигнали, що приймають неперервні значення в дискретні відліки часу (див. рис. 2.3.2.б);

3) неперервні сигнали з неперервним часом – сигнали, що приймають неперервні значення упродовж деякого плинного часу (див. рис. 2.3.2.в).

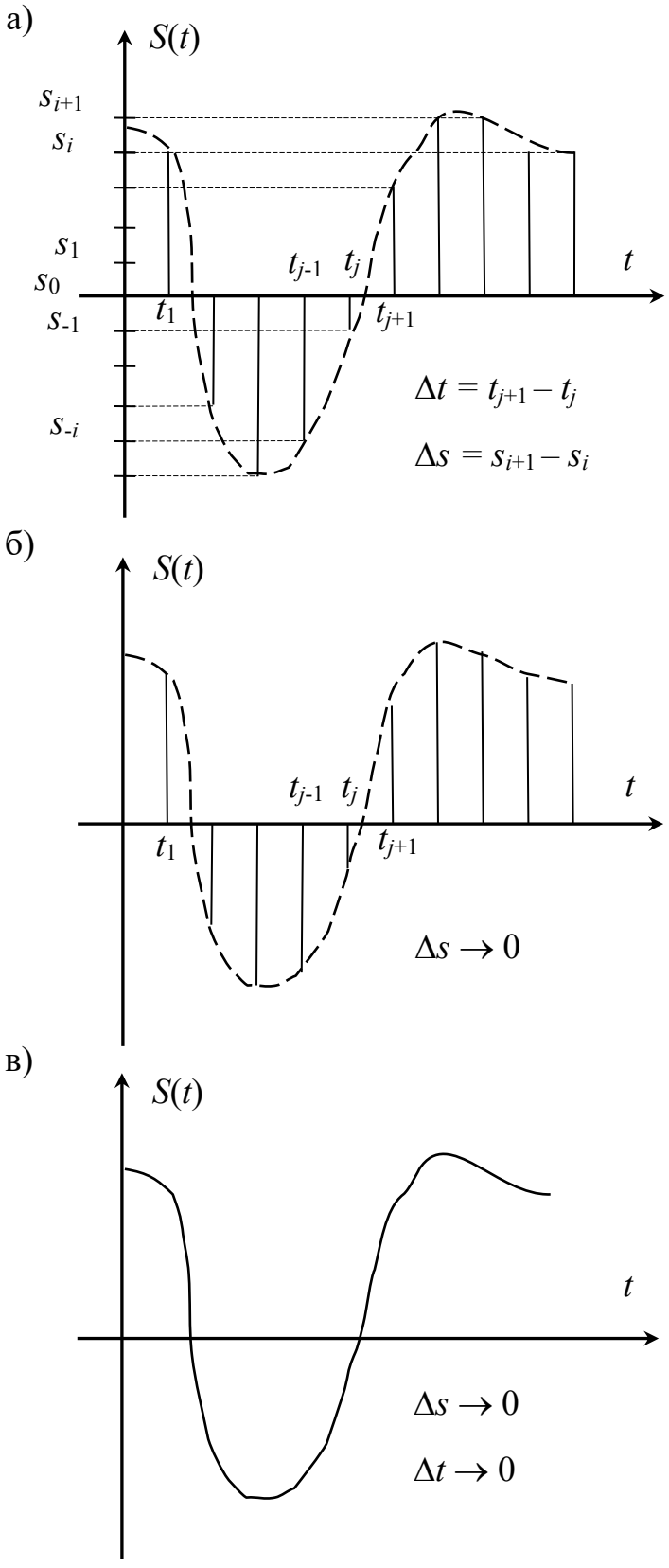


Рис.2.3.2. Типи інформаційних сигналів: а) дискретні сигнали; б) неперервні сигнали з дискретним часом; в) неперервні сигнали з неперервним часом

Четвертий тип сигналу, який випливає з використаної класифікації, а саме з дискретними значеннями упродовж неперервного часу для перенесення інформації практично не використовується, а тому як тип інформаційного сигналу розглядатися не буде.

Відповідно до типів сигналів мають назву і джерела, що їх формують, та канали, через які вони проходять.

Так, наприклад, для дискретних сигналів використовуються дискретні джерела та канали. При цьому значенням сигналів у відліках часу можна поставити у відповідність символи деякого алфавіту, а заваді – помилку на прийомі. Як очевидно, кількість інформації на один символ співпадатиме з кількістю інформації на один дискретний відлік.

Формування неперервного сигналу здійснюється за допомогою неперервних джерел, а його передача – за допомогою неперервних каналів.

Вказані типи сигналів мають між собою зв'язок (див. рис. 2.3.2). Слід зазначити, що дискретний сигнал з дискретним часом можна вважати приблизно неперервним у відлік часу, якщо спрямувати крок дискретизації до нуля $\Delta s \to 0$, та з неперервним часом, якщо спрямувати до нуля відстань поміж відліками $\Delta t \to 0$ і навпаки, округлення значень сигналу та плинного часу до дискретних значень дозволить здійснити перехід від неперервного сигналу до наближеного дискретного.

Прикладом вказаного може служити електричний струм, який є направленим рухом заряджених дискретних частинок – електронів. З одного боку, його можна вважати неперервною величиною (як правило, протікання струмів зв'язано з протіканням мільйонів електронів), а з іншого (для малих струмів) – його значення залежить від дискретних значень зарядів.

Вказані зв'язки дозволяють здійснювати аналіз та проводити оцінки інформаційних показників складних процесів аналогічно до більш простих.

Нехай має місце неперервний випадковий процес з неперервним часом (див. рис. 2.3.2.в). Розглянемо його на прикладі випадкового значення $s = S(t_1)$ в перетині ансамблю реалізацій в довільний, але фіксований відлік часу t_1, так як для процесу з дискретним часом (див рис. 2.3.2.б), вважаючи, що аналогічні міркування та оцінки будуть справедливими й для інших відліків часу.

Нехай задано ансамбль випадкових значень s з щільністю розподілу ймовірностей $\omega(s)$ (див. рис. 2.3.3).

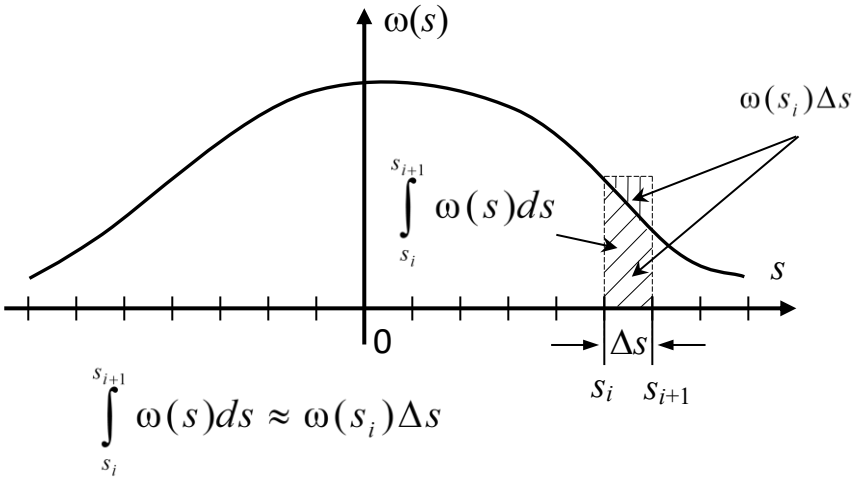


Рис. 2.3.3. Щільність розподілу ймовірностей випадкової неперервної величини *s*

Якщо діапазон величини *s* розбити на дискретні значення, кратні значенням Δs то неперервний процес з дискретним часом можна апроксимувати дискретним процесом з дискретним часом. Імовірності значень s_i можна виразити через щільність розподілу ймовірностей $\omega(s)$:

$$p(s = s_i) = \omega(s_i)\,\Delta s,$$

де i – індекс випадкової величини s_i на множині цілих чисел.

Приблизні імовірності для неперервної s можна виразити через дискретні:

$$p(s_i \le s < s_{i+1}) \approx \omega(s_i)\,\Delta s.$$

Точні значення ймовірностей для неперервної s знаходяться шляхом спрямування $\Delta s \to 0$:

$$p(s_i \le s < s_{i+1}) = \lim_{\Delta s \to 0} \omega(s_i)\Delta s = \int_{s_i}^{s_{i+1}} \omega(s)ds$$

та

$$p(s_m \le s < s_{m+n}) = \lim_{\Delta s \to 0} \sum_{i=m}^{m+n} \omega(s_i)\Delta s = \int_{s_m}^{s_{m+n}} \omega(s)ds\,,$$

де m, n – довільні, але фіксовані значення індексів i.

Неперервний випадковий процес має подвійний характер. З одного боку це є ансамбль випадкових реалізацій, з іншого – кожна реалізація є функцією часу.

Основними характеристиками сигналу, як випадкової реалізації в довільний, але фіксований відлік часу є:

1. Математичне сподівання:

$$M\{s\} = \int_{-\infty}^{+\infty} s\omega(s)ds \,, \tag{2.3.1}$$

де ω(*s*) – одномірна щільність розподілу ймовірностей значень *s* у відлік часу t_1.

2. Дисперсія:

$$D\{s\} = \int_{-\infty}^{+\infty} [s - M\{s\}]^2 \omega(s)ds \,, \tag{2.3.2}$$

3. Функція кореляції:

$$R(t_1, t_2) = \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} [s - M\{s\}][s' - M\{s'\}]\omega(s, s')dsds' \,, \tag{2.3.3}$$

де ω(*s*, *s'*) – двомірна щільність розподілу ймовірностей значень *s* та *s'* в фіксовані відліки часу t_1 та t_2.

Серед всіх можливих випадкових процесів має місце так званий *стаціонарний процес*, під яким будемо розуміти такий випадковий процес, для якого математичне сподівання $M\{s\}$, дисперсія $D\{s\}$ не залежать від часу t_1, а функція кореляції $R(t_1, t_2)$ залежить лише від різниці $\tau = t_2 - t_1$. В цьому випадку пишуть $R(t_1, t_2) = R(\tau)$.

Аналогічними характеристиками сигналу, як функції часу для довільно взятої, але фіксованої реалізації є:

1. Постійна складова реалізації сигналу:

$$\overline{S}_r = \overline{S_r(t)} = \lim_{T\to\infty} \frac{1}{T} \int_{-\frac{T}{2}}^{+\frac{T}{2}} S_r(t)dt \,, \tag{2.3.4}$$

де $S_r(t)$ – функція, що описує реалізацію сигналу, *r* – індекс, що означає номер реалізації;

T – період (тривалість) сигналу.

При цьому змінна складова реалізації сигналу матиме вираз:

$$\tilde{S}_r(t) = S_r(t) - \overline{S}_r$$

2. Середнє значення квадрата реалізації змінної складової сигналу:

$$\widetilde{P}_r = \overline{(S_r(t) - \overline{S}_r)^2} = \overline{\widetilde{S}_r^2(t)} = \lim_{T\to\infty} \frac{1}{T} \int_{-\frac{T}{2}}^{+\frac{T}{2}} \widetilde{S}_r^2(t)dt\,, \qquad (2.3.5)$$

Якщо прийняти $S(t)$, як міру струму, то $\widetilde{P}_r$ буде потужністю реалізації сигналу на опорі 1 Ом.

3. Часова функція кореляції реалізації сигналу:

$$R°(\tau) = \lim_{T\to\infty} \frac{1}{T} \int_{-\frac{T}{2}}^{+\frac{T}{2}} \tilde{S}_r(t)\tilde{S}_r(t+\tau)dt\,. \qquad (2.3.6)$$

Стаціонарні процеси, для яких середні значення по ансамблю (математичне сподівання, дисперсія та функція кореляції) співпадають з середніми значеннями по часу (постійною складовою, середнім квадратичним змінної складової та часової функції кореляції):

$$M\{s\} = \overline{S}_r,$$
$$D\{s\} = \tilde{P}_r,$$
$$R(\tau) = R°(\tau),$$

називають *ергодичними випадковими процесами*.

Як очевидно, ергодичні процеси є ідеалізованим різновидом випадкових процесів, а їх використання дозволить спростити знаходження інформаційних показників для неперервних джерел та каналів.

Таким чином, проведено огляд неперервного джерела як опису джерела витоку інформації. Введено поняття ансамблів реалізацій та ансамблів значень, поняття стаціонарних та ергодичних процесів. Це дозволяє ідеалізувати реальні неперервні процеси та застосувати до них різного характеру аналітичні описи, обґрунтувати кількісну міру інформації на виході неперервного джерела.

Ентропія та диференційна ентропія неперервного процесу. Нехай, для простоти, джерело, що виробляє неперервний сигнал, являє собою стаціонарний процес.

Нехай для довільного, але фіксованого відліку часу t_1 задано ансамбль значень $S(t_1) = s$ з щільністю розподілу ймовірностей $\omega(s)$ (див. рис. 2.3.4). При цьому можна вважати, що якщо судження та отримані оцінки справедливі для відліку часу t_1, то вони будуть справедливими і для інших відліків за умови їхньої незалежності.

Для знаходження ентропії випадкової s на відлік часу апроксимуємо неперервний процес дискретним, розбивши його динамічний діапазон на

дискретні значення …, s_i, s_{i+1},… з кроком квантування $\Delta s = s_{i+1} - s_i$ та округливши до них неперервні, де i – індекс дискретного значення s_i, може приймати цілі значення від $-\infty$ до $+\infty$.

Згадаємо, що ентропія дискретного джерела без пам'яті (вихідні символи незалежні між собою) X на елемент повідомлення визначається як математичне сподівання кількості інформації по всім знакам алфавіту:

$$H(X) = \mathrm{M}\left\{\log_2 \frac{1}{p(x_i)}\right\} = \sum_{i=1}^{N} p(x_i) \log_2 \frac{1}{p(x_i)}, \qquad (2.3.7)$$

де x_i – знак (буква, цифра) алфавіту, що використаний як елемент повідомлення; i – порядковий номер знака x_i в множини знаків об'єму N.

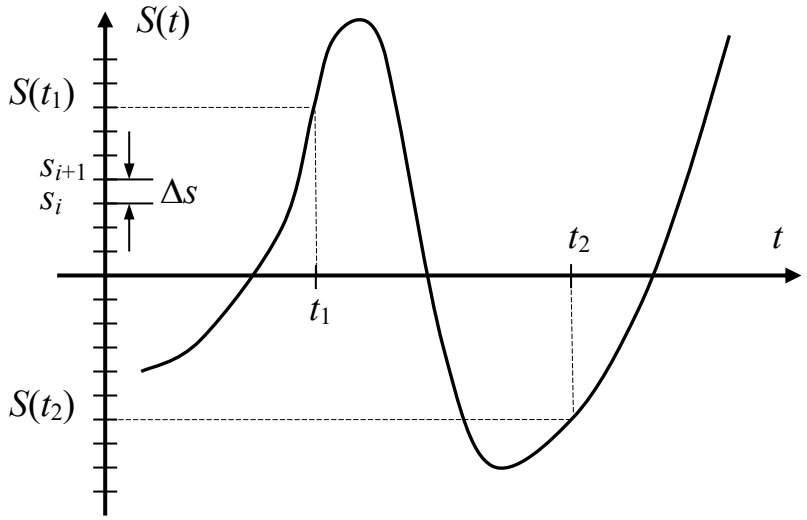


Рис. 2.3.4. Реалізація неперервного процесу

За аналогією ентропію для дискретної випадкової величини s виражатиметься за формулою:

$$H(S) \approx H_\Delta(S) = \mathrm{M}\left\{\log_2 \frac{1}{p(s_i)}\right\} = \sum_i p(s_i) \log_2 \frac{1}{p(s_i)} =$$

$$= \sum_i \omega(s_i)\Delta s \log_2 \frac{1}{\omega(s_i)\Delta s}, \qquad (2.3.8)$$

де $p(s_i) = \omega(s_i)\,\Delta s$ – імовірність значення s_i.

Спрямувавши $\Delta s \to 0$, отримаємо точне значення ентропії:

$$H(S) = \lim_{\Delta s \to 0} H_\Delta(S) = \lim_{\Delta s \to 0} \sum_i \omega(s_i)\Delta s \log_2 \frac{1}{\omega(s_i)\Delta s} =$$

$$= \lim_{\Delta s \to 0} \sum_i \omega(s_i) \log_2 \frac{1}{\omega(s_i)} \Delta s + \lim_{\Delta s \to 0} (\log_2 \frac{1}{\Delta s}) \sum_i \omega(s_i) \Delta s =$$

$$= \int_{-\infty}^{+\infty} \omega(s) \log_2 \frac{1}{\omega(s)} \mathrm{d}s + \lim_{\Delta s \to 0} \log_2 \frac{1}{\Delta s}. \qquad (2.3.9)$$

Перша складова співвідношення (2.3.9)

$$h(s) = \int_{-\infty}^{+\infty} \omega(s) \log_2 \frac{1}{\omega(s)} \mathrm{d}s \qquad (2.3.10)$$

має назву диференційної ентропії. Вона повністю визначена характером величини s та щільністю розподілу ймовірностей $\omega(s)$. Слід також зазначити, що якщо сигнал s обмежений знизу s_1 та зверху s_2, то, відповідно, ці значення будуть границями інтеграла.

Друга складова:

$$\lim_{\Delta s \to 0} \log_2 \frac{1}{\Delta s} = \infty \qquad (2.3.11)$$

отримана, виходячи з того, що:

$$\lim_{\Delta s \to 0} \sum_i \omega(s_i) \Delta s = \int_{-\infty}^{+\infty} \omega(s) \mathrm{d}s = 1,$$

як імовірність повної групи подій.

Як очевидно, складова (2.3.11) незалежно від розподілу ймовірностей сигналу спрямовує ентропію джерела в нескінченність:

$$H(S) = h(s) + \lim_{\Delta s \to 0} \log_2 \frac{1}{\Delta s} = h(s) + \infty = \infty. \qquad (2.3.12)$$

Тому для аналізу джерела користуються диференційною ентропією. Сама диференційна ентропія є допоміжною величиною і не має фізичного сенсу, може приймати від'ємні значення хоча і вимірюється в бітах.

Розглянемо приклад спрямування ентропії неперервного джерела в нескінченність.

Нехай джерело для формування дискретного повідомлення використовує алфавіт з 10 знаків: x_1, x_2, x_3,…, x_{10}. Якщо вважати, що імовірності по знаках розподілені рівномірно, то ентропія джерела $H(X) = \log_2 10 \approx 3{,}21$ (біт).

Нехай для передачі цих дискретних знаків використовується неперервний сигнал s, наприклад, напруга u від 0 до 1 вольт. Тоді кожному дискретному знаку можна поставити у відповідність значення напруги з кроком дискретизації $\Delta u = 0{,}1$ V:

$$x_1 \to u_1 = 0{,}1V;$$
$$x_2 \to u_2 = 0{,}2V;$$
$$x_3 \to u_3 = 0{,}3V;$$
$$\ldots\ldots\ldots\ldots$$
$$x_{10} \to u_{10} = 1{,}0V.$$

При цьому ентропія джерела дорівнює:

$$H(U) = H(X) \approx 3{,}21 \text{біт}.$$

Нехай тепер дискретне джерело використовує алфавіт не з 10, а із 100 знаків: x_1, x_2, x_3,…, x_{99}, x_{100}. Ентропія цього джерела при рівномірному розподілі імовірностей по знаках алфавіту: $H(X) = \log_2 100 \approx 6{,}42$ (біт).

Для того ж діапазону кожному дискретному знаку можна поставити у відповідність наступні значення напруги неперервного сигналу з кроком дискретизації $\Delta u = 0{,}01\ V$:

$$x_1 \to u_1 = 0{,}01V;$$
$$x_2 \to u_2 = 0{,}02V;$$
$$x_3 \to u_3 = 0{,}03V;$$
$$\ldots\ldots\ldots\ldots$$
$$x_{100} \to u_{100} = 1{,}00V.$$

При цьому ентропія джерела дорівнює:

$$H(U) = H(X) = 6{,}42 \text{біт}.$$

Аналогічно можна навести приклад для алфавітів з 1000 знаків 10000 і більше. При цьому зменшення кроку дискретизації приводитиме до збільшення ентропії джерела, що відповідає сутності спрямування в нескінченність ентропії (2.3.12).

Таким чином, обґрунтовано кількісну міру інформації випадкового неперервного процесу. Введено поняття диференційної ентропії джерела. Отримано співвідношення щодо їх оцінювання. Розглянуті приклади щодо того, як залежить ентропія від кроку дискретизації неперервного сигналу та спрямовується в нескінченність при спрямуванні кроку дискретизації в нуль.

Ентропія джерела гауссівського неперервного процесу. Знайдемо оцінку стаціонарного процесу з гауссівським нормальним розподілом ймовірностей.

Щільність нормального розподілу ймовірностей визначається формулою:

$$\omega(s) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(s-a)^2}{2\sigma^2}}, \qquad (2.3.13)$$

де s – неперервна нормально розподілена випадкова величина; a – математичне сподівання величини s; σ – середньоквадратичне відхилення (σ^2 – дисперсія) сигналу від його середнього значення.

Диференційну ентропію можна знайти, скориставшись формулою (2.3.10), підставивши в неї (2.3.13):

$$h(s) = \int_{-\infty}^{+\infty} \omega(s) \log_2 \frac{1}{\omega(s)} ds = \int_{-\infty}^{+\infty} \omega(s) \log_2 \frac{1}{\frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(s-a)^2}{2\sigma^2}}} ds =$$

$$= \int_{-\infty}^{+\infty} \omega(s) \log_2 (\sqrt{2\pi\sigma^2} e^{\frac{(s-a)^2}{2\sigma^2}}) ds =$$

$$= \log_2 (\sqrt{2\pi\sigma^2}) \int_{-\infty}^{+\infty} \omega(s) ds + \frac{\log_2 e}{2\sigma^2} \int_{-\infty}^{+\infty} (s-a)^2 \omega(s) ds . \qquad (2.3.14)$$

Виходячи з того, що:

$$\int_{-\infty}^{+\infty} \omega(s) ds = 1$$

як повна група подій та

$$\int_{-\infty}^{+\infty} (s-a)^2 \omega(s) ds = D\{s\} = \sigma^2$$

є дисперсією випадкової величини s, шукана величина отримає остаточний вигляд:

$$h(s) = \log_2 (\sqrt{2\pi\sigma^2}) + \frac{\log_2 e}{2} = \frac{1}{2} \log_2 (2\pi e \sigma^2) .$$

З отриманого співвідношення випливає, що диференційна ентропія неперервного сигналу з гауссівським нормальним розподілом ймовірностей залежить лише від його середньоквадратичного відхилення.

Якщо даний випадковий процес ергодичний ($\sigma^2 = P$), то його диференційна ентропія може бути вираженою через потужність:

$$h(s) = \frac{1}{2} \log_2 (2\pi e P) . \qquad (2.3.15)$$

Якщо випадковий процес вважати ергодичним та гауссівським, його диференціальну ентропію можна знайти за формулою (2.3.15).

Таким чином, здійснено оцінювання диференційної ентропії випадкового неперервного процесу з гауссівським розподілом та отрамно відповідне співвідношення. Показано, що для гауссівських ергодичних процесів диференційна ентропія повністю визначається потужністю джерела.

Отже, проведено огляд неперервного джерела як опису джерела витоку інформації. Введено поняття ансамблів реалізацій та ансамблів значень, поняття стаціонарних та ергодичних процесів. Це дозволяє ідеалізувати реальні неперервні процеси та застосувати до них різного характеру аналітичні описи.

Обґрунтовано кількісну міру інформації випадкового неперервного процесу. Введено поняття диференційної ентропії джерела. Отримано співвідношення щодо їх оцінювання. Розглянуті приклади щодо того, як залежить ентропія від кроку дискретизації неперервного сигналу та спрямовується в нескінченність при спрямуванні кроку дискретизації в нуль.

Здійснено оцінювання диференційної ентропії випадкового неперервного процесу з гауссівським розподілом та отрамно відповідне співвідношення. Показано, що для гауссівських ергодичних процесів диференційна ентропія повністю визначається потужністю джерела.

Контрольні питання:

1. Неперервне джерело. Опис повідомлення на виході неперервного джерела. Ансамбль реалізацій та ансамбль значень.
2. Переходи між неперервними та дискретними представленнями неперервних процесів. Щільність розподілу імовірностей на виході джерела.
3. Характеристики реалізацій як випадкових величин та функції залежності величини від часу. Стаціонарний та ергодичний процеси.
4. Ентропія неперервного процесу та диференційна ентропія.
5. Ентропія джерела гауссівського неперервного процесу.

2.4. Неперервний канал як опис каналу витоку та кількість інформації, що проходить через неперервний канал

Неперервний канал та постійний гауссівський канал з адитивною завадою. Під неперервним каналом розумітимемо канал, для якого вхідні та вихідні сигнали є неперервними (див. рис. 2.4.1). На вхід каналу потрапляє деякий інформаційний сигнал (реалізація) $S(t)$ з ансамблю

реалізацій $\{S(t)\}$ та, проходячи через канал, під впливом завад перетворюється в деякий вихідний сигнал $U(t)$. Відповідно всі сигнали (реалізації) $U(t)$ представлятимуть ансамбль реалізацій $\{U(t)\}$.

$$I(S;\, U) = I(U;\, S)$$

Рис. 2.4.1. Схема неперервного каналу

Завади являють собою багатопричинні фізичні процеси в каналі, які, як правило, неможливо ні передбачити, ні повторити. Тому їх, як і інформаційні джерела та сигнали, відносять до випадкових процесів з тими ж характеристиками, що й попередні.

Завади розрізняють на наступні види:

(*за способом впливу*)

– адитивні завади – завади, що арифметично складаються з повідомленнями;

– мультиплікативні завади – завади, що мультиплікативно впливають на повідомлення. Такий вплив відповідає математичній операції множення (згортки);

(*за формою*)

– імпульсні завади – короткі за часом завади у формі імпульсів, мають широкий спектр частот;

– вузькосмугові завади – завади з вузьким спектром частот, в часі періодичні, схожі на синусоїду;

– шум – довготривалі за часом та широкі за спектром частот завади. Ідеальним шумом є так званий *білий* шум, для якого:

1) будь-які два відліки часу не залежні між собою;

2) для кожного відліку часу ансамбль реалізація має нормальний закон розподілу;

3) енергетичний спектр рівномірно розподілений по частоті від нуля до нескінченності.

Нехай неперервний канал матиме адитивну заваду. Для нього справедливо:

$$U(t) = \mu S(t) + N(t), \qquad (2.4.1)$$

де μ – коефіцієнт послаблення сигналу; $N(t)$ – адитивна завада.

Канал з адитивною завадою має назву *адитивного каналу*.

Якщо величина μ = const, то адитивний канал називають *постійним* адитивним каналом**.**

Якщо адитивна завада має нормальний гауссівський розподіл ймовірностей, то канал називають *адитивним гауссівським каналом.*

Нехай, для простоти, всі процеси, що розглядаються, будуть стаціонарними та нехай в кожен відлік часу значення сигналу та завади не залежать від будь-яких попередніх відліків.

Розглянемо процес проходження інформації через канал для довільного, але фіксованого відліку t_1, вважаючи, що всі міркування та отримані оцінки будуть справедливими і для інших відліків. Зауважимо, що такий канал є подібним до неперервного каналу з дискретним часом.

Для вказаного відліку внесемо позначення:

$$S(t_1) = s,$$

$$N(t_1) = n,$$

$$U(t_1) = u.$$

Як очевидно для даного випадку, формула (2.4.1) може бути перетвореною в інший вигляд:

$$u = \mu s + n. \qquad (2.4.2)$$

Неперервний гауссівський канал з врахуванням останніх обмежень вважається заданим, якщо визначено:

1. Ансамбль реалізацій випадкового процесу на вході каналу $\{S(t)\}$ з щільністю розподілу ймовірностей $\omega(s)$.

2. Ансамбль реалізацій випадкового процесу на виході каналу $\{U(t)\}$.

3. Щільність розподілу ймовірностей $\omega(u/s)$ того, що на виході каналу з'явиться значення сигналу u, якщо на вхід потрапив сигнал s.

Розбіжність сигналу u та ослабленого μs повністю визначається завадою n ($n = u - \mu s$). Для випадку, якщо в каналі відсутнє послаблення ($\mu = 1$), або воно враховане у вхідному сигналі s, то з врахуванням (2.4.2) щільність розподілу ймовірностей переходів дорівнюватиме:

$$\omega(u/s) = \omega(s+n/s) = \omega(n). \qquad (2.4.3)$$

З останнього випливає, що для адитивного каналу перехідний процес повністю визначається ансамблем реалізацій джерела завади.

Таким чином, проведено огляд неперервного каналу як опису каналу витоку інформації. Введено поняття постійного гауссівського каналу з адитивною завадою.

Кількість взаємної інформації в неперервному гауссівському каналі. Знайдемо кількість взаємної інформації для вище заданого каналу на відлік часу.

Для цього розділимо області визначення величин s, n, u на дискретні значення, кратні деякому значенню Δ з відповідним позначенням – Δs, Δn, Δu. Такий канал є апроксимацією неперервного каналу з допустимою помилкою на крок Δ, а ансамбль значень у відлік часу t_1 – набір дискретних значень s_i n_g, u_j. Вказаним значенням можна поставити у відповідність елементи деякого алфавіту та, заа аналогією з дискретними каналами, оцінити кількість взаємної інформації.

Згадаємо, що для дискретного каналу з входом X та виходом Y кількість взаємної інформації на відлік дорівнюватиме:

$$I(X;Y) = M\left\{\log\frac{p(x_i, y_j)}{p(x_i)p(y_j)}\right\} =$$

$$= \sum_{i=1}^{N}\sum_{j=1}^{N} p(x_i, y_j)\log\frac{p(x_i, y_j)}{p(x_i)p(y_j)}, \qquad (2.4.4)$$

де x_i та y_j – вхідні та вихідні символи дискретного каналу з алфавіту об'єму N; i та j – номери символів в алфавіті об'єму N.

Якщо в формулі (2.4.4) дискретні значення x_i та y_j замінити значеннями s_i та u_j, то можна виразити співвідношення ентропії для дискретних s_i та u_j:

$$I_\Delta(S;U) = M\left\{\log\frac{p(s_i, u_j)}{p(s_i)p(u_j)}\right\} =$$

$$= \sum_{i}\sum_{j} p(s_i, u_j)\log\frac{p(s_i, u_j)}{p(s_i)p(u_j)}, \qquad (2.4.5)$$

Імовірності для дискретних величин s_i n_g, u_j можна виразити через щільності розподілів ймовірностей:

$$\begin{gathered} p(s_i) = p(s = s_i) = \omega(s_i)\,\Delta s; \\ p(n_g) = p(n = n_g) = \omega(n_g)\,\Delta n; \\ p(u_i) = p(u = u_i) = \omega(u_j)\,\Delta u; \\ p(s_i, u_i) = p(s = s_i, u = u_i) = \omega(s_i, u_j)\,\Delta s\,\Delta u = \\ = \omega(s_i)\,\Delta s\,\omega(u_j/s_i)\,\Delta u = \omega(s_i/u_j)\,\Delta s\,\omega(u_j)\,\Delta u. \end{gathered} \qquad (2.4.6)$$

Внісши заміну (2.4.6) в (2.4.5) отримаємо:

$$I_\Delta(S;U) = \sum_{i}\sum_{j}\omega(s_i, u_j)\Delta s\Delta u\log\frac{\omega(s_i, u_j)\Delta s\Delta u}{\omega(s_i)\Delta s\omega(u_j)\Delta u}. \qquad (2.4.7)$$

За аналогією з дискретними каналами можна показати, що:

$$I_{\Delta}(S,U) = H_{\Delta}(S) - H_{\Delta}(S/U) = H_{\Delta}(U) - H_{\Delta}(U/S) = I_{\Delta}(U,S), \quad (2.4.8)$$

де $H_{\Delta}(S)$ та $H_{\Delta}(U)$ – безумовні ентропії:

$$H_{\Delta}(S) = \sum_i \omega(s_i)\Delta s \log \frac{1}{\omega(s_i)\Delta s},$$

$$H_{\Delta}(U) = \sum_i \omega(u_j)\Delta u \log \frac{1}{\omega(u_j)\Delta u},$$

$H_{\Delta}(S/U)$ та $H_{\Delta}(U/S)$ – умовні ентропії:

$$H_{\Delta}(S/U) = \sum_i \sum_j \omega(s_i,u_j)\Delta s\Delta u \log \frac{1}{\omega(s_i/u_j)\Delta s},$$

$$H_{\Delta}(U/S) = \sum_i \sum_j \omega(s_i,u_j)\Delta s\Delta u \log \frac{1}{\omega(u_j/s_i)\Delta u}.$$

Для знаходження точних значень взаємної кількості інформації в неперервному каналі дослідимо функцію (2.4.7) при $\Delta \to 0$:

$$I(S;U) = I(U;S) = \lim_{\substack{\Delta s\to 0\\ \Delta u\to 0}} I_{\Delta}(S;U) =$$

$$= \lim_{\substack{\Delta s\to 0\\ \Delta u\to 0}} \sum_i \sum_j \omega(s_i,u_j) \log \frac{\omega(s_i,u_j)}{\omega(s_i),\omega(u_j)} \Delta s\Delta u =$$

$$= \int_{-\infty-\infty}^{+\infty+\infty} \omega(s,u) \log_2 \frac{\omega(s,u)}{\omega(s)\omega(u)} dsdu. \quad (2.4.9)$$

Співвідношення для взаємної інформації (2.4.9) можна перетворити та виразити через безумовні та умовні диференціальні ентропії:

а) $$I(S;U) = \int_{-\infty-\infty}^{+\infty+\infty} \omega(s,u) \log_2 \frac{\omega(s,u)}{\omega(s)\omega(u)} dsdu =$$

$$= \int_{-\infty-\infty}^{+\infty+\infty} \omega(s)\omega(u/s) \log_2 \frac{1}{\omega(s)} dsdu - \int_{-\infty-\infty}^{+\infty+\infty} \omega(s,u) \log_2 \frac{\omega(u)}{\omega(s,u)} dsdu =$$

$$= \int_{-\infty}^{+\infty} \omega(s) \log_2 \frac{1}{\omega(s)} ds - \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} \omega(s,u) \log_2 \frac{1}{\omega(s/u)} dsdu =$$

$$= h(S) - h(S/U),$$

де $h(S)$ – безумовна диференційна ентропія:

$$h(S) = \int_{-\infty}^{+\infty} \omega(s) \log_2 \frac{1}{\omega(s)} ds ,$$

$h(S/U)$ – умовна диференційна ентропія:

$$h(S/U) = \int_{-\infty-\infty}^{+\infty+\infty} \omega(s,u) \log_2 \frac{1}{\omega(s/u)} dsdu ;$$

б) $$I(U;S) = \int_{-\infty-\infty}^{+\infty+\infty} \omega(s,u) \log_2 \frac{\omega(s,u)}{\omega(s)\omega(u)} dsdu =$$

$$= \int_{-\infty-\infty}^{+\infty+\infty} \omega(u)\omega(s/u) \log_2 \frac{1}{\omega(u)} dsdu - \int_{-\infty-\infty}^{+\infty+\infty} \omega(s,u) \log_2 \frac{\omega(s)}{\omega(s,u)} dsdu =$$

$$= \int_{-\infty}^{+\infty} \omega(u) \log_2 \frac{1}{\omega(u)} du - \int_{-\infty-\infty}^{+\infty+\infty} \omega(s,u) \log_2 \frac{1}{\omega(u/s)} dsdu =$$

$$= h(U) - h(U/S) ,$$

де $h(U)$ – безумовна диференційна ентропія:

$$h(U) = \int_{-\infty}^{+\infty} \omega(u) \log_2 \frac{1}{\omega(u)} du ,$$

$h(U/S)$ – умовна диференційна ентропія:

$$h(U/S) = \int_{-\infty-\infty}^{+\infty+\infty} \omega(s,u) \log_2 \frac{1}{\omega(u/s)} dsdu .$$

Якщо завада адитивна $u = s + n$ (μ=1), то з врахуванням (2.4.3) можна показати, що умовна диференційна ентропія $h(U/S)$ дорівнюватиме безумовній диференційній ентропії завади в каналі:

$$h(U/S) = \int_{-\infty-\infty}^{+\infty+\infty} \omega(s)\omega(u/s) \log_2 \frac{1}{\omega(u/s)} dsdu =$$

$$= \int_{-\infty-\infty}^{+\infty+\infty} \omega(s)\omega(s+n/s) \log_2 \frac{1}{\omega(s+n/s)} dsd(s+n) =$$

$$= \int_{-\infty}^{+\infty} \omega(s)ds \int_{-\infty}^{+\infty} \omega(n) \log_2 \frac{1}{\omega(n)} dn = \int_{-\infty}^{+\infty} \omega(n) \log_2 \frac{1}{\omega(n)} dn = h(N) ,$$

де $h(N)$ – диференційна ентропія завади.

