

## КОНЦЕПЦІЯ СТВОРЕННЯ СИСТЕМИ ЕЛЕКТРОННИХ ДОКУМЕНТІВ

### Вступ

З давніх часів людство передавало свої знання із покоління в покоління. Вся отримана і створена інформація відповідним чином фіксувалась. Матеріальні носії, що містять у зафіксованому вигляді інформацію, оформлену у заведеному порядку, є документи. Документи виконують офіційну, ділову і оперативну функції, оскільки вони – письмовий доказ, джерело відомостей. Із віку в вік не було цінності більшої, чим документи. Наш вік – вік інформаційних технологій, інформаційно-телекомунікаційних систем і інформаційних систем управління у різних галузях народного господарства України. Проблеми створення, обробки, передавання, одержання, зберігання, використання та знищення документів встають на новий, більш якісний рівень. З прийняттям законів „Про електронні документи та електронний документообіг”, „Про електронний цифровий підпис” та ряд інших директивних документів, в тому числі стандарт ДСТУ 4145-2002 на електронний цифровий підпис [1...3]. Сучасні документи не тільки носії інформації, але ще мають властивість губитися, не виконуватися в строк та ставатися все більше вразливими з різних причин, а саме:

- збільшується обсяг збережених і переданих документів з обмеженим доступом;
- збільшується коло користувачів, які мають доступ до ресурсів інформаційної системи і документам;
- ускладнюється режим експлуатації інформаційних систем.

Тому все більшу важливість набуває проблема захисту інформації з обмеженим доступом від несанкціонованого доступу під час підготовки та зберігання документів. Суть цієї проблеми – постійна боротьба спеціалістів по захисту інформації з обмеженим доступом із своїми „опонентами”.

В даній роботі розглянуті основні положення створення електронних документів та захист інформацію з обмеженим доступом, що міститься в них.

### Електронний документ

Закон України „Про електронні документи та електронний документообіг” встановлює основні організаційно-правові засади використання електронних документів.

Електронний документ – документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов’язкові реквізити документа. Електронний документ може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму. Візуальною формою подання електронного документа є відображення даних, які містять, електронними засобами або на папері у формі, придатній для приймання його змісту людиною.

Оригіналом електронного документа вважається електронний примірник документа з обов’язковими реквізитами – обов’язкові дані в електронному документі, без яких він не може бути підставою для його обліку і не матиме юридичної сили, у тому числі з електронно цифровим підписом автора. Електронний підпис є обов’язковим реквізитом електронного документа, який використовується для ідентифікації автора або підписувала електронного документа іншими суб’єктами електронного документообігу.

У разі надсилання електронного документа кільком адресатам або його зберігання на кількох електронних носіях інформації кожний з електронних примірників вважається оригіналом електронного документа.

Якщо автором (фізична або юридична особа, яка створила електронний документ) створюються ідентичні за документальною інформацією та реквізитами електронний документ та документ на папері, кожен з документів є оригіналом і має однакову юридичну силу.

Впровадження інформаційних технологій обробки документів повинен здійснюватися

фахівцями у даній сфері, оскільки будь-яка управлінська діяльність, а особливо діяльність фахівців які здійснюють обробку документів з обмеженим доступом, потребує знань як в системі документообігу, так і стосовно новітніх технологій обробки і захисту інформації з обмеженим доступом. Обробку документів в системі доцільно поділити на модулі, один для введення і редагування переліку користувачів, інші для реєстрації документів, проведення щоденних перевірок тощо [4]. Схему алгоритму створення електронного документа ілюструє рис. 1.

