Предполагая без потери общности, что ЛССОИ являются подсистемами комплексной или интегрированной системы безопасности и выполняют различные задачи, можно считать, что состояние тревоги имеет место при выполнении $p_{ij} \geq Q_{ij}$, где значение порога определяется алгоритмом работы ЦССОИ.

Заметим, что в общем случае должны быть введены временные окна анализа состояния УОУ при принятии решения на среднем уровне СБ – ЛССОИ.

Кроме того, зачастую необходимо учитывать приоритетность тех или иных событий в системе, точнее приоритетность реакции системы противодействия и ликвидации угроз на решения отдельных уровней системы по обнаружению угроз защищаемому объекту. В общем случае порядок приоритетов может не совпадать с порядком системных уровней. Разные события на одном уровне могут иметь разный приоритет и, наоборот, события на разных уровнях – одинаковый приоритет.

Литература: 1. В. В. Волхонский. Устройства охранной сигнализации. Изд. 2 допол. и перераб. Экополис и культура. СПб., 2000, 312 с. 2. Волхонский В. В. Системы охранной сигнализации. Экополис и культура, СПб, 2000, 164 с. 3. Волхонский В. В. Устройства охранной сигнализации. Часть 1. Извещатели. Изд. 3 допол. и перераб. Экополис и культура, СПб, 2001, 239 с.

УДК 621.395, 621.391.82

МЕТОД ЗАХИСТУ ЦІЛІСНОСТІ ІНФОРМАЦІЇ, ЩО ПЕРЕДАЄТЬСЯ В СИСТЕМАХ АБОНЕНТСЬКОГО РАДІОДОСТУПУ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Олександр Корнейко, Олексій Кувшинов, Сергій Лівенцев

Військовий інститут телекомунікацій та інформатизації НТУУ "КПІ"

Анотація: **Запропоновано метод забезпечення цілісності інформації в системах абонентського радіодоступу спеціального призначення з псевдовипадковим перестроюванням робочої частоти. В основу методу покладено структурну адаптацію системи передачі інформації. Наведені рекомендації з побудови захищених систем абонентського радіодоступу. Отримані аналітичні вирази дозволяють визначити ступінь руйнування цілісності інформації, переданої в системах зв'язку спеціального призначення в умовах впливу найгірших завад.**

Summary: **In this task was offered the method of maintenance of integrity of the information in systems of user's radioaccess of special purpose with pseudo-casual reorganization of working frequency. In a basis of a method was fixed the structural adaptation of system of transfer of the information. There were given the recommendations from construction of the protected systems of user's radioaccess. In this fask were received the analytical expressions allowing to define a degree of destruction of integrity of the information transferred in systems of communication of special purpose in conditions of influence of the worst handicapes.**

Ключові слова: **Цілісність, захищеність, інформація, абонентський радіодоступ, псевдовипадкове перестроювання робочої частоти (ППРЧ), навмисні завади.**

I Вступ

Інформаційна безпека відіграє важливу роль у забезпеченні життєво важливих інтересів будь-якої держави. Створення розвинутого і захищеного інформаційного середовища є невід'ємною умовою розвитку суспільства. Поряд з цим необхідно створення систем керування, які забезпечують мінімальний ризик інформації, що пов'язаний з можливістю нанесення збитків власникам інформації (державі, юридичним особам усіх форм власності і громадянам) у результаті впливу природних і навмисних завад, незаконного її одержання і/або спотворення.

Розвиток захищеного радіозв'язку є невід'ємною частиною підвищення ефективності систем керування і передачі інформації рухомим об'єктам. Радіозв'язок характеризується зростаючими потребами в обміні цифровою інформацією з мобільними і віддаленими абонентами, які у сукупності утворюють територіально розподілені інформаційно-обчислювальні й інформаційно-керуючі мережі.

Актуальність застосування захищених радіомереж пояснюється об'єднанням переваг системи радіозв'язку, яка має загальне середовище поширення радіохвиль для всіх користувачів, з перевагами інформаційних мереж з комутацією повідомлень, заснованих на розгалуженій обчислювальній інфраструктурі.

Багаторівнева організація керування процесами в мережі породжує необхідність модифікувати на кожному рівні передачі повідомлення стосовно функцій, реалізованих на цьому рівні. Транспортний рівень забезпечує інтерфейс між мережею передачі даних і верхніми трьома рівнями еталонної моделі взаємодії відкритих систем (ЕМВВС) [1]. Саме цей рівень надає користувачу факультативні можливості одержання сервісу визначеної якості (і вартості) від самої мережі (тобто мережного рівня).