Таким чином кількість взаємної інформації в неперервному адитивному каналі можна виразити:

$$I(U;S) = h(U) - h(N) .$$

Умовні та безумовні диференційні ентропії не мають такого сенсу, як умовні та безумовні ентропії. Вони не визначають середню кількість інформації і їх потрібно розуміти, як деяку допоміжну величину. Слід зазначити, що диференційні ентропії можуть набувати від'ємних значень. Однак їх використання дозволяє оцінювати кількість взаємної інформації в неперервному каналі.

Таким чином, за аналогією з дискретним каналом обґрунтовано кількісну міру інформації, що проходить через неперервний канал. Введено поняття безумовних та умовних диференційних ентропій. Отримані співвідношення відносно входу та відносно виходу каналу через безумовні та умовні диференційні ентропії.

Отже, проведено огляд неперервного каналу як опису каналу витоку інформації. Введено поняття постійного гауссівського каналу з адитивною завадою.

За аналогією з дискретним каналом обґрунтовано кількісну міру інформації, що проходить через неперервний канал. Введено поняття безумовних та умовних диференційних ентропій. Отримані співвідношення відносно входу та відносно виходу каналу через безумовні та умовні диференційні ентропії.

Контрольні питання:

1. Неперервний канал з адитивною гауссівською завадою та його опис. Повідомлення на вході та на виході каналу.
2. Неперервний канал з адитивною гауссівською завадою для стаціонарних та ергодичних процесів та його опис.
3. Імовірності дискретних значень неперервних величин та їхній зв'язок з щільністю розподілу ймовірностей.
4. Наближена кількість взаємної інформації у неперервному каналі при дискретизації неперервних процесів. Наближені безумовні та умовні ентропії.
5. Кількість взаємної інформації у неперервному каналі. Безумовні та умовні диференційні ентропії.

2.5. Пропускна здатність дискретного каналу та умова його відсутності

Пропускна здатність дискретного каналу та умова його відсутності. Під *пропускною здатністю дискретного каналу на символ повідомлення* розумітимемо максимум кількості інформації, що можна передати по каналу, яка визначається по всіх можливих джерелах з їхніми розподілами ймовірностей. Вона виражається формулою:

$$C = \max_{p(X_k^n),n,k} I(X;Y), \tag{2.5.1}$$

де $I(X;Y)$ – кількість взаємної інформації в каналі; $p(X^n{}_k)$ – імовірність послідовності символів $X^n{}_k = (x_1, x_2, x_3,\ldots, x_n)$ довжиною n на виході джерела. Для джерел з двійковим алфавітом $x = \{0, 1\}$, $k = 1, 2, 3,\ldots, 2^n$. Індекс k означає номер комбінації символів із всіх можливих 2^n. Якщо ж алфавіт має об'єм l більший ніж 2, $x = \{0, 1,\ldots, l–1\}$, то $k = 1, 2, 3,\ldots, l^n$.

Інколи зручно користуватися пропускною спроможністю дискретного каналу, розрахованого не на символ повідомлення, а за одиницю часу.

Під *пропускною здатністю дискретного каналу за одиницю часу* будемо розуміти максимум кількості інформації, що можна передати по каналу за одиницю часу, яка визначається по всіх можливих джерелах з їхніми розподілами ймовірностей. Вона виражається формулою:

$$C' = V_к C = V_к \max_{p(X_k^n),n,k} I(X;Y), \tag{2.5.2}$$

де $V_к$ – канальна швидкість.

Кількість взаємної інформації в каналі виражається формулою:

$$I(X;Y) = H(X) - H(X/Y) = H(Y) - H(Y/X) = I(Y;X), \tag{2.5.3}$$

де $H(X)$, $H(Y)$, $H(X/Y)$ та $H(Y/X)$ – безумовні та умовні ентропії входу та виходу каналу (див. рис. 2.5.1).

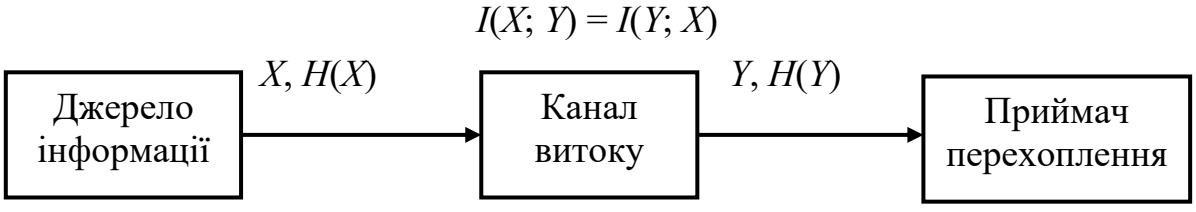


Рис. 2.5.1. Схема дискретного каналу

Пропускну здатність дискретного каналу можна виразити, підставивши ліву та праву частини співвідношення (2.5.3) в (2.5.2):

$$C = \max_{p(X_k^n),n,k} \left[H(X) - H(X/Y)\right], \tag{2.5.4}$$

$$C = \max_{p(X_k^n),n,k} \left[H(Y) - H(Y/X)\right]. \tag{2.5.5}$$

Із (2.5.4) та (2.5.5) очевидно, що максимум кількості інформації, що проходить через канал по всіх можливих джерелах досягатиметься за умови, якщо безумовні ентропії каналу $H(X)$ та $H(Y)$ будуть максимальними, а умовні ентропії $H(X/Y)$ та $H(Y/X)$ – мінімальними.

Знайдемо максимум ентропії $H(X)$.

Нехай ентропія джерела має співвідношення:

$$H(X) = \sum_{i=1}^{N} p(x_i) \log_2 \frac{1}{p(x_i)}, \tag{2.5.6}$$

де N – об'єм алфавіту X.

Зазначимо, що співвідношення ентропії (2.5.6) для джерела без пам'яті з об'єм алфавіту N є еквівалентним до співвідношення:

$$H(X) = \lim_{n\to\infty} \sum_{k=1}^{2^n} p(X_k^n) \log_2 \frac{1}{p(X_k^n)},$$

з об'єм алфавіту 2, якщо прирівняти $N = 2^n$ та спрямувати N в нескінченність.

Виразимо імовірність знака x_N через імовірності всіх інших знаків і зробимо заміну у співвідношенні для ентропії:

$$p(x_N) = 1 - p(x_1) - p(x_2) - p(x_3) - ... - p(x_{N-1});$$

$$H(X) = -\sum_{i=1}^{N-1} p(x_i) \log_2 p(x_i) - [1 - p(x_1) - p(x_2) - ... - p(x_k) - ... - p(x_{N-1})] \times$$

$$\times \log_2 [1 - p(x_1) - p(x_2) - ... - p(x_k) - ... - p(x_{N-1})] =$$

$$= -p(x_1) \log_2 p(x_1) - p(x_2) \log_2 p(x_2) - ... - \underline{p(x_k) \log_2 p(x_k)} - ...$$

$$- p(x_{N-1}) \log_2 p(x_{N-1}) - [1 - p(x_1) - p(x_2) - ... - \underline{p(x_k)} - ... - p(x_{N-1})] \times$$

$$\times \log_2 [1 - p(x_1) - p(x_2) - ... - \underline{p(x_k)} - ... - p(x_{N-1})]. \tag{2.5.7}$$

Знайдемо похідну відносно довільно взятої, але фіксованої імовірності $p(x_k)$, де $k = 1, 2, 3, ..., N\text{-}1$, і прирівняємо її до нуля.

$$\frac{dH(X)}{dp(x_k)} = -\log_2 p(x_k) - \log_2 e +$$

$$+\log_2[1-p(x_1)-p(x_2)-...-p(x_k)-...-p(x_{N-1})]+\log_2 e=$$

$$=\log_2\frac{1-p(x_1)-p(x_2)-...-p(x_k)-...-p(x_{N-1})}{p(x_k)}=$$

$$=\log_2\frac{p(x_N)}{p(x_k)}=0. \qquad (2.5.8)$$

Співвідношення (2.5.8.) отримано з використанням правила диференціювання:

$$(uv)'=u'v+uv'$$

та табличних похідних:

$$x'=1,$$

$$(\log_a x)'=\frac{1}{x}\log_a e.$$

Таким чином для кожного значення k (k = 1, 2, 3, ..., N–1):

$$p(x_k)=p(x_N).$$

Отже, максимум дискретного джерела досягається при рівноймовірності вихідних символів:

$$p(x_1)=p(x_2)=p(x_3)=...=p(x_{N-1})=p(x_N)=\frac{1}{N}. \qquad (2.5.9)$$

При цьому максимум ентропії набуває значення:

$$H(X)=\log_2 N.$$

Слід зазначити, що для двійкових джерел (N = 2):

$$H_{\max}(X)\underset{p(X_k^n)=\frac{1}{2^n}}{=}1 \text{ біт.} \qquad (2.5.10)$$

Знаходження мінімуму ентропії $H(X/Y)$ для співвідношення (2.5.4) через складність його аналізу не є доцільним.

Для знаходження пропускної спроможності скористаємося співвідношення (2.5.5). Нехай, для простоти, канал буде двійковим.

Знайдемо ентропію $H(Y)$ за умови максимуму $H(X)$ та дослідимо її на предмет максимуму.

$$H(Y)=\lim_{n\to\infty}\frac{1}{n}\sum_{l=1}^{2^n}p(Y_l^n)\log_2\frac{1}{p(Y_l^n)}=$$

$$= \lim_{n\to\infty} \frac{1}{n} \sum_{l=1}^{2^n} \sum_{k=1}^{2^n} p(X_k^n) p(Y_l^n / X_k^n) \log_2 \frac{1}{\sum_{k=1}^{2^n} p(X_k^n) p(Y_l^n / X_k^n)}. \quad (2.5.11)$$

З урахуванням умови максимуму ентропії (2.5.10) співвідношення (2.5.11) спроститься:

$$H(Y) = \lim_{n\to\infty} \frac{1}{n} \sum_{l=1}^{2^n} \sum_{k=1}^{2^n} \frac{1}{2^n} p(Y_l^n / X_k^n) \log_2 \frac{1}{\sum_{k=1}^{2^n} \frac{1}{2^n} p(Y_l^n / X_k^n)} =$$

$$= \lim_{n\to\infty} \frac{1}{2^n} \frac{1}{n} \sum_{l=1}^{2^n} \sum_{k=1}^{2^n} p(Y_l^n / X_k^n) \log_2 \frac{2^n}{\sum_{k=1}^{2^n} p(Y_l^n / X_k^n)}. \quad (2.5.12)$$

Як очевидно, у співвідношенні (2.5.12)

$$\sum_{k=1}^{2^n} p(Y_l^n / X_k^n) = 1$$

як повні групи подій.

З урахуванням останнього ентропія виходу каналу

$$H_{\max}(Y) \underset{p(X_k^n)=\frac{1}{2^n}}{=} 1 \text{ біт}. \quad (2.5.13)$$

Отже, $H(Y)$ досягає максимуму за умови максимуму ентропії джерела $H(X)$ та рівноймовірності його вихідних символів.

Знайдемо умовну ентропію $H(Y/X)$ та дослідимо її на предмет мінімуму.

$$H(Y / X) = \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{2^n} \sum_{l=1}^{2^n} p(X_k^n) p(Y_l^n / X_k^n) \log \frac{1}{p(Y_l^n / X_k^n)} =$$

$$= \lim_{n\to\infty} \frac{1}{n} \frac{1}{2^n} \sum_{k=1}^{2^n} \sum_{l=1}^{2^n} p(Y_l^n / X_k^n) \log \frac{1}{p(Y_l^n / X_k^n)}. \quad (2.5.14)$$

Як видно зі співвідношення (2.5.14), умовна ентропія повністю визначається переходами вхідних X^n_k у вихідні Y^n_l. Якщо дискретний канал адитивний (симетричний), то його переходи можна описати формулою:

$$y = (x + e) \bmod N, \quad (2.5.15)$$

де e – символ помилки, на який відрізняється вихідний символ y від вхідного x (як очевидно e – елемент того ж алфавіту, що і x та y); N – об'єм алфавіту.

Відповідно, перехід блоків довжини n в каналі можна виразити:

$$Y_l^n = (X_k^n + E_s^n) \bmod N^n , \qquad (2.5.16)$$

де $E^n_s = (e_1, e_2, \ldots, e_n)$ – послідовність помилки довжиною n, на яку відрізняється вихідна послідовність Y^n_l від вхідної X^n_k. Як очевидно, структура послідовності E^n_s та алфавіт, що використовуються, такі ж, як і для X^n_k та Y^n_l;

s – номер комбінації E^n_s.

Наприклад, для каналів з двійковим алфавітом ($e = \{0, 1\}$ та $s = 1, 2, 3, \ldots, 2^n$) співвідношення (2.5.16) можна записати у вигляді:

$$Y_l^n = (y_1, y_2, ..., y_n) = (x_1 \oplus e_1, x_2 \oplus e_2, ..., x_n \oplus e_n) ,$$

де $\oplus$ – операція додавання за модулем 2.

З врахуванням (16) умовна імовірність:

$$p(Y_l^n / X_k^n) = p(X_k^n \to Y_l^n) = p((X_k^n + E_s^n) \bmod N^n / X_k^n) =$$

$$= p((X_k^n + E_s^n - X_k^n) \bmod N^n) = p(E_s^n) . \qquad (2.5.17)$$

Якщо в співвідношенні (2.5.14) внести заміну (2.5.17), то отримаємо:

$$H(Y / X) = \lim_{n\to\infty} \frac{1}{n} \sum_{s=1}^{2^n} p(E_s^n) \log \frac{1}{p(E_s^n)} = H(E). \qquad (2.5.18)$$

де $H(E)$ – ентропія джерела помилок.

Підставивши співвідношення (2.5.13) та (2.5.18) в (2.5.5), отримаємо остаточне співвідношення пропускної спроможності дискретного адитивного каналу:

$$C = 1 - H(E) \text{ [біт]}. \qquad (2.5.19)$$

Умовою відсутності каналу є відсутність його пропускної спроможності ($C = 0$ [біт]). Вочевидь, вона досягається за умови максимуму $H(E)$. При цьому, як вже було показано, максимум ентропії досягається за рівноймовірності послідовностей помилок.

Отже, обґрунтовано пропускну здатність дискретного каналу, яка по суті визначається кількістю взаємної інформації в каналі за умови максимуму ентропії (кількості інформації) на виході джерела. Отримано співвідношення, яке зв'язує цей показник з імовірностями переходів комбінацій даних в каналі. Показано, що якщо канал адитивний, то пропускна здатність є протилежно пропорційною та повністю визначається ентропією джерела помилок.

Обґрунтовано умову відсутності каналу, яка досягається за його нульової пропускної здатності та, відповідно, за рівноймовірності послідовностей помилок у каналі.

Пропускна здатність дискретного симетричного каналу без пам'яті та умова його відсутності. Якщо дискретний симетричний канал без пам'яті має джерело помилок з бернуллііївським розподілом, то його ентропія знаходиться через ентропійну функцію:

$$H(E) = p\log_2\frac{1}{p} + (1-p)\log_2\frac{1}{1-p} = h(p), \qquad (2.5.20)$$

де p – імовірність помилки.

З урахуванням співвідношення (2.5.20) формула пропускної спроможності дискретного симетричного каналу без пам'яті (2.5.19) прийме остаточний вигляд:

$$C = 1 + p\log_2 p + (1-p)\log_2(1-p) \text{ [біт]}. \qquad (2.5.21)$$

Пропускна здатність дискретного симетричного каналу без пам'яті, що розрахована за одиницю часу виражатиметься формулою:

$$C' = V_к C = V_к\left[1 + p\log_2 p + (1-p)\log_2(1-p)\right] \text{ [біт/с]}. \qquad (2.5.22)$$

Графік залежностей (2.5.21) та (2.5.22) пропускної здатності від імовірності помилки в дискретному симетричному каналі без памяті подано на рис.2.5.2.

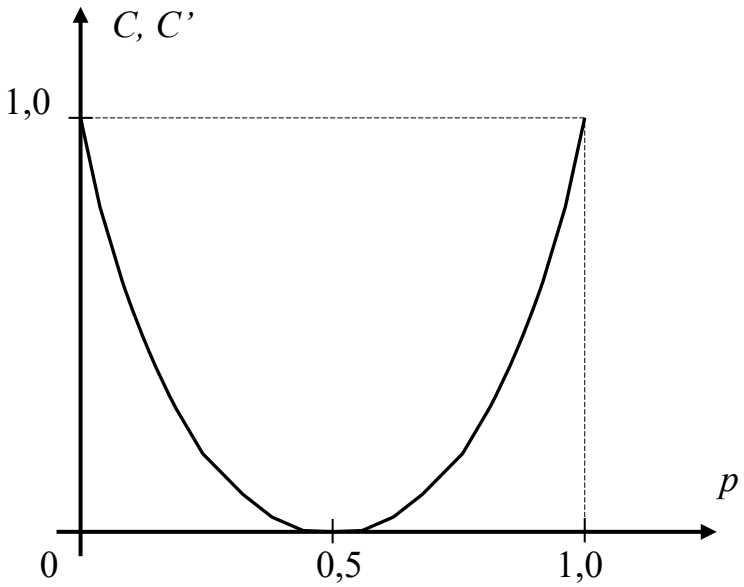


Рис.2.5.2. Графік залежності пропускної здатності C та C' від імовірності помилки p

Як очевидно, *умова відсутності дискретного симетричного каналу без пам'яті* досягається при рівноймовірності помилок:

$$p = 1 - p = \frac{1}{2}.$$

Таким чином, обґрунтовано пропускну здатність дискретного симетричного каналу без пам'яті. Отримано співвідношення, яке зв'язує цей показник з імовірністю остями помилки в каналі. Обґрунтовано умову відсутності каналу, яка досягається за умови рівноймовірності помилок.

Отже, обґрунтовано пропускну здатність дискретного каналу, яка, по суті, визначається кількістю взаємної інформації в каналі за умови максимуму ентропії (кількості інформації) на виході джерела. Отримано співвідношення, яке зв'язує цей показник з імовірностями переходів комбінацій даних у каналі. Показано, що якщо канал адитивний, то пропускна здатність є протилежно пропорційною та повністю визначається ентропією джерела помилок.

Обґрунтовано пропускну здатність дискретного симетричного каналу без пам'яті. Отримано співвідношення, яке зв'язує цей показник з імовірністю помилки в каналі.

Здійснено обґрунтування умови відсутності каналу, яка досягається за його нульової пропускної здатності та, відповідно, за рівноймовірності послідовностей помилок у каналі. Для дискретного симетричного каналу без пам'яті умова його відсутності досягається за умови рівноймовірності помилок.

Контрольні питання:

1. Пропускна здатність дискретного каналу та її оцінювання відносно входу та відносно виходу каналу.
2. Дослідження максимуму безумовної та умовної ентропій у каналі відносно його входу.
3. Дослідження максимуму безумовної та умовної ентропій у каналі відносно його виходу.
4. Пропускна здатність дискретного симетричного каналу без пам'яті.
5. Умова відсутності дискретного каналу та дискретного симетричного каналу без пам'яті.

2.6. Пропускна здатність неперервного каналу та умова його відсутності

Пропускна здатність неперервного каналу та умова його відсутності. Під *пропускною здатністю неперервного каналу з дискретним часом* на один відлік повідомлення розумітимемо максимум кількості інформації, що можна передати по каналу, яка визначається по всіх можливих джерелах з їхніми розподілами ймовірностей. Вона виражається формулою:

$$C = \max_{\omega(s)} I(U;S)\,, \tag{2.6.1}$$

де $I(U;S)$ – кількість взаємної інформації в каналі; $\omega(s)$ – щільність розподілу ймовірностей неперервної величини s повідомлення.

Інколи зручно користуватися пропускною спроможністю дискретного каналу, розрахованого не на відлік повідомлення, а за одиницю часу.

Під *пропускною здатністю неперервного каналу з дискретним часом за одиницю часу* розумітимемо максимум кількості інформації, що можна передати по каналу за одиницю часу, яка визначається по всіх можливих джерелах з їхніми розподілами ймовірностей. Вона виражається формулою:

$$C' = V_{\text{к}} C = V_{\text{к}} \max_{\omega(s)} I(U;S)\,, \tag{2.6.2}$$

де $V_{\text{к}}$ – канальна швидкість.

Кількість взаємної інформації в каналі виражається формулою:

$$I(S;U) = h(S) - h(S/U) = h(U) - h(U/S) = I(U;S)\,, \tag{2.6.3}$$

де $h(S)$, $h(U)$, $h(S/U)$ та $h(U/S)$ – безумовні та умовні диференційні ентропії входу та виходу каналу (див. рис. 2.6.2).

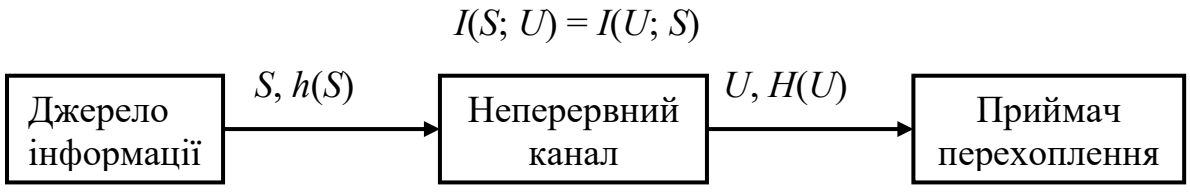


Рис. 2.6.2. Схема неперевного каналу

Пропускну здатність неперервного каналу можна виразити, підставивши окремо праву та ліву частини співвідношення (2.6.3) в (2.6.2):

$$C = \max_{\omega(s)} \left[h(S) - h(S/U) \right], \tag{2.6.4}$$

$$C = \max_{\omega(s)} \left[h(U) - h(U/S) \right]. \qquad (2.6.5)$$

Із (2.6.4) та (2.6.5) очевидно, що максимум кількості інформації, що проходить через канал по всіх можливих джерелах досягатиметься за умови, якщо безумовні диференційні ентропії каналу $h(S)$ та $h(U)$ будуть максимальними, а умовні диференційні ентропії $h(S/U)$ та $h(U/S)$ – мінімальними.

Знайдемо максимум диференційної ентропії $h(S)$.

Нехай диференційна ентропія джерела має співвідношення:

$$h(S) = \int_{-\infty}^{+\infty} \omega(s) \log_2 \frac{1}{\omega(s)} ds \,. \qquad (2.6.6)$$

Як відомо, диференційна ентропія досягає максимуму при нормальному законі розподілу ймовірностей випадкової величини s. Як вже було показано раніше, вказана величина, яка є водночас максимумом, виражається формулою:

$$h(S)_{\max} = \frac{1}{2} \log_2 (2\pi e \sigma_s^2) \,, \qquad (2.6.7)$$

де σ_s – середньоквадратичне відхилення випадкової величини s.

Знаходження мінімуму диференційної ентропії $h(S/U)$ для співвідношення (2.6.4) через складність його аналізу не є доцільним.

Для знаходження пропускної спроможності скористаємося співвідношенням (2.6.5). Нехай, для простоти, неперервний канал буде адитивним гауссівським.

Знайдемо диференційну ентропію $h(U)$ за умови максимуму $h(S)$ та дослідимо її на предмет максимуму.

Для адитивного каналу вихідний сигнал є сумою вхідного сигналу та завад:

$$u = \mu s + n = c + n, \qquad (2.6.8)$$

де μ – коефіцієнт ослаблення інформаційного сигналу; $c = \mu s$ – послаблений інформаційний сигнал; n – шумова завада, для гауссівського каналу величина n підпорядкована нормальному закону розподілу ймовірностей.

Як видно з (2.6.8), випадкова величина u є сумою двох нормально розподілених процесів, а отже і вона є нормально розподіленою. Тому її диференційна ентропія матиме максимум та виражатиметься формулою:

$$h(U)_{\max} = \int_{-\infty}^{+\infty} \omega(u) \log_2 \frac{1}{\omega(u)} du = \frac{1}{2} \log_2 (2\pi e \sigma_u^2) \,, \qquad (2.6.9)$$

де σ_u – середньоквадратичне відхилення випадкової величини u.

З умови адитивності (2.6.8) також випливає, що потужність вихідного сигналу *u*:

$$P_u = P_с + P_з, \tag{2.6.10}$$

де $P_с$ – потужність сигналу $c = \mu s$; $P_з$ – потужність завади *n*.

Для ергодичних процесів середньоквадратичне відхилення дорівнюватиме потужності:

$$\sigma^2_u = P_u. \tag{2.6.11}$$

З урахуванням (2.6.9) та (2.6.10) максимум диференційної ентропії *u* матиме співвідношення:

$$h(U)_{\max} = \frac{1}{2}\log_2(2\pi e(P_c + P_з)). \tag{2.6.12}$$

Знайдемо умовну диференційну ентропію $h(U/S)$ та дослідимо її на предмет мінімуму.

Для адитивного каналу, як було показано раніше, умовну диференційну ентропію $h(U/S)$ повністю визначає безумовна диференційна ентропія джерела завади. Оскільки остання – нормально розподілена, то шукана величина для ергодичного процесу має вигляд:

$$h(U/S) = h(N) = \frac{1}{2}\log_2(2\pi e\sigma_з^2) = \frac{1}{2}\log_2(2\pi eP_з), \tag{2.6.13}$$

де $\sigma_з$ – середньоквадратичне відхилення випадкової величини *n*. Для ергодичного процесу $\sigma_з^2 = P_з$.

Підставивши співвідношення (2.6.12) та (2.6.13) в (2.6.5), отримаємо остаточний вигляд пропускної спроможності неперервного гауссівського каналу з дискретним часом

$$C = \frac{1}{2}\log_2(2\pi e(P_c + P_з)) - \frac{1}{2}\log_2(2\pi eP_з),$$

$$C = \frac{1}{2}\log_2\left(1 + \frac{P_c}{P_з}\right) \text{ [біт]}. \tag{2.6.14}$$

Пропускна здатність неперервного гауссівського каналу з дискретним часом, що розрахована на одиницю часу (2.6.14) виражатиметься формулою:

$$C' = V_к C = \frac{1}{2}V_к \log_2\left(1 + \frac{P_c}{P_з}\right) \text{ [біт/с]}. \tag{2.6.15}$$

Графік залежностей (2.6.14) та (2.6.15) пропускної спроможності від відношення потужностей сигналу до завади зображено на рис. 2.6.3.

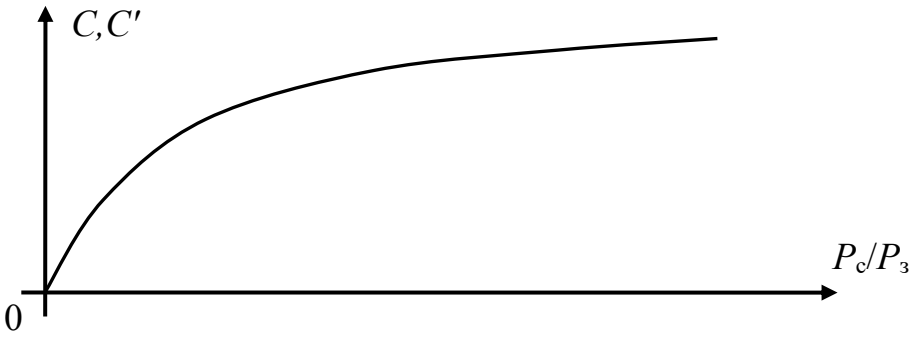


Рис. 2.6.3. Графік залежностей пропускної спроможності від відношення потужностей сигналу до завади

Як видно з (2.6.14) та (2.6.15), *умова відсутності каналу* не може бути абсолютно забезпечена. Пропускна здатність прямуватиме до нуля при нескінченному збільшенні потужності завади $P_з$, але теоретично ніколи не буде йому рівною:

$$\lim_{P_з \to \infty} \log_2 (1 + \frac{P_c}{P_з}) = 0 . \qquad (2.6.16)$$

Таким чином, обґрунтовано пропускну здатність неперервного каналу, яка за аналогією з дискретним каналом визначається максимальною кількістю взаємної інформації в каналі по всіх розподілах ймовірностей джерела. При цьому було використане твердження (без доведення), що диференційна ентропія досягає максимуму при нормальному законі розподілу ймовірностей.

Отримано співвідношення, яке зв’язує пропускну здатність каналу з відношенням потужностей сигналу до завади. Знайдено умову відсутності каналу, яка досягається за нескінченної потужності завади.

Пропускна здатність неперервного каналу з неперервним часом та фіксованою смугою пропускання. Умова відсутності каналу. З деяким наближенням канал з фіксованою смугою пропускання можна вважати ідеальним фільтром, а сигнал, пропущений через ідеальний смуговий фільтр – фінітним сигналом. Під фінітним сигналом розумітимемо сигнал, що має обмежений спектр частот, нехай – $F = f_в - f_н$ (див. рис. 2.6.4).

За теоремою Котельникова фінітні сигнали, що зосереджені в спектрі частот шириною F, можуть повністю визначатися без втрат послідовністю значень, відліченими в дискретні моменти часу з інтервалом $\Delta t = \frac{1}{2F}$.

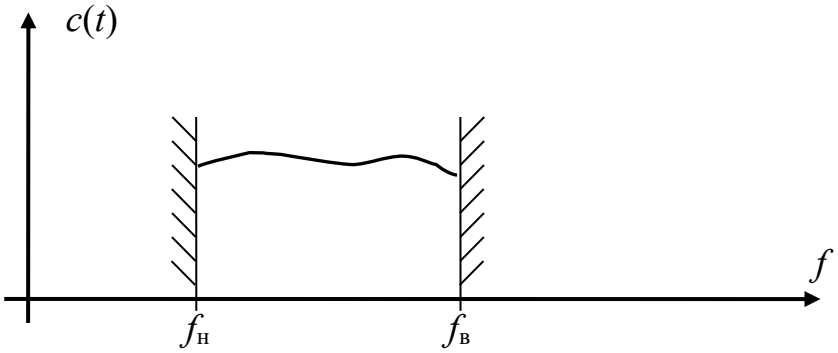


Рис. 2.6.4. Спектр сигналу, що пройшов через ідеальний смуговий фільтр

Таким чином вся інформація, що передається за одиницю часу, міститься у $2Ft$ відліках сигналу. Відповідно, неперервний канал з такою смугою пропускання можна замінити каналом з дискретним часом та з канальною швидкістю, яка визначається кількістю відліків, що проходить за одиницю часу:

$$V_{к} = \frac{1}{\Delta t} = 2F\,. \qquad (2.6.17)$$

Як очевидно, вказані канали будуть еквівалентними.

Для адитивного каналу, який визначається формулою $u(t) = c(t) + n(t)$, вихідний сигнал також визначатиметься відповідними $2Ft$ відліками, кожен з яких представлятиме суміш відліку вхідного сигналу з відповідним відліком завади.

Таким чином, пропускну здатність неперервного каналу з неперервним часом можна отримати, підставивши (2.6.17) в співвідношення (2.6.15):

$$C' = F\log_2(1+\frac{P_c}{P_з})\ \text{[біт/с]}. \qquad (2.6.18)$$

Умова відсутності каналу, як і для попереднього випадку, не визначається. Якщо має місце вхідний сигнал з потужністю $P_{с}$, то пропускна здатність прямує до нуля при нескінченному збільшенні потужності завади $P_{з}$, але теоретично ніколи не буде йому рівною, як показано у співвідношенні (2.6.15).

Отже, обґрунтовано пропускну здатність неперервного каналу з неперервним часом та фіксованою смугою пропускання. Внесено поправку до співвідношення, яке зв’язує пропускну здатність каналу з відношенням потужностей сигналу до завади та фіксованою смугою частот пропускання. Умова відсутності каналу, як і в попередньому випадку, досягається за нескінченної потужності завади. Але на відміну від попереднього випадку

потужності та сигналу, і завади мають бути зосередженими в цій же фіксованій смузі частот.

Пропускна здатність неперервного каналу з неперервним часом та плаваючою смугою пропускання. Умова відсутності каналу. При розгляданні каналу з фіксованою смугою частот як ідеального смугового фільтра вважалося, що на обмежений за спектром сигнал накладається така ж обмежена за спектром завада і при цьому вважалося, що їхні потужності $P_с$ та $P_з$, кінцеві та повністю визначені в цій смузі частот.

Розглянемо випадок, якщо канал має смугу частот пропускання з плаваючими верхньою та нижньою межами.

Нехай спектр сигналу $c(t)$ буде деяким фіксованим та знаходитися в межах смуги пропускання, а його потужність $P_с$ – величиною фіксованою і не залежатиме від вибору меж смуги.