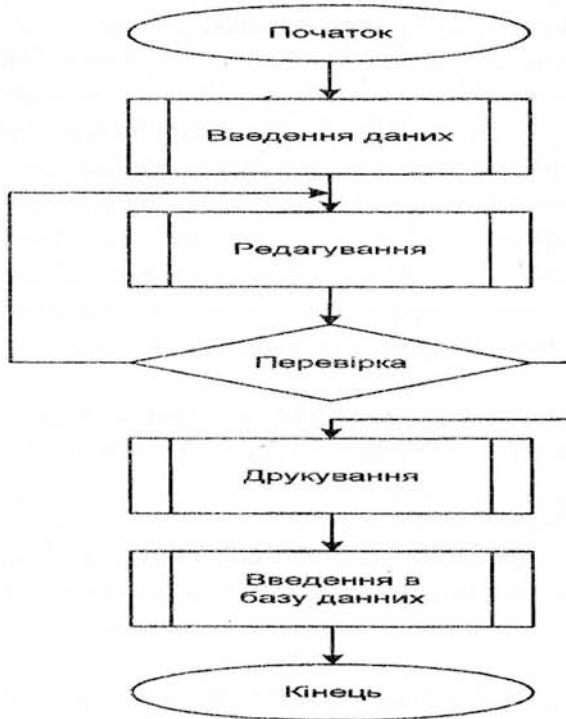


Рис. 1. Схема алгоритму створення електронного документа

Кожний електронний документ в процесі свого життєвого циклу проходить різні стадії і попадає до свого виконавця в різних якість. Загальну модель життєвого циклу електронного документа ілюструє рис. 2.

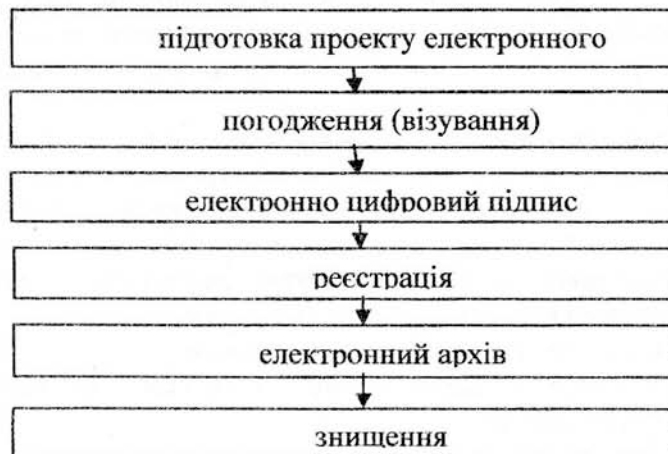


Рис. 2. Загальна модель життєвого циклу електронного документа

На етапі створення електронного документа, він не має юридичної сили, а є проектом електронного документа. Після того як документ створений – погоджений (завізований),

підписаний (затверджений) проект стає документом, наданням електронного підпису завершується створення електронного документа, і з цього моменту і до кінця життєвого циклу він має юридичну силу.

Електронний архів – система призначена для фізичного зберігання електронних документів та їх пошуку. Строк зберігання електронних документів на електронних носіях інформації повинен бути не меншим від строку, встановленого законодавством для відповідних документів на папері. Зберігання документів здійснюється або в файльовій системі, або в базі даних інформаційної системи. Пошук документів повинен здійснюватися, як за реквізітам, так і за документальною інформацією.

#### **Концепція безпеки інформації з обмеженим доступом в електронному документі**

Концепція базується:

– на створенні єдиної інформаційної системи документообігу в межах однієї організації системи організацій міністерства, відомства на організаційно-правових засадах електронного документообігу з використання електронних документів на основі упорядкованої системи документування управлінської діяльності;

- сучасних інформаційно-телекомунікаційних та інформаційних системах;
- класифікація інформаційних потоків на відкриті та з обмеженим доступом;
- ієрархічної структури системи для реалізації різних форм обмеження доступу до інформації (конфіденційної та таємної інформації);
- відповідних технічних та нормативних методів захисту інформації з обмеженим доступом.

Комплексна система захисту інформації повинна представляти сукупність правових (законодавчих), організаційних і технічних засобів та норм, направлених на попередження або унеможливлення нанесення збитків інтересам авторів електронного документа.

Політику безпеки інформації в інформаційній системі і її складових частинах визначає автор (користувача інформаційної системи).

Об'єктами захисту в інформаційній системі і її складових частинах є:

- документація і інформаційні процеси в інформаційних системах;
- інформація про інформаційну систему і її елементи;
- управляючі процеси в інформаційній системі;
- ресурси інформаційної системи і її складових частин (засоби зв'язку і управління, інформаційно-програмне забезпечення, лінії зв'язку тощо).

Циркулюючі в інформаційній системі електронні документи і інформація по забезпеченню функціонування системи (підсистеми, елемента), як об'єкти захисту, мають різний статус:

- відкрита інформація;
- інформація з обмеженим доступом (конфіденційна і таємна інформація. До таємної інформація належить інформація, що містить відомості, які становлять державну таємницю, а також інша передбачена законом таємницю).