Система інформаційної безпеки телекомунікаційних мереж повинна бути реалізована у виді комплексу програмно-технічних засобів і організаційних (процедурних) рішень з захисту інформації від несанкціонованого доступу і складатися з таких функціональних підсистем.

1. Керування доступом.
2. Реєстрації й обліку.
3. Криптозахисту.
4. Забезпечення цілісності даних.

Одним із критеріїв захищеності є збереження цілісності інформації [2]. Цілісність забезпечується шляхом дотримання вимог політики безпеки при переміщенні інформації до об'єкта з боку користувача або процесу. Цілісність при обміні дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, яка міститься в них, при їх експорті/імпорті через незахищене середовище. Найчастіше дана послуга реалізується з використанням таких механізмів криптографічного захисту, як цифровий підпис і коди автентифікації повідомлень.

Найчастіше стан цілісності визначається на рівні користувача, тобто сьомому рівні ЕМВВС. Стосовно мобільного радіозв'язку ЕМВВС поділяється на два укрупнених шари. Верхній – охоплює рівні, безпосередньо не пов'язані з наданням доступу. Нижній – забезпечує обслуговування всіх елементів системи, пов'язаних з організацією радіозв'язку і забезпеченням доступу.

II Постановка задачі

Типова схема канального кодера передавальної частини системи безпровідного абонентського доступу подана на рис. 1.

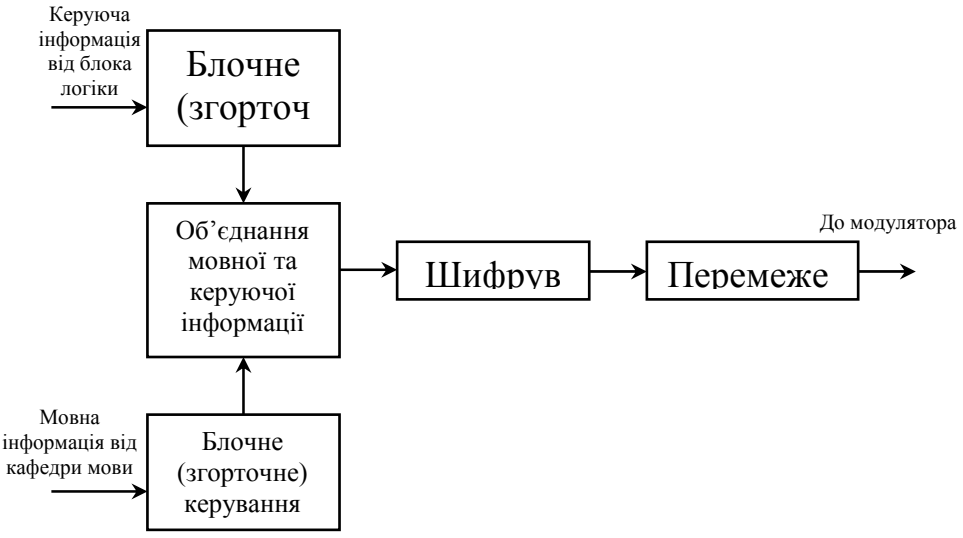

Рисунок 1 – Схема канального кодера передавальної частини системи безпровідного абонентського доступу

Якщо користувач забезпечує цілісність і вірогідність пакетів даних, запропонована система може надавати «прозорий» канал зв'язку, не вносячи додаткових символів коректувального коду. Якщо користувач не забезпечує вірогідність інформації власними засобами, то використовується система завадостійкого кодування і структурної адаптації системи. При цьому запропоновано контроль стану цілісності інформації здійснювати на транспортному рівні. Як відомо, транспортний протокол визначає п'ять класів. Далі будуть розглянуті мережні з'єднання класу 4 типи *B* [1].

Задачею, яка розв'язується в роботі, є розробка методу забезпечення цілісності інформації, переданої в системах абонентського радіодоступу спеціального призначення з псевдовипадковим перестроюванням робочої частоти (ППРЧ). У системах з ППРЧ розширення спектра в межах заданої смуги частот здійснюється

за допомогою стрибкоподібної зміни частоти сигналу за псевдовипадковим законом, який невідомий постановнику завад [3, 4].