Щодо шумової завади: якщо канал постійний гауссівський, то її спектр нескінченно великий (див. рис. 2.6.5). Для білого шуму з рівномірно розподіленою спектральною щільністю N_0 в смузі пропускання $F = f_в - f_н$ потужність:

$$P_з = FN_0. \tag{2.6.19}$$

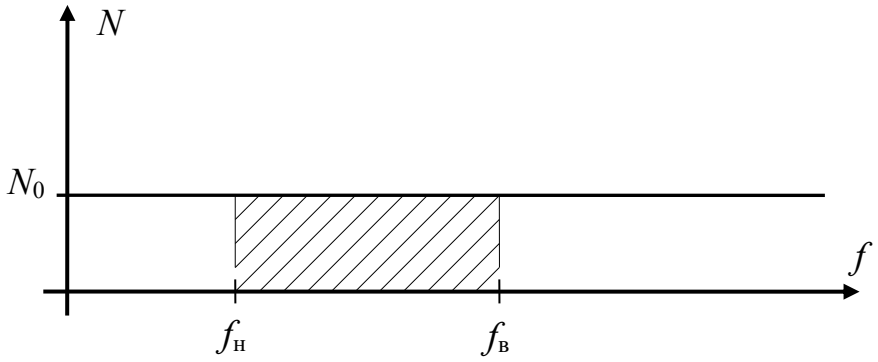


Рис. 2.6.5. Спектральна щільність білого шуму

Підставивши (2.6.19) в формулу (2.6.18), знайдемо співвідношення для пропускної спроможності неперервного каналу з плаваючою смугою пропускання:

$$C' = F\log_2(1+\frac{P_c}{N_0F}) \text{ [біт/с]}. \tag{2.6.20}$$

Умова відсутності каналу, як і для попереднього випадку, забезпеченням потрібного відношення потужностей сигналу та завади не визначається. Виявлення поведінки пропускної спроможності при

нескінченному розширенні смуги пропускання каналу та відповідно спектру шумової завади потребує окремого аналізу.

Таким чином, обґрунтовано пропускну здатність неперервного каналу з неперервним часом та плаваючою смугою пропускання. Отримано співвідношення, яке зв'язує пропускну здатність каналу з смугою частот пропускання, потужністю завади та спектральною щільністю завади. Як очевидно, умова відсутності каналу досягається при спрямуванні спектральної щільності до нескінченності, що на практиці не є можливим.

Пропускна здатність неперервного каналу з неперервним часом та нескінченною смугою пропускання. Умова відсутності каналу. Пропускну здатність неперервного каналу з нескінченною смугою пропускання можна знайти, спрямувавши в співвідношенні (2.6.20) останню в нескінченність:

$$C'_{\max} = \lim_{F\to\infty} F \log_2(1+\frac{P_c}{N_0 F}). \qquad (2.6.21)$$

Як видно зі співвідношення (2.6.21), величина F присутня і в чисельнику, і в знаменнику. При нескінченному збільшенні F в чисельнику пропускна здатність повинна також нескінченно зростати та водночас при нескінченному збільшенні F в знаменнику спрямуватися до нуля. Для знаходження границі помітимо, що співвідношення (2.6.21) при нескладному перетворенні можна привести до стандартного вигляду однієї з відомих границь типу:

$$\lim_{x\to\infty}(1+\frac{1}{x})^x = e \approx 2{,}71\ldots. \qquad (2.6.22)$$

При перетворенні матимемо:

$$C'_{\max} = \lim_{F\to\infty} F \log_2(1+\frac{P_c}{N_0 F}) = \lim_{F\to\infty} \frac{P_c}{N_0}\left[\frac{N_0 F}{P_c}\log_2(1+\frac{P_c}{N_0 F})\right] =$$

$$= \lim_{F\to\infty} \frac{P_c}{N_0}\left[\log_2(1+\frac{P_c}{N_0 F})^{\frac{N_0 F}{P_c}}\right]. \qquad (2.6.23)$$

Внесемо в (2.6.23) заміну $x = \frac{N_0 F}{P_c}$ Із $F \to \infty$ випливає, що і $x \to \infty$.

Пропускна здатність неперервного каналу з неперервним часом та необмеженою смугою частот отримає остаточний вигляд:

$$C' = \frac{P_c}{N_0} \lim_{F\to\infty} \log_2 (1+\frac{1}{x})^x = \frac{P_c}{N_0} \log_2 e \text{ [біт/с].} \qquad (2.6.24)$$

Як очевидно, при збільшенні смуги пропускання каналу його пропускна здатність не перевищує своєї межі, яка визначається співвідношенням (2.6.24). Графік залежності пропускної спроможності від смуги пропускання представлено на рис. 2.6.6.

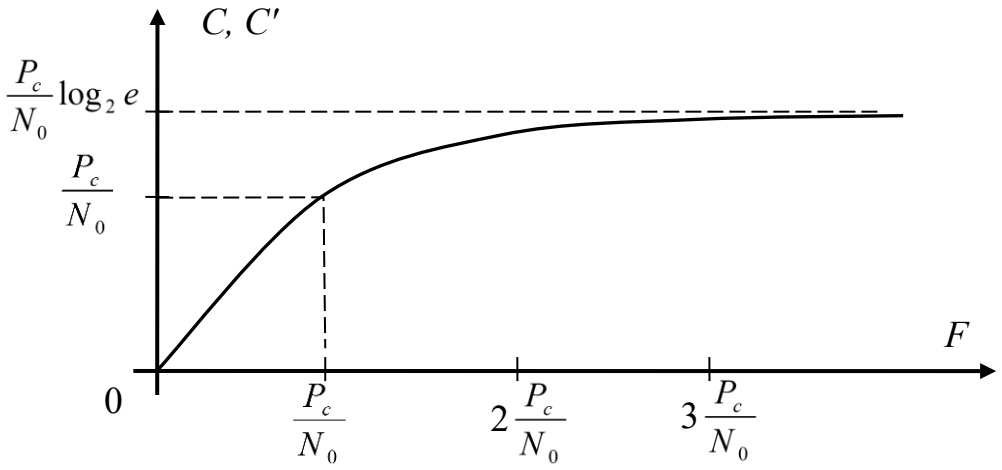


Рис. 2.6.6. Графік залежності пропускної спроможності від смуги пропускання каналу

Реально в природі білого шуму не існує. Вважається, що найбільш близьким до білого шуму є тепловий шум. Для нього спектральна щільність знаходиться із формули:

$$N_0 = kT^0, \qquad (2.6.25)$$

де k = 1,38×10^{-23} Дж/градуси – стала Больцмана, T^0 – абсолютна температура по системі Кельвіна.

Використання співвідношення (2.6.25) дозволяє практично оцінювати пропускну здатність неперервного каналу.

Таким чином, обґрунтовано пропускну здатність неперервного каналу з неперервним часом та нескінченною смугою пропускання. Дослідження співвідношення щодо пропускної здатності показало, що нескінченне розширення смуги частот пропускання не приводить до нескінченного зростання пропускної здатності.

Знайдено верхню межу пропускної здатності, яка визначається суто відношенням потужності сигналу до спектральної щільності завади. Тобто в якій би смузі частот не здійснювався прийом, неможливе перехоплення інформації, що перевищує пропускну здатність каналу. Умова відсутності каналу досягається за тих самих умов, що й у попередньому випадку.

Таким чином, обґрунтовано пропускну здатність неперервного каналу, яка за аналогією з дискретним каналом визначається максимальною кількістю взаємної інформації в каналі по всіх розподілах ймовірностей джерела. При цьому було використане твердження (без доведення), що диференційна ентропія досягає максимуму при нормальному законі розподілу ймовірностей.

Обґрунтовано пропускну здатність неперервного каналу фіксованою та плаваючою смугами частот пропускання. Досліджено пропускну здатність при спрямуванні смуги пропускання в нескінченність. Отримані співвідношення, які для вище вказаних випадків зв’язують пропускну здатність каналу з потужностями сигналу та завади, спектральними характеристиками завади та смуги пропускання.

Показано, що при розширенні смуги частот пропускання пропускна здатність має верхню межу, яка визначається суто відношенням потужності сигналу до спектральної щільності завади. Це є дуже важливим твердженням для каналів витоку, оскільки за будь-якої смуги частот прийому, неможливе перехоплення більше інформації, ніж це визначає відношення потужності сигналу до спектральної щільності завади.

Знайдено умову відсутності каналу, яка для всіх випадків досягається за нескінченної потужності чи спектральної щільності завади, що на практиці не є можливим.

Контрольні питання:

1. Пропускна здатність неперевного каналу та її оцінювання відносно входу та відносно виходу каналу.
2. Дослідження максимуму/мінімуму безумовної та умовної диференційних ентропій в неперервному каналі відносно його входу та відносно його виходу. Умова відсутності каналу.
3. Пропускна здатність неперервного каналу з неперервним часом та фіксованою смугою пропускання. Умова відсутності каналу.
4. Пропускна здатність неперервного каналу з неперервним часом та плаваючою смугою пропускання. Умова відсутності каналу.
5. Дослідження пропускної здатності неперервного каналу з розширенням в нескінченність смуги пропускання. Умова відсутності каналу.

РОЗДІЛ 3. ПОТЕНЦІЙНА ЗАВАДОСТІЙКІСТЬ. ЗВ'ЯЗОК ІМОВІРНІСНИХ ТА ЕНЕРГЕТИЧНИХ ПОКАЗНИКІВ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ ВІД ВИТОКУ ТЕХНІЧНИМИ КАНАЛАМИ

3.1. Оптимальний прийом як опис потенційної можливості перехоплення інформації технічними каналами. Вирішальна схема оптимального прийому

Дискретно-неперервний канал як опис технічного каналу витоку інформації. Сутність оптимального прийому дискретних повідомлень. З теорії інформації відомо, що головним поняттям щодо ефективності передачі інформації по дискретному чи неперервному каналу є його пропускна здатність C, яка характеризує його як максимум кількості інформації, що може бути передано по каналу.

В теорії інформації також показано, що для вказаних каналів умову "відсутності каналу" $C = 0$, яка є бажаною для захисту інформації від витоку технічними каналами, в реальності забезпечити практично неможливо, оскільки вона досягається лише для ідеальних випадків: для дискретних каналів з рівноймовірністю наявності та відсутності помилки, а для неперервних при заданих потужності, тривалості та спектру сигналу – нескінченною потужністю завади. При цьому окремо розглядалися дискретні канали – канали з дискретним входом та виходом без способів їх реалізацій в неперервному середовищі, та неперервні – з неперервним входом та виходом без способів передачі ними інформації від дискретних джерел.

Однак на практиці в технічних засобах дискретні знаки, що несуть інформацію, представлені неперервними реалізаціями, які при обробці, передачі, зокрема й при просочуванні в канали витоку, спотворюються завадами, в результаті чого утворюються помилки.

Як відомо з теорії завадостійкого прийому, помилка при реєстрації знаків на прийомі залежить не тільки від завади, а й від самого способу прийому та обробки. Пошук найкращого способу прийому є головним завданням вказаної теорії та приводить до таких понять, як оптимальний приймач та критерій оптимальності.

Розглянемо сутність оптимального прийому на схемі передачі дискретних повідомлень (даних) по неперервному каналу (див. рис. 3.1.1).

Нехай задано дискретне джерело, що формує повідомлення X з алфавіту об'ємом N, $x \in \{x_1, x_2, \ldots, x_N\}$.

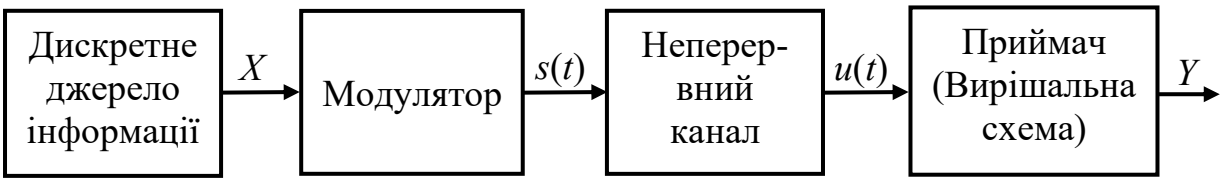


Рис. 3.1.1. Схема передачі дискретного повідомлення по неперервному каналу

Нехай задано правило модуляції, де кожному дискретному елементу ставиться у відповідність деяка реалізація неперервного сигналу тривалістю T (див. табл. 3.1.1) так, щоб за відповідними реалізаціями однозначно можливо було визначити, який знак передавався від дискретного джерела.

Таблиця 3.1.1

Правило модуляції

Дискретний елемент	Неперервний сигнал
x_1	$s_1(t)$
x_2	$s_2(t)$
...	...
x_r	$s_r(t)$
...	...
x_N	$s_N(t)$

Таким чином, на вхід каналу потрапляє повідомлення – послідовність інформаційних знаків від дискретного джерела у вигляді неперервних реалізацій $s_r(t)$ тривалістю T, $r = 1 \div N$.

Нехай задано канал як неперервний адитивний. Сигнал, що формується на виході каналу в результаті передачі реалізації $s_r(t)$, може бути вираженою співвідношенням:

$$u(t) = \mu s_r(t-\tau) + n(t) = c_r(t) + n(t), \qquad (3.1.1)$$

де μ – коефіцієнт ослаблення сигналу в каналі, τ – час затримки сигналу в каналі, $c_r(t)$ – ослаблений сигнал на виході каналу з урахуванням затримки, $n(t)$ – адитивна завада в каналі.

Нехай $\mu = 1$ та $\tau = 0$ так, щоб сигнали на виході джерела та їх реалізації на виході каналу при відсутності завад були еквівалентними $s_r(t) = c_r(t)$. Дане припущення є справедливим та на практиці може бути врахованим на прийомі, знаючи μ та τ.

Отримавши на прийомі $u(t)$, можна зробити N гіпотез (див. табл. 3.1.2).

Таблиця 3.1.2

Гіпотези, що формуються на прийомі, в результаті аналізу сигналу, отриманого на виході каналу

№ з/п	Гіпотеза про сигнал, що передавався	Гіпотеза про заваду, що була в каналі
1	$s_1(t)$	$n_1(t) = u(t) - \mu s_1(t-\tau)$
2	$s_2(t)$	$n_2(t) = u(t) - \mu s_2(t-\tau)$
...	...	...
r	$s_r(t)$	$n_r(t) = u(t) - \mu s_r(t-\tau)$
...	...	...
N	$s_N(t)$	$n_2(t) = u(t) - \mu s_N(t-\tau)$

Очевидно, що *завдання приймача (демодулятора, вирішальної схеми)* зводиться до прийняття рішення та вибору однієї з N гіпотез.

Також очевидно, що найкращим буде той приймач, який забезпечить найбільшу вірність правильного прийому.

Отже, під *оптимальним приймачем* будемо розуміти схему (пристрій, алгоритм чи послідовність дій), яка щодо всіх інших схем (вирішень) забезпечить у середньому найбільшу вірність прийому, а під *оптимальним прийомом* – процес прийняття рішення та вибору гіпотези, за якого забезпечується максимальна імовірність правильного вирішення.

Для побудови такої схеми або вибору приймача необхідно визначити критерій оптимальності.

Отже, розглянуто дискретно-неперервний канал як опис технічного каналу витоку інформації. Заначено сутність оптимального прийому дискретних повідомлень, який забезпечуватиме найкращий прийом повідомлень. Зазначений прийом може бути використаний як потенційна можливість перехоплення інформації.

Критерій оптимальності прийому дискретних повідомлень – максимум апостеріорної імовірності. Нехай задано розподіл ймовірностей джерела $p(x_r)$. Кожен знак представлено у формі реалізації $s_r(t)$ відповідно до табл. 3.1.1:

$$x_r \to s_r(t).$$

Реалізація $u(t)$ формується на виході адитивного гауссівського каналу в результаті проходження $s_r(t)$ та впливу на неї завади $n(t)$, згідно зі співвідношенням (3.1.1).

Визначимо розподіл ймовірностей вихідного сигналу $u(t)$ на основі початкових даних. Для цього розіб'ємо часовий інтервал T реалізацій на k перетинів (див. рис. 3.1.2).

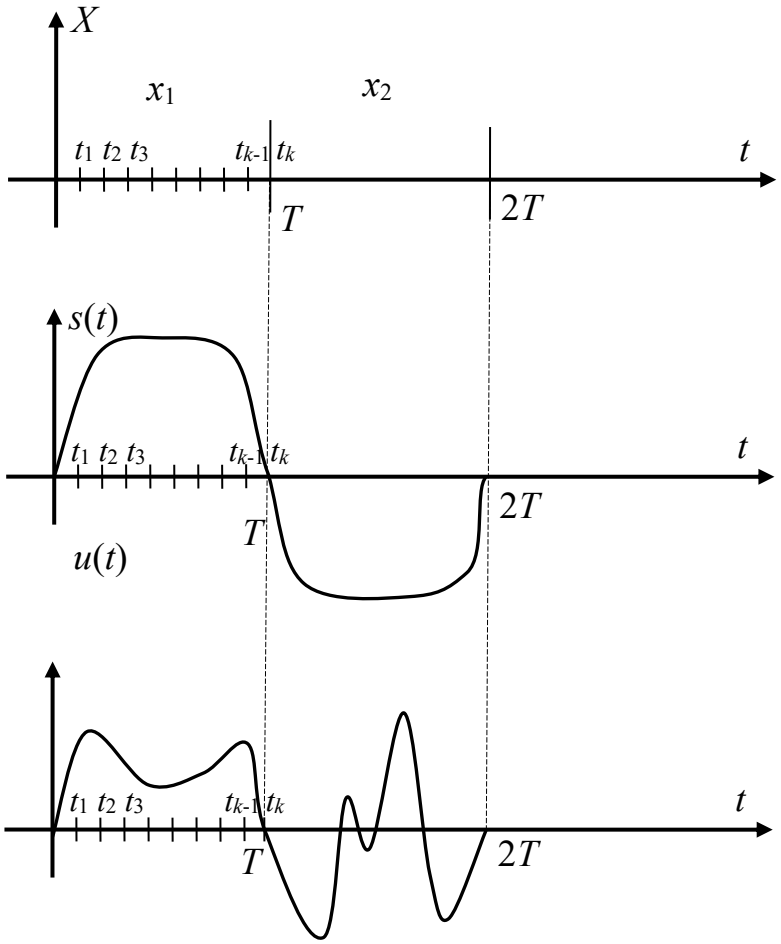


Рис.3.1.2. Приклад часового представлення відповідності даних X та сигналів $s(t)$, $u(t)$

Нехай задано перехідний процес в каналі k-вимірною умовною щільністю розподілу ймовірностей $\omega_k(u/x_r) = \omega(u_{t1}, u_{t2},\ldots, u_{tk}/x_r)$ в точках $t_1, t_2, t_3,\ldots, t_k$.

Тоді безумовна k-вимірна щільність ймовірностей вихідного сигналу $u(t)$, що визначається сумішшю реалізацій сигналу $s_r(t)$ та завади $n(t)$, виражатиметься за формулою Байєса:

$$\omega_k(u) = \sum_{r=1}^{n} p(x_r)\omega_k(u/x_r), \qquad (3.1.2)$$

а умовні імовірності вхідних символів відносно вихідного сигналу визначатимуться співвідношенням:

$$p(x_r / u) = \frac{p(x_r)\omega_k(u / x_r)}{\omega_k(u)}. \qquad (3.1.3)$$

Таким чином маємо апостеріорні $p(x_r/u)$ та апріорні $p(x_r)$ імовірності символів x_r із алфавіту об'ємом n на виході джерела.

Завдання оптимального приймача полягає в ухваленні рішення, про те, який символ був вироблений на виході джерела. При цьому оптимальність рішення повинна бути обґрунтованою.

Вважатимемо, що якщо на вхід каналу подано символ x_l і на прийомі буде ухвалено рішення y_l, то воно буде вірним, в іншому випадку, якщо y_r, де $r \neq l$, – хибним.

Правильне рішення можна зобразити у вигляді ланцюга:

$$x_l \to s_l(t) \to u(t) \to y_l .$$

Імовірність правильного рішення буде повністю визначатися величиною апостеріорної імовірності $p(x_l/u)$, а імовірність помилкового, відповідно,

$$p(пом./u, y_l) = 1 - p(x_l / u). \qquad (3.1.4)$$

Очевидно, що обґрунтування оптимальної схеми обробки сигналу з метою ухвалення найбільш правильного рішення полягає у виборі з усіх можливих найкращої. Для попарного порівняння візьмемо дві довільні схеми та порівняємо їх.

Так, якщо дві схеми ухвалюють різні рішення: y_i та y_j, які кожною з цих схем вважають правильними, то кращою буде та, яка забезпечить (обґрунтує) більшу апостеріорну імовірність правильного рішення та, відповідно, меншу імовірність помилки. Наприклад, якщо:

$$p(x_i / u) > p(x_j / u),$$

або

$$p(пом./u, y_i) < p(пом./u, y_j), \qquad (3.1.5)$$

то схема i вважатиметься кращою ніж j.

Таким чином, під *критерієм оптимального прийому* (*вирішення*) будемо розуміти прийом, який забезпечує максимум апостеріорної імовірності $p(x_l/u)$ правильного вирішення за всіма можливими схемами та ймовірностями $p(x_r/u)$, де $r = 1 \div N$:

$$p(x_l / u) = \max_{r=1\div N} p(x_r / u). \qquad (3.1.6)$$

Таким чином, *правило оптимального прийому* полягає в наступному. При надходженні $u(t)$ вирішальна схема ухвалює рішення y_l в тому випадку, якщо апостеріорна імовірність символу x_l найбільша серед всіх інших ймовірностей символів:

$$p(x_l / u) \underset{\substack{r=1\div N \\ r\neq l}}{>} p(x_r / u). \tag{3.1.7}$$

Очевидно, що правило (3.1.7) зводиться до перевірки $N - 1$ гіпотез, або розв'язку системи з $N - 1$ нерівностей:

$$\begin{cases} p(x_l / u) > p(x_1 / u) \\ p(x_l / u) > p(x_2 / u) \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ p(x_l / u) > p(x_N / u) \end{cases}, \; l \neq r, \; r = 1\div N. \tag{3.1.8}$$

Нерівності в системі (3.1.8) можна переписати з використанням формули Байеса у вигляді:

$$\frac{p(x_l)\omega(u / x_l)}{\omega(u)} > \frac{p(x_r)\omega(u / x_r)}{\omega(u)}, \tag{3.1.9}$$

Розв'язок (3.1.9) приведе до наступного:

$$\frac{p(x_l)\omega(u / x_l)}{p(x_r)\omega(u / x_r)} > 1. \tag{3.1.10}$$

Зауважимо, що відношення щільностей розподілу ймовірностей в (3.1.10) є відношенням правдоподібності:

$$\frac{\omega(u / x_l)}{\omega(u / x_r)} = \lambda_{l/r}(u). \tag{3.1.11}$$

З врахуванням (3.1.11) нерівність (3.1.10) отримає вигляд:

$$\lambda_{l/r}(u) = \frac{\omega(u / x_l)}{\omega(u / x_r)} > \frac{p(x_r)}{p(x_l)}. \tag{3.1.12}$$

Якщо розподіл ймовірностей джерела рівномірний $p(x_1) = p(x_2) = p(x_3) = \ldots = p(x_r) = \ldots = p(x_N)$, то критерій (3.1.12) спроститься:

$$\lambda_{l/r}(u) = \frac{\omega(u / x_l)}{\omega(u / x_r)} > 1. \tag{3.1.13}$$

Як очевидно, обчислення відношення правдоподібності (3.1.13) при великих n є досить складним та зводиться до не більше ніж (в середньому

$\frac{(N-1)!}{N}$) їх обчислень. Кількість цих обчислень може бути зниженою в результаті введення так званої нульової реалізації, тобто реалізації, при якій нічого не передається.

$$\lambda_{l/r}(u) = \frac{\omega(u / x_l)\omega(u / 0)}{\omega(u / x_r)\omega(u / 0)} =$$

$$= \frac{\omega(u / x_l)}{\omega(u / 0)} \times \frac{\omega(u / 0)}{\omega(u / x_r)} = \frac{\lambda_{l/0}(u)}{\lambda_{r/0}(u)}. \qquad (3.1.14)$$

При цьому нерівність (3.1.13) зводитиметься до

$$\lambda_{l/0}(u) > \lambda_{r/0}(u), \qquad (3.1.15)$$

а складність обчислень відношень правдоподібностей знизиться до N:

Відповідно, k-вимірне відношення правдоподібності визначатиметься за формулою:

$$\lambda_{r/0}(u_{t1}, u_{t2}, ..., u_{tk}) = \frac{\omega_k(u / x_r)}{\omega_k(u / 0)} =$$

$$= \frac{\omega(u_{t1}, u_{t2}, ..., u_{tk} / x_r)}{\omega(u_{t1}, u_{t2}, ..., u_{tk} / 0)}, \qquad (3.1.16)$$

через яке можна знайти і відношення правдоподібності для нерівності (3.1.15):

$$\lambda_{r/0}(u) = \lim_{k\to\infty} \lambda_{r/0}(u_{t1}, u_{t2}, ..., u_{tk}) =$$

$$= \lim_{k\to\infty} \frac{\omega(u_{t1}, u_{t2}, ..., u_{tk} / x_r)}{\omega(u_{t1}, u_{t2}, ..., u_{tk} / 0)}. \qquad (3.1.17)$$

Отже, розглянуто критерій оптимальності прийому дискретних повідомлень, в якості якого обґрунтовано максимум апостеріорної імовірності. Це виходить із того, що для правильного прийому тим більшою є вірність рішення, чим більша ця імовірність. Її рівність одиниці забезпечує безпомилковість передачі.

Критерій максимуму відношення правдоподібності та його зв'язок з енергетичними умовами на вході приймача. Знайдемо відношення правдоподібності для співвідношення (3.1.15) та виразимо критерій оптимального прийому для дискретних повідомлень з заданими параметрами.

Нехай $c_r(t)$ – фінітний за спектром та повністю зосереджений в смузі частот F. Тоді за теоремою Котельникова його можна повністю представити у відліках з інтервалом:

$$\Delta t = \frac{1}{2F}. \tag{3.1.18}$$

Розбивши тривалість T на інтервали Δt, отримаємо кількість відліків для реалізації:

$$k = \frac{T}{\Delta t} = 2FT. \tag{3.1.19}$$

Вказані в співвідношенні (3.1.15) відношення правдоподібності можна виразити як k-мірні, які з врахуванням (3.1.19) матимуть вигляд:

$$\lambda_{r/0}(u_{t1}, u_{t2}, ..., u_{tk}) = \lambda_{r/0}(u_1, u_2, ..., u_{2FT}) =$$

$$= \frac{\omega(u_1, u_2, ..., u_{2FT} / x_r)}{\omega(u_1, u_2, ..., u_{2FT} / 0)}, \tag{3.1.20}$$

де u_1, u_2, u_{2FT} – значення сигналу $u(t)$ у $2FT$ відліках.

Зауважимо, що при "нульовій" реалізації, оскільки джерелом знак не виробляється та ніякий сигнал не передається $c_0(t) = 0$, сигнал на виході каналу повністю визначатиметься завадою:

$$u(t) = c_0(t) + n(t) = n(t). \tag{3.1.21}$$

Тому $2FT$-вимірну умовну щільність за умови "нульової" реалізації, виходячи з незалежності відліків білого шуму, щільність розподілу ймовірностей якого дорівнює, $\omega(n) = \frac{1}{\sqrt{2\pi\sigma_n^2}} e^{-\frac{n_i^2}{2\sigma^2}}$ можна виразити як добуток одномірних:

$$\omega(u_1, u_2, ..., u_{2FT} / 0) = \prod_{i=1}^{2FT} \omega(u_i / 0) =$$

$$= \prod_{i=1}^{2FT} \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{u_i^2}{2\sigma^2}} = \frac{1}{(\sqrt{2\pi\sigma^2})^{2FT}} e^{-\frac{\sum_{i=1}^{2FT} u_i^2}{2\sigma^2}}, \tag{3.1.22}$$

де σ – середньоквадратичне відхилення випадкової величини u_i, яке для всіх $i = 1 \div 2FT$ однакове.

Для сигналу $u(t)$ при передачі "ненульових" реалізацій в кожному відліку i:

$$u_i = c_{ri} + n_i. \tag{3.1.23}$$

Тому відповідна умовну щільність за аналогією з (3.1.22) можна виразити у вигляді:

$$\omega(u_1, u_2, ..., u_{2FT} / c_r) = \omega(u_1 - c_{r1}, u_2 - c_{r2}, ..., u_{2FT} - c_{r2FT} / 0) =$$

$$= \frac{1}{(\sqrt{2\pi\sigma^2})^{2FT}} e^{-\frac{\sum_{i=1}^{2FT} (u_i - c_{ri})^2}{2\sigma^2}} = \frac{1}{(\sqrt{2\pi\sigma^2})^{2FT}} \exp\left\{-\frac{1}{2\sigma^2} \sum_{i=1}^{2FT} (u_i - c_{ri})^2\right\}, \tag{3.1.24}$$

Розділивши співвідношення (3.1.24) на (3.1.22) для знаходження відношення правдоподібності (3.1.20), отримаємо:

$$\lambda_{r/0}(u_1, u_2, ..., u_{2FT}) = \exp\left\{\frac{1}{2\sigma^2} \sum_{i=1}^{2FT} u_i^2\right\} \exp\left\{-\frac{1}{2\sigma^2} \sum_{i=1}^{2FT} (u_i - c_{ri})^2\right\}. \tag{3.1.25}$$

Враховуючи, що білий шум є ергодичним процесом, квадрат середньоквадратичного відхилення завади можна замінити її потужністю:

$$\sigma^2 = P_з, \tag{3.1.26}$$

яка може бути вираженою через її спектральну щільність N_0:

$$P_з = N_0 F = \frac{N_0}{2\Delta t}. \tag{3.1.27}$$

Підставивши співвідношення (3.1.27) в (3.1.26) та, відповідно, в (3.1.25), отримаємо:

$$\lambda_{r/0}(u_1, u_2, ..., u_{2FT}) = \exp\left\{\frac{1}{N_0} \sum_{i=1}^{2FT} u_i^2 \Delta t\right\} \exp\left\{-\frac{1}{N_0} \sum_{i=1}^{2FT} (u_i - c_{ri})^2 \Delta t\right\}. \tag{3.1.28}$$

Спрямувавши $F \to \infty$, або $\Delta t \to 0$, що еквівалентно, знайдемо інтегроване відношення правдоподібності:

$$\lambda_{r/0}(u) = \lim_{\Delta t \to 0} \lambda_{r/0}(u_1, u_2, ..., u_{2FT}) =$$

$$= \exp\left\{\frac{1}{N_0} \int_0^T u^2(t) dt\right\} \exp\left\{-\frac{1}{N_0} \int_0^T (u(t) - c_r(t))^2 dt\right\}. \tag{3.1.29}$$

З розкладом квадрата різниці (3.1.29) перетвориться:

$$\lambda_{r/0}(u) = \exp\left\{\frac{1}{N_0}\left[\int_0^T u^2(t)dt - \int_0^T (u^2(t) - 2u(t)c_r(t) + c_r^2(t))dt\right]\right\} =$$

$$= \exp\left\{\frac{1}{N_0}\left[2\int_0^T u(t)c_r(t)dt - \int_0^T c_r^2(t)dt\right]\right\}. \quad (3.1.30)$$

Зауважимо, що в (3.1.30) інтеграл:

$$\int_0^T c_r^2(t)dt = E_r \quad (3.1.31)$$

є енергією сигналу, що дозволяє внести заміну та виконати ряд перетворень:

$$\lambda_{r/0}(u) = e^{-\frac{E_r}{N_0}} \exp\left\{\frac{2}{N_0}\int_0^T u(t)c_r(t)dt\right\} =$$

$$= e^{-\frac{E_r}{2T}\frac{2T}{N_0}} \exp\left\{\frac{2T}{N_0}\frac{1}{T}\int_0^T u(t)c_r(t)dt\right\}. \quad (3.1.32)$$

Зауважимо, що в (3.1.32) відношення:

$$\frac{E_r}{T} = P_r \quad (3.1.33)$$

є потужністю реалізації $c_r(t)$.

Введемо позначання:

$$Z_r(u) = \frac{1}{T}\int_0^T u(t)c_r(t)dt\,. \quad (3.1.34)$$

Підставимо співвідношення (3.1.34) та (3.1.33) в (3.1.32) отримаємо остаточне співвідношення для шуканого відношення правдоподібності:

$$\lambda_{r/0}(u) = e^{-\frac{P_r}{2}\frac{2T}{N_0}} e^{\frac{2T}{N_0}Z_r(u)}$$

$$\lambda_{r/0}(u) = \exp\left\{\frac{2T}{N_0}\left[Z_r(u) - \frac{P_r}{2}\right]\right\}. \quad (3.1.35)$$

З врахуванням (3.1.35) критерій оптимального прийому (3.1.15) прийме вигляд:

$$\exp\left\{\frac{2T}{N_0}\left[Z_l(u)-\frac{P_l}{2}\right]\right\} > \exp\left\{\frac{2T}{N_0}\left[Z_r(u)-\frac{P_r}{2}\right]\right\}. \qquad (3.1.36)$$

Прологарифмувавши натуральним логарифмом праву та ліву частини, а також розділивши на, $\frac{2T}{N_0}$ критерій (3.1.15) прийме остаточний вигляд:

$$Z_l(u)-\frac{P_l}{2} > Z_r(u)-\frac{P_r}{2}, \qquad (3.1.37)$$

де P_r – потужність реалізації $c_r(t)$:

$$P_r = \frac{1}{T}\int_0^T c_r^2(t)dt,$$

$Z_r(u)$ – допоміжна величина, яка по суті є часовою функцією кореляції реалізацій $u(t)$ та $c_r(t)$ або їх взаємною потужністю:

$$Z_r = \frac{1}{T}\int_0^T u(t)c_r(t)dt.$$

Таким чином, в якості критерію оптимальності прийому дискретних повідомлень замість максимуму апостеріорної імовірності обґрунтовано можливість використання максимуму відношення правдоподібності. Він відрізняється від максимум апостеріорної імовірності тим, що працює за умови рівності апріорних ймовірностей. Обґрунтовано зв'язок відношення правдоподібності та його максимуму з енергетичними умовами на вході приймача.

Вирішальна схема оптимального приймача дискретних повідомлень за критерієм максимуму відношення правдоподібності. На основі критерію максимуму відношення правдоподібності (3.1.15) та співвідношення (3.1.37) для каналу на рис. 3.1.1 можна побудувати вирішальну схему (див. рис. 3.1.3).

Вирішальна схема оптимального приймача побудована для довільного, але фіксованого алфавіту джерела.

Таким чином, побудовано вирішальну схему, яка є описом оптимального приймача в дискретно-неперервному каналі. Зазначений прийом є потенційною можливістю перехоплення та може бути взятим за основу обґрунтування захищеності інформації від витоку технічними каналами для джерел з рівноймовірним розподілом.