Щоб гарантувати безпеку інформаційній системі, необхідно застосовувати таке програмне забезпечення, яке дозволяє пересвідчитися у відсутності елементів, що уможливають дистанційний контроль за роботою системи, або несанкціоноване зняття інформації. Саме тому код програми повинен бути доступним під час перевірки, оскільки знання його усуває ризик застосування програм, до яких вбудовано інші програми (підпрограми). Відкрите (вільне) програмне забезпечення дозволяє повну і всеосяжну інспекцію механізмів за допомогою яких таке програмне забезпечення обробляє дані, усебічно вивчити програму – чудовий механізм безпеки.

Відкрите програмне забезпечення дозволяє:

- використання програм для будь-якої мети;
- безперешкодний доступ до програмного коду або набору інструкцій;
- будь-яке вивчення механізмів (принципів) функціонування програм;
- можливість використання механізмів (принципів) функціонування і будь-яких

довільних частин коду програми (програм, програмних комплексів) для створення інших програм або адаптації до власних потреб;

– можливість зміни і вільного поширення як оригінальної програми так і зміненої, за тими ж умовами, під які підпадає і оригінальна програма.

По появі і положенню джерела виникнення загроз відносно складових частин інформаційної системи і її елементів загрози групуються в класи. В свою чергу класи загроз включають сукупність загроз, згруповані по каналам реалізації. Виходячи з переліку можливих загроз, комплексна система захисту інформації інформаційної системи повинна забезпечити [5]:

- цілісність електронних документів на всіх етапах її обертання при любых загрозах;
- підтвердження справжності електронних документів на всіх етапах їх обробки при усій безлічі потенційних загроз;
- скритність інформації з обмеженим доступом яка циркулює в інформаційній системі;
- захист від несанкціонованого доступу до захищеної інформації і ресурсів інформаційної системи;
- організаційно-технічні засоби захисту інформації з обмеженим доступом від витоку.

Реалізація функцій і задач комплексної системи захисту інформації з обмеженим доступом в інформаційній системі може забезпечуватися комплексним використанням методів і засобів криптографічного і технічного захисту інформації з обмеженим доступом.

Комплекс правових (законодавчих), організаційних (адміністративних), технічних і фізичних засобів, що реалізують функції і задачі комплексної системи захисту інформації в інформаційній системі, повинен забезпечувати:

- попередження появи загроз;
- виявлення появи загроз;
- попередження впливу загроз на інформаційну систему;
- виявлення впливу загроз на інформаційну систему;
- локалізацію впливу загроз на інформаційну систему;
- ліквідацію наслідків впливу загроз на інформаційну систему.

Забезпечення безпеки інформації в складових частинах та інформаційній системі в цілому повинен здійснюватися комплексом правових (законодавчих), організаційних (адміністративних), технічних і фізичних засобів, реалізуючих наступні методи забезпечення безпеки:

- перешкоду (фізична перешкода шляху);
- управління доступом (регулювання використання всіх ресурсів інформаційної системи);
- маскування (закриття змісту електронного документа криптографічними засобами);
- регламентація (створення умов, мінімізуючи умови несанкціонованого доступу до електронних документів);
- примушення (дотримання встановлених правил використання ресурсів системи у тому числі документів під загрозою відповідальності);

Забезпечення безпеки інформації в інформаційній системі може бути ефективним тільки в тому випадку, коли захист інформації з обмеженим доступом буде представляти собою безперервний і цілеспрямований процес, постійно здійснений на всіх етапах життєвого циклу документа. Так комплексна система захисту інформації інформаційної системи крім функцій, задач і засобів власне забезпечення захисту документів повинна включати функції, задачі і засоби управління в якості одного із основних компонентів.

Комплексна система захисту інформації інформаційної системи та її складових повинна реалізуватися на принципах:

- системності;
- комплектності;
- адекватності;
- функціональній самостійності;



- зручності користування;
- обмеження доступ до інформації ;
- повний контроль за роботою інформаційної системи;
- своєчасне реагування на появу загроз;
- економічності.

#### **Висновки**

Наведений матеріал є частиною теоретичної методології підготовки і розробки відкритих та з обмеженим доступом електронних документів. Представлено методологічні основи концепції безпеки інформації з обмеженим доступом в електронному документі.