Для забезпечення цілісності інформації переданої в мережах зв'язку спеціального призначення пропонується використання додаткового блоку кодування (рис. 2).

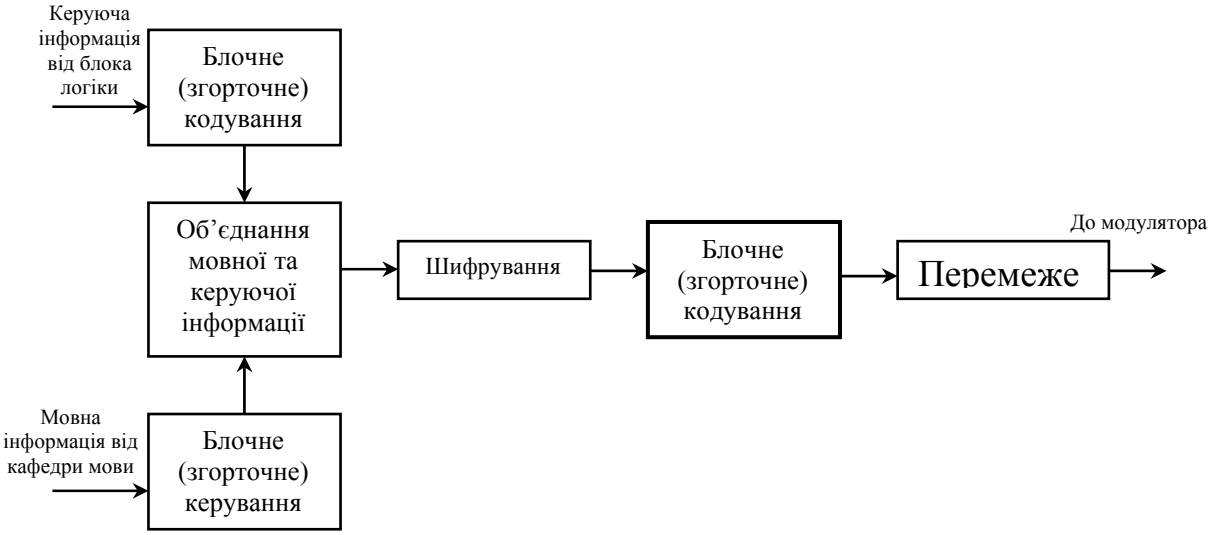

Рисунок 2 – Схема канального кодера передавальної частини схеми з додатковим блоком кодування

Проблема забезпечення цілісності інформації при передачі за допомогою некриптографічних методів обумовлена тим, що в каналах передачі даних систем спеціального призначення використання криптографічних методів захисту інформації не завжди є ефективним, оскільки збільшується час на закриття і відкриття інформації, що приводить до роботи в режимі псевдореального часу, що не завжди припустимо.

У системах абонентського радіодоступу спеціального призначення з ППРЧ основною проблемою є забезпечення захисту повідомлень від несанкціонованої модифікації інформації, яка міститься в них, при їх передачі через незахищене середовище.

III Визначення кількісної міри оцінки цілісності інформації

Система зв'язку має в максимальному ступені враховувати розмаїтість можливих завад і, зокрема, швидкість зміни параметрів завади. У будь-яких стаціонарних каналах найбільшу захищеність забезпечують адаптивні системи зв'язку, що змінюють структуру сигналу і метод його обробки відповідно до стану каналу.

Визначимо кількісну міру оцінки цілісності інформації. Для цього скористаємося основами теорії інформації, викладеними К. Шенноном [5].

Наявність у каналі завад призводить до спотворення переданих сигналів і, отже, до руйнування переданої інформації.

Процес втрати інформації наочно ілюструє рис. 3. Тут $H_{\text{повн}}$ – продуктивність джерела повідомлень, $H_{\text{ціл}}$ – повна власна інформація про прийнятий сигнал за одиницю часу (визначає її цілісність). Величина H_1 являє собою міру «витоку» інформації при проходженні через канал зв'язку, а H_2 – міра передачі сторонньої інформації не має відносини до джерела і створюваної присутніми в каналі завадами.