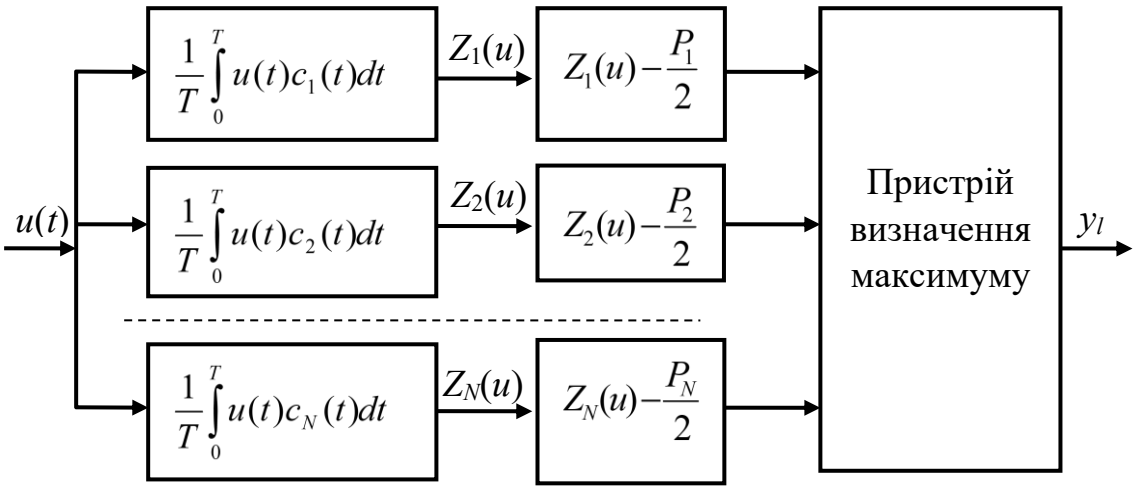


Рис. 3.1.3. Вирішальна схема оптимального приймача дискретних повідомлень

Отже, здійснено огляд оптимального прийому як опису потенційної можливості перехоплення інформації технічними каналами витоку. Водночас в якості технічного каналу використано дискретно-неперервний канал. Заначено сутність оптимального прийому дискретних повідомлень, який забезпечуватиме найкращий прийом повідомлень.

Розглянуто критерій оптимальності прийому дискретних повідомлень, в якості якого обґрунтовано максимум апостеріорної імовірності. Показано, що за умови рівності апріорних ймовірностей він може бути заміненим максимумом відношення правдоподібності. Обґрунтовано зв'язок відношення правдоподібності та його максимуму з енергетичними умовами на вході приймача.

На основі критерію максимуму відношення правдоподібності побудовано вирішальну схему оптимального приймача в дискретно-неперервному каналі. Зазначений прийом є найкращим прийомом з усіх можливих, а тому є описом потенційної можливості перехоплення та може бути взятим за основу при обґрунтуванні захищеності інформації від витоку технічними каналами для джерел з рівноймовірним розподілом.

Контрольні питання:

1. Оптимальний прийом як опис потенційної можливості перехоплення інформації технічними каналами.
2. Дискретно-неперервний канал як опис технічного каналу витоку інформації від дискретних джерел.
3. Критерій оптимальності прийому та максимум апостеріорної імовірності.

4. Критерій максимуму відношення правдоподібності як критерій оптимальності прийому та його зв'язок з енергетичними умовами на вході приймача.

5. Вирішальна схема оптимального приймача.

3.2. Вирішальна схема оптимального прийому двійкових повідомлень. Імовірність помилки в каналі та її зв'язок з відношенням сигнал/завада на вході приймача

Вирішальна схема оптимального приймача для двійкових дискретних повідомлень за критерієм максимуму відношення правдоподібності. Нехай задано двійкове джерело, що виробляє відповідні знаки x_1 та x_2 ($N = 2$), спосіб представлення цих знаків в реалізації неперервних сигналів $s_1(t)$ і $s_2(t)$ та канал, через який проходять ці реалізації, спотворюючись завадами. Нехай канал є адитивним гауссівським, на виході якого формується сигнал $u(t)$.

Так, якщо джерело сформувало знак, наприклад x_1, то на виході каналу

$$u(t) = \mu s_1(t-\tau) + n(t) = c_1(t) + n(t), \qquad (3.2.1)$$

де μ – коефіцієнт ослаблення сигналу в каналі, τ – час затримки сигналу в каналі, $c_r(t)$ – ослаблений сигнал на виході каналу з урахуванням затримки, $n(t)$ – адитивна завада в каналі.

Якщо ж джерело сформувало знак x_2, то на виході каналу

$$u(t) = \mu s_2(t-\tau) + n(t) = c_2(t) + n(t). \qquad (3.2.2)$$

Якщо джерело виробило знак x_1, то оптимальний приймач ухвалить правильне рішення при виконанні критерію:

$$\frac{1}{T}\int_0^T u(t)c_1(t)dt - \frac{P_1}{2} > \frac{1}{T}\int_0^T u(t)c_2(t)dt - \frac{P_2}{2}, \qquad (3.2.3)$$

де P_1 – потужність реалізації $c_1(t)$:

$$P_1 = \frac{1}{T}\int_0^T c_1^2(t)dt,$$

P_2 – потужність реалізації $c_2(t)$:

$$P_2 = \frac{1}{T}\int_0^T c_2^2(t)dt.$$

Перетворимо співвідношення критерію оптимальності (3.2.3), перенісши інтеграли в ліву сторону, потужності в праву та звівши подібні доданки:

$$\frac{1}{T}\int_0^T u(t)\left[c_1(t)-c_2(t)\right]dt > \frac{1}{2}(P_1-P_2) \qquad (3.2.4)$$

або

$$\frac{1}{T}\int_0^T u(t)c_\Delta(t)dt > \frac{1}{2}(P_1-P_2),$$

де $c_\Delta(t)$ – різницевий сигнал:

$$c_\Delta(t) = c_1(t) - c_2(t).$$

За критерієм (3.2.4) можна побудувати схему оптимального прийому двійкових повідомлень (див. рис. 3.2.1).

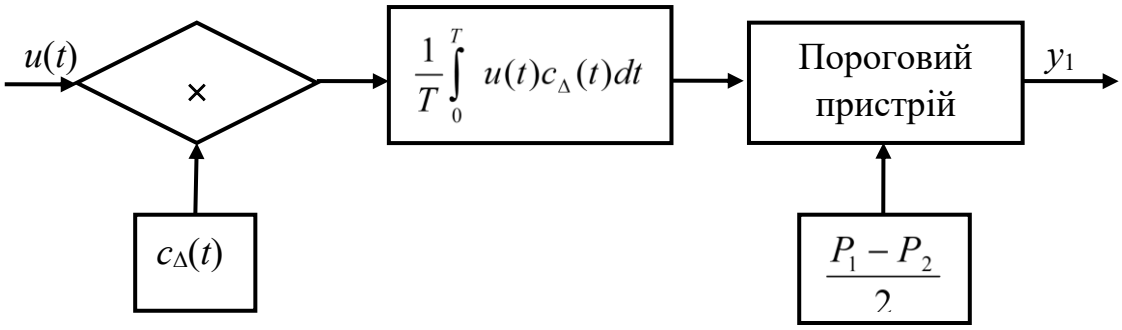


Рис. 3.2.1. Вирішальна схема оптимального приймача двійкових повідомлень з відомими параметрами

Якщо потужності реалізацій рівні між собою $P_1 = P_2$, то суть роботи порогового пристрою полягатиме у визначенні полярності.

Отже, на основі критерію максимуму відношення правдоподібності побудовано вирішальну схему оптимального приймача в дискретно-неперервному каналі для двійкових даних. Отримана схема може бути використана для оцінювання імовірності помилки в технічному каналі витоку як показника захищеності інформації.

Імовірність помилки оптимального прийому двійкових повідомлень за критерієм максимуму відношення правдоподібності. Нехай джерело виробило знак x_1, який представлено реалізацією $s_1(t)$ та потрапляє в канал:

$$x_1 \to s_1(t-\tau) \to u(t) = c_1(t) + n(t). \qquad (3.2.5)$$

Нехай на виході каналу побудовано оптимальний приймач, який на основі обробки прийнятого $u(t)$ ухвалює рішення y_1 при виробленні джерелом x_1 за критерієм (3.2.3) або (3.2.4).

Однак, при обчисленні даного критерію цим же приймачем не виключена можливість, що через спотворюючі властивості шумів в каналі знак в нерівності (3.2.3) буде протилежним. Тобто оптимальний приймач ухвалить помилкове рішення y_2.

Позначимо імовірність правильного прийому $p(y_1/x_1)$, а помилкового – $p(y_2/x_1)$ та знайдемо останню.

Нехай оптимальний приймач ухвалює помилкове рішення та в (3.2.3) виконується протилежна нерівність. Формально імовірність такої події може мати вигляд:

$$p(y_2/x_1) = p\left\{\frac{1}{T}\int_0^T u(t)\left[c_1(t)-c_2(t)\right]dt < \frac{1}{2}(P_1-P_2)\right\}, \qquad (3.2.6)$$

Підставимо в (3.2.6) співвідношення для потужностей сигналів $c_1(t)$ та $c_2(t)$ та співвідношення (3.2.5) для $u(t)$. Перетворивши його, отримаємо:

$$p(y_2/x_1) = p\left\{\frac{1}{T}\int_0^T \left(c_1(t)+n(t)\right)\left[c_1(t)-c_2(t)\right]dt < \frac{1}{2}\left(\frac{1}{T}\int_0^T c_1^2(t)dt - \frac{1}{T}\int_0^T c_2^2(t)dt\right)\right\} =$$

$$= p\left\{\frac{1}{T}\int_0^T c_1^2(t)dt - \frac{1}{T}\int_0^T c_1(t)c_2(t)dt + \frac{1}{T}\int_0^T n(t)\left[c_1(t)-c_2(t)\right]dt < \right.$$

$$\left. < \frac{1}{2T}\int_0^T c_1^2(t)dt - \frac{1}{2T}\int_0^T c_2^2(t)dt\right\} =$$

$$= p\left\{\frac{1}{T}\int_0^T n(t)\left[c_1(t)-c_2(t)\right]dt < \right.$$

$$\left. < -\frac{1}{2T}\int_0^T c_1^2(t)dt + 2\frac{1}{2T}\int_0^T c_1(t)c_2(t)dt - \frac{1}{2T}\int_0^T c_2^2(t)dt\right\} =$$

$$= p\left\{\frac{1}{T}\int_0^T n(t)c_\Delta(t)dt < -\frac{1}{2T}\int_0^T \left[c_1(t)-c_2(t)\right]^2 dt\right\} =$$

$$= p\left\{\frac{1}{T}\int_0^T n(t)c_\Delta(t)dt < -\frac{1}{2T}\int_0^T c_\Delta^2(t)dt\right\}. \qquad (3.2.7)$$

Зауважимо, що сутність події, імовірність якої визначається в (3.2.7.), полягає у виконанні нерівності, де в лівій частині подається випадкова величина, позначимо її через ξ:

$$\frac{1}{T}\int_0^T n(t)c_\Delta(t)dt = \xi, \tag{3.2.8}$$

а в правій – постійна, яка являє собою половину потужності різницевого сигналу – $c_\Delta(t)$, позначимо її через P_Δ:

$$\frac{1}{T}\int_0^T c_\Delta^2(t)dt = P_\Delta. \tag{3.2.9}$$

З урахуванням (3.2.8) та (3.2.9) імовірність (3.2.7) можна виразити в простішому вигляді:

$$p(y_2 / x_1) = p\left\{\xi < -\frac{P_\Delta}{2}\right\}. \tag{3.2.10}$$

Зауважимо, що в (3.2.10) випадкова ξ є нормально розподіленою величиною, оскільки вона отримана в результаті лінійної операції над гауссівським процесом $n(t)$. Очевидно, що імовірність виконання умови в (3.2.10) може бути знайдено через щільність розподілу ξ, для чого потрібно визначити його математичне сподівання та дисперсію.

Математичне сподівання випадкової величини ξ визначається за формулою:

$$\mathrm{M}[\xi] = \mathrm{M}\left[\frac{1}{T}\int_0^T n(t)c_\Delta(t)dt\right] = \frac{1}{T}\int_0^T \mathrm{M}[n(t)]c_\Delta(t)dt = 0. \tag{3.2.11}$$

В співвідношенні (3.2.11) її рівність нулю обґрунтовується тим, що завада не має постійної складової, а отже і її математичне сподівання як ергодичного процесу дорівнює нулю.

Дисперсія випадкової величини ξ:

$$\mathrm{D}[\xi] = \mathrm{D}\left[\frac{1}{T}\int_0^T n(t)c_\Delta(t)dt\right] = \mathrm{M}\left[\left\{\frac{1}{T}\int_0^T n(t)c_\Delta(t)dt\right\}^2\right] =$$

$$= \frac{1}{T^2}\mathrm{M}\left[\int_0^T n(t)c_\Delta(t)dt\int_0^T n(t')c_\Delta(t')dt'\right] =$$

$$= \frac{1}{T^2} \int_0^T \int_0^T c_\Delta(t) c_\Delta(t') \mathrm{M}\left[n(t) n(t')\right] dt dt' . \qquad (3.2.12)$$

З теорії сигналів відомо, що для білого шуму:

$$\mathrm{M}\left[n(t) n(t')\right] = R(t - t') = N_0 \delta(t - t') , \qquad (3.2.13)$$

$$\int_a^b f(x_0) \delta(x - x_0) dx = f(x_0) , \text{ для } a < x_0 < b. \qquad (3.2.14)$$

З використанням (3.2.13) та (3.2.14) дисперсія (3.2.12) перетвориться та набуде остаточного вигляду:

$$\mathrm{D}[\xi] = \frac{N_0}{T^2} \int_0^T \int_0^T c_\Delta(t) c_\Delta(t') \delta(t - t') dt dt' =$$

$$= \frac{N_0}{T^2} \int_0^T c_\Delta^2(t) dt = \frac{N_0 P_\Delta}{T} . \qquad (3.2.15)$$

Отже щільність розподілу випадкової величини ξ:

$$\omega(\xi) = \frac{1}{\sqrt{2\pi \dfrac{N_0 P_\Delta}{T}}} \exp\left\{ - \frac{\xi^2}{2 \dfrac{N_0 P_\Delta}{T}} \right\} . \qquad (3.2.16)$$

Таким чином, з використанням щільності (3.2.16) імовірність (3.2.10) може бути знайденим як визначений інтеграл, тобто площа, обмежена кривою щільності та межами величини ξ (див рис. 3.2.2):

$$p(y_2 / x_1) = p\left\{ \xi < -\frac{1}{2} P_\Delta \right\} = \int_{-\infty}^{-\frac{1}{2} P_\Delta} \omega(\xi) d\xi =$$

$$= \frac{1}{\sqrt{2\pi \dfrac{N_0 P_\Delta}{T}}} \int_{-\infty}^{-\frac{1}{2} P_\Delta} \exp\left\{ - \frac{\xi^2}{2 \dfrac{N_0 P_\Delta}{T}} \right\} d\xi . \qquad (3.2.17)$$

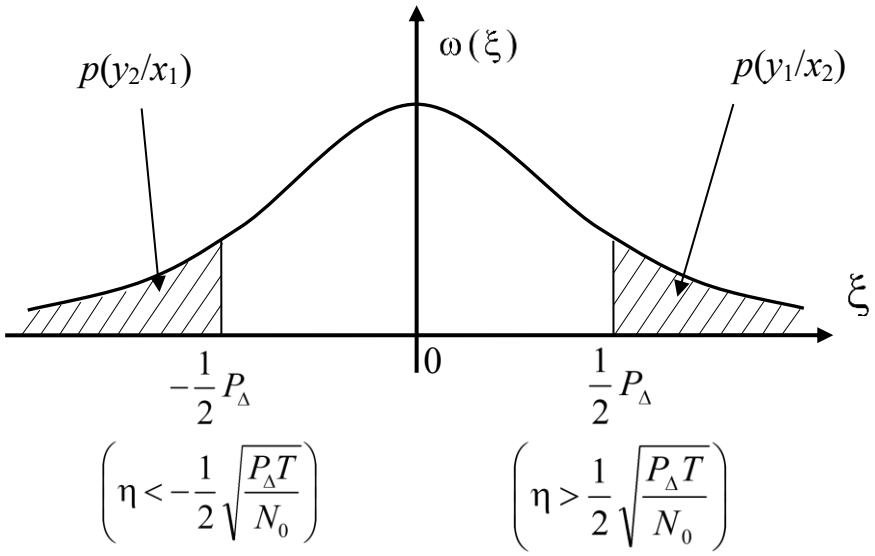


Рис. 3.2.2. Щільність розподілу ймовірностей випадкової величини ξ

Для спрощення знаходження значення інтегралу введемо позначення:

$$\frac{\xi}{\sqrt{\frac{N_0 P_\Delta}{T}}} = \eta . \qquad (3.2.18)$$

Відповідно верхня гранична межа інтегралу:

$$\eta_{\text{гр}} = \frac{-\frac{1}{2}P_\Delta}{\sqrt{\frac{N_0 P_\Delta}{T}}} = -\frac{1}{2}\sqrt{\frac{P_\Delta T}{N_0}} , \qquad (3.2.19)$$

а диференціал ξ:

$$d\xi = \sqrt{\frac{N_0 P_\Delta}{T}} d\eta . \qquad (3.2.20)$$

Зробивши заміну в (3.2.17) відповідно до (3.2.18), (3.2.19) та (3.2.10), отримаємо остаточний вигляд шуканої імовірності:

$$p(y_2 / x_1) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{-\frac{1}{2}\sqrt{\frac{P_\Delta T}{N_0}}} e^{-\frac{\eta^2}{2}} d\eta = F(-\frac{1}{2}\sqrt{\frac{P_\Delta T}{N_0}}) , \qquad (3.2.21)$$

де $F(x)$ – інтеграл Лапласа, що знаходиться за допомогою довідника:

$$F(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-\frac{\eta^2}{2}} d\eta .$$

Нехай тепер джерело виробило знак x_2, для якого аналогічно до співвідношення (3.2.5):

$$x_2 \rightarrow s_2(t-\tau) \rightarrow u(t) = c_2(t) + n(t). \qquad (3.2.22)$$

Відповідно імовірність помилки визначатиметься співвідношенням:

$$p(y_1 / x_2) = p\left\{ \frac{1}{T} \int_0^T u(t)\left[c_1(t) - c_2(t)\right]dt > \frac{1}{2}(P_1 - P_2) \right\} =$$

$$= p\left\{ \frac{1}{T} \int_0^T \left(c_2(t) + n(t)\right)\left[c_1(t) - c_2(t)\right]dt > \frac{1}{2}\left(P_1 - P_2\right) \right\} =$$

$$= p\left\{ \frac{1}{T} \int_0^T n(t) c_\Delta(t) dt > \frac{1}{2T} \int_0^T c_\Delta^2(t) dt \right\}. \qquad (3.2.23)$$

Користуючись уведеними позначеннями (3.2.8) та (3.2.9), співвідношення (3.2.22) набуде вигляду:

$$p(y_1 / x_2) = p\left\{ \xi > \frac{P_\Delta}{2} \right\}. \qquad (3.2.24)$$

Аналогічно, як для $p(y_2/x_1)$, отримаємо, що

$$p(y_1 / x_2) = \frac{1}{\sqrt{2\pi}} \int_{\frac{1}{2}\sqrt{\frac{P_\Delta T}{N_0}}}^{+\infty} e^{-\frac{\eta^2}{2}} d\eta = 1 - \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{-\frac{1}{2}\sqrt{\frac{P_\Delta T}{N_0}}} e^{-\frac{\eta^2}{2}} d\eta =$$

$$= 1 - F\left(-\frac{1}{2}\sqrt{\frac{P_\Delta T}{N_0}}\right) = F\left(-\frac{1}{2}\sqrt{\frac{P_\Delta T}{N_0}}\right).. \qquad (3.2.25)$$

Зауважимо, що останнє отримано, виходячи з властивостей симетричності щільності нормального закону розподілу (див. рис. 3.2.2).

Узагальнюючу імовірність помилки в каналі можна знайти через математичне сподівання у вигляді:

$$p = p(x_1)p(y_2 / x_1) + p(x_2)p(y_1 / x_2) = F\left(-\frac{1}{2}\sqrt{\frac{P_\Delta T}{N_0}}\right). \qquad (3.2.26)$$

Графік залежності імовірності помилки p від енергетичного аргументу $\frac{1}{2}\sqrt{\frac{P_\Delta T}{N_0}}$ при оптимальному прийомі двійкових сигналів зображено на рис. 3.2.3. Аргумент $\frac{1}{2}\sqrt{\frac{P_\Delta T}{N_0}}$ означає відношення сигнал/завада на вході приймача.

Таким чином, на основі критерію та вирішальної схеми оптимального приймача обґрунтовано імовірність помилки в каналі витоку як показника захищеності інформації. Ця імовірність є мінімально досяжною при застосуванні у перехопленні будь-яких ефективних засобів, а тому є описом потенційної можливості перехоплення.

Показано залежність зазначеної імовірності від енергетичного показника сигнал/завада на вході приймача.

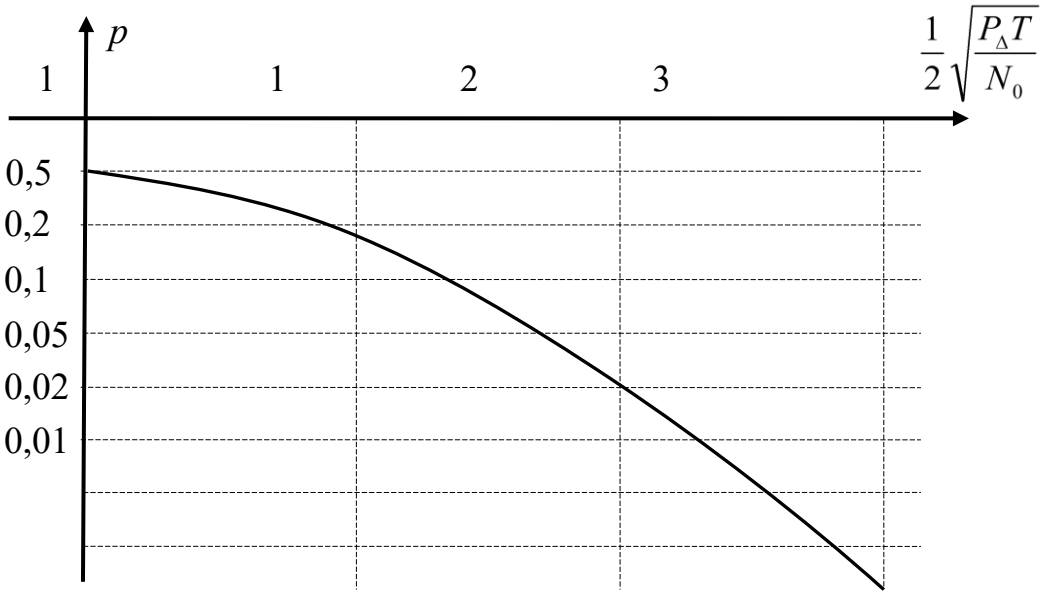


Рис. 3.2.3. Графік залежності імовірності помилки оптимального прийому двійкових сигналів від відношення сигнал/завада на вході приймача

Отже, на основі критерію максимуму відношення правдоподібності побудовано вирішальну схему оптимального приймача в дискретно-неперервному каналі для двійкових даних.

На основі критерію та отриманої вирішальної схеми обґрунтовано імовірність помилки в каналі витоку як показника захищеності інформації. Ця імовірність є мінімально досяжною при застосуванні у перехопленні будь-яких ефективних засобів, а тому є описом потенційної можливості перехоплення.

Показано залежність зазначеної імовірності від енергетичного показника сигнал/завада на вході приймача.

Контрольні питання:

1. Вирішальна схема оптимального приймача для двійкових повідомлень.
2. Умова помилковості прийому вирішальною схемою для двійкових повідомлень.
3. Імовірність помилкового прийому знака з алфавіту двійкових даних.
4. Використання гауссівського нормального закону розподілу імовірностей для оцінювання імовірності помилкового прийому двійкового знака. Оцінювання математичного сподівання та дисперсії.
5. Імовірність помилки в каналі витоку двійкових даних та її залежність від відношення сигнал/завада на вході приймача.

3.3. Вирішальна схема за критерієм максимуму апостеріорної імовірності. Імовірність помилки в каналі та її зв'язок з відношенням сигнал/завада на вході приймача

Особливості енергетичних умов на вході приймача, що забезпечують критерій максимуму апостеріорної імовірності, та вирішальна схема оптимального прийому. Нехай задано дискретне джерело, що виробляє знаки x_r, спосіб модуляції (представлення, реалізації) цих знаків в реалізації неперервних сигналів $s_r(t)$. Нехай задано канал як неперервний адитивний гауссівський канал, через який проходять зазначені реалізації знаків та спотворюються завадами (див. рис. 3.3.1). Опис вказаного каналу має вигляд:

$$u(t) = \mu s_r(t-\tau) + n(t) = c_r(t) + n(t), \qquad (3.3.1)$$

де μ – коефіцієнт послаблення сигналу в каналі, τ – час затримки сигналу в каналі, $c_r(t)$ – ослаблений сигнал на виході каналу з урахуванням затримки, $n(t)$ – адитивна завада в каналі, $r = 1 \div N$.

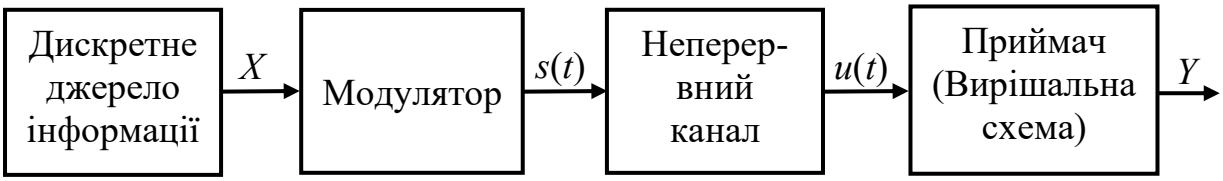


Рис. 3.3.1. Схема передачі дискретного повідомлення по неперервному каналу

На вхід приймача потрапляють суміші сигналів, що відповідають переданим знакам, та завад $u(t)$, які він повинен демодулювати – прийняти рішення про те, який знак передавався. При чому спосіб прийому повинен бути оптимальним – найкращим з точки зору вірності ухвалення рішення.

У попередніх лекціях при обґрунтуванні критерію оптимального прийому було використано припущення щодо рівноймовірності знаків на виході джерела. Тобто, якщо

$$p(x_1) = p(x_2) = p(x_3) = \ldots = p(x_r) = \ldots = p(x_N), \qquad (3.3.2)$$

то критерій максимуму апостеріорної імовірності може бути замінено критерієм максимуму відношення правдоподібності. При цьому прийняття рішення щодо виробленого джерелом знака x_l на прийомі зводився до перебору гіпотез та знаходження по всім r максимуму зазначеного відношення правдоподібності:

$$\lambda_{l/r}(u) = \frac{\omega(u/x_l)}{\omega(u/x_r)} > \frac{p(x_r)}{p(x_l)} = 1 \ . \qquad (3.3.3)$$

Це дозволило відносно нескладно знайти зв'язок $\lambda_{l/r}(u)$ з енергетичними умовами на вході приймача, побудувати вирішальну схему ідеального приймача та оцінити імовірність помилки, яка є найменшою щодо всіх інших можливостей прийому. Очевидно, що забезпечення зазначених енергетичних умов – відношення сигнал/завада в каналі витоку дозволить гарантувати імовірність помилки прийому та використовувати її як норму на гранично допустимий показник.

Однак, як відомо, на практиці умова (3.3.2) не завжди виконується, практично завжди мають місце випадки дисбалансу знаків, особливо на обмежених ділянках їх послідовностей. А це може призвести до похибки при оцінюванні гранично допустимих показників та заниження захищеності інформації від витоку.

Нехай джерело витоку інформації має довільний розподіл ймовірностей. Обґрунтуємо для зазначеного розподілу енергетичні умови оптимального прийому та, відповідно до них, побудуємо вирішальну схему оптимального приймача.

Нехай має місце критерій прийняття рішення у вигляді нерівності:

$$\lambda_{l/r}(u) = \frac{\lambda_{l/0}(u)}{\lambda_{r/0}(u)} > \frac{p(x_r)}{p(x_l)},$$

або

$$p(x_l)\lambda_{l/0}(u) > p(x_r)\lambda_{r/0}(u), \qquad (3.3.4)$$

де $\lambda_{r/0}(u)$ – відношення правдоподібності знака x_r відносно нульової реалізації.

Для обґрунтування енергетичного критерію щодо прийняття рішення оптимальним приймачем, що відповідатиме критерію максимуму відношення правдоподібності, виразимо відношення правдоподібності $\lambda_{r/0}(u)$ через енергетичні параметри сигналів.

В попередніх лекціях було зазначено, що

$$\lambda_{r/0}(u_{t1}, u_{t2}, ..., u_{tk}) = \frac{\omega_k(u/x_r)}{\omega_k(u/0)}, \qquad (3.3.5)$$

де $\omega_k(u/x_r)$ – k-вимірна умовна щільність неперервного процесу на виході каналу (див. рис.3.3.1), за умови, якщо дискретне джерело виробило знак x_r, $\omega_k(u/0)$ – та ж щільність за умови так названої "нульової" реалізації на вході каналу, тобто якщо дискретне джерело не виробило жодного знака з алфавіту N.

За припущення, що $c_r(t)$ є фінітною реалізацією в часі та за спектром, згідно з теоремою Котельникова кількість вимірів k можна замінити:

$$k = \frac{T}{\Delta t} = 2FT, \qquad (3.3.6)$$

де T – тривалість реалізації $c_r(t)$, Δt – інтервал часу зчитування миттєвих значень $u(t)$ за період T. За теоремою Котельникова $\Delta t = \frac{1}{2F}$, F – ширина спектру частот $c_r(t)$. На вході у вирішальну схему F може співпадати зі смугою пропускання частот приймача.

Згідно з (3.3.6) співвідношення для відношення правдоподібності (3.3.5) матиме вигляд:

$$\lambda_{r/0}(u_1, u_2, ..., u_{2FT}) = \frac{\omega(u_1, u_2, ..., u_{2FT}/x_r)}{\omega(u_1, u_2, ..., u_{2FT}/0)}, \qquad (3.3.7)$$

де u_1, u_2, u_{2FT} – значення сигналу $u(t)$ в $2FT$ відліках.

Слід зауважити, що за "нульової" реалізації на вході каналу, сигнал на його виході повністю визначається завадою:

$$u(t) = c_0(t) + n(t) = n(t). \tag{3.3.8}$$

В зв'язку з цим умовну щільність, що має місце у знаменнику співвідношення (3.3.7), можна виразити щільністю нормального розподілу ймовірностей, якою володіє "білий" шум в каналі. Згідно з властивістю статистичної незалежності відліків для "білого" шуму

$$\omega(u_1, u_2, ..., u_{2FT} / 0) = \prod_{i=1}^{2FT} \omega(u_i / 0) =$$

$$= \prod_{i=1}^{2FT} \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{u_i^2}{2\sigma^2}} = \frac{1}{(\sqrt{2\pi\sigma^2})^{2FT}} e^{-\frac{\sum_{i=1}^{2FT} u_i^2}{2\sigma^2}}, \tag{3.3.9}$$

де σ – середньоквадратичне відхилення випадкової величини u_i, яке для всіх $i = 1 \div 2FT$ однакове, $\omega(u_i/0)$ – щільність нормального розподілу ймовірностей:

$$\omega(u_i / 0) = \omega(n_i) = \frac{1}{\sqrt{2\pi\sigma_n^2}} e^{-\frac{n_i^2}{2\sigma^2}}.$$

Для сигналу $u(t)$ при передачі "ненульових" реалізацій в кожному відліку i:

$$u_i = c_{ri} + n_i. \tag{3.3.10}$$

Тому відповідну умовну щільність за аналогією з (3.3.11) можна виразити у вигляді:

$$\omega(u_1, u_2, ..., u_{2FT} / c_r) = \omega(u_1 - c_{r1}, u_2 - c_{r2}, ..., u_{2FT} - c_{r2FT} / 0) =$$

$$= \frac{1}{(\sqrt{2\pi\sigma^2})^{2FT}} e^{-\frac{\sum_{i=1}^{2FT} (u_i - c_{ri})^2}{2\sigma^2}} = \frac{1}{(\sqrt{2\pi\sigma^2})^{2FT}} \exp\left\{-\frac{1}{2\sigma^2} \sum_{i=1}^{2FT} (u_i - c_{ri})^2\right\}, \tag{3.3.11}$$

Розділивши співвідношення (3.3.11) на (3.3.9), отримаємо відношення правдоподібності (3.3.5):

$$\lambda_{r/0}(u_1, u_2, ..., u_{2FT}) = \exp\left\{\frac{1}{2\sigma^2} \sum_{i=1}^{2FT} u_i^2\right\} \exp\left\{-\frac{1}{2\sigma^2} \sum_{i=1}^{2FT} (u_i - c_{ri})^2\right\}. \tag{3.3.12}$$

Враховуючи, що білий шум є ергодичним процесом, квадрат середньоквадратичного відхилення завади можна замінити її потужністю:

$$\sigma^2 = P_з, \tag{3.3.13}$$

яка може бути вираженою через її спектральну щільність N_0:

$$P_з = N_0 F = \frac{N_0}{2\Delta t}. \tag{3.3.14}$$

Підставивши співвідношення (3.3.14) в (3.3.13) та, відповідно, в (3.3.12), отримаємо:

$$\lambda_{r/0}(u_1,u_2,...,u_{2FT}) = \exp\left\{\frac{1}{N_0}\sum_{i=1}^{2FT} u_i^2\Delta t\right\}\exp\left\{-\frac{1}{N_0}\sum_{i=1}^{2FT}(u_i - c_{ri})^2\Delta t\right\}. \tag{3.3.15}$$

Спрямування $F \to \infty$, що рівносильно з $\Delta t \to 0$, дозволить знайти точний вираз для відношення правдоподібності:

$$\lambda_{r/0}(u) = \lim_{\Delta t\to 0}\lambda_{r/0}(u_1,u_2,...,u_{2FT}) =$$

$$= \exp\left\{\frac{1}{N_0}\left[\int_0^T u^2(t)dt - \int_0^T (u(t)-c_r(t))^2 dt\right]\right\}. \tag{3.3.16}$$

Підставивши (3.3.16) в нерівність (3.3.4), отримаємо:

$$p(x_l)\exp\left\{\frac{1}{N_0}\left[\int_0^T u^2(t)dt - \int_0^T (u(t)-c_l(t))^2 dt\right]\right\} >$$

$$> p(x_r)\exp\left\{\frac{1}{N_0}\left[\int_0^T u^2(t)dt - \int_0^T (u(t)-c_r(t))^2 dt\right]\right\}$$

Прологарифмувавши праву і ліву частини нерівності натуральним логарифмом та замінивши операцію множення під логарифмом на додавання логарифмів, отримаємо:

$$\frac{1}{N_0}\int_0^T u^2(t)dt - \frac{1}{N_0}\int_0^T (u(t)-c_l(t))^2 dt + \ln p(x_l) >$$

$$> \frac{1}{N_0}\int_0^T u^2(t)dt - \frac{1}{N_0}\int_0^T (u(t)-c_r(t))^2 dt + \ln p(x_r). \tag{3.3.17}$$

Розкриття дужок під квадратами спростить нерівність (3.3.17) та приведе до вигляду:

$$\frac{2}{N_0}\int_0^T u(t)c_l(t)dt - \frac{P_l T}{N_0} + \ln p(x_l) > \frac{2}{N_0}\int_0^T u(t)c_r(t)dt - \frac{P_r T}{N_0} + \ln p(x_r),$$

або

$$Z_l(u) - \frac{P_l}{2} + \frac{N_0}{2T} \ln p(x_l) > Z_r(u) - \frac{P_r}{2} + \frac{N_0}{2T} \ln p(x_r), \qquad (3.3.18)$$

де $Z_r(u)$ – допоміжна величина (в попередніх матеріалах вже використовувалась):

$$Z_r(u) = \frac{1}{T} \int_0^T u(t) c_r(t) dt .$$

Співвідношення (3.3.18) дозволяє побудувати схему ідеального приймача перехоплення дискретної інформації (див. рис.3.3.2), яка відрізняється від раніше обґрунтованої схеми тим, що враховує розподіл апріорних ймовірностей джерела витоку інформації.