#### **Список літератури**

1. Закон України „Про електронні документи та електронний документообіг”. Закон України від 22.05.03 № 851-IV // Відомості Верховної Ради України. – 2003. – № 35. – Ст. 275.
2. Закон України „Про електронний цифровий підпис”. Закон України від 22.05.03 № 852-IV // Відомості Верховної Ради України. – 2003. – № 36. – Ст. 276.
3. Закон України „Про захист інформації в інформаційно-телекомунікаційних системах”. Закон України від 11.05.43 № 1703-IV // Відомості Верховної Ради України. – 1994. – № 31. – Ст. 286.
4. *Голозань С.М., Давиденко А.М., Душеба В.В., Щербина В.П.* Підвищення ефективності процесу діловодства / Науково-технічний журнал „Захист інформації”, –2004.– № 1. – С. 66-71.
5. *Бондаренко М.Ф., Черных С.П., Горбенко И.Д.* и др. Методологические основы концепции и политики информационных технологий // Радиотехника: Всеукр. межвед. науч.-техн. сб. 2001. Вып. 119. С.5-16.

*Надійшла 19.01.2005р.*

УДК 621.396.96

Ксендзук А.В.

### **КОДОВЫЕ СИГНАЛЬНЫЕ ГРУППЫ В МНОГОПОЗИЦИОННЫХ СИСТЕМАХ ДИСТАНЦИОННОГО ЗОНДИРОВАНИЯ**

#### **Постановка задачи и связь с научными и практическими задачами.**

Одной из наиболее важных задач в многопозиционных системах с синтезированием апертуры антенны (МПРСА) является обеспечение высоких энергетических отношений сигнал/помеха, которое необходимо для эффективного комплексирования. Фактором, оказывающим существенное влияние на энергетические показатели системы, является степень ортогональности пространственно-временных процессов в различных приемных элементах.

Количественно степень ортогональности можно определить с помощью величины межканальной помехи на выходе оптимального устройства обработки. Использование различных групп сигналов позволяет уменьшить межканальные помехи в МПРСА. В данной работе рассмотрено использование кодовой группы сигналов, – сигналов, отличающихся комплексной огибающей. Такой ансамбль сигналов обеспечивает высокую степень защиты данных систем ДЗ, высокую помехозащищенность и скрытность. Однако при этом происходит существенное повышение взаимных помех в системе дистанционного зондирования, которые должны быть уменьшены путем оптимизации вида сигналов и выбором пространственной конфигурации элементов МПРСА.

#### **Анализ публикаций и исследований по данной теме.**

Вопрос о необходимости использования групп сигналов, позволяющих эффективно

использовать частотный диапазон и, в то же время, обеспечивать высокую защищенность передаваемых данных в задачах построения систем радиолокации обычно не рассматривается. Подобные вопросы достаточно хорошо изучены в теории передачи информации и построения многоадресных (многоканальных) систем связи. особенность

При исследовании особенностей использования групп сигналов в системах дистанционного зондирования с синтезированием апертуры антенны необходимо учитывать ряд специфических характеристик: принципов функционирования РСА, алгоритмов выделения полезной информации из отраженного от поверхности сигнала, методов устранения неоднозначностей, энергетических соотношений и их влияние на качественные характеристики системы и.т.д.

**Цель статьи.**

Разработка и исследование принципов использования групп сигналов в МПРСА для обеспечения высокоточных измерений, высокой помехозащищенности и скрытности.

**Основной материал.**

В многопозиционной системе с синтезированием апертуры антенны (МПРСА), [1] при решении задач выделения радиолокационных изображений по бистатистическим парам  $i$ -й приемник  $k$ -й передатчик оптимальный выходной эффект  $\dot{Y}_{ik}$  (в рамках функционально-детерминированных моделей поверхности) можно представить в виде суммы сигнальной  $\dot{Y}_{Sik}$ , помеховой  $\dot{Y}_{Nik}$  и межканальной помеховой  $\dot{Y}_{ICik}$  компонент

$$\dot{Y}_{ik}(r) = \dot{Y}_{Sik}(r) + \dot{Y}_{Nik}(r) + \dot{Y}_{ICik}(r), \tag{1}$$

где  $\dot{Y}_{Sik}(r_1) = \hat{F}_{ik}(r_1) = \frac{1}{2} \int_D \dot{F}_{ik}(r) \dot{\Psi}_{ik}(r, r_1) dr$ ,  $D$  - область обзора;  $T$  - время

синтеза;  $\dot{Y}_{Nik}(r_1) = \int_0^T n(t) S_{ik}^*(t, r_1) dt$ ,  $\dot{Y}_{ICik}(r_1) = \frac{1}{2} \sum_{j=1..Tr} \int_D \dot{F}_{ij}(r) \int_0^T S_{ij}(t, r) S_{ik}^*(t, r_1) dt dr$ ,  $j = 1..Tr$  - число передатчиков.