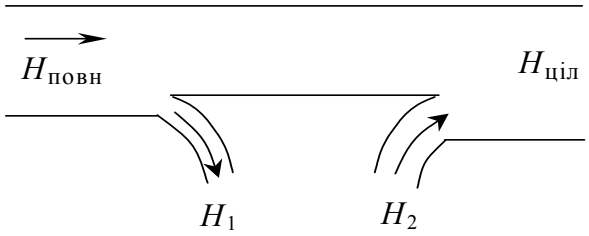

Рисунок 3 – Модель процесу втрати інформації

Тоді величина цілісності інформації визначається

$$H_{\text{ціл}} = H_{\text{повн}} - H_1 + H_2 . \quad (1)$$

Приймаючи значення продуктивності джерела повідомлень $H_{\text{полн}} = 1$, можна розрахувати нормований коефіцієнт цілісності інформації

$$K_{\text{ціл}} = 1 - \Delta H , \quad (2)$$

де ΔH – враховує втрати інформації в каналі зв'язку.

При передачі цифрових сигналів для двійкового симетричного каналу зв'язку величина ΔH розраховується за формулою [6]

$$\Delta H = -(P_{\text{пом}} \log P_{\text{пом}} + (1 - P_{\text{пом}}) \log(1 - P_{\text{пом}})), \quad (3)$$

де $P_{\text{пом}}$ – імовірність помилкового приймання двійкового символу.

Тоді вираз (2) можна переписати у вигляді

$$K_{\text{ціл}} = 1 + P_{\text{пом}} \log P_{\text{пом}} + (1 - P_{\text{пом}}) \log(1 - P_{\text{пом}}). \quad (4)$$

Коефіцієнт цілісності може приймати значення $0 \le K_{\text{ціл}} \le 1$ при $0{,}5 \ge P_{\text{пом}} \ge 0$.

Таким чином, отриманий вираз дозволяє оцінити цілісність інформації при передачі через незахищене середовище.

Розглянемо коефіцієнт цілісності для системи зв'язку без ППРЧ при некогерентному прийманні сигналів з відносною фазовою маніпуляцією. Як відомо імовірність помилкового прийому елемента сигналу дорівнює [4]:

$$P_{\text{пом}} = \frac{1}{2} e^{-Q^2} .$$

де $Q^2 = E_{\text{с}} / G_0$ – відношення енергії сигналу до спектральної щільності потужності власних шумів приймача.

Тоді

$$K_{\text{ціл}} = 1 + \frac{1}{2} e^{-\frac{1}{2}Q^2} \log\left(\frac{1}{2} e^{-\frac{1}{2}Q^2}\right) + \left(1 - \frac{1}{2} e^{-\frac{1}{2}Q^2}\right) \log\left(1 - \frac{1}{2} e^{-\frac{1}{2}Q^2}\right). \quad (5)$$

IV Розрахунок коефіцієнта цілісності інформації в системі передачі з ППРЧ

Для системи зв'язку з ППРЧ ймовірність помилкового приймання елемента сигналу буде визначатися не тільки видом маніпуляції але і видом завад. Так при некогерентному прийманні сигналів з відносною фазовою маніпуляцією в умовах впливу шумової завади в частині смуги [7]

$$P_{\text{пом}} = \frac{1}{2} \gamma e^{-\left(\frac{G_0}{E_{\text{с}}} + \frac{P_{\text{з}}}{\gamma K_{\text{с}} P_{\text{с}}}\right)^{-1}} + \frac{1}{2}(1 - \gamma) e^{-Q^2} , \quad (6)$$

де $K_{\text{с}} = \Delta f_{\text{с}} / \Delta F_{\text{с}}$ – коефіцієнт розширення спектра сигналу;

γ – коефіцієнт, який характеризує частину смуги пропускання системи передачі, займаної завадою ($0 \le \gamma \le 1$);

$\Delta F_{\text{с}} = 1/\tau_{\text{і}}$ – ширина спектра первинного інформаційного сигналу;

$\tau_{\text{і}}$ – тривалість імпульсу первинного сигналу;

$P_{\text{с}} = E_{\text{с}}/\tau_{\text{і}}$ – потужність сигналу;

$P_{\text{з}}$ – потужність шумової завади.