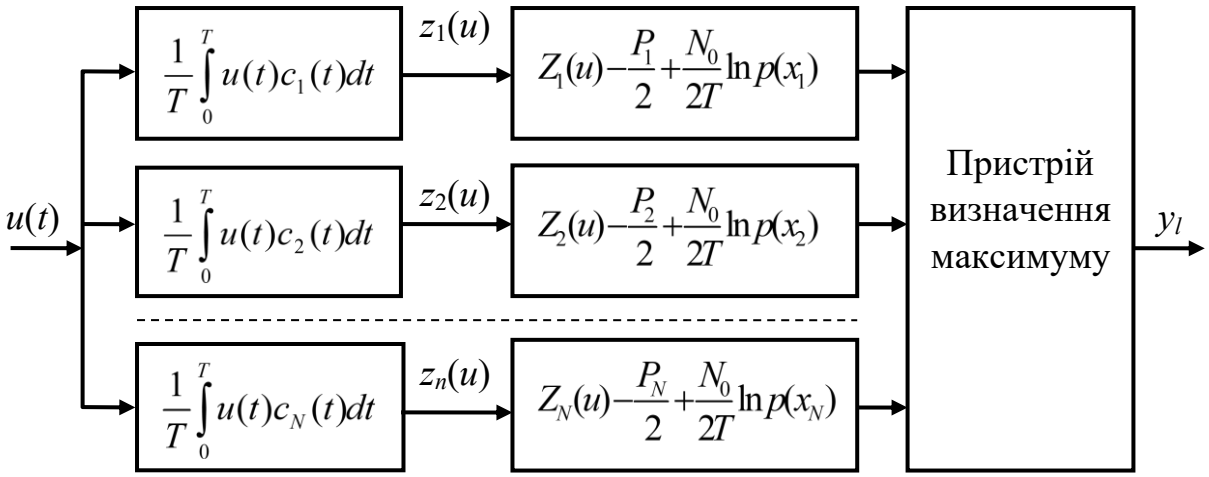


Рис.3.3.2. Вирішальна схема оптимального прийому перехоплення дискретної інформації

Отже, обґрунтовано особливості енергетичних умов на вході приймача, що забезпечують критерій максимуму апостеріорної імовірності. На основі цього критерію побудовано вирішальну схему оптимального приймача в дискретно-неперервному каналі. Зазначений прийом є найкращим прийомом із всіх можливих, а тому є описом потенційної можливості перехоплення та може бути взятим за основу при обґрунтуванні захищеності інформації від витоку технічними каналами для джерел з нерівномірним розподілом імовірностей.

Імовірність помилки оптимального прийому за критерієм максимуму апостеріорної імовірності. Вирішальна схема, що показана на рис. 2, є вирішальною схемою ідеального приймача перехоплення дискретної інформації, яка, спостерігаючи за джерелом через адитивний

канал з гауссівською завадою, з максимальною вірністю визначає, яким був вироблений джерелом знак.

Однак, ця схема не позбавлена й помилкових вирішень. Безперечно очевидно, що обчислюючи у формулі (3.3.18) ліву та праву сторони, вирішальна схема може знайти й протилежну нерівність:

$$\frac{2}{N_0}\int_0^T u(t)c_l(t)dt - \frac{P_l T}{N_0} + \ln p(x_l) < \frac{2}{N_0}\int_0^T u(t)c_r(t)dt - \frac{P_r T}{N_0} + \ln p(x_r)\,. \quad (3.3.19)$$

Як правило, сучасні технічні засоби і системи обробки та передачі інформації для подання інформації використовують двійковий код. При цьому може мати місце й укрупнення алфавіту, яке в основному здійснюється шляхом розширення вказаного коду так, що об'єм алфавіту практично завжди кратний $N = 2^n$, де n – довжина кодового слова.

Для простоти нехай $N = 2$. Знайдемо ймовірність помилкового рішення вирішальною схемою.

Нехай джерело витоку інформації є двійковим та виробляє знак x_1 з імовірністю $p(x_1)$, а x_2 з імовірністю $p(x_2)$ так, що:

$$p(x_1) + p(x_2) = 1.$$

Під імовірністю помилки розумітимемо ймовірність $p(y_1/x_2)$ того, що вирішальна схема приймає рішення y_1, якщо на вхід каналу потрапив знак x_2, та імовірність $p(y_2/x_1)$ того, що вирішальна схема приймає рішення y_2, якщо на вхід каналу потрапив знак x_1 (див рис.3.3.3). Умовні ж імовірності $p(y_1/x_1)$ та $p(y_2/x_2)$ характеризуватимуть імовірності вірного прийому.

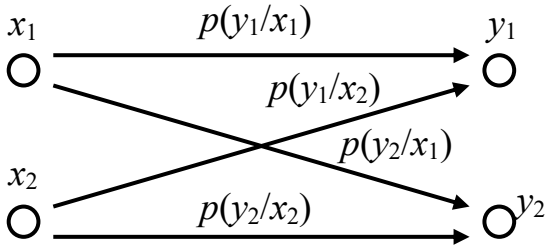


Рис.3.3.3. Граф станів та перехідних процесів в дискретному двійковому каналі

Зазначимо, що імовірності вірних рішень $p(y_1/x_1)$ та $p(y_2/x_2)$ і ймовірності помилкових рішень $p(y_1/x_2)$ та $p(y_2/x_1)$ є не обов'язково рівними. Тому оцінювання імовірності помилки в каналі можна здійснити шляхом усереднення $p(y_1/x_2)$ та $p(y_2/x_1)$, скориставшись знаходженням їх математичного сподівання:

$$p = p(x_1)p(y_2/x_1) + p(x_2)p(y_1/x_2)\,. \quad (3.3.20)$$

Почергово зафіксуємо на виході джерела x_1 і x_2 та знайдемо для них відповідні ймовірності помилкових рішень: $p(y_2/x_1)$ та $p(y_1/x_2)$.

Нехай на виході джерела виробляється знак x_1, тоді помилкове рішення прийматиметься у випадку виконання у співвідношенні (3.3.19) протилежної нерівності, тобто

$$\int_0^T [u(t)-c_1(t)]^2 dt - N_0 \ln p(x_1) > \int_0^T [u(t)-c_2(t)]^2 dt - N_0 \ln p(x_2), \quad (3.3.21)$$

де $u(t)$ – суміш сигналу та завади на вході приймача (виході каналу):

$$u(t)=c_1(t)+n(t). \quad (3.3.22)$$

Спростимо співвідношення (3.3.21). Для цього замінимо в ньому функцію $u(t)$ співвідношенням (3.3.22) та розкриємо квадрати різниць під інтегралами:

$$\int_0^T n^2(t)dt - N_0 \ln p(x_1) > \int_0^T [(c_1(t)-c_2(t))+n(t)]^2 dt - N_0 \ln p(x_2),$$

$$\int_0^T n^2(t)dt - N_0 \ln p(x_1) >$$

$$> \int_0^T (c_1(t)-c_2(t))^2 dt + 2\int_0^T (c_1(t)-c_2(t))n(t)dt + \int_0^T n^2(t)dt - N_0 \ln p(x_2). \quad (3.3.23)$$

Як очевидно, інтеграли квадратів шумових сигналів в плечах співвідношенні (3.3.23) взаємно знищуються.

Розділимо доданки нерівності на тривалість сигналу $2T$ та перенесемо в ліву частину випадкову складову, а в праву – все, що залишилося, зі зміною знака на протилежний. В результаті співвідношення (3.3.23) отримає вигляд:

$$\frac{1}{T}\int_0^T c_\Delta(t)n(t)dt < -\frac{1}{2T}\int_0^T c_\Delta^2(t)dt - \frac{N_0}{2T}\ln\frac{p(x_1)}{p(x_2)}, \quad (3.3.24)$$

де $c_\Delta(t)$ – різницевий сигнал:

$$c_\Delta(t) = c_1(t) - c_2(t).$$

Зауважимо, що у правій частині співвідношення (3.3.24)

$$\frac{1}{T}\int_0^T c_\Delta^2(t)dt = P_\Delta \quad (3.3.25)$$

є потужністю різницевого сигналу.

Таким чином, помилкове рішення вирішальною схемою приймається за знаходження нею наступної нерівності:

$$\frac{1}{T}\int_0^T c_\Delta(t)n(t)dt < -\frac{P_\Delta}{2} - \frac{N_0}{2T}\ln\frac{p(x_1)}{p(x_2)}. \qquad (3.3.26)$$

При цьому ймовірність помилки може бути виражена формулою:

$$p(y_2/x_1) = p\left\{\xi \le -\frac{P_\Delta}{2} - \frac{N_0}{2T}\ln\frac{p(x_1)}{p(x_2)}\right\}, \qquad (3.3.27)$$

де ξ – внесена заміна:

$$\xi = \frac{1}{T}\int_0^T c_\Delta(t)n(t)dt.$$

Нескладно помітити, що випадкова величина ξ має нормальний закон розподілу, оскільки отримана в результаті лінійної операції над гауссівським процесом.

Слід зазначити, що знаходження імовірності за співвідношенням (3.3.27) вже здійснювалось раніше, яке зводилося до знаходження інтегралу Лапласа. Для цього знайдемо математичне сподівання та дисперсію випадкової величини ξ.

Математичне сподівання випадкової величини ξ визначається за формулою:

$$\mathrm{M}[\xi] = \mathrm{M}\left[\frac{1}{T}\int_0^T n(t)c_\Delta(t)dt\right] = \frac{1}{T}\int_0^T \mathrm{M}[n(t)]c_\Delta(t)dt = 0. \qquad (3.3.28)$$

У співвідношенні (3.3.28) її рівність нулю обґрунтовується тим, що завада не має постійної складової, а отже і її математичне сподівання як ергодичного процесу дорівнює нулю.

Дисперсія випадкової величини ξ:

$$\mathrm{D}[\xi] = \mathrm{D}\left[\frac{1}{T}\int_0^T n(t)c_\Delta(t)dt\right] = \mathrm{M}\left[\left\{\frac{1}{T}\int_0^T n(t)c_\Delta(t)dt\right\}^2\right] =$$

$$= \frac{1}{T^2}\mathrm{M}\left[\int_0^T n(t)c_\Delta(t)dt\int_0^T n(t')c_\Delta(t')dt'\right] =$$

$$= \frac{1}{T^2}\int_0^T\int_0^T c_\Delta(t)c_\Delta(t')\mathrm{M}[n(t)n(t')]dtdt'. \qquad (3.3.29)$$

З теорії сигналів відомо, що для білого шуму:

$$\mathrm{M}\left[n(t)n(t')\right] = R(t-t') = N_0\delta(t-t'), \tag{3.3.30}$$

$$\int_a^b f(x)\delta(x-x_0)dx = f(x_0), \text{ для } a < x_0 < b. \tag{3.3.31}$$

З використанням (3.3.30) та (3.3.31) дисперсія (3.3.29) перетвориться та набуде остаточного вигляду:

$$\mathrm{D}[\xi] = \frac{N_0}{T^2}\int_0^T\int_0^T c_\Delta(t)c_\Delta(t')\delta(t-t')dtdt' =$$

$$= \frac{N_0}{T^2}\int_0^T c_\Delta^2(t)dt = \frac{N_0P_\Delta}{T}. \tag{3.3.32}$$

Таким чином щільність розподілу випадкової величини ξ:

$$\omega(\xi) = \frac{1}{\sqrt{2\pi\dfrac{N_0P_\Delta}{T}}}\exp\left\{-\frac{\xi^2}{2\dfrac{N_0P_\Delta}{T}}\right\}. \tag{3.3.33}$$

Отже, з використанням щільності (3.3.33) імовірність (3.3.27) може бути знайденою як визначений інтеграл, тобто площа, обмежена кривою щільності та межами величини ξ (див рис.3.3.4):

$$p(y_2/x_1) = p\left\{\xi < -\frac{P_\Delta}{2} - \frac{N_0}{2T}\ln\frac{p(x_1)}{p(x_2)}\right\} =$$

$$= \int_{-\infty}^{-\frac{P_\Delta}{2}-\frac{N_0}{2T}\ln\frac{p(x_1)}{p(x_2)}}\omega(\xi)d\xi = \int_{-\infty}^{-\frac{P_\Delta}{2}-\frac{N_0}{2T}\ln\frac{p(x_1)}{p(x_2)}}\frac{1}{\sqrt{2\pi\dfrac{N_0P_\Delta}{T}}}\exp\left\{-\frac{\xi^2}{2\dfrac{N_0P_\Delta}{T}}\right\}d\xi =$$

$$= \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{-\frac{1}{2}\sqrt{\frac{P_\Delta T}{N_0}}-\frac{1}{2}\sqrt{\frac{N_0}{P_\Delta T}}\ln\frac{p(x_1)}{p(x_2)}}\exp\left\{-\frac{\eta^2}{2}\right\}d\eta = F\left(-\frac{1}{2}\sqrt{\frac{P_\Delta T}{N_0}} - \frac{1}{2}\sqrt{\frac{N_0}{P_\Delta T}}\ln\frac{p(x_1)}{p(x_2)}\right), \tag{3.3.34}$$

де $F(t)$ – інтеграл Лапласа, що знаходиться з довідника:

$$F(x) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x}\exp\left\{-\frac{\eta^2}{2}\right\}d\eta$$

Аналогічним чином можна знайти ймовірність помилки $p(y_1/x_2)$ за умови, якщо на виході джерела, що має той самий розподіл ймовірностей, виробляється знак x_2. Для цього випадку співвідношення, що визначатиме помилкове рішення ідеального приймача, матиме вигляд:

$$\int_0^T [u(t)-c_2(t)]^2 dt - N_0 \ln p(x_2) > \int_0^T [u(t)-c_1(t)]^2 dt - N_0 \ln p(x_1), \quad (3.3.35)$$

де $u(t)$ – суміш сигналу та завади на вході приймача (виході каналу):

$$u(t)=c_1(t)+n(t).$$

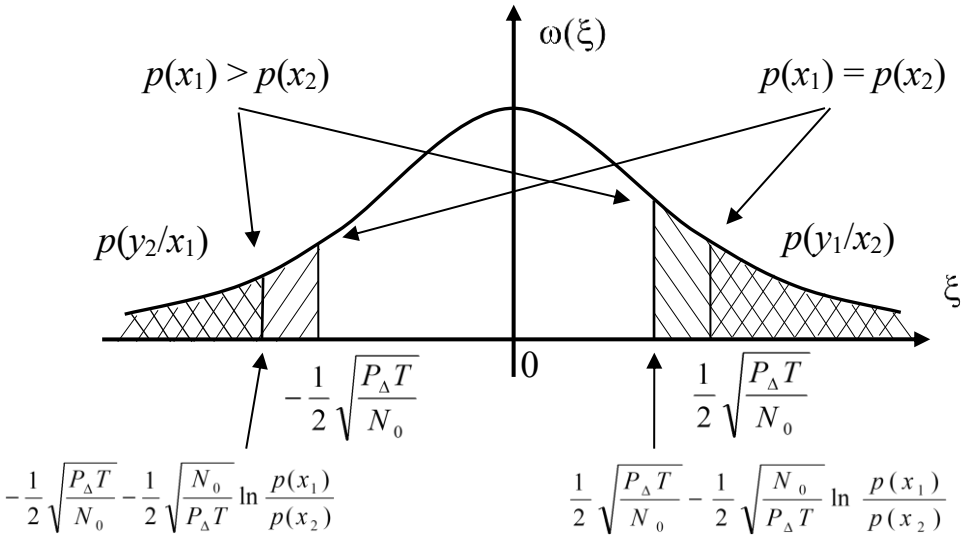


Рис.4. Щільність розподілу ймовірностей випадкової величини ξ

Виконавши ті ж міркування та дії, що і для x_1, отримаємо шукану ймовірність:

$$p(y_1/x_2) = p\left\{\xi \le -\frac{P_\Delta}{2} + \frac{N_0}{2T}\ln\frac{p(x_1)}{p(x_2)}\right\} = F\left(-\frac{1}{2}\sqrt{\frac{P_\Delta T}{N_0}} + \frac{1}{2}\sqrt{\frac{N_0}{P_\Delta T}}\ln\frac{p(x_1)}{p(x_2)}\right). \quad (3.3.36)$$

Результуюча ймовірність помилки з урахуванням (3.3.33), (3.3.36) та (3.3.20) матиме вигляд:

$$p = p(x_1)F\left(-\frac{1}{2}\sqrt{\frac{P_\Delta T}{N_0}} - \frac{1}{2}\sqrt{\frac{N_0}{P_\Delta T}}\ln\frac{p(x_1)}{p(x_2)}\right) +$$

$$+ p(x_2)F\left(-\frac{1}{2}\sqrt{\frac{P_\Delta T}{N_0}} + \frac{1}{2}\sqrt{\frac{N_0}{P_\Delta T}}\ln\frac{p(x_1)}{p(x_2)}\right). \quad (3.3.37)$$

Слід зауважити, що для випадку рівноймовірності знаків на виході джерел $p(x_1) = p(x_2)$ за співвідношенням (3.3.36) оцінка імовірності

помилки повністю співпадає з оцінкою за критерієм максимуму відношення правдоподібності:

$$p = F\left(-\frac{1}{2}\sqrt{\frac{P_{\Delta}T}{N_0}}\right). \qquad (3.3.38)$$

Як видно зі співвідношення (3.3.37), разом з нерівноймовірністю знаків на виході джерела, наприклад, $p(x_1) > p(x_2)$, з'являється, відповідно, протилежна нерівноймовірність помилок $p(y_2/x_1) < p(y_1/x_2)$ (див. рис. 3.3.4). Однак, з аналізу (3.3.37) складно сказати, як саме вплине наростання/спадання однієї імовірності та спадання/наростання іншої на імовірність помилки в каналі витоку інформації. Тому все це вимагає окремих досліджень та вирішень, які будуть здійснені далі.

Таким чином, на основі критерію максимуму відношення правдоподібності, обґрунтовано та отримано співвідношення щодо оцінювання імовірності помилки перехоплення інформації від дискретних джерел в каналі витоку з адитивною завадою. Дана ймовірність є мінімально досяжною при перехопленні противником інформації та враховує статистичні властивості джерел витоку. Вона визначається завадами в каналі витоку, не залежить від ефективності засобів та способів перехоплення, а отже є гарантованою.

Використання цього показника гарантовано забезпечуватиме достовірність захисту інформації, а його нормування – розрахунок гранично допустимих відношень сигнал/завада.

Отже, обґрунтовано особливості енергетичних умов на вході приймача, що забезпечують критерій максимуму апостеріорної імовірності та побудовано вирішальну схему оптимального приймача в дискретно-неперервному каналі. Зазначений прийом є найкращим прийомом з усіх можливих, а тому є описом потенційної можливості перехоплення та може бути взятим за основу при обґрунтуванні захищеності інформації від витоку технічними каналами для джерел з нерівномірним розподілом імовірностей.

На основі критерію максимуму відношення правдоподібності, обґрунтовано та отримано співвідношення щодо оцінювання імовірності помилки перехоплення інформації від дискретних джерел в каналі витоку з адитивною завадою. Дана ймовірність є мінімально досяжною при перехопленні противником інформації та враховує статистичні властивості джерел витоку. Вона визначається завадами в каналі витоку, не залежить від ефективності засобів та способів перехоплення, а отже є гарантованою.

Використання цього показника гарантовано забезпечуватиме достовірність захисту інформації, а його нормування – розрахунок гранично допустимих відношень сигнал/завада.

Контрольні питання:

1. Особливості енергетичних умов на вході приймача, що забезпечують критерій максимуму апостеріорної імовірності.
2. Вирішальна схема оптимального приймача за критерієм максимуму апостеріорної імовірності.
3. Умова помилковості прийому вирішальною схемою за критерієм максимуму апостеріорної імовірності для двійкових повідомлень.
4. Імовірність помилкового прийому вирішальною схемою за критерієм максимуму апостеріорної імовірності.
5. Імовірність помилки в каналі витоку двійкових даних та її залежність від відношення сигнал/завада на вході приймача.

3.4. Вирішальна схема оптимального прийому та імовірність неможливості щодо виявлення ознак інформаційного сигналу в технічному каналі витоку

Унеможливлення виявлення ознак інформаційного сигналу як спосіб захисту даних від витоку технічними каналами. В попередніх матеріалах було розглянуто вирішальні схеми оптимального прийому за критеріями максимумів апостеріорної імовірності та відношення правдоподібності, які в технічних каналах витоку були взятими в якості прототипів технічних засобів перехоплення як найкращих засобів прийому (див. рис. 3.4.1).

$$I(X;\ Y) = I(Y;\ X)$$

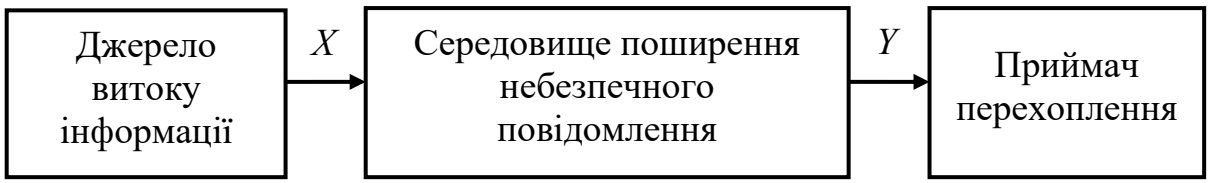


Рис. 3.4.1. Технічний канал витоку інформації у вигляді дискретного

Критерій максимуму апостеріорної імовірності був обраний в якості критерію оптимальності прийому саме тому, що він відображає якість передавання інформації по каналу. З теорії інформації відомо, що кількість інформації, що пройшла через канал, є тим більшою, чим більша апостеріорна імовірність щодо вірного прийому повідомлення. В цьому нескладно переконатися, проаналізувавши формулу для кількості взаємної інформації в дискретному каналі:

$$I(X;Y) = \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{2^n} \sum_{l=1}^{2^n} p(X_k^n, Y_l^n) \log \frac{p(X_k^n / Y_l^n)}{p(X_k^n)}, \qquad (3.4.1)$$

де $I(X;Y)$ – взаємна кількість інформації в каналі між його входом та виходом, $p(X^n_k)$ та $p(X^n_k/Y^n_l)$ – апріорна та апостеріорна імовірності джерела, $X^n_k = (x_1, x_2, x_3,\ldots, x_n)$ та $Y^n_l = (y_1, y_2, y_3,\ldots, y_n)$ – послідовності знаків $x = \{0, 1\}$ та $y = \{0, 1\}$, k та l – номери комбінацій X^n_k та Y^n_l, $k = 1, 2, 3,\ldots, 2^n$, $l = 1, 2, 3,\ldots, 2^n$, n – довжина комбінацій.

Так, з формули (3.4.1) видно, що в ідеальному випадку при $p(X^n_k/Y^n_l) = 1$ через канал проходить вся інформація, що вироблена джерелом, без втрат:

$$I(X;Y) = \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{2^n} p(X_k^n) \log \frac{1}{p(X_k^n)} \sum_{l=1}^{2^n} p(Y_l^n / X_k^n) = \qquad (3.4.2)$$

$$= \lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{2^n} p(X_k^n) \log \frac{1}{p(X_k^n)} = H(X),$$

де $H(X)$ – ентропія джерела.

Критерій оптимальності максимуму правдоподібності є окремим випадком критерію максимуму апостеріорної імовірності та випливає за умови рівноймовірності інформаційних знаків на виході джерела. При цьому, як було показано раніше, ентропія джерела $H(X)$ досягає свого максимуму, тобто джерело виробляє найбільшу кількість інформації в одному розряді послідовності.

Результативністю зазначеного підходу є приведення пропускної здатності технічного каналу витоку до певного мінімуму, який би не перевищував заданої величини, що визначена ризиком безпеки. При цьому допускалося, що певну кількість розрядів приймач перехоплення все-таки може прийняти безпомилково. Передбачалося, що вирішальна схема оптимального прийому приймає рішення щодо переданого знака з певного заданого алфавіту цих знаків об’ємом N і не більше того. Так, навіть в разі відсутності сигналу на вході приймача, тобто коли дані не передаються або повністю втрачаються в середовищі поширення, схема все одно має перебирати N гіпотез та здійснювати вибір однієї з них, що, вочевидь, не має сенсу.

Такий канал має N станів по входу та N станів по виходу. Він передбачає можливість помилки при прийомі інформаційних даних та не передбачає можливості повної втрати даних в каналі, що відповідає унеможливленню виявлення ознак небезпечного сигналу та повній захищеності інформації від витоку.

Розглянемо процес унеможливлення виявлення ознак небезпечного сигналу як спосіб захисту інформації від витоку технічними каналами. Цей

технічний канал витоку інформації на відміну від попереднього можна представити як такий, що має N станів по входу та $N + 1$ станів по виходу. При цьому, доданим є такий один стан, за якого приймач не в змозі виявити наявність сигналу на його вході.

Не складно показати, що пропускна здатність спрямовується в нуль не тільки за наявності помилок та завад в каналі, а й за відсутності самих даних чи сигналів, що несуть інформацію.

Так, при представленні технічного каналу витоку у вигляді дискретного каналу відсутність сигналу на його виході означає, що $Y^n_l = 0$, а тому апріорна та апостеріорна імовірності джерела будуть рівними $p(X^n_k/Y^n_l) = p(X^n_k/0) = p(X^n_k)$. Відповідно до зазначених умов за формулою (3.4.1) кількість взаємної інформації в каналі $I(X;Y) = 0$ та його пропускна здатність:

$$C = \max_{p(X_k^n),n,k} I(X;Y) = 0 \text{ [біт]}, \tag{3.4.3}$$

Технічний канал витоку інформації можна представити й у вигляді неперервного каналу, наприклад, адитивного гауссівського (див. рис. 3.4.2).

$$I(S;\ U) = I(U;\ S)$$

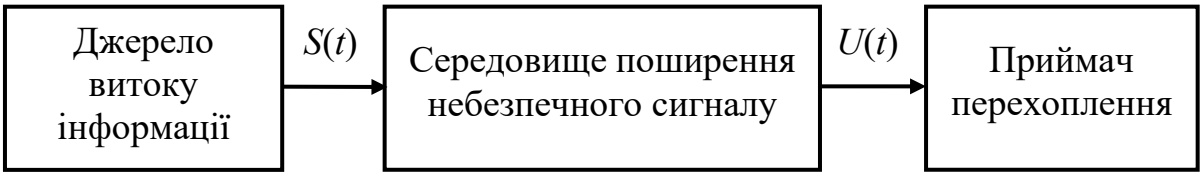


Рис. 3.4.2. Технічний канал витоку інформації у виді неперервного каналу

Відсутність ознак небезпечного сигналу на його виході означає, що неспотворений небезпечний сигнал $c(t) = \mu s(t) = 0$, де $s(t)$ – сигнал на вході каналу, μ – коефіцієнт послаблення сигналу в каналі. Потужність такого сигналу:

$$P_c = \frac{1}{T}\int_0^T c^2(t)dt = 0 \tag{3.4.4}$$

Відповідно пропускна здатність:

$$C = \frac{1}{2}\log_2(1+\frac{P_c}{P_з}) = 0 \text{ [біт]}. \tag{3.4.5}$$

де $P_з$ – потужність завади, що діє на сигнал в каналі.

Подаючи технічний канал витоку інформації у вигляді дискретно-неперервного каналу, знайдемо імовірність неможливості виявлення ознак

небезпечного сигналу, яка, як і пропускна здатність, може бути поставлена у відповідність до імовірності ризику інформаційної безпеки та використана як показник захищеності інформації від витоку (див. рис. 3.4.3). Для цього обґрунтуємо вирішальну схему оптимального прийому.

Таким чином, здійснено огляд підходу щодо унеможливлення виявлення ознак інформаційного сигналу як способу захисту даних від витоку технічними каналами. Для цього було використано дискретний та неперервний канали як описи технічних каналів витоку та необхідні обґрунтування умов відсутності каналів у разі відсутності ознак сигналів на вході приймача.

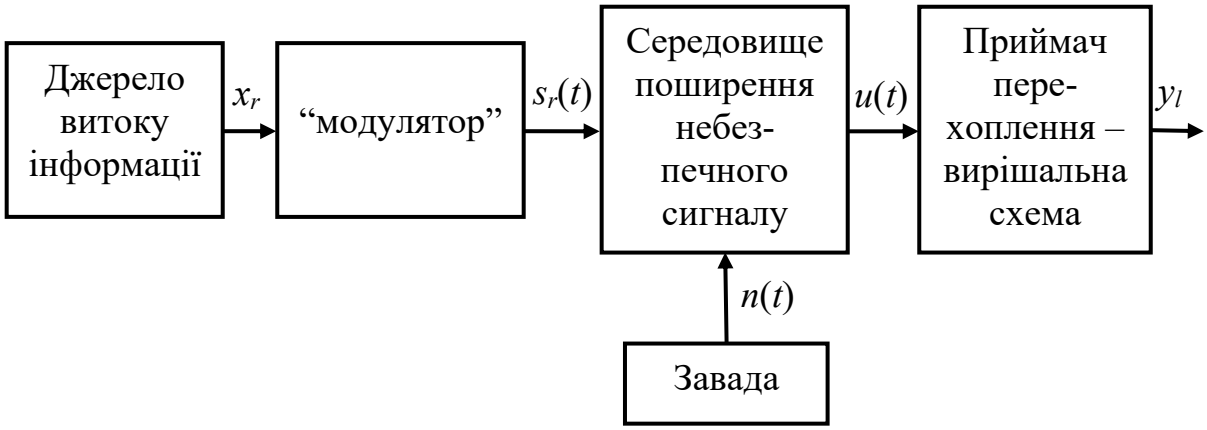


Рис.3.4.3. Технічний канал витоку інформації у вигляді дискретно-неперервного каналу

Для дискретно-неперервного каналу з оптимальним приймачем, що також може бути описом технічного каналу витоку, запропоновано окреме обґрунтування критерію оптимальності прийому та вирішальної схеми щодо виявлення ознак небезпечного сигналу, а також обґрунтування імовірності неможливості виявлення ознак як показника захищеності інформації від витоку технічними каналами.

Критерій оптимальності прийому та вирішальна схема щодо виявлення ознак небезпечного сигналу. Нехай задано дискретне джерело, що виробляє знаки x_r, спосіб модуляції (представлення) цих знаків у вигляді реалізацій неперервних сигналів $s_r(t)$. Нехай задано канал як неперервний адитивний гауссівський канал, через який проходять зазначені реалізації. В середовищі поширення на реалізації (інформаційний сигнал) спотворююче діють завади (див. рис.3.4.3). Опис процесів у вказаному каналі має вигляд:

$$u(t) = \mu s_r(t-\tau) + n(t) = c_r(t) + n(t), \qquad (3.4.6)$$

де μ – коефіцієнт послаблення сигналу в каналі, τ – час затримки сигналу в каналі, $c_r(t)$ – сигнал на виході каналу з урахуванням його ослаблення та затримки, $n(t)$ – адитивна завада в каналі, $r = 1 \div N$.

На вхід приймача (вирішальної схеми) потрапляє суміш $u(t)$ сигналів $c_r(t)$ та завад $n(t)$, яку він повинен демодулювати. При цьому на відміну від завдання, що ставилося раніше щодо прийняття рішення про те, який знак передавався, до вирішальної схеми тепер ставиться інакше завдання демодуляції: приймач (вирішальна схема) повинен приймати рішення щодо того, чи мають місце ознаки небезпечного сигналу на його вході, чи ні.

Для цього введемо $N + 1$ гіпотезу, яку додатково має розглядати вирішальна схема та яка відповідатиме так званій "нульовій" реалізації $s_0(t)$. Це гіпотеза, за якої вирішальна схема приймає рішення про те, що жоден з інформаційних знаків джерелом не вироблявся. Відповідно, позначимо відсутність інформаційних знаків на виході джерела через x_0. Це позначення є формальним, оскільки насправді такого знака не існує, але має бути введеним з точки зору математичної коректності.

Закон відповідності дискретних знаків та неперервних реалізацій, що здійснює "модулятор" на рис. 3.4.3, має вигляд:

$$\begin{gathered} x_0 \leftrightarrow s_0(t), \\ x_1 \leftrightarrow s_1(t), \\ x_2 \leftrightarrow s_2(t), \\ \ldots\ldots\ldots\ldots \\ x_r \leftrightarrow s_r(t), \\ \ldots\ldots\ldots\ldots \\ x_N \leftrightarrow s_N(t). \end{gathered} \qquad (3.4.7)$$

Згідно з правилом вироблення модулятором реалізацій, знаючи $u(t)$, на прийомі можна висунути та зробити перевірку $N + 1$ гіпотез:

1) передавався сигнал $s_0(t)$ та до нього додалася реалізація завади $n(t) = u(t) - \mu s_0(t - \tau)$,

2) передавався сигнал $s_1(t)$ та до нього додалася реалізація завади $n(t) = u(t) - \mu s_1(t - \tau)$,

3) передавався сигнал $s_2(t)$ та до нього додалася реалізація завади $n(t) = u(t) - \mu s_2(t - \tau)$,

……

N+1) передавався сигнал $s_N(t)$ та до нього додалася реалізація завади $n(t) = u(t) - \mu s_N(t - \tau)$.