Отношение сигнал/помеха на выходе согласованного фильтра

$$\mu_{ik}(r_1) = \frac{\langle |\dot{Y}_{Sik}(r_1)|^2 \rangle}{\langle |\dot{Y}_{ICik}(r_1)|^2 \rangle + \langle |\dot{Y}_{Nik}(r_1)|^2 \rangle} \tag{2}$$

существенно зависит от величины

$$\langle |\dot{Y}_{ICik}(r_1)|^2 \rangle = \frac{1}{4} \left[ \sum_{j \neq k}^{Tr} \sum_{m \neq k}^{Tr} \int_D \int_D \langle \dot{F}_{ij}(r) \dot{F}_{im}^*(r') \rangle \langle \dot{\Psi}_{ijk}(r, r_1) \dot{\Psi}_{imk}^*(r', r_1) \rangle dr dr' \right],$$

которая для упрощенной модели поверхности может быть представлена в виде

$$\langle |\dot{Y}_{ICik}(r_1)|^2 \rangle = \frac{1}{4} \left[ \sum_{j \neq k}^m \int_D \sigma_{ij}^0(r) \langle |\dot{\Psi}_{ijk}(r, r_1)|^2 \rangle dr \right],$$

где  $\sigma_{ij}^0(r)$  - значение УЭПР в бистатистической паре  $i$ -й приемник -  $j$ -й передатчик.

После ряда преобразований, полагая, что удельная эффективная поверхность рассеяния (УЭПР) является факторизуемой функцией относительно параметров наблюдения  $\sigma_{ij}^0(r) = \sigma^0(r) \alpha_{ij}(r)$ , при аппроксимации  $\sigma^0(r)$  ее средним значением, а также при равенстве энергии излучаемых сигналов получим следующее выражение для оценки сигнал/помеха в многопозиционной системе

$$\mu_{ik}(\mathbf{r}_1) \cong SNR_{ik}(\mathbf{r}_1) \frac{1}{1 + \left[ \frac{X}{\Delta X} \frac{Y}{\Delta Y} \sum_{j \neq k} K_{ijk}^2 \alpha_{ijkD} \chi_{ijk}(\mathbf{r}_1) \right] SNR_{ik}(\mathbf{r}_1)}, \quad (3)$$

где  $SNR(\mathbf{r}_1)$  отношение сигнал/помеха в бистатической PCA ( $i$ -й приемник,  $k$ -й передатчик), определяемое выражением  $SNR(\mathbf{r}_1) = \frac{\langle |\dot{Y}_{Sik}(\mathbf{r}_1)|^2 \rangle}{\langle |\dot{Y}_{Nik}(\mathbf{r}_1)|^2 \rangle}$ ;  $K_{ijk}^2 = \frac{K_{ij}^2}{K_{ik}^2}$  -

отношение, зависящее от расстояний, проходимых сигналом в бистатической системе;

$\alpha_{ijkD} = \langle \frac{\alpha_{ij}}{\alpha_{ik}} \rangle_D$  - среднее значение по области обзора коэффициента влияния геометрии

наблюдения (углов визирования);  $\chi_{ijk}(\mathbf{r}_1) = \int_D \langle |\dot{\Psi}_{ijk}(\mathbf{r}, r_1)|^2 \rangle d\mathbf{r}$  - среднеквадратический

уровень боковых лепестков взаимной корреляционной функции в пространственных координатах.

Значение искажений, вызванных межканальными помехами для широкого класса поверхностей, определяется взаимной пространственной функцией неопределенности

$\dot{\Psi}_{ijk}(r, r_1) = \int_0^T \dot{S}_{ij}(t, r) \dot{S}_{ik}^*(t, r_1) dt$ , которая, в свою очередь зависит от пространственной

конфигурации элементов МПРСА и вида сигналов, используемых различными передатчиками.

Понятие ортогональности сигналов в усиленном смысле [2]

$$|\dot{\Psi}_{12}| = \left| \frac{1}{2E} \int_{T_1}^{T_2} \dot{S}_1(t) \dot{S}_2^*(t) dt \right| = 0$$

для МПРСА должно быть модифицировано с учетом особенностей пространственно-временной обработки.

Два сигнала назовем точечно-ортогональными (ортогональными в точке пространства  $r_1$ ) в усиленном смысле, если для заданных условий наблюдения выполняется равенство

$$|\dot{\Psi}_{ijk}(r_1)| = \left| \int_0^{T_C} \int_D \dot{S}_{ij}(t, r) \dot{S}_{ik}^*(t, r_1) dr dt \right| = 0, \quad (4)$$

где  $\dot{S}_{ij}(t, r)$ ,  $\dot{S}_{ik}(t, r)$  - траекторные сигналы в бистатических парах  $i-j$  и  $i-k$ .