Якщо врахувати вирази (4) і (6) $K_{\text{ціл}}$ можна визначити як

$$K_{\text{ціл}} = 1 + \left(\frac{1}{2}\gamma e^{-\left(\frac{G_0}{E_c} + \frac{P_з}{\gamma K_c P_c}\right)^{-1}} + \frac{1}{2}(1-\gamma)e^{-Q^2} \right) \times \log\left(\frac{1}{2}\gamma e^{-\left(\frac{G_0}{E_c} + \frac{P_з}{\gamma K_c P_c}\right)^{-1}} + \frac{1}{2}(1-\gamma)e^{-Q^2} \right) +$$

$$+ \left(1 - \frac{1}{2}\gamma e^{-\left(\frac{G_0}{E_c} + \frac{P_з}{\gamma K_c P_c}\right)^{-1}} + \frac{1}{2}(1-\gamma)e^{-Q^2} \right) \log\left(1 - \frac{1}{2}\gamma e^{-\left(\frac{G_0}{E_c} + \frac{P_з}{\gamma K_c P_c}\right)^{-1}} + \frac{1}{2}(1-\gamma)e^{-Q^2} \right) \quad (7)$$

На рис. 4 побудовані графіки залежності $K_{\text{ціл}}(\gamma)$ при Q^2 = 10,34 дБ (що відповідає значенню імовірності помилки $P_{\text{пом}} = 10^{-5}$ при відсутності завад) для різних значень $Q^2_{\text{екв}} = \frac{K_c P_c}{P_з}$.

Таким чином, при впливі шумової завади в частині смуги для будь-якого відношення сигнал/завада існує оптимальне значення частини смуги пропусканняння $\gamma_{\text{опт}}$, при якій коефіцієнт цілісності інформації в системі передачі з ППРЧ буде мінімальним.

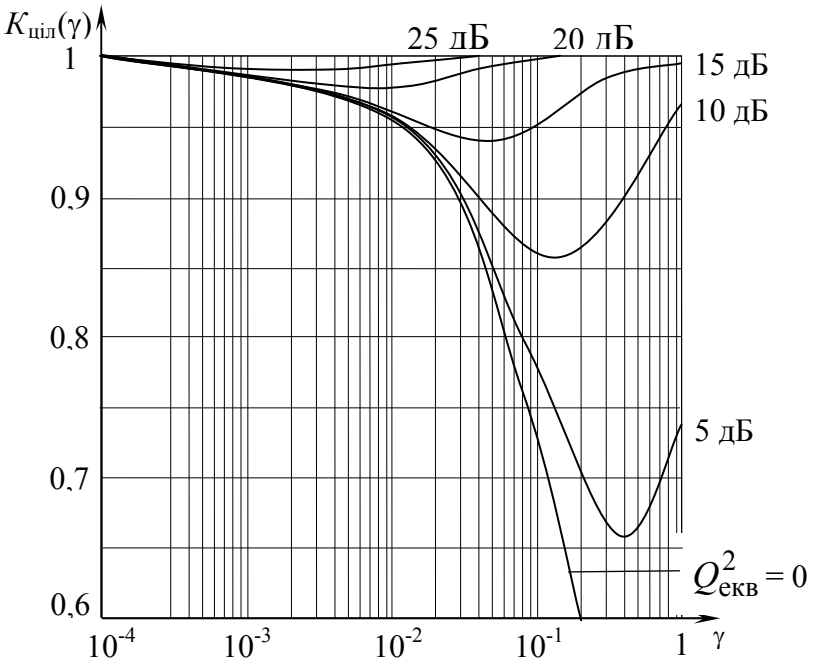

Рисунок 4 – Залежність коефіцієнта цілісності від коефіцієнта γ

При зниженні величини коефіцієнта цілісності інформації нижче припустимого рівня може бути застосована структурна адаптація системи передачі, що дозволяє істотно підвищити захищеність переданої інформації.

V Побудова системи зі структурною адаптацією

Наявність зворотного зв'язку при передачі повідомлень дозволяє здійснити послідовну процедуру аналізу стану каналу, а також дає можливість одержати на передавальній стороні дані про стан цілісності інформації. Використовуючи ці дані можна побудувати різні адаптивні системи передачі інформації зі структурною адаптацією.

Варіант структурної схеми системи передачі з ППРЧ зі структурною адаптацією зображений на рис. 5. Каналом зворотного зв'язку передається прийнятий сигнал $c'(t)$, який у пристрої визначення коефіцієнта цілісності, порівнюється з переданим. Після цього обчислюється значення $K_{\text{ціл}}$, по величині якого і здійснюється адаптація.