Нехай критерієм оптимальності прийому є максимум апостеріорної імовірності:

$$p(x_l / u) = \max_{r = 0 \div N} p(x_r / u) . \qquad (3.4.8)$$

Пошук максимуму (3.4.8) зводиться до попарного порівняння:

$$p(x_l / u) > p(x_r / u) , \qquad (3.4.9)$$

де l – є індексом вірного вирішення схемою оптимального прийому, $l = 0 \div N$.

У попередніх матеріалах було показано, що порівняння апостеріорних імовірностей зводиться до порівняння відношень правдоподібності:

$$p(x_l)\lambda_{l/0}(u) > p(x_r)\lambda_{r/0}(u) , \qquad (3.4.10)$$

де $\lambda_{r/0}(u)$ – відношення правдоподібності знака x_r відносно нульової реалізації.

За умови ергодичності процесів в каналі нерівність (3.4.10) може бути перевіреною з використанням енергетичних показників за допомогою нерівності:

$$Z_l(u) - \frac{P_l}{2} + \frac{N_0}{2T} \ln p(x_l) > Z_r(u) - \frac{P_r}{2} + \frac{N_0}{2T} \ln p(x_r) , \qquad (3.4.11)$$

де P_r – потужність реалізації $c_r(t)$ тривалістю T:

$$P_r = \frac{1}{T} \int_0^T c_r^2(t) dt ,$$

$Z_r(u)$ – допоміжна величина (в попередніх матеріалах вже використовувалась):

$$Z_r(u) = \frac{1}{T} \int_0^T u(t) c_r(t) dt ,$$

N_0 – спектральна щільність білого шуму, $p(x_r)$ – імовірність знака x_r алфавіту об’ємом N.

При цьому вирішальна схема отримає вигляд, як показано на рис. 3.4.4.

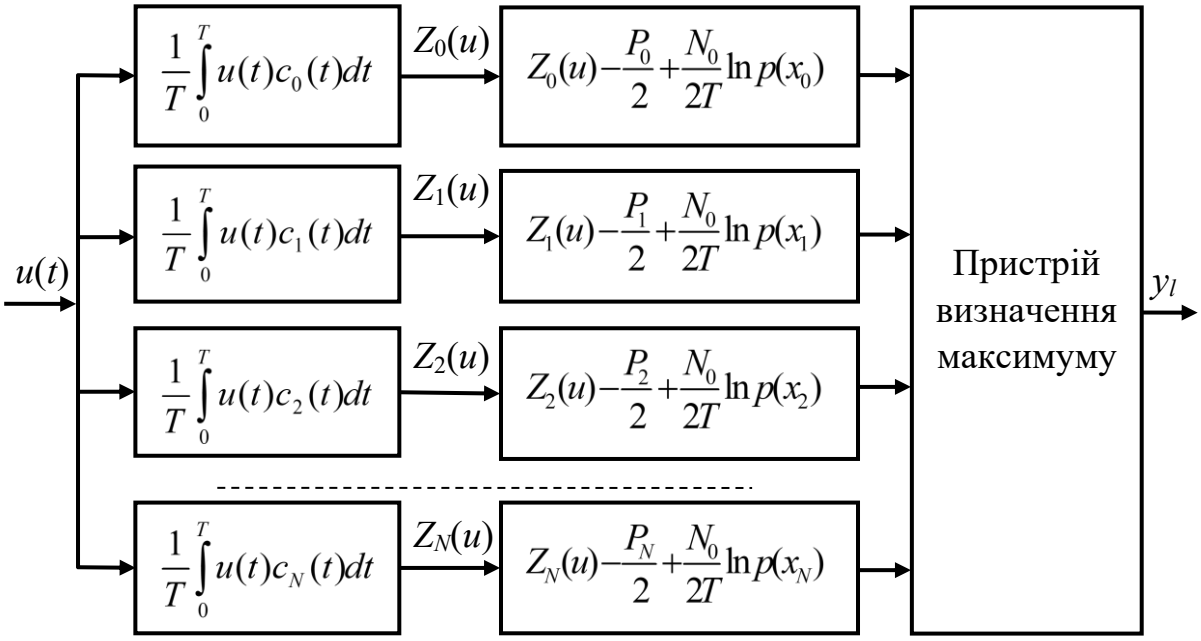


Рис. 3.4.4. Вирішальна схема оптимального прийому дискретної інформації щодо отримання смислового змісту та виявлення ознак небезпечного сигналу

Однак, як вже зазначалося вище, завдання щодо такого формату вирішальної схеми не ставиться. Вирішальна схема повинна відповідати на запитання, чи є ознаки сигналу на вході приймача, чи ні. Крім того завдання щодо перебору N гіпотез (без "нульової" реалізації) та ухвалення рішення щодо того, який знак передавався, вже має вирішення в попередніх матеріалах.

З урахуванням зазначеного вирішальну схему можна перетворити на дещо іншу (див. рис. 3.4.5). Гіпотези з 1 до N можна представити однією гіпотезою, що демаскуватиме факт наявності зазначених ознак на вході приймача. Для цього можуть бути допустимими дві стратегії, а саме:

1. Виявлення демаскуючих ознак небезпечного сигналу, що підтверджує факт обробки та передачі інформації шляхом перевірки однієї з N гіпотез *за максимумом демаскування* (наприклад, за потужністю, або за параметром амплітуди) однієї з реалізацій інформаційних знаків. Максимум демаскування є найгіршим випадком з точки зору захищеності об'єкта від виявлення. В подальшому реалізація інформаційного сигналу (знака) за максимумом демаскування може бути використана як тестовий сигнал для дослідження технічних каналів витоку інформації.

2. Виявлення ознак небезпечного сигналу *за демаскуванням в середньому*, що підтверджує факт обробки та передачі інформації шляхом

перевірки всіх N+1 гіпотез щодо реалізацій інформаційних знаків та прийняття рішення за підтвердженням хоча б однієї.

Очевидно, що перша стратегія є практичнішою, оскільки вона надає розвиток попереднім вже розглянутим вирішальним схемам оптимального прийому та працює з ними в комплексі. Вона додає до N гіпотез, що відповідають алфавіту інформаційних знаків, одну "нульову" гіпотезу, за якої джерело не виробляє жодного з сигналів. При цьому на рис. 3.4.5 пристрій визначення максимуму №1 обирає одну з усіх N найбільш демаскуючу реалізацію та ретранслює її до пристрою визначення максимуму №2.

Друга ж стратегія щодо побудови вирішальної схеми є простішою щодо реалізації, може працювати без розглянутих раніше вирішальних схем оптимального прийому щодо отримання інформаційних даних. Як недолік, вона ж вимагає знання статистики реалізацій в середньому, що не завжди є постійною величиною та вимагає періодичного контролю.

Побудуємо вирішальну схему оптимального прийому за першою стратегією, а саме – за виявленням ознак небезпечного сигналу за максимумом демаскування.

Рис. 3.4.5. Вирішальна схема оптимального прийому дискретної інформації з метою виявлення ознак небезпечного сигналу та з виділенням схеми щодо отримання інформаційних даних

Нехай з усіх $r = 1 \div N$ реалізація $c_r(t)$, позначимо її як $c_q(t)$, володіє найбільшими дамаскуючими ознаками та забезпечує максимум із всіх N гіпотез (див. рис. 3.4.5). Якщо відхилити завдання щодо отримання інформаційних даних, то схему каналу на рис. 3.4.5 можна зобразити в суттєво спрощеному вигляді, яка зводитиметься до порівняння двох гіпотез: q-ї, як найбільш демаскуючої, та 0-ї, за якої відсутні знаки на виході джерела (див. рис. 3.4.6).

Отримана вирішальна схема є зручною для знаходження імовірності неможливості виявлення ознак небезпечного сигналу як показника захищеності інформації від витоку технічними каналами.

Таким чином, обґрунтовано критерій оптимальності прийому та отримано вирішальну схему щодо виявлення ознак небезпечного сигналу. Вирішальна схема може надати можливість оцінювання імовірності неможливості виявлення ознак небезпечного сигналу в каналі витоку інформації.

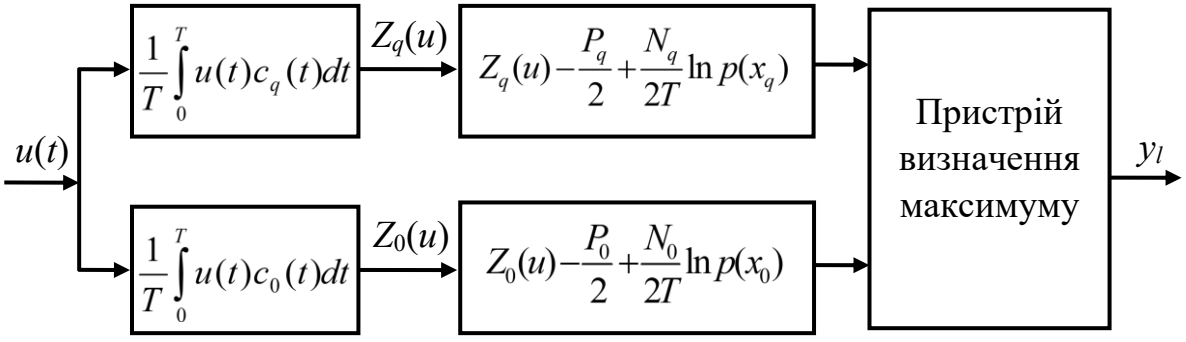


Рис. 3.4.6. Вирішальна схема оптимального прийому щодо виявлення ознак небезпечного сигналу за максимумом демаскування реалізацій інформаційних знаків

Імовірність щодо неможливості виявлення ознак небезпечного сигналу в каналі витоку інформації. Нехай вирішальна схема, що зображена на рис. 3.4.6, є вирішальною схемою оптимального прийому перехоплення дискретної інформації, яка, спостерігаючи за джерелом через адитивний канал з гауссівською завадою, з максимальною вірністю визначає, чи є в каналі ознаки небезпечного сигналу, чи ні.

Слід зауважити, що виявлення цих ознак має здійснюватися під час роботи джерела інформації. Тому імовірністю неможливості виявлення цих ознак є ніщо інше, як імовірність помилкового рішення на прийомі про те, що джерело не виробляє інформації в той час, коли воно дійсно виробляє.

Незалежно від того, з якого об’єму алфавіту джерело виробляє інформаційні дані, відповідно до стратегії виявлення ознак небезпечного

сигналу за максимумом демаскування, граф станів та перехідних процесів в дискретному каналі з точки зору приймача матиме вигляд, як показано на рис. 3.4.7.

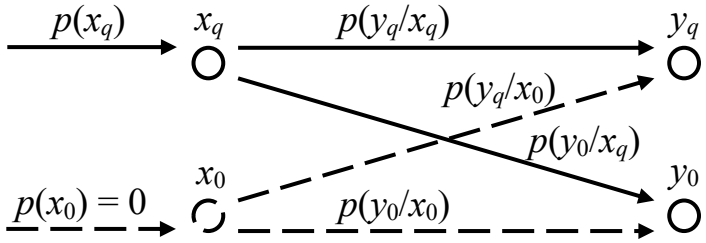


Рис. 3.4.7. Граф станів та перехідних процесів в дискретному каналі

Нехай на рис. 3.4.7 стан входу каналу x_q є довільним, але фіксованим, обирається вирішальною схемою окремо з усіх N станів щодо прийому даних за демаскуванням ознак сигналу $s_q(t)$, $x_q \in \max\{x_1 \vee x_2 \vee x_3 \vee \ldots \vee x_{N-1} \vee x_N\}$, $q = 1 \div N$.

Стан входу x_0 – це стан, за якого технічний засіб або система не працюють. Тобто джерело інформації не виробляє та, відповідно, інформаційний сигнал на вхід каналу не потрапляє. Відсутність сигналу формально позначили "нульовою" реалізацією $s_0(t)$ або $c_0(t)$, де $s_0(t) = 0$ та $c_0(t) = 0$.

На рис. 3.4.7 стан входу каналу x_0 та стрілки від нього показані пунктиром, оскільки реально цей стан виключається із процесу при виявленні ознак небезпечного сигналу в технічних каналах витоку інформації. Тому апріорні імовірності $p(x_0) = 0$ та $p(x_q) = p(x_1 \vee x_2 \vee x_3 \vee \ldots \vee x_N) = 1$, а зображення переходів від x_0 є необхідними з точки зору математичної коректності.

Станами виходу каналу є: $y_l = y_q$ – рішення вирішальної схеми про те, що мають місце в каналі ознаки небезпечного сигналу; $y_l = y_0$ – рішення вирішальної схеми про те, що відсутні в каналі ознак небезпечного сигналу.

Слід зазначити, що реалізація $s_q(t)$ може бути обрана будь-якою із об'єму алфавіту N. А тому це дозволяє застосувати всі міркування щодо знаходження імовірності неможливості виявлення q-ї реалізації і для стратегії №1 – виявлення ознак небезпечного сигналу за демаскуванням в середньому. При цьому шукана імовірність може бути знайденою без врахування схожості імовірнісного процесу інформаційних даних з шумовими процесами як засобами маскування.

Наявність на виході джерела витоку реалізації $s_q(t)$ є узагальненням факту роботи технічного засобу або системи обробки та передачі інформації, яке є найгіршим випадком з точки зору неможливості виявлення ознак інформаційного сигналу.

З усього зазначеного очевидно, що імовірністю неможливості виявлення ознак інформаційного сигналу в каналі вирішальною схемою, яка є найкращою щодо виявлення цих ознак, є імовірність $p_{\text{н.в.о.с.}} = p(y_0/x_q)$. За аналогією до вирішальних схем оптимального прийому, що були вже розглянутими раніше, та відповідно до вирішальної схеми на рис. 3.4.6, ця імовірність може бути знайденою як імовірність того, що виконується нерівність:

$$p_{\text{н.в.о.с.}} = p(y_0 / x_q) = p\left\{\frac{1}{T}\int_0^T u(t)c_q(t)dt - \frac{P_q}{2} + \frac{N_q}{2T}\ln p(x_q) < \right.$$

$$\left. < \frac{1}{T}\int_0^T u(t)c_0(t)dt - \frac{P_0}{2} + \frac{N_0}{2T}\ln p(x_0)\right\}. \qquad (3.4.12)$$

де $u(t)$ – сигнал на виході каналу, для співвідношення (3.4.12) дорівнює:

$$u(t) = c_q(t) + n(t).$$

Не складно побачити, що за умови $p(x_0) = 0$ та $p(x_q) = 1$ співвідношення (3.4.12) набуде такого вигляду та дорівнюватиме нулю, оскільки нічого не може бути меншим за від'ємну нескінченність:

$$p_{\text{н.в.о.с.}} = p(y_0 / x_q) = p\left\{\frac{1}{T}\int_0^T u(t)c_q(t)dt - \frac{P_q}{2} < -\infty\right\} = 0. \qquad (3.4.13)$$

І дійсно це буде так. Зазначене зручно показати за допомогою рис. 3.4.8 на прикладі роботи вирішальної схеми оптимального приймача двійкових знаків.

Якщо сигнал на вході приймача $u > c_0$, то приймач приймає рішення y_1, тобто вважає, що джерело виробило знак x_1; якщо $u < c_0$, то приймач приймає рішення y_2, тобто вважає, що джерело виробило знак x_2. Відповідно, імовірності вірних $p(y_1/x_1)$ і $p(y_2/x_2)$ та помилкових $p(y_1/x_2)$ і $p(y_2/x_1)$ вирішень на рис. 3.4.8 являють собою площі під відповідними кривими. З графіків видно, що чим меншою буде різниця між ослабленими сигналами c_1 та c_2 або чим більшою буде потужність завади (виражається через розмах графіків), тим більшими будуть площі під кривими та імовірності помилкових вирішень.

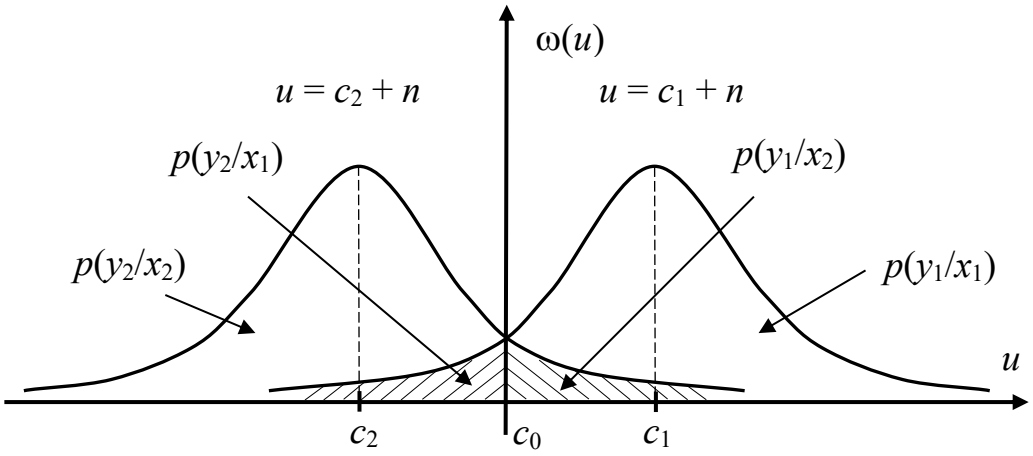


Рис. 3.4.8. Щільності розподілу ймовірностей випадкової величини *u* на вході приймача щодо двійкових гіпотез вирішень

Однак, відсутність сигналів на вході приймача виражається однією точкою $u = c_0$, а тому її імовірність $p(y_0/x_1 \vee x_2) = 0$.

Отримане співвідношення (3.4.13) є оцінюванням імовірності щодо неможливості виявлення ознак сигналу в загальному випадку для одного довільного, але фіксованого інформаційного– знака. При застосуванні стратегії №1 *за максимумом демаскування* оцінювання цієї імовірності буде відрізнятися (3.4.13) тим, що в якості інформаційного знака вибиратиметься той, у якого реалізація володіє найбільшими демаскувальними властивостями. При застосуванні стратегії №2 *за демаскуванням в середньому* оцінювання імовірності здійснюватиметься як математичне сподівання по всіх інформаційних знаках, а тому якщо імовірність щодо неможливості виявлення ознак сигналу по кожній реалізації дорівнює нулю, та і по всіх реалізаціях у середньому також буде дорівнювати нулю.

Отже, на основі використання вирішальної схеми оптимального прийому здійснено оцінювання імовірності щодо неможливості виявлення ознак небезпечного сигналу в каналі витоку інформації. Оцінювання здійснювалося за умови постійної наявності сигналу на виході джерела в каналі. На практиці це – умова постійної роботи об’єктів інформаційної діяльності, зокрема й технічних засобів обробки та передачі інформації тощо, як потенційних джерел витоку інформації.

В результаті оцінювання стало очевидним, що приховування ознак небезпечного сигналу в технічних каналах витоку інформації є складним, а то й зовсім неможливим.

Таким чином, здійснено обґрунтування вирішальної схеми оптимального прийому та імовірності неможливості щодо виявлення ознак

інформаційного сигналу в технічному каналі витоку. Для цього було проведено огляд підходу щодо унеможливлення виявлення цих ознак як способу захисту інформації від витоку технічними каналами та обґрунтовано відповідний критерій оптимальності.

Здійснено оцінювання імовірності щодо неможливості виявлення ознак небезпечного сигналу в каналі витоку інформації. Воно здійснювалося відносно однієї довільно взятої, але фіксованої реалізації, за умови постійної наявності сигналу на виході джерела. На практиці це є умовою постійної роботи об’єкта інформаційної діяльності, технічних засобів обробки та передачі інформації тощо, які можуть бути потенційним джерелом витоку інформації.

В результаті оцінювання стало очевидним, що приховування ознак небезпечного сигналу в технічних каналах витоку інформації є складним, а то й зовсім неможливим.

Контрольні питання:

1. Унеможливлення виявлення ознак інформаційного сигналу як спосіб захисту даних від витоку технічними каналами на основі дискретного каналу.
2. Унеможливлення виявлення ознак інформаційного сигналу як спосіб захисту даних від витоку технічними каналами на основі неперервного каналу.
3. Критерій оптимальності прийому щодо виявлення ознак небезпечного сигналу.
4. Вирішальна схема щодо виявлення ознак небезпечного сигналу.
5. Імовірність неможливості виявлення ознак небезпечного сигналу в каналі витоку інформації.

3.5. Імовірність щодо неможливості впевненого виявлення ознак інформаційного сигналу для приймача, що має поріг чутливості

Імовірність щодо неможливості впевненого виявлення ознак інформаційного сигналу для приймача, що має поріг чутливості. Як було показано раніше, імовірність щодо неможливості виявлення ознак небезпечного сигналу в каналі витоку інформації для абсолютно чутливих приймачів під час роботи об’єкта інформаційної діяльності завжди дорівнює нулю. Це свідчить про те, що відносно цих приймачів не є можливим приховати ознаки сигналу та, відповідно, факт обробки об’єктом інформації.

Однак, на практиці всі приймачі мають поріг чутливості. Цей поріг для високочутливої техніки може бути як завгодно малим, але все таки відмінним від нуля. Тому має сенс розглянути зазначений підхід щодо убезпечення інформації від витоку технічними каналами для приймачів, що має поріг чутливості та, відповідно, зайти імовірність, що характеризуватиме ступінь неможливості виявлення ознак інформаційного сигналу.

Так, нехай має місце схема каналу, як показано раніше на рис. 3.5.3. На вході приймача формується суміш сигналу та завади (3.5.6), за якою вирішальна схема (див рис. 3.5.5) приймає рішення щодо того чи передавався хоча б один із знаків, чи ні. В такому разі граф станів перехідних процесів матиме вигляд, як показано на рис. 3.5.1.

Нехай на виході каналу побудовано оптимальний приймач, що на рис. 3.5.5 має деякий "ненульовий" поріг чутливості, який на основі обробки прийнятого $u(t)$ оцінює наявність ознак небезпечного сигналу $c_0(t)$, $c_1(t)$, $c_2(t)$,…, $c_r(t)$,…, $c_N(t)$.

Це відповідає стратегії №2 за демаскуванням ознак інформаційного сигналу в середньому.

За стратегією ж №1, що відповідає максимуму демаскування ознак інформаційного сигналу, схема вирішальної схеми набуде вигляду, як показано на рис. 3.5.6, а граф станів перехідних процесів – як на рис. 3.5.7. При цьому гіпотеза x_q визначається не по факту вироблення джерелом даних x_1, x_2, x_3,…, x_{N-1}, x_N в середньому, а як максимум по всіх даних $x_q \in \max\{x_1 \vee x_2 \vee x_3 \vee \ldots \vee x_{N-1} \vee x_N\}$, $q = 1 \div N$.

При цьому імовірність щодо неможливості виявлення ознак інформаційного сигналу за стратегією №1 буде визначатися безпосередньо як імовірність неможливості виявлення ознак $c_q(t)$, а за стратегією №2 – як математичне сподівання по всіх реалізаціях $c_1(t)$, $c_2(t)$, $c_3(t)$, …, $c_N(t)$. Імовірність же щодо неможливості виявлення ознак реалізацій $c_1(t)$, $c_2(t)$, $c_3(t)$, …, $c_N(t)$ та $c_q(t)$ окремо визначатиметься однаково, незалежно від стратегії оцінювання.

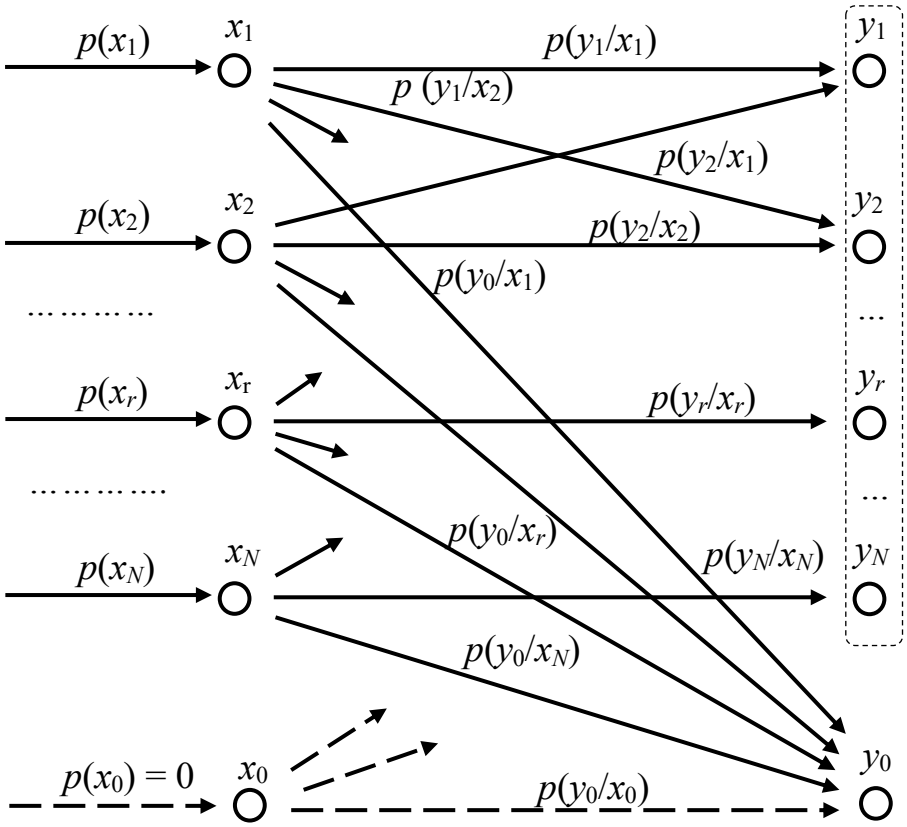


Рис. 3.4.1. Граф станів та перехідних процесів в дискретному каналі з можливістю виявлення/невиявлення ознак інформаційного сигналу

Слід зазначити, що всі реальні приймачі мають який завгодно малий, але певний “ненульовий” поріг чутливості, що визначається його власними шумами. Поріг чутливості – це той проміжок значень сигналів навколо “нуля”, в межах якого приймач “не бачить” ненульових реалізацій. Це проміжок, в якому приймач не має можливості впевненого виявлення ознак небезпечного сигналу і здійснює судження, що швидше за все сигнал відсутній. В такому разі “нульова” реалізація вже не дорівнюватиме нулю, а перебуватиме у проміжку значень (див. рис. 3.5.2):

$$c_0(t) \in [-c_{\text{пор.}}; +c_{\text{пор.}}]. \qquad (3.5.1)$$

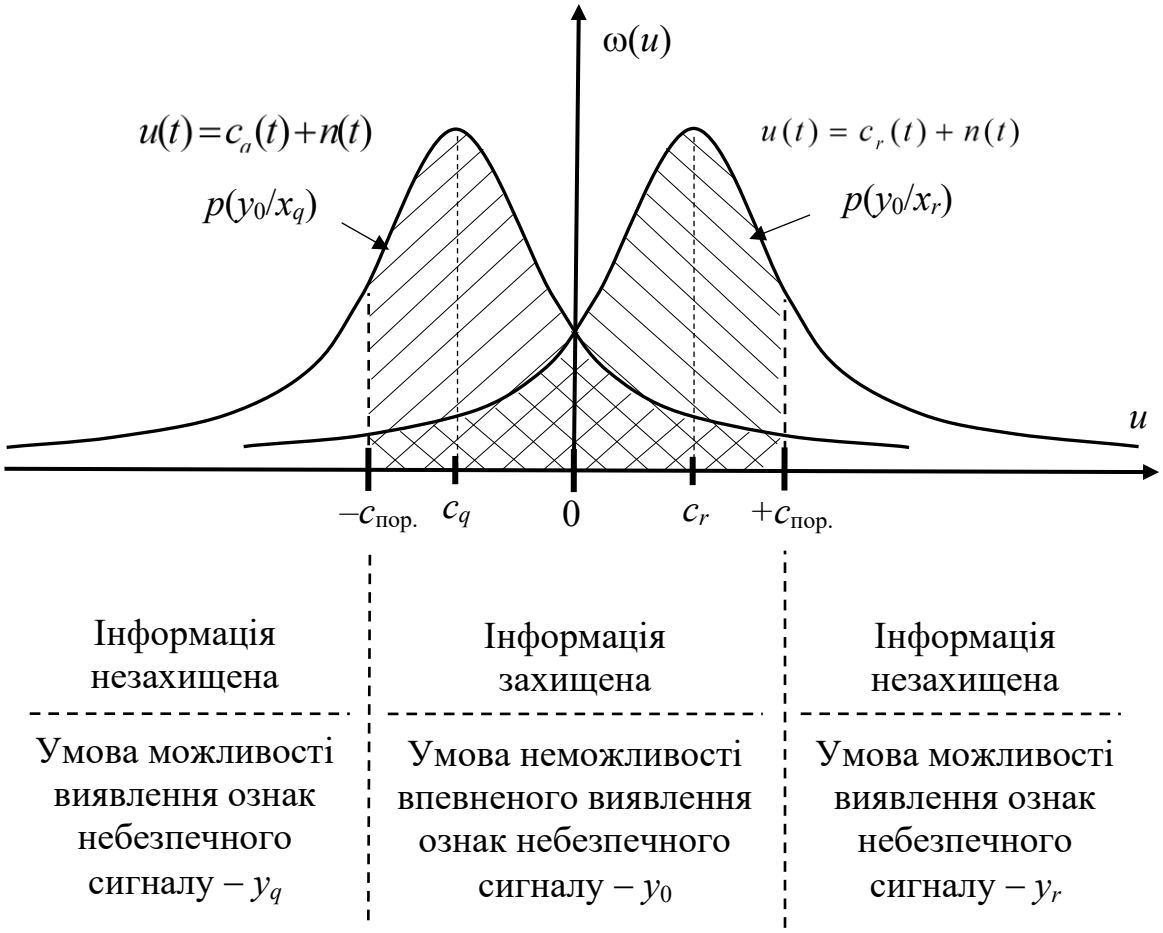


Рис. 3.4.2. Шкала стану приймача з “ненульовим” порогом чутливості щодо умов можливості/неможливості виявлення ознак інформаційного сигналу в каналі з адитивною гауссівською завадою

Судячи з графу станів на рис. 3.5.1 та того, що $p(x_0) = 0$, імовірність неможливості *впевненого* виявлення ознак небезпечного сигналу в каналі витоку інформації може бути знайденою через математичне сподівання (див. рис. 3.5.1):

$$p_{\text{н.в.в.о.с.}} = p(y_0) = \sum_{r=1}^{N} p(x_r) p(y_0 / x_r) . \qquad (3.5.2)$$

Слід згадати, що в попередніх матеріалах оцінювання помилкових вирішень схемою оптимального приймача здійснювалося з використанням *k*-мірних щільностей розподілу випадкової неперервної величини та відношень правдоподібності. Це було здійснено виходячи з того, що, по-перше, це один із відомих способів, який дозволяє статистично подати випадкові процеси, що протікають в часі, за допомогою відліків з подальшим спрямуванням інтервалів між ними в нуль. По-друге, в реальності прийняття неперервних сигналів сучасними засобами прийому

здійснюється саме у вигляді миттєвих значень сигналу з дискретним часом з подальшою їх обробкою.

Аналогічним чином імовірність $p(y_0/x_r)$ може бути знайденою як добуток k площ під кривими щільностей розподілу ймовірностей випадкових величин u_i, $i = 1, 2, 3, \ldots, k$,що описують суміш сигналу c_{ri} та шумового процесу n_i в середовищі поширення цього ж сигналу, в кожному з k відліків (див. рис. 3.5.2). Це є допустимим, оскільки випадковою складовою є білий шум, для якого будь-які два відліки є статистично незалежними.

У попередніх матеріалах також було показано, що за теоремою Котельникова кількість відліків k доцільно брати не більше ніж $2FT$, де F – смуга пропускання приймача, в якому повністю зосереджений спектр сигналу $c_r(t)$, T – період (тривалість розряду) сигналу $c_r(t)$.

Слід зазначити, що k може бути будь-яким та визначається засобами прийому. Однак, це не впливатиме на зменшення захищеності інформації. Так, якщо k буде малим ($k < 2FT$), то прийом сигналів буде не найкращим і імовірність неможливості впевненого виявлення ознак небезпечного сигналу буде більшою ніж насправді. Якщо k буде великим ($k > 2FT$), то в зв'язку з обмеженням спектру шумів між відліками з'явиться кореляційна залежність, яка не приводитиме до зменшення імовірності неможливості впевненого виявлення ознак небезпечного сигналу. Адже всі зайві (понад $2FT$) відліки матимуть певну статистичну (кореляційну) залежність, через кореляцію (неортогональність) будуть проєкційними повторами попередніх (з числа $2FT$) відліків та не матимуть додаткової інформативності.

Таким чином, умовна імовірність визначатиметься як добуток по всіх $2FT$-відліках:

$$p(y_0 / x_r) = \prod_{i=1}^{2FT} p(y_{0i} / x_{ri}) = \prod_{i=1}^{2FT} p\left\{-c_{\text{пор.}} \le u_i \le +c_{\text{пор.}}\right\} = \tag{3.5.3}$$

$$= \prod_{i=1}^{2FT}\left\{-c_{\text{пор.}} \le c_{ri} + n_i \le +c_{\text{пор.}}\right\} = \prod_{i=1}^{2FT}\left\{-c_{\text{пор.}} - c_{ri} \le n_i \le +c_{\text{пор.}} - c_{ri}\right\} =$$

$$= \prod_{i=1}^{2FT} \int_{-c_{\text{пор.}}-c_{ri}}^{+c_{\text{пор.}}-c_{ri}} \omega(n)dn = \prod_{i=1}^{2FT} \int_{-c_{\text{пор.}}-c_{ri}}^{+c_{\text{пор.}}-c_{ri}} \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{n^2}{2\sigma^2}} dn .$$

Для приведення у співвідношенні (3.5.3) інтегралу щільності нормального розподілу до вигляду інтегралу Лапласа зробимо заміни:

$$\frac{n}{\sigma} = \eta, \quad dn = \sigma d\eta, \; \eta_{\text{гр.}\pm} = \frac{n_{\text{гр.}\pm}}{\sigma} = \frac{\pm c_{\text{пор.}} - c_{ri}}{\sigma}. \tag{3.5.4}$$

З урахуванням замін (3.5.4) співвідношення (3.5.3) набуде вигляду:

$$p(y_0 / x_r) = \prod_{i=1}^{2FT} \int_{\frac{-c_{\text{пор.}} - c_{ri}}{\sigma}}^{\frac{+c_{\text{пор.}} - c_{ri}}{\sigma}} \frac{1}{\sqrt{2\pi}} e^{-\frac{\eta^2}{2}} d\eta . \qquad (3.5.5)$$

Якщо шумовий процес є ергодичним процесом, то його дисперсію (квадрат середньоквадратичного відхилення) можна замінити потужністю завади $P_з$, та виразити через спектральну щільність N_0:

$$\sigma^2 = P_з = N_0 F . \qquad (3.5.6)$$

Таким чином, співвідношення імовірності неможливості впевненого виявлення ознак небезпечного сигналу в каналі витоку інформації, що означено формулою (3.5.2), з урахуванням поправка (3.5.6) має вигляд:

$$p_{\text{н.в.в.о.с.}} = \sum_{r=0}^{N} p(x_r) \prod_{i=1}^{2FT} \int_{\frac{-c_{\text{пор.}} - c_{ri}}{\sqrt{N_0 F}}}^{\frac{+c_{\text{пор.}} - c_{ri}}{\sqrt{N_0 F}}} \frac{1}{\sqrt{2\pi}} e^{-\frac{\eta^2}{2}} d\eta . \qquad (3.5.7)$$

Формула (3.5.7) дозволяє знаходження імовірності неможливості виявлення ознак сигналу за його демаскуванням в середньому за всіма реалізаціями. Щодо означених вище стратегій виявлення, це є стратегія №2.