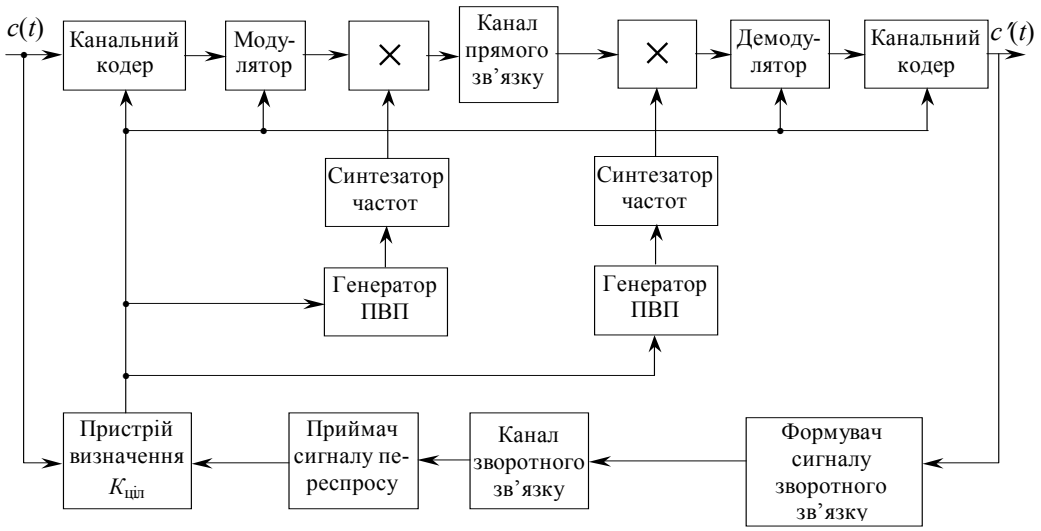

Рисунок 5 – Структурна схема системи передачі з ППРЧ зі структурною адаптацією

Як видно з рис. 5 залежно від стану цілісності інформації в системі передачі з ППРЧ може бути змінена метод кодування і декодування, вид сигналу (вид модуляції) або порядок чергування частот, обумовлений генератором псевдовипадкової послідовності.

VI Висновки

Таким чином, отримані аналітичні вирази дозволяють визначити ступінь руйнування цілісності інформації, переданої в системах зв'язку спеціального призначення в умовах впливу навмисних завад, а також визначити доцільність методу некриптографічного захисту цілісності інформації.

При зниженні величини коефіцієнта цілісності інформації нижче припустимого значення може бути застосована структурна адаптація системи передачі інформації, що дозволяє істотно підвищити захищеність переданої інформації. У системах передачі з виправленням помилок в принципі можна одержати коефіцієнт цілісності інформації близький до одиниці, але при цьому необхідно використовувати коди з великими коригувальними здібностями.

Оптимальна система зв'язку повинна складатися з прямого і зворотного каналів зв'язку, призначених для передачі як основних повідомлень, так і вимірювальної інформації і команд. Така система має містити в своєму складі пристрій обробки вимірювальної інформації, що формує сигнали керування, які оптимізують структуру сигналу (кодування), тобто бути адаптивною.

Для підвищення вірності рекомендується застосування максимально можливого числа засобів: змінюваного кодека в сполученні зі змінюваним алгоритмом перезапиту і явним рознесенням змінюваної кратності, що залежать від мінливих умов передачі і приймання.

При адаптації за структурою сигналів важливу роль здобувають адаптивні (змінювані) параметри: надлишковість коду, глибина перемеження, кількість використовуваних частот, затримка, рівні і розташування порогів м'якого декодеру, потужність ансамблю широкосмугового сигналу.

Найбільш перспективним є комбінований метод адаптації, який використовує спільно оптимальні вид сигналу і вид кодування. Це не тільки підвищує захищеність інформації, яка циркулює в каналах керування від несанкціонованого доступу, але робить систему зв′язку менш сприйнятливою до завад природного і навмисного характеру.

Можна сформулювати наступні рекомендації з побудови систем абонентського радіодоступу спеціального призначення:

1. Використовуючи вираз (4), оцінити цілісність інформації при передачі через незахищене середовище для прийняття рішення стосовно структури системи передачі.

2. У системі абонентського радіодоступу спеціального призначення має бути присутнім зворотний зв'язок по величині коефіцієнта цілісності інформації.

3. Система абонентського радіодоступу спеціального призначення має бути адаптивною стосовно ступеня зміни коефіцієнта цілісності інформації.

4. Як адаптивний параметр може використовуватися вид модуляції, режим роботи ППРЧ, метод кодування і декодування або комбінована зміна перерахованих параметрів.

Література: 1. Горелов Г. В., Казанский Н. А., Кудряшов В. А., Ромашкова О. Н. Цифровые телекоммуникационные сети / Под ред. Г. В. Горлова, Г. И. Загария. – Харьков: ХФИ "Транспорт Украины", 2000. – 216 с. 2. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемшин А. В. Основы криптографии : Учебное пособие. – М.: Гелиос, 2001. – 480 с. 3. Варакин Л. Е. Системы связи с шумоподобными сигналами. – М.: Радио и связь, 1985. – 364 с. 4. Бабич В. Д., Кувшинов О. В., Лежнюк О. П., Лівенцев С. П. Завадостійкість каналів зв'язку : Навчальний посібник. – К.: КВІУЗ, 2001. – 150 с. 5. Шеннон К. Работы по теории информации и кибернетике / Пер. с англ. под ред. Железнова. Н. А.. – М.: ИЛ, 1963. – 829 с. 6. Бабич В. Д., Кувшинов О. В., Лівенцев С. П. Основи теорії інформації : Навчальний посібник. – К.: КВІУЗ, 2000. – 42 с. 7. Завадостійкість систем передачі з ППРЧ при впливі шумової завади в частині смуги / О. В. Кувшинов, С. П. Лівенцев, С. М. Боголій, В. П. Павлов // Збірник праць КВІУЗ. – 2001. – Вип. 5. – С. 33–38.

УДК 621.391.82

К ВОПРОСУ О ПРИМЕНЕНИИ ЭКРАНИРУЮЩИХ КОНСТРУКЦИЙ И КАБИН

Александр Архипов, Владимир Луценко, Валерий Худяков*

Национальный Технический Университет Украины «КПИ»

**НИИ Электромеханических приборов*

Аннотация: **Рассмотрены вопросы практической реализации экранирующих конструкций и кабин, их характеристики, применение.**

Summary: **Screening equipment and screening cabins are considered from the point of their practical production and application.**

Ключевые слова: **Экранирование, эффективность экранирования, диапазон частот, конструкция.**

Введение

В настоящей статье представлены результаты, полученные в ходе проведения анализа имеющихся экранированных сооружений с целью определения оптимальной конструкции сборно–разборной экранированной камеры (ЭК) с эффективным экранированием магнитной составляющей электромагнитного поля в диапазоне частот от 30 Гц до 150 кГц. Исследованы возможности применения перспективных магнитных материалов, обеспечивающих решение этой задачи, некоторые технологические особенности его практической реализации.

Существующий ряд экранированных сооружений, как возводимых стационарно (неразборных), так и блочно–модульных, конструировался в основном для диапазона частот от 150 кГц и выше [1–5]. Как правило, ЭК изготавливаются из стальных листов нормального сортамента (сталь 20 и др.), сваренных для получения цельной конструкции. Сборно–разборные (блочно–модульные камеры) изготавливаются на облегченных стальных либо алюминиевых или деревянных каркасах в зависимости от материала экрана и требуемой эффективности экранирования (ЭЭ) в низкочастотной части диапазона, и представляют собой конструкцию с болтовыми соединениями [1–4, 6, 7].

Для большинства экранированных помещений применяют оцинкованную листовую сталь, и сетки из тонкой медной проволоки или тонкие медные листы. При равных затратах на материал стальной экран обеспечивает примерно ту же ЭЭ, что и медный экран на частотах порядка 150 кГц. Ниже этой частоты сказывается сравнительно более высокая магнитная проницаемость стали, благодаря чему стальной экран обеспечивает более высокую эффективность магнитного экранирования. Но магнитная проницаемость ферромагнитных сплавов с высоким содержанием железа (стали разных марок) является слишком малой, чтобы обеспечить высокую ЭЭ магнитных полей низких частот.

Сплавы на основе никеля (например, МЮ–металл, пермаллой, гиперном, конетик) имеют проницаемость (и стоимость) приблизительно на два порядка выше, чем сплавы на основе железа. Однако эти сплавы имеют большую чувствительность к давлению и изменению температуры, после отжига не допускают никаких механических операций (сварка, изгиб, сверление и т. п.). Монтаж указанных материалов на каркас экранирующего сооружения требует высокой технологичности конструкции и высокого качества сборки [6].