За максимумом демаскування небезпечного сигналу, це відповідає означеній вище стратегії №1, співвідношення імовірності (3.5.5) дещо спроститься:

$$p_{\text{н.в.в.о.с.}} = \prod_{i=1}^{2FT} \int_{\frac{-c_{\text{пор.}} - c_{qi}}{\sqrt{N_0 F}}}^{\frac{+c_{\text{пор.}} - c_{qi}}{\sqrt{N_0 F}}} \frac{1}{\sqrt{2\pi}} e^{-\frac{\eta^2}{2}} d\eta . \qquad (3.5.8)$$

Отже, здійснено оцінювання імовірності щодо неможливості впевненого виявлення ознак інформаційного сигналу в каналі витоку інформації. Ця імовірність була знайдена за двома стратегіями оцінювання, а саме стратегією неможливості виявлення ознак інформаційного сигналу в середньому та за стратегією максимуму демаскування. Для цього відповідно до стратегій було використано окремі графи станів та перехідних процесів в дискретному каналі з можливістю виявлення/невиявлення ознак інформаційного сигналу.

Отримані співвідношення дозволяють розрахунок імовірності щодо неможливості впевненого виявлення ознак інформаційного сигналу в каналі витоку інформації за заданим відношенням сигнал/завада та навпаки – оцінювання відношення сигнал/завада за заданою імовірністю щодо неможливості впевненого виявлення ознак інформаційного сигналу та відповідно заданій імовірності ризику безпеки.

Контрольні питання:

1. Граф станів та перехідних процесів в дискретному каналі з можливістю виявлення/невиявлення ознак інформаційного сигналу.
2. “Ненульовий” поріг чутливості приймача.
3. Шкала стану приймача з “ненульовим” порогом чутливості щодо умов можливості/неможливості виявлення ознак інформаційного сигналу в каналі з адитивною гауссівською завадою.
4. Імовірність неможливості впевненого виявлення ознак інформаціного сигналу в каналі витоку інформації за стратегією демаскування в середньому.
5. Імовірність неможливості впевненого виявлення ознак інформаційного сигналу в каналі витоку інформації за стратегією максимум демаскування.

РОЗДІЛ 4. НАДЛИШКОВІСТЬ ЯК ЧИННИК ПІДВИЩЕННЯ ЗАВАДОСТІЙКОСТІ. КОРИГУВАННЯ ПОКАЗНИКІВ ЗАХИЩЕНОСТІ ДЛЯ НАДЛИШКОВИХ ДЖЕРЕЛ

4.1. Способи підвищення достовірності передачі інформації в каналах зв'язку. Сутність завадостійкого кодування в каналі

Теорема Шеннона щодо підвищення достовірності передачі інформації в каналах. У попередніх розділах було показано, що будь-який канал передачі, як канал зв'язку, так і канал витоку, можна охарактеризувати їхньою пропускною здатністю C. Пропускна здатність визначається як максимум кількості інформації, яка може бути переданою по каналу, знаходиться по всіх можливих джерелах інформації з їх розподілами ймовірностей, а тому повністю визначається завадо-спотворювальними умовами в каналі та залежить від їхніх параметрів. Для дискретного каналу ця здатність залежить від імовірності помилки в каналі, а для неперервного – від відношення сигнал/завада на виході каналу. Коригування пропускної здатності може забезпечити потрібну якість як каналів зв'язку щодо можливості передавання інформації, так і для технічних каналів витоку інформації.

Для технічних каналів з метою забезпечення умови неможливості витоку інформації, або (так говорять) "відсутності каналу", в ідеалі потрібно, щоб пропускна здатність дорівнювала нулю $C = 0$. В дискретному каналі це забезпечується рівноймовірністю помилкової та безпомилкової передачі, в неперервному – нульовим відношенням сигнал/завада. Однак, на практиці виконання цих умов є складним, а то й неможливим. Пропускна здатність, як теоретичний показник, як завгодно може бути наближеною до нуля, але ніколи не досягатиме його.

Слід зазначити, що забезпечення заданої пропускної спроможності в каналі витоку, тобто для випадків, коли $C \neq 0$, не завжди є умовою безпеки. Цей показник може характеризувати канал для джерел, які виробляють максимум інформації, тобто мають мінімальну, а теоретично – нульову надлишковість. Реальні ж джерела є надлишковими. Надлишковість може покращувати якість передачі й тим самим погіршувати захищеність інформації від витоку.

Відповідно до цього має місце *теорема Шеннона*, яка говорить про наступне (без доведення):

А. Якщо канал має пропускну здатність C, що розрахована на один символ повідомлення, та задані будь-які числа $\delta > 0$ та $H < C$, де H – ентропія джерела, то завжди знайдеться таке n_0, що для всіх $n > n_0$, існує блочний код довжиною n, що складається з $m = 2^{nH}$ комбінацій, та

вирішальна схема (Y^n_1, Y^n_2, …, Y^n_l, …, Y^n_m), які забезпечують виконання нерівності:

$$p(Y^n_l/X^n_i) \geq 1 - \delta, \text{ для } i = l, \qquad (4.1.1)$$

де X^n_i, Y^n_l – кодові слова, відповідно, на вході та на виході каналу:

$$X^n_i = (x_1, x_2, x_3, \ldots, x_n),$$

$$Y^n_l = (y_1, y_2, y_3, \ldots, y_n),$$

де x та y – символи алфавіту, $i = 1, 2, 3, \ldots, 2^n$, l – індекс вірного рішення, $l = 1, 2, 3, \ldots, 2^n$.

Б. Якщо $H > C$, то нерівність (4.1.1) для довільного δ не виконується, яким би не було великим n.

В рамках цієї теореми на практиці завдяки внесенню у повідомлення надлишковості існують два способи підвищення достовірності передачі:

1. Виявлення помилок та здійснення запиту на повтор, а також повтор сеансу передачі.
2. Виправлення помилок.

Виявлення та виправлення помилок в каналі, як правило, реалізується посередництвом застосування завадостійкого кодування. Згідно з правилом кодування в повідомлення даних додатково вносяться певні перевірочні символи, які відграють роль індикатора щодо наявності чи відсутності помилок. Відповідно до ознак за перевірочними символами, згідно з правилом декодування, приймач ухвалює рішення щодо виправлення помилок або повтору сеансу передачі. Це надлишковість, яка створюється штучно та в рамках вище зазначеної теореми Шеннона дозволяє підвищення достовірності передачі.

Окрім штучної надлишковості смислові джерела можуть мати й природну надлишковість. Її зручно показати на прикладі мовних або візуальних джерел. Наприкалад:

– *мовні джерела.* Слова будь-якого тексту певної, нехай української чи іншої, мови формуються за правилами так, що вони дозволяють виправляти помилки. Як правило, слово складається з префікса, кореня, суфікса та закінчення. За смислом, що є найважливішою ознакою розрізнення, слова розділяються коренем. Слова з однаковим коренем можуть модифікуватися в самому корені, а також відрізнятися префіксами та суфіксами. Слова зі спільними суфіксами у зв’язку, наприклад, з належністю до родів можуть відрізнятися закінченнями.

Всі частини слова: префікс, корень, суфікс та закінчення – є комбінацією літер та, відповідно, звуків при їх озвученні. Ці комбінації можна розділити на дозволені, тобто прийняті мовою префікси, корені, суфікси та закінчення, та недозволені, яких мова не використовує. У разі наявності недозволених комбінацій літер (звуків) їх можна порівняти зі

схожими дозволеними та за ознакою найбільшої схожості (імовірності схожості) ухвалити рішення щодо вірності зазначеної комбінації.

Таким чином виправляються помилки мовлення завдяки її природній надлишковості. Зазвичай це здійснюється інтуїтивно чи автоматизовано, під час перевірки тексту чи під час прослуховування озвучення його слів. Оскільки слова є продуктом мовлення, тобто інформацією, яку виробила людина, вони мають суб'єктивне походження;

– *візуальні джерела.* Зображення відображає зовнішній вигляд об'єкта, а тому є інформацією об'єктивного походження. Як правило, зображення є двовимірною матрицею точок-пікселів різного кольору, різної яскравості та різного розподілу цих параметрів за статистикою.

Однак, в межах однієї картинки не всі пікселі можуть нести корисну інформацію про об'єкт, що є цікавими (корисними) на прийомі. Наприклад, зображення об'єкта на фоні містить окремі пікселі-інформацію про об'єкт та пікселі-інформацію про фон. Якщо корисною є інформація про об'єкт, то взагалі байдуже, яким є фон. Може бути навпаки: фон є важливим, а об'єкт на фоні – ні. В першому випадку є очевидним, що пікселі фону не є інформативними та займають лише місце у повідомленні.

Щодо природної надлишковості – суттєву роль відіграє детальність картинки. Так, одна справа, коли для зображення деталі, наприклад лінії літери алфавіту, використано багато однойменних пікселів – це крупнодетальне надто надлишкове зображення, інша справа, коли для дрібнодетального слабко надлишкового зображення використано декілька пікселів. Очевидно, що виправлення одного пікселя з великої кількості однойменних здійснюється простіше, ніж із малої кількості цих пікселів.

Отже, відповідно до власної природної надлишковості зображення, як і для мовлення, також можуть виправлятися помилки в разі їх спотворення. Ці виправлення може здійснюватися як зоровим апаратом людини інтуїтивно, так і автоматизовано засобами обробки інформації.

Як випливає з теореми, показник пропускної здатності каналу витоку інформації може бути мірилом захищеності лише для безнадлишкових джерел, для яких ентропія є максимальною. При цьому нормування пропускної здатності C по максимуму цієї ентропії $H_{\max}$ відображатиме ту долю інформації, яка може пройти від джерела через канал. Очевидно, що ця доля є нічим іншим, як імовірністю ризику щодо витоку інформації технічним каналом, яка виражається формулою:

$$R \geq \frac{C}{H_{\max}}. \qquad (4.1.2)$$

Для надлишкових джерел нерівність (4.1.2) не є коректною, оскільки порушується визначення пропускної здатності. Використання ж

пропорційності щодо коригування потрібної пропускної здатності для забезпечення заданого ризику, наприклад

$$C \le RH\ , \qquad (4.1.3)$$

відповідає нашим інтуїтивним уявленням, але не випливає з теореми Шеннона та не є доведеним.

При цьому слід зазначити, що на практиці мають місце приклади ефективних завадостійких кодів, які мають велику кодову відстань та дозволяють забезпечити більшу пропускну здатність, ніж показано формулою (4.1.3) (зазначене буде наведено пізніше).

Як наслідок *теореми Шеннона* для технічних каналів витоку інформації можна *стверджувати* наступне:

А. Якщо технічний канал витоку має пропускну здатність C, що розрахована на один символ повідомлення та задані будь-які числа $\delta > 0$ та $H < C$, де H – ентропія джерела, то завжди знайдеться таке n_0, що для всіх $n > n_0$, (n – смисловий відрізок, n_0 – нижня межа смислового відрізку) існує такий спосіб обробки, що здійснюватиметься на основі перебору $m = 2^{nH}$ комбінацій смислових відрізків, які для імовірності вірного прийому забезпечують виконання нерівності (4.1.1).

Б. Якщо $H > C$, то нерівність (4.1.1) не виконується, якими б не були δ та n.

Таким чином, пропускна здатність технічних каналів витоку безпосередньо для надлишкових джерел інформації не може бути показником захищеності. Надлишковість даних дозволяє їх тотальний перебір та будь-які інші способи обробки, що приводить до виправлення помилок та підвищення пропускної спроможності каналу.

Очевидно, що забезпечення потрібної імовірності ризику та, відповідно, пропускної спроможності технічних каналів витоку для надлишкових джерел вимагає коригування останньої. Розрахунок гранично допустимої пропускної спроможності каналу витоку має здійснюватися з запасом, який врахує надлишковість та компенсує ті недоліки, які вносить остання в захищеність. Це можливо шляхом відповідної поправки ймовірностей помилок в каналах та розрахунку еквівалентної імовірності, яка аналогічним чином враховуватиме та компенсуватиме вище вказані недоліки.

Отже, розглянуті способи підвищення достовірності передачі як чинники, що можуть покращувати перехоплення інформації технічними каналами витоку та тим самим знижувати інформаційну безпеку. Наведені теореми Шеннона, які показують верхню межу щодо можливості підвищення достовірності передачі залежно від надлишковості повідомлення.

Для знаходження шляхів врахування надлишковості джерела при оцінюванні його захищеності має місце необхідність розгляду наявних способів підвищення достовірності передачі інформації, яка забезпечується шляхом завадостійкого кодування.

Сутність завадостійкого кодування. Лінійні, систематичні та циклічні коди. Твірні та перевірочні матриці завадостійких кодів. Завадостійке кодування в дискретних каналах передачі вирішують два завдання: (1) виявлення помилок та (2) виправлення помилок, що виникають в каналі.

Як правило, завдання виявлення помилок є актуальним для каналів зв'язку лише тоді, коли канал використовує повтор передавання повідомлень із перезапитом. Так, якщо на прийомі система виявляє факт наявності помилок, то вона по зворотному каналу повідомляє про це передавач, який має повторно здійснити сеанс передачі. Це може здійснюватися за декілька циклів, в результаті чого повідомлення буде або передано без помилок, або канал визнається таким, що не може передавати інформацію.

Для технічних же каналів витоку інформації, завдання виявлення помилок не є актуальним. І це очевидно, оскільки в силу власних особливостей канал витоку не може мати зворотних каналів для перезапиту і є одностороннім від джерела витоку інформації до приймача перехоплення. В зв'язку з цим розгляд сутності виявлення помилок для технічних каналів витоку інформації, що виникають від технічних засобів обробки та передачі з використанням завадостійкого кодування, не є доцільним.

Розглянемо сутність завадостійкого кодування з точки зору виправлення помилок.

Нехай задано канал, як показано на рис. 4.1.1.

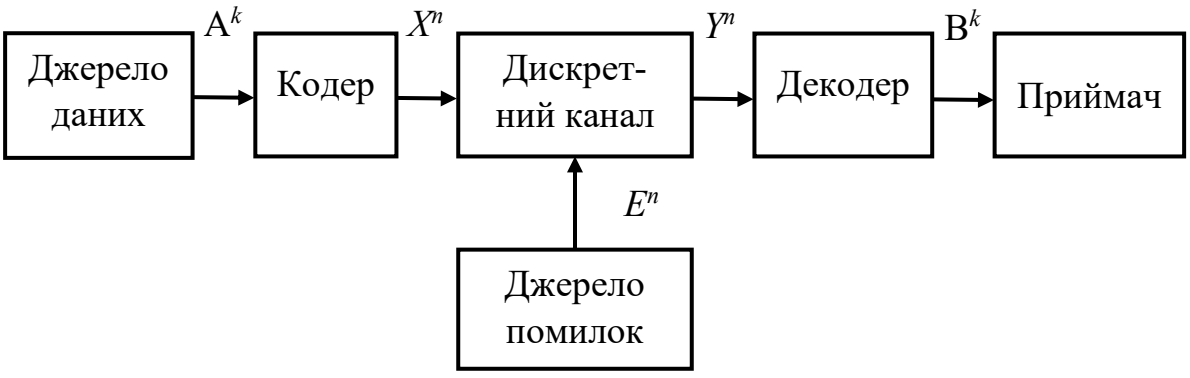


Рис. 4.1.1. Канал передачі дискретних даних з використанням завадостійкого кодування

Джерело виробляє послідовність дискретних даних $A^k_i = (\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_k)$ довжиною k, де $\alpha = \{0, 1\}$, i – номер комбінації, $i = 1, 2, \ldots, 2^k$.

В кодері здійснюється кодування $A^k_i \to X^n_i$, яке вносить в повідомлення надлишковість. Завадостійкий код надає можливість на прийомі виправляти помилки.

Сформована після кодера послідовність $X^n_i = (x_1, x_2, x_3, \ldots, x_n)$ довжиною n ($n > k$), де $x = \{0, 1\}$ потрапляє на вхід каналу.

Такий код називають (n, k) кодом.

Каналом є дискретний симетричний канал без пам'яті з імовірністю помилки p, який реалізує передачу знаків x у вихідні знаки y, $y = \{0, 1\}$ (див. рис. 4.1.2):

$$y = (x + e) \bmod 2, \tag{4.1.4}$$

де e – помилка в дискретному каналі, $e = \{0, 1\}$.

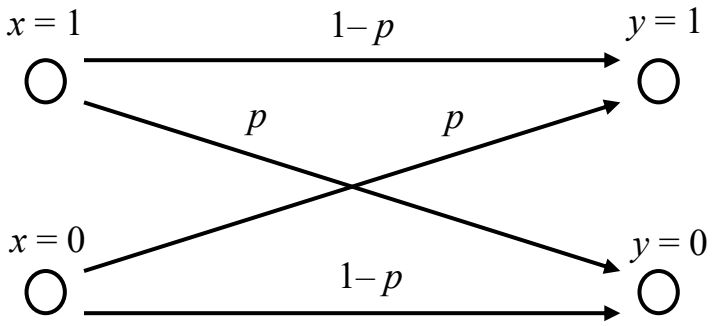


Рис. 4.1.2. Граф станів дискретного симетричного каналу без пам'яті

Згідно зі співвідношенням (4.1.4) імовірність помилки $p\,(e = 1) = p\,(x \neq y) = p$ та безпомилкової передачі $p\,(e = 0) = p\,(x = y) = 1 - p$ та перехід комбінацій $X^n \to Y^n$ можна виразити як

$$Y^n_l = (X^n_i + E^n_s) \bmod 2^n, \tag{4.1.5}$$

де E^n – послідовність помилок $E^n{}_s = (e_1, e_2, \ldots, e_n)$ довжиною n:

$$E^n{}_s = (e_1, e_2, \ldots, e_n),$$

на яку відрізняється вихідна послідовність $Y^n{}_l$ від вхідної $X^n{}_i$, s – номер комбінації $E^n{}_s$, $s = 1, 2, 3, \ldots, 2^n$.

Співвідношення (5) з урахуванням (4) можна записати в іншому вигляді:

$$Y^n_l = (y_1, y_2, \ldots, y_n) = (x_1 \oplus e_1, x_2 \oplus e_2, \ldots, x_n \oplus e_n), \tag{4.1.6}$$

де $\oplus$ – операція додавання за модулем 2.

Декодер завдяки внесеній надлишковості виправляє деякі комбінації помилок E^n, що виникли в каналі при передачі $X^n_i \to Y^n_{lg}$, $l = 1, 2,\ldots, 2^k$, $g = 1, 2,\ldots, 2^{n-k}$, та декодує Y^n_{lg} в B^k_l довжиною k, $B^k_l = (\beta_1, \beta_2, \beta_3, \ldots, \beta_k)$. Виправленням помилок декодер зменшує імовірність p до деякої еквівалентної імовірності помилки $p_{\text{екв.}}$. Еквівалентна імовірність помилки є імовірністю того, що після декодування $Y^n \to B^k$ знаки α та β відрізнятимуться.

Досить поширеним класом завадостійких кодів є *лінійні коди*.

Це коди, які можна записати у вигляді добутку:

$$\mathbf{X} = \mathbf{A} \times \mathbf{G}, \tag{4.1.7}$$

де $\mathbf{X}$ – одномірна матриця розмірністю n, елементами якої є значенні послідовності X^n, $\mathbf{A}$ – одномірна матриця розмірністю k, що відповідає послідовності A^k, $\mathbf{G}$ – твірна матриця завадостійкого коду розмірністю $n \times k$.

Для лінійних кодів в деяких випадках твірна матриця може мати вигляд:

$$\mathbf{G} = [\mathbf{I} \mid \mathbf{C}], \tag{4.1.8}$$

де $\mathbf{I}$ – одинична діагональна матриця у вигляді:

$$\mathbf{I} = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix}, \tag{4.1.9}$$

$\mathbf{C}$ – матриця, що складається з лінійно незалежних рядків та стовпців. Вона формує перевірочні символи коду.

Якщо твірна матриця має вигляд, як показано співвідношенням (4.1.8), то лінійний код називають *систематичним*.

Наприклад, твірна матриця систематичного коду Хеммінга (7, 4) має вигляд:

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}. \tag{4.1.10}$$

Серед лінійних кодів мають місце *циклічні коди*. Це коди, які можна записати у вигляді добутку:

$$R(x) = P(x) \times x^N \bmod G(x), \tag{4.1.11}$$

де N – степінь твірного многочлена. Циклічні коди також можуть мати твірну матрицю, яка утворюється з систематичного коду шляхом перестановок та лінійних операцій над рядками. Так матриця $\mathbf{G}'$ є утворенням від матриці $\mathbf{G}$, кожен рядок якої є циклічним зсувом від попереднього рядка:

$$\mathbf{G}' = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}. \qquad (4.1.12)$$

Існують і інші коди, які завдяки надлишковості можуть виправляти помилки, що виникають в каналі. Це також поточні, турбо- та інші, гібридні коди.

Завадостійкі коди, що виправляють помилки, ще називають корегувальними, оскільки вони корегують якість каналу, яким передається інформація.

Декодування здійснюється шляхом перемноження виходу каналу на обернену до твірної матрицю:

$$\mathbf{B} = \mathbf{Y} \times \mathbf{G}^{-1}, \qquad (4.1.13)$$

де $\mathbf{Y}$ – одномірна матриця розмірністю n, елементами якої є значенні послідовності Y^n, $\mathbf{B}$ – одномірна матриця розмірністю k, що відповідає послідовності даних B^k, $\mathbf{G}^{-1}$ – обернена до твірної матриця розмірністю $k \times n$.

Для систематичного коду з твірною матрицею (4.1.8) обернена матиме вигляд:

$$\mathbf{G}^{-1} = \begin{bmatrix} \mathbf{I} \\ \mathbf{O} \end{bmatrix}, \qquad (4.1.14)$$

де $\mathbf{O}$ – нульова матриця:

$$\mathbf{O} = \begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \end{pmatrix}. \qquad (4.1.15)$$

Нескладно перевірити оберненість матриць (4.1.8) та (4.1.14), перемноживши їх між собою:

$$\mathbf{G} \times \mathbf{G}^{-1} = [\mathbf{I} \mid \mathbf{C}] \times \begin{bmatrix} \mathbf{I} \\ \mathbf{O} \end{bmatrix} = \mathbf{I}, \qquad (4.1.14)$$

Наприклад, для матриці (4.1.10) обернена дорівнюватиме:

$$\mathbf{G}^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \tag{4.1.16}$$

а добуток (4.1.10) та (4.1.16):

$$\mathbf{G} \times \mathbf{G}^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{4.1.16}$$

Окрім оберненої твірна матриця **G** має передбачати наявність *перевірочної* матриці **H**, яка має бути такою, що:

$$\mathbf{A} \times \mathbf{G} \times \mathbf{H}^{\mathrm{T}} = \mathbf{X} \times \mathbf{H}^{\mathrm{T}} = \mathbf{O}, \tag{4.1.17}$$

Слід звернути увагу, що якщо твірна матриця **G** має розмірність $n \times k$, то розмірністю перевірочної **H** є $n \times (n - k)$.

Тому для систематичних кодів, що мають твірну матрицю у вигляді (4.1.8), перевірочна матиме вигляд:

$$\mathbf{H}^{\mathrm{T}} = \begin{bmatrix} \mathbf{C} \\ \hline \mathbf{I} \end{bmatrix}, \tag{4.1.18}$$

Не складно побудувати перевірочну матрицю для твірної (4.1.10):

$$\mathbf{H}^{\mathrm{T}} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \tag{4.1.19}$$

Однак перевірити добуток $\mathbf{G} \times \mathbf{H}^{\mathrm{T}} = \ldots$ не є можливим через різні розмірності матриць.

Таким чином, розглянуто сутність завадостійкого кодування, яке завдяки внесенню в повідомлення надлишковості може виправляти помилки в каналі і тим самим підвищувати достовірність передачі інформації. Як приклад для розгляду механізмів кодування та декодування повідомлень в каналі розглянуті лінійні, систематичні та циклічні коди, сутність їх твірної та перевірочної матриць.

Кодування та декодування повідомлень в каналі. Розглянемо сутність кодування та декодування з виправленням помилок на прикладі лінійних кодів.

Нехай задано твірну матрицю завадостійкого коду **G**.

1. Як вже було з'ясовано, кодування може бути представленим операцією множення (4.1.7):

$$\mathbf{X}^n = \mathbf{A}^k \times \mathbf{G}^{n\times k}. \qquad (4.1.20)$$

2. Якщо в каналі діє помилка, то

$$\mathbf{Y}^n = \mathbf{X}^n \oplus \mathbf{E}^n, \qquad (4.1.21)$$

3. При декодуванні здійснюється перевірка на синдром:

$$\mathbf{S}^{n-k} = \mathbf{Y}^n \times \left[\mathbf{H}^{n\times(n-k)}\right]^{\mathrm{T}}. \qquad (4.1.22)$$

4. За синдромом $\mathbf{S}^{n-k}$ знаходять найбільш імовірну комбінацію помилок:

$$\mathbf{S}^{n-k} \leftrightarrow \mathbf{E}'^n. \qquad (4.1.23)$$

Синдром $\mathbf{S}^{n-k}$ представляє собою комбінацію $S^{n-k}{}_g$, $g = 1, 2,\ldots, 2^{n-k}$, яка відповідає деяким комбінаціям помилок $E'^n{}_s = (e_1, e_2,\ldots, e_n)$ довжини n, $s = 1, 2, 3,\ldots, 2^{n-k}$.

Як правило, з усіх можливих комбінацій E^n обирають найбільш імовірні $E'^n{}_s$ тобто меншої ваги. Це потрібно для підвищення достовірності передачі в каналах зв'язку, оскільки для імовірності помилки $p < 0{,}5$ справедлива нерівність:

$$p^n < p^{n-1}(1-p) < p^{n-2}(1-p)^2 < \ldots < p(1-p)^{n-1} < (1-p)^n. \qquad (4.1.24)$$

5. Від отриманої на виході каналу послідовності Y^n віднімають визначену посередництвом синдрому $S^{n-k}{}_g$ комбінацію помилок $E'^n{}_s$:

$$\mathbf{Y}'^n = \mathbf{Y}^n \oplus \mathbf{E}'^n = \mathbf{X}^n \oplus \mathbf{E}^n \oplus \mathbf{E}'^n, \qquad (4.1.25)$$

6. Здійснюється перетворення згідно зі співвідношенням (4.1.10) з використанням оберненої до твірної матриці коду:

$$\mathbf{B}^k = \mathbf{Y}'^n \times \mathbf{G}^{-1} = \left[\mathbf{X}^n \oplus \mathbf{E}^n \oplus \mathbf{E}'^n\right] \times \mathbf{G}^{-1} =$$

$$= \mathbf{X}^n \times \mathbf{G}^{-1} \oplus \left[\mathbf{E}^n \oplus \mathbf{E}'^n\right] \times \mathbf{G}^{-1} = \mathbf{A}^k \oplus \left[\mathbf{E}^n \oplus \mathbf{E}'^n\right] \times \mathbf{G}^{-1}. \qquad (4.1.26)$$

З (4.1.26) випливає наступне:

– якщо $E^n = (\underbrace{0,0,...,0}_{n})$ тобто помилки в каналі не було, то $S^{n-k} = 0$ та $E'^n = (\underbrace{0,0,...,0}_{n})$, а це означає, що $\mathbf{Y}^n = \mathbf{X}^n$. При цьому співвідношення (4.1.26) матиме вигляд:

$$\mathbf{B} = \mathbf{Y} \times \mathbf{G}^{-1} = \mathbf{X} \times \mathbf{G}^{-1} = \left[\mathbf{A} \times \mathbf{G}\right] \times \mathbf{G}^{-1} = \mathbf{A} \times \left[\mathbf{G} \times \mathbf{G}^{-1}\right] = \mathbf{A}. \qquad (4.1.27)$$

– якщо $E^n \neq (\underbrace{0,0,...,0}_{n})$, то $S^{n-k}{}_s \leftrightarrow E'^n{}_s$ і виправлятимуться лише помилки $E^n = E'^n{}_s$ для $s = 1, 2, \ldots, 2^{n-k}$.

– якщо $E^n \neq E'^n{}_s$ помилка залишиться невиправленою.

Однак ті помилки, що виправляються, є найбільш імовірними, особливо для невеликих p.

Таким декодуванням виправляється $2^{n-k} - 1$ комбінацій помилок із всіх можливих 2^n. Це, відповідно, вносить перерозподіл ймовірностей за комбінаціями і в цілому зменшує імовірність помилки.

Отже, розглянуто сутність кодування та декодування з виправленням помилок на прикладі лінійних кодів. При цьому показано, що не всі помилки можуть бути виправленими. Кількість помилок, що виправляються, визначаються ефективністю кодів та надлишковістю джерела, що доцільно розглянути з використанням стандартного розташування коду в суміжних класах.

Таким чином, розглянуті способи підвищення достовірності передачі як чинники, що можуть покращувати перехоплення інформації технічними каналами витоку та тим самим знижувати інформаційну безпеку. Наведені теореми Шеннона, які показують верхню межу щодо можливості підвищення достовірності передачі залежно від надлишковості повідомлення.

Розглянуто сутність завадостійкого кодування, яке завдяки внесенню в повідомлення надлишковості може виправляти помилки в каналі й тим самим підвищувати достовірність передачі інформації. Як приклад для розгляду механізмів кодування та декодування повідомлень в каналі розглянуті лінійні, систематичні та циклічні коди, сутність їх твірної та перевірочної матриць.

На основі лінійних кодів розглянуто приклад кодування та декодування з виправленням помилок. При цьому показано, що не всі помилки можуть бути виправленими. Кількість помилок, що виправляються, визначаються ефективністю кодів та надлишковістю

джерела, що доцільно розглянути з використанням стандартного розташування коду в суміжних класах.

Контрольні питання.

1. Способи підвищення достовірності передачі інформації в каналах зв'язку та їхня сутність.
2. Теореми Шеннона щодо підвищення достовірності передачі інформації.
3. Сутність завадостійкого кодування.
4. Лінійні, систематичні та циклічні коди. Твірні та перевірочні матриці завадостійких кодів.
5. Механізм кодування та декодування повідомлень в каналі на основі лінійних кодів.

4.2. Представлення завадостійких кодів в суміжних класах. Їхнє стандартне розташування та принцип виправлення помилок

Представлення завадостійких кодів у суміжних класах та їхнє стандартне розташування. Нехай задано канал, який використовує завадостійкий систематичний (n, k) код з твірною матрицею **G**, що виправляє помилки (див. рис. 4.1.1):

$$\mathbf{G} = [\mathbf{I} \mid \mathbf{C}], \tag{4.2.1}$$

де **I** – одинична діагональна матриця, **C** – матриця, що формує перевірочні символи коду та складається з лінійно незалежних рядків та стовпців.

Джерело виробляє послідовність дискретних даних $A^k_i = (\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_k)$ довжиною k, де $\alpha = \{0, 1\}$, i – номер комбінації, $i = 1, 2, \ldots, 2^k$.

В *кодері* здійснюється кодування $A^k_i \rightarrow X^n_i$, яке вносить в повідомлення надлишковість ($n > k$):

$$\mathbf{X}^n = \mathbf{A}^k \times \mathbf{G}^{n \times k}, \tag{4.2.2}$$

де **X** – одномірна матриця розмірністю n, елементами якої є значення послідовності X^n, **A** – одномірна матриця розмірністю k, що відповідає послідовності A^k, **G** – твірна матриця завадостійкого коду розмірністю $n \times k$.

Завадостійкий код надає можливість на прийомі виправляти помилки.

Сформована після кодера послідовність $X^n_i = (x_1, x_2, x_3, \ldots, x_n)$ довжиною n, де $x = \{0, 1\}$, потрапляє на вхід каналу.

Каналом є дискретний симетричний канал без пам'яті з імовірністю помилки p, $p \in (0; ½)$, який реалізує передачу знаків x у вихідні знаки y, $y = \{0, 1\}$ (див. рис. 4.1.2):

$$y = (x + e) \bmod 2, \tag{4.2.3}$$

де e – помилка в дискретному каналі, $e = \{0, 1\}$.

Згідно з співвідношенням (4.2.3) вихідна послідовність каналу:

$$Y^n_{gl} = (y_1, y_2, ..., y_n) = (X^n_i + E^n_s) \bmod 2^n = (x_1 \oplus e_1, x_2 \oplus e_2, ..., x_n \oplus e_n), \tag{4.2.4}$$

де E^n – послідовність помилок довжиною n, на яку відрізняється вихідна послідовність Y^n_{gl} від вхідної X^n_i, $l = 1, 2, \ldots, 2^k$, $g = 1, 2, \ldots, 2^{n-k}$:

$$E^n_s = (e_1, e_2, \ldots, e_n),$$

s – номер комбінації E^n_s, $s = 1, 2, 3, \ldots, 2^n$, $\oplus$ – операція додавання за модулем 2.

Для матриць співвідношення (4.2.4) матиме опис:

$$\mathbf{Y}^n = \mathbf{X}^n \oplus \mathbf{E}^n, \tag{4.2.5}$$

При *декодуванні* здійснюється перевірка на синдром S^{n-k}_g, $g = 1, 2, \ldots, 2^{n-k}$, який відповідає деяким найбільш імовірним комбінаціям помилок $E'^n_s = (e_1, e_2, \ldots, e_n)$ довжини n, $s = 1, 2, 3, \ldots, 2^{n-k}$:

$$\mathbf{S}^{n-k} = \mathbf{Y}^n \times \left[\mathbf{H}^{n \times (n-k)}\right]^{\mathrm{T}}. \tag{4.2.6}$$

де $\mathbf{H}$ – перевірочна матриця коду розмірністю $n \times (n - k)$.

За синдромом $\mathbf{S}^{n-k}$ знаходять відповідну комбінацію помилок:

$$\mathbf{S}^{n-k} \leftrightarrow \mathbf{E}'^n. \tag{4.2.7}$$

Від отриманої на виході каналу послідовності Y^n віднімають E'^n_s:

$$\mathbf{Y}'^n = \mathbf{Y}^n \oplus \mathbf{E}'^n = \mathbf{X}^n \oplus \mathbf{E}^n \oplus \mathbf{E}'^n, \tag{4.2.8}$$

Здійснюється перетворення з використанням оберненої до твірної матриці коду:

$$\mathbf{B}^k = \mathbf{Y}'^n \times \mathbf{G}^{-1} = \left[\mathbf{X}^n \oplus \mathbf{E}^n \oplus \mathbf{E}'^n\right] \times \mathbf{G}^{-1} =$$

$$= \mathbf{X}^n \times \mathbf{G}^{-1} \oplus \left[\mathbf{E}^n \oplus \mathbf{E}'^n\right] \times \mathbf{G}^{-1} = \mathbf{A}^k \oplus \left[\mathbf{E}^n \oplus \mathbf{E}'^n\right] \times \mathbf{G}^{-1}, \tag{4.2.9}$$

де $\mathbf{B}$ – матриця, що відповідає послідовності B^k_l довжиною k, $\mathrm{B}^k_l = (\beta_1, \beta_2, \beta_3, \ldots, \beta_k)$, $\beta = \{0, 1\}$.

1. Якщо $E^n = (\underbrace{0,0,...,0}_{n})$, тобто помилки в каналі не було, то $S^{n-k} = 0$ та $E'^n = (\underbrace{0,0,...,0}_{n})$, а це означає, що $\mathbf{Y}^n = \mathbf{X}^n$. При цьому співвідношення (4.2.9) матиме вигляд:

$$\mathbf{B} = \mathbf{Y} \times \mathbf{G}^{-1} = \mathbf{X} \times \mathbf{G}^{-1} = \left[\mathbf{A} \times \mathbf{G}\right] \times \mathbf{G}^{-1} = \mathbf{A} \times \left[\mathbf{G} \times \mathbf{G}^{-1}\right] = \mathbf{A}. \qquad (4.2.10)$$

2. Якщо $E^n \neq (\underbrace{0,0,...,0}_{n})$, то $S^{n-k}{}_s \leftrightarrow E'^n{}_s$ і виправлятимуться лише помилки $E^n = E'^n{}_s$ для $s = 1, 2, \ldots, 2^{n-k}$.

3. Якщо $E^n \neq E'^n{}_s$, помилка залишиться невиправленою.

Вище зазначене кодування можна представити в суміжних класах. Це здійснюється наступним чином (див. рис. 4.2.1):

1. Перебираються всі комбінації $\mathrm{A}^k{}_i = (\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_k)$ довжиною k.

2. За допомогою правила кодування (4.2.2) формуються відповідні надлишкові двійкові n-послідовності, з тим самим індексом $X^n{}_i = (x_1, x_2, x_3, \ldots, x_n)$ більшої довжини, ніж $\mathrm{A}^k{}_i$, $n > k$.

3. Суміжні класи формуються шляхом додавання до комбінацій помилок найменшої ваги, як найбільш імовірні, та які будуть виправлятися завадостійким кодом при декодуванні. Для суміжних класів властивим є те, що вони відрізняються між собою поелементно на одну і ту ж комбінацію вектора помилок $E'^n{}_s$.

Кожному суміжному класу має відповідати синдром $S^{n-k}{}_s$, за яким і знаходиться E'^n.

Оскільки код лінійний та перша комбінація $\mathrm{A}^k{}_1$ складатиметься з нулів, то з нулів складатиметься і $X^n{}_1$ як результат добутку (4.2.2). А це означає, що в суміжних класах $Y^n{}_{g\ 1} = E'^n{}_s$, де $g = 1, 2, \ldots, 2^{n-k}$, та $s = 1, 2, 3, \ldots, 2^{n-k}$. Тому всі комбінації $Y^n{}_{g1}$, що розташовані в першому стовпці суміжних класів стандартного розташування коду, називають лідерами суміжних класів. Як наслідок, лідери в суміжних класах мають найменшу вагу.

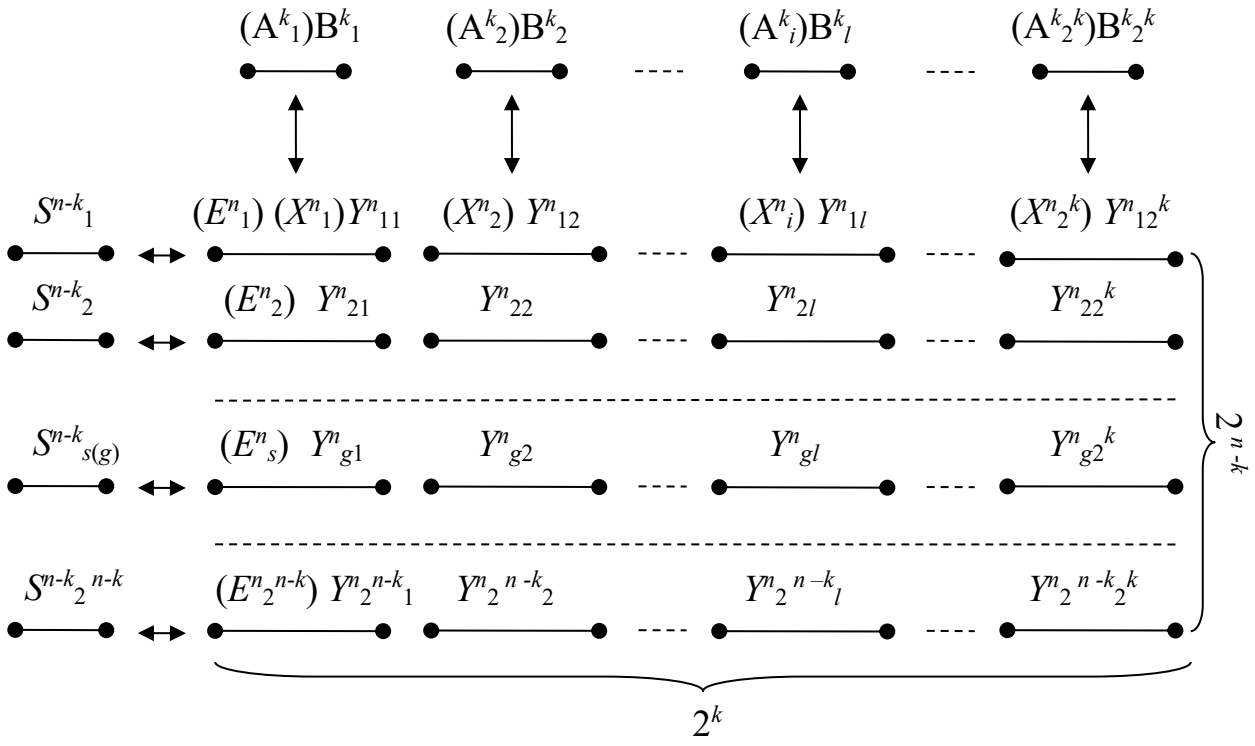


Рис. 4.2.1. Стандартне розташування завадостійкого коду в суміжних класах

Комбінацію Y^n, що на виході каналу, перевіряють на синдром. Віднімають від отриманої Y^n лідер відповідного суміжного класу та переходять в код X^n, за яким нескладно знаходиться комбінація B^k, яка має відповідати переданій A^k. При цьому слід зазначити, що ця операція віднімання відповідає операції додавання за модулем 2.

Таким чином, здійснено представлення завадостійких кодів в суміжних класах, які сукупно являють собою стандартне розташування коду. Суміжні класи утворюються шляхом порозрядного додавання до кодових слів комбінацій помилок, які мають виправлятися кодом. Ці комбінації є лідерами суміжних класів та обираються як найбільш імовірні в каналі, тобто комбінації, що мають мінімальну вагу.

Приклад побудови стандартного розташування суміжних класів для коду Хеммінга (7, 4). Побудуємо стандартне розташування коду Хеммінга (7, 4) в суміжних класах. Для цього скористаємося його твірною матрицею 7×4 у вигляді:

$$\mathbf{G}^{7\times4} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \tag{4.2.11}$$

та перевірочною матрицею розмірністю 7×3 в транспонованому вигляді:

$$\mathbf{H}^{7\times3\mathrm{T}} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{4.2.12}$$

Представимо для стандартного розташування коду всі комбінації двійкових знаків A^4_i, $i = 0 \div 15$. Здійснимо кодування кожної з них в кодові слова X^7_i за допомогою формули (4.2.2):

$$\mathbf{X}^7 = \mathbf{A}^4 \times \mathbf{G}^{7\times4}. \tag{4.2.13}$$

Нехай лідером суміжних класів є:

1. Для нульового суміжного класу (коду):

$$E^7_0 = (\underbrace{0,0,0,...,0}_{7}). \tag{4.2.14}$$

2. Для першого суміжного класу:

$$E^7_1 = (\underbrace{0,0,0,...,1}_{7}). \tag{4.2.15}$$

3. Для другого суміжного класу:

$$E^7_2 = (\underbrace{0,0,...,1,0}_{7}). \tag{4.2.16}$$

…….

8. Для сьомого суміжного класу:

$$E^7_7 = (\underbrace{1,0,...,0,0}_{7}). \tag{4.2.17}$$

Відповідно, синдромами суміжних класів стануть рядки матриці (4.2.12) починаючи з нижнього, а для коду або нульового суміжного класу:

$$S^3_0 = (0, 0, 0),$$

$$Y^n_{gl} = X^n_l \oplus E^n_g, \tag{4.2.18}$$

де індекси $g = 0 \div 7$, $l = 0 \div 15$.

Наприклад, для $A^4_3 = (0, 0, 1, 1)$ та $E^7_2 = (0, 0, 0, 0, 0, 1, 0)$:

$$X^7_3 = (0, 0, 1, 1, 1, 1, 0),$$

$$Y^7_{23} = (0, 0, 1, 1, 1, 0, 0),$$

$$S^3_2 = (0, 1, 0).$$

Слід звернути увагу, що

$$S_2^7 = Y_{23}^7 \times H^{\mathrm{T}} = E_2^7 \times H^{\mathrm{T}}.$$

Приклад побудованого стандартного розташування коду Хеммінга (7, 4) у суміжних класах представлено в Додатку А.

Отже, наведено приклад побудови стандартного розташування суміжних класів для коду Хеммінга (7, 4). Воно надає можливість наочного розуміння механізму виправлення помилок та тим самим зменшення помилок в каналі.

Таким чином, здійснено представлення завадостійких кодів в суміжних класах, які сукупно являють собою стандартне розташування коду. Суміжні класи утворюються шляхом порозрядного додавання до кодових слів комбінацій помилок, які мають виправлятися кодом. Ці комбінації є лідерами суміжних класів та обираються як найбільш імовірні в каналі, тобто комбінації, що мають мінімальну вагу.

Наведено приклад побудови стандартного розташування суміжних класів для коду Хеммінга (7, 4). Воно надає можливість наочного розуміння механізму виправлення помилок та тим самим зменшення помилок в каналі.

Контрольні питання.

1. Стандартне розташування завадостійкого коду.
2. Суміжні класи та лідери суміжних класів.
3. Синдроми суміжних класів та їхня сутність.
4. Побудова стандартного розташування суміжних класів для коду Хеммінга (7, 4).
5. Лідери та синдроми суміжних класів стандартного розташування коду Хеммінга (7, 4).

4.3. Еквівалентна імовірність помилки в каналі із завадостійким кодуванням

Коригування імовірності помилки в каналі для надлишкового джерела та оцінювання її еквівалентної імовірності на основі представлення завадостійких кодів в стандартному розташуванні суміжних класів. Нехай задано канал, який використовує завадостійкий систематичний (n, k) код, що виправляє помилки, з твірною матрицею **G** (див. рис. 4.1.1):

Нехай (n, k) код представлений в суміжних класах, як це показано на рис. 4.2.1. У верхньому рядку представлені всі комбінації двійкових знаків $A^k_i = (\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_k)$ довжиною k, де $\alpha = \{0, 1\}$, i – номер комбінації, $i = 1, 2,\ldots, 2^k$, які може виробляти джерело та які потрапляють на вхід кодера. Цими ж комбінаціями і є вихідні комбінації знаків з декодера $B^k_l = (\beta_1, \beta_2, \beta_3, \ldots, \beta_k)$, $\beta = \{0, 1\}$, $l = 1, 2,\ldots, 2^k$ тієї ж довжини.

За допомогою правила кодування формуються відповідні надлишкові двійкові n-послідовності, з тим самим індексом $X^n_i = (x_1, x_2, x_3, \ldots, x_n)$ більшої довжини, ніж A^k_i, $n > k$. Слід зазначити, що для лінійних кодів кодування здійснюється операцією множення матриць:

$$\mathbf{X}^n = \mathbf{A}^k \times \mathbf{G}^{n \times k}, \tag{4.3.1}$$

де **X** – одномірна матриця розмірністю n, елементами якої відповідають знакам послідовності X^n, **A** – одномірна матриця розмірністю k, що відповідає послідовності A^k, **G** – твірна матриця коду розмірністю $n \times k$.

Суміжні класи формуються шляхом додавання до кодових слів X^n_i комбінацій помилок E'^n_s, де $s = 1, 2, 3,\ldots, 2^{n-k}$. Як правило, комбінації E'^n_s вибираються якнайменшої ваги, оскільки це забезпечує їхню найбільшу імовірність та оптимізує виправляючу здатності коду. Таким чином, суміжні класи відрізняються між собою на один і той самий випадковий вектор E'^n_s:

$$Y^n_{is} = (y_1, y_2, ..., y_n) = X^n_i \oplus E'^n_s, \tag{4.3.2}$$

Кожному суміжному класу відповідає синдром S^{n-k}_s – комбінація даних (номер суміжного класу в двійковій системі обчислення), якій відповідає певний випадковий вектор E'^n_s.

Оскільки перша комбінація A^k_1 складається з нулів, то для лінійного коду з нулів складатиметься і X^n_1 як результат добутку (4.3.1). А це означає, що в суміжних класах $Y^n_{s1} = E'^n_s$. Тому всі комбінації $Y^n_{s1} = E'^n_s$, що розташовані в першому стовпці на рис. 4.3.2, називають лідерами суміжних класів. Як наслідок, лідери – це комбінації, які в суміжних класах мають найменшу вагу.

Нехай дискретним каналом, що між X та Y, є дискретний симетричний канал без пам'яті з імовірністю помилки $p < 0{,}5$. Тоді існує імовірність того, що з усіх 2^n комбінацій помилок E^n_{si} знайдуться такі, що не належатимуть до 2^{n-k} лідерів суміжних класів $E^n_{si} \neq E'^n_s$.

Це ті помилки, які код не може виправляти. Ними є випадкові $E^n_{si} \neq E'^n_s$, де $i \neq 1$. Помилки ж $E^n_{s1} = E'^n_s$ є комбінаціями нулів та одиниць, що виправляються кодом.

При передачі даних по каналу $X \rightarrow Y$ на виході з'являються послідовності:

$$Y^n_{gl} = (y_1, y_2, ..., y_n) = X^n_i \oplus E^n_{sj}, \tag{4.3.4}$$

де $g = 1, 2, 3, \ldots, 2^{n-k}$, $l = 1, 2, 3, \ldots, 2^k$, $j = 1, 2, 3, \ldots, 2^k$.

В результаті цього X^n_i перейде необов'язково в Y^n свого i-го стовпця на рис. 4.3.2, а в будь-який інший Y^n_{gl}. При цьому виправлення помилки, що здійснюватиметься при декодуванні, буде пов'язане з переходом Y^n_{gl} в Y^n_{1l} та B^k_l, які можуть не співпадати з X^n_i та A^k_i. А це означає, що помилка не виправлена, тобто $\mathrm{A}^k_i \neq \mathrm{B}^k_l$.

Тому, аналогічним чином, як для каналу $X \rightarrow Y$, опис якого виражено формулою (4.3.4), можна описати й канал $\mathrm{A} \rightarrow \mathrm{B}$:

$$\mathrm{B}^k_l = \mathrm{A}^k_i \oplus \Gamma^k_j, \tag{4.3.4}$$

де Γ^k_j – послідовність помилок довжини k, яка відрізняє A^k_i від B^k_l, $\Gamma^k_j = (\gamma_1, \gamma_2, \gamma_3, \ldots, \gamma_k)$, $\gamma = \{0, 1\}$, $j = 1, 2, \ldots, 2^k$.

Як очевидно, імовірність помилки p, що має місце в каналі $X \rightarrow Y$, $p = p$ ($e = 1$), сукупно зі здатністю коду щодо виправлення в ньому помилок, визначають еквівалентну імовірність помилки $p_{екв.}$, що має місце в каналі $\mathrm{A} \rightarrow \mathrm{B}$, $p_{екв} = p$ ($\gamma = 1$).

Таким чином, під еквівалентною імовірністю помилки в каналі витоку будемо розуміти таку імовірність, яка з урахуванням надлишковості джерела забезпечуватиме таку ж пропускну здатність, як і для безнадлишкових джерел.

Знайдемо зв'язок $p_{екв}$ з p. Для цього скористаємося стандартним розташуванням завадостійкого коду в суміжних класах.

Імовірність помилки є показником, який в середньому характеризує можливість появи цієї помилки. Тому безперечно очевидно, що цю імовірність можна виразити як математичне сподівання ваги $wt(\Gamma^k_j)$, поділеної на довжину k комбінацій Γ^k_j:

$$p(\gamma = 1) = \frac{1}{k} \sum_{j=1}^{2^k} wt(\Gamma^k_j) p(\Gamma^k_j), \tag{4.3.5}$$

де $p(\Gamma^k_j)$ – імовірність комбінації еквівалентних помилок Γ^k_j.

В свою чергу нескладно побачити, що

$$p(\Gamma_j^k) = \sum_{g=1}^{2^{n-k}} p(E_{gj}^n), \tag{4.3.6}$$

де $p(E^n_{gj})$ – імовірність комбінації помилок E^n_{gj} в стандартному розташуванні коду:

$$p(E_{gj}^n) = p^{wt(E_{gj}^n)}(1-p)^{n-wt(E_{gj}^n)}, \tag{4.3.7}$$

$wt(E^n_{gj})$ – вага комбінації помилок E^n_{gj}, визначається стандартним розташуванням коду.

Підставивши співвідношення (4.3.7) в (4.3.6) та (4.3.6) в (4.3.5), отримаємо остаточну формулу для еквівалентної помилки $p\,(\alpha \neq \beta)$ відносно $p\,(x \neq y)$:

$$p_{екв.} = \frac{1}{k}\sum_{j=1}^{2^k} wt(\Gamma_j^k)\sum_{g=1}^{2^{n-k}} p^{wt(E_{gj}^n)}(1-p)^{n-wt(E_{gj}^n)}. \tag{4.3.8}$$

Таким чином, обґрунтовано еквівалентну імовірність помилки в каналі із завадостійким кодуванням, яка є коригованою імовірністю, що утворюють в каналі завади. Коригування здійснюється на основі представлення завадостійких кодів в стандартному розташуванні суміжних класів з врахуванням перерозподілу імовірностей по всім комбінаціям можливих помилок

Контрольні питання.

1. Комбінації помилок в каналі, що можуть виправлятися та не можуть виправлятись завадостійким кодом.
2. Еквівалентна помилка в каналі із завадостійким кодом.
3. Імовірність еквівалентної помилки в каналі із завадостійким кодом.

4.4. Коригування імовірності помилки в каналі витоку для надлишкових джерел. Смисловий відрізок повідомлення

Побудова схеми оптимальної обробки даних в каналі витоку для надлишкових джерел. Смисловий відрізок повідомлення та еквівалентна імовірність помилки в каналі. Раніше було розглянуто канал з корекцією помилок завадостійким кодуванням (див. рис. 4.1.1). Було розглянуто

різновиди лінійних блочних кодів, для яких побудовано стандартне розташування коду в суміжних класах.

Сам код (нульовий суміжний клас) $X^n_i = (x_1, x_2, x_3, \ldots, x_n)$ був побудованим шляхом перебору всіх комбінацій $A^k_i = (\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_k)$, довжиною k, де $\alpha = \{0, 1\}$, i – номер комбінації, $i = 1, 2, \ldots, 2^k$, $n > k$, які може виробляти джерело. Цими ж комбінаціями і є вихідні комбінації знаків з декодера $B^k_l = (\beta_1, \beta_2, \beta_3, \ldots, \beta_k)$, $\beta = \{0, 1\}$, $l = 1, 2, \ldots, 2^k$ тієї ж довжини.

Суміжні класи будувалися відповідно до адитивності впливу помилок в каналі поміж X та Y, де з них вибрано найбільш імовірні. Слід зазначити, що для каналів зв'язку, де імовірність помилки $p << 0{,}5$, найбільш імовірними комбінаціями помилок є ті, що мають меншу вагу. Це нескладно перевірити за допомогою нерівності:

$$(1-p)^n > p(1-p)^{n-1} > \ldots > p^{wt}(1-p)^{n-wt} > \ldots > p^{n-1}(1-p) > p^n . \qquad (4.4.1)$$

Стандартне розташування (n, k) коду в суміжних класах мало вигляд, як показано на рис. 4.2.1. На стандартному розташуванні:

E'^n_s – комбінації помилок, що виправляються кодом, $s = 1, 2, 3, \ldots, 2^{n-k}$,

S^{n-k}_s – синдром суміжного класу, якому відповідає комбінації помилок E'^n_s. По суті синдром є номером суміжного класу, що виражений у двійковому обчисленні.

У каналі на вхідну послідовність X^n_i накладається комбінація помилок E^n_s, де $s = 1, 2, 3, \ldots, 2^n$:

$$Y^n_{gl} = (y_1, y_2, \ldots, y_n) = X^n_i \oplus E^n_s , \qquad (4.4.2)$$

Слід звернути увагу, що комбінацій E^n_s в 2^k разів більше, ніж E'^n_s, тому декодер може виправляти не всі помилки, а лише частину найбільш імовірних 2^{n-k} з усіх можливих 2^n.

Для *технічних каналів витоку* має місце природна надлишковість джерел, правила формування якої здебільшого можуть бути невідомими. Як вже було показано, ця надлишковість може дозволити виправлення помилок, тому нею при обґрунтуванні захищеності інформації від витоку технічними каналами неможна нехтувати. Тому виникає питання, як її врахувати в захищеності, здійснити перерозрахунок потрібної помилки p в каналі $X \to Y$ відносно гранично допустимої $p_{\text{екв.}}$ в каналі $A \to B$.

Для цього скористаємося досвідом подібних оцінювань для каналів зв'язку.

Так, за аналогією з каналом зв'язку технічний канал витоку з надлишковим джерелом можна представити у вигляді дискретного каналу, як показано на рис. 4.4.1.

Надлишкове джерело витоку інформації представлене сукупністю двох складових:

– це безнадлишкове джерело, яке уявно інформує про стан матеріальної системи, безнадлишковим кодом $\alpha^{n'}_{k} = (\alpha_1, \alpha_2, \ldots, \alpha_{n'})$, де $\alpha \in \{0, 1\}$, $k = 1 \div 2^{n'}$. Тобто, якщо система має $2^{n'}$ станів, то для інформування про них безнадлишкове джерело має використати двійкове повідомлення довжиною не більше ніж n'.

– це "кодер", який уявно вносить надлишковість до безнадлишкової послідовності $\alpha^{n'}_{k}$, в результаті чого утворюється послідовність X^{n}_{k} більшої довжини n ($n > n'$). Різниця поміж n та n' і визначає цю надлишковість.

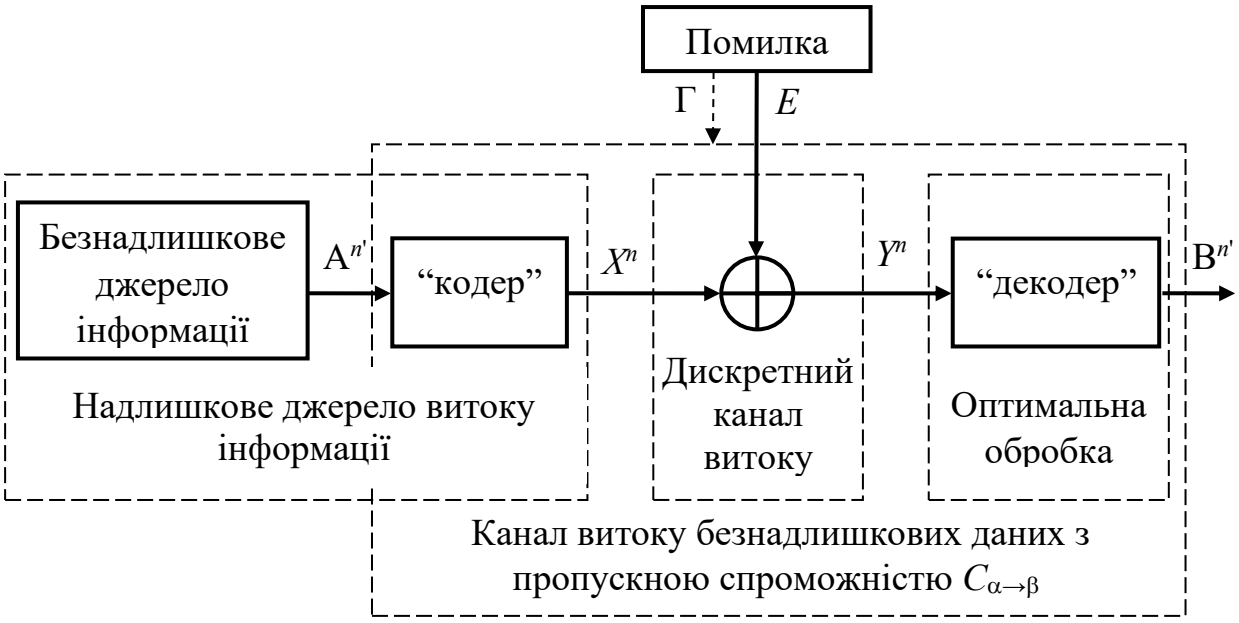


Рис. 4.4.1. Дискретний канал витоку інформації від надлишкових джерел

Сукупність уявного безнадлишкового джерела та уявного "кодера" являє собою реальне надлишкове дискретне джерело. При цьому, вочевидь, правило кодування в більшості випадків для смислових джерел може бути невідомим. Виключенням зазначеного може бути навмисне внесення надлишковості завадостійким кодуванням, або повтором передачі.

Дискретний канал витоку інформації являє собою засіб для проходження надлишкових комбінацій X^{n}_{k} у вихідні Y^{n}_{l}. Він утворюється шляхом витоку неперервних процесів, що реалізують дані x, через середовище із завадою за рахунок побічних електромагнітних випромінювань, їх наведень на сторонні провідники та технічні засоби, просочування в ланцюги заземлення та електроживлення тощо.

Передбачається, що вироблений на виході дискретного каналу y є результатом вирішення схемою чи алгоритмом оптимального приймача щодо того, який знак x був вироблений джерелом. Зазначене вирішення здійснюється на основі статистичної та іншої обробки суміші небезпечного сигналу, реалізація якого відповідає знаку x, та маскувальної завади в середовищі при перехопленні інформації. Як правило, для усереднення показників, що характеризують передачу даних в каналах, перехід $x \to y$ прийнято апроксимувати дискретним симетричним каналом без пам'яті, як це вже було показано раніше для каналів зв'язку.

Завданням "декодера" є "декодування" – обробка повідомлення Y^n так, щоб з нього можливо було добути корисну для противника-зловмисника інформацію. Це відомості $A^{n'}_k$, щодо формування яких на схемі заміщення технічного каналу витоку інформації (див. рис. 4.4.1) має призначення безнадлишкового джерела. Зазначене джерело є дійсно уявним, оскілки в матеріальному сенсі його не існує. Це джерело є певним еквівалентом для уявлення та представлення тільки корисних відомостей у безнадлишковому вигляді, щодо яких і здійснюється перехоплення. Адже реальні джерела смислової інформації та вироблені ними послідовності даних X^n_k поряд з корисними відомостями можуть містити й інші (некорисні відомості), які не є цікавими для перехоплення, але захаращують дані $A^{n'}_k$ в послідовності X^n_k.

Очевидно, що для каналу на рис. 4.4.1 також можна побудувати схему обробки, що є аналогічною до стандартного розташування коду в суміжних класах.

Однак, через відсутність відомостей щодо правила кодування необхідне певне нововведення.

1. Довжина смислового відрізка n_0, яка для стандартного розташування має бути прирівненою до довжини послідовності X^n, тобто $n_0 = n$. Вона має визначатись експертом відповідно до технічних та технологічних можливостей статистичної обробки комбінації даних.

2. Довжина відрізку n' послідовності $A^{n'}$ може визначатися величиною відносної надлишковості ρ ($\rho < 1$) за формулою:

$$n' = \rho \times n \,. \tag{4.4.3}$$

3. Критерій побудови схеми обробки даних, яка має бути найкращою з точки зору перехоплення, має вигляд:

$$p(\beta/\alpha) \underset{\alpha=\beta}{\to} \max \,. \tag{4.4.4}$$

Критерій (4) випливає з наступного:

– з критерію оптимальності Котельникова – максимуму апостеріорної імовірності:

$$p(\alpha/\beta) \underset{\alpha=\beta}{\rightarrow} \max, \tag{4.4.5}$$

– з рівноймовірності знаків для безнадлишкового джерела А:

$$p(\alpha = 1) = p(\alpha = 0) = \frac{1}{2}, \tag{4.4.6}$$

– з формули Байєса випливає:

$$p(\alpha/\beta) = \frac{p(\alpha)p(\beta/\alpha)}{\sum\limits_{\alpha} p(\alpha)p(\beta/\alpha)} = \frac{\frac{1}{2}p(\beta/\alpha)}{\sum\limits_{\alpha} \frac{1}{2}p(\beta/\alpha)} = p(\beta/\alpha), \tag{4.4.7}$$

Слід звернути увагу, що здійснені нововведення ще не дозволяють побудувати схему оптимальної обробки даних аналогічно до схеми декодування в суміжних класах для відомих кодів (див. рис. 4.4.2).

Потрібно також зазначити, що побудова таких оптимальних схем взагалі є проблемою пошуку ефективних завадостійких кодів, що відповідатимуть теоремі щодо сферичної упаковки в теорії завадостійкого кодування.

Слід підкреслити, що пошуку досконалих завадостійких кодів була приділена увага багатьох вчених світу, зокрема Хеммінга, Боуза, Чоудхурі, Хоквінгема, Галлея та інших.

Тому будемо передбачати, що нехай ця схема все таки існує і нехай ця схема використовує найкращий завадостійкий код.

Якщо схема декодування для надлишкових джерел існує, то з її урахуванням можна знайти еквівалентну імовірність помилки $p_{екв.} = p\ (\alpha \neq \beta)$ відносно $p = p\ (x \neq y)$ за формулою:

$$p_{екв.} = \frac{1}{n'} \sum_{j=1}^{2^{n'}} wt(\Gamma_j^{n'}) \sum_{g=1}^{2^{n-n'}} p^{wt(E_{gj}^n)} (1-p)^{n-wt(E_{gj}^n)}. \tag{4.4.8}$$

Побудова ж схеми розташування E_{gj}^n, $j = 1, 2, 3, \ldots, 2^{n'}$, $g = 1, 2, 3, \ldots, 2^{n-n'}$ з метою визначення розподілу ваг у стовпцях та рядках $wt(E_{gj}^n)$ (див. рис. 4.2.1) щодо формули (4.4.8) для розмірностей кодів, що не існують, залишається відкритим питанням.

Отже, здійснено огляд підходу щодо коригування імовірності помилки в каналі витоку для надлишкових джерел. Для цього має місце необхідність побудови схеми оптимальної обробки даних. Для побудови схеми має біти означено смисловий відрізок повідомлення. Наявність

схеми оптимальної обробки дозволяє коригування імовірності помилки в каналі та знаходження відповідної еквівалентної імовірності помилки для надлишкових джерел.

Контрольні питання.

1. Схема оптимальної обробки даних в каналі витоку для надлишкових джерел.
2. Смисловий відрізок повідомлення Еквівалентна помилка в каналі із завадостійким кодом.
3. Коригування імовірності помилки в каналі та еквівалентна імовірність помилки для надлишкових джерел.

ЗАКЛЮЧЕННЯ

У навчальному посібнику наведений ризик-орієнтований підхід щодо обґрунтування умов захищеності інформації від витоку технічними каналами, які утворюються завдяки побічним ефектам у фізичних середовищах навколо джерела витоку. Здійснено огляд особливостей захисту найпоширеніших видів джерел, якими є мовні, візуальні та цифрові джерела витоку інформації.

Наведені показники захищеності інформації від витоку та обґрунтовано їхній взаємозв'язок. Це імовірність ризику як загальний показник інформаційної безпеки для всіх видів джерел. Це окремі імовірнісні показники щодо особливостей джерел витоку інформації – розбірливість для мовних джерел, розпізнання для візуальних джерел та пропускна здатність технічного каналу витоку для цифрових джерел витоку інформації. Це окремі енергетичні показники відношення сигнал/завада на вході приймача перехоплення з урахуванням особливостей небезпечних сигналів.

Оглянуто підхід щодо коригування імовірності помилки в технічному каналі для надлишкових джерел, оскільки надлишковість може виправляти помилки й тим самим знижувати захищеність інформації від витоку.

Матеріал посібника є основою для отримання знань щодо розуміння процесу забезпечення захисту інформації від витоку технічними каналами та може бути використаний для подальшого освоєння методик спеціальних досліджень та інструментального контролю об'єктів інформаційної діяльності й засобів обробки інформації. Матеріал також може бути корисним для розроблення нових інформаційних технологій та впровадження автоматизації управління кібербезпекою та інформаційною безпекою щодо витоку інформації технічними каналами.

СПИСОК ВИКОРИСТАНОЇ ТА РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Богуш В.М. Технічний захист інформації: теоретичні основи та організаційно-технічне забезпечення: Навч. посібник. /Богуш В.М., Бровко В.Д., Кобус О.С., В.Д. Козюра В.Д./ К.: Видавництво Ліра-К, 2023. 484 с. [https://knushop.com.ua/image/catalog/lira20230617/pdf/13054.pdf?srsltid=AfmBOoqh2qiMOOTgBdpwtoqKHBSgasmzG4lOhVuKNBdc-mvcvigt7CyL]

2. Гребенюк А.М. Основи управління інформаційною безпекою: Навч. посібник. / Гребенюк А.М., Рибальченко Л.В./ Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. 144 с. [https://vstup.htek.com.ua/wp-content/uploads/2024/10/34.1-Grebenyuk.pdf]

3. Гусєв О. Ю. Теорія електричного зв'язку: Навч. посібник. /Гусєв О. Ю., Конахович Г. Ф., Корнієнко В. І., Кузнецов Г. В., Пузиренко О. Ю./ Львів: «Магнолія 2006», 2024. 364 с. [https://magnolia.lviv.ua/wp-content/uploads/2024/04/Teoriia-elektr.zviazku_zmist.pdf]