С учетом возможности преобразования пространственных координат подстилающей поверхности  $r$  в координаты время задержки  $\tau$  - частота Доплера  $F$ , [3], условие ортогональности в точке  $r_1$  может быть записано в виде

$$|\dot{\Psi}_{ijk}(\tau, F)| = \left| \int_0^{T_C} \int_F \int_\tau \dot{S}_{ij}(t, \tau, F) \dot{S}_{ik}^*(t, \tau_1, F_1) dt d\tau dF \right| = 0.$$

Для ортогональных сигналов (то есть сигналов, ортогональных на всей области обзора  $D$ :  $|\dot{\Psi}_{12}(r_1)| \equiv 0, r_1 \in D$ ) должно выполняться условие

$$\left| \dot{\Psi}_{ijk} \right| = \left| \int_0^T \int_D \int_D \dot{S}_{ij}(t, r) \dot{S}_{ik}^*(t, r_1) dr dr_1 dt \right| = 0, \quad (5)$$

или

$$\left| \dot{\Psi}_{ijk} \right| = \left| \int_0^{T_C} \int_{F'} \int_{\tau'} \int_{F'} \dot{S}_{ij}(t, \tau, F) \dot{S}_{ik}^*(t, \tau_1, F_1) dt d\tau dF d\tau_1 dF_1 \right| = 0$$

Увеличить отношение сигнал/помеха (3) целесообразно за счет уменьшения  $\left| \dot{\Psi}_{ijk} \right|$  путем выбора сигнальных групп и/или путем оптимизации пространственной конфигурации МПРСА. При выборе сигналов можно использовать разделение по виду комплексной огибающей (для дискретных систем - кодовое разделение), по несущей частоте и совместное по несущей частоте и комплексной огибающей.

Для обеспечения высокой скрытности и помехозащищенности системы дистанционного зондирования целесообразно использовать кодовое разделение каналов. Более того, при таком разделении сохраняется относительно небольшая полоса частот, занимаемая системой дистанционного зондирования. При этом используется группа сигналов

$$\dot{S}_k(t) = \dot{S}_{0k}(t) e^{j\omega_0 t} \quad (6)$$

с одинаковыми несущими частотами, но различными комплексными огибающими (кодowymi последовательностями).

Размерность кода определяется требуемой частотой повторения, определяемой из условия однозначного отсчета:

$$\text{Max} |t_3(t, \vec{r}_1) - t_3(t, \vec{r})| < T_0, \quad T_0 < \frac{L}{2v},$$

где  $L$  - протяженность раскрыва в азимутальной плоскости;  $v$  - скорость движения носителя по этой оси.

При использовании максимально возможной частоты повторения размерность кода  $N = \frac{L}{2v\tau}$  определяется длительностью элементарного импульса, выбираемой их технических ограничений. Обеспечение более высокой скрытности в многопозиционной системе возможно при использовании различных кодов в различных передатчиках.

Величина  $\dot{\Psi}_{ijk}$  (4) для сигналов (9) определяется выражением

$$\begin{aligned} \dot{\Psi}_{ijk} &= \int_0^T \int_D \dot{S}_{0ij}(t, r) e^{-j\omega_0 \tau_{ij}(t, r)} dr \int_D \dot{S}_{0ik}^*(t, r) e^{j\omega_0 \tau_{ik}(t, r)} dr dt = \\ &= \int_0^T \int_D \int_D S_{0ij}(t, r) S_{0ik}^*(t, r_1) e^{-j\omega_0 [\tau_{ij}(t, r) - \tau_{ik}(t, r_1)]} dt dr dr_1 \end{aligned} \quad (7)$$

Для такого вида разделения величина межканальной помеховой компоненты не может быть сколь угодно уменьшена исключительно за счет выбора комплексных огибающих.

Оптимизация пространственной конфигурации МПРСА позволяет уменьшить помехи, обусловленные использованием частично ортогональных сигналов. Аппроксимируем спектры пространственно-временных процессов финитными функциями для обеспечения ортогональности (в усиленном смысле)  $S_{ij}(t, r)$ ,  $S_{ik}(t, r)$ ,  $r \in D$  необходимо выполнение условия (при  $\omega_{0k} \geq \omega_{0j}$ )

$$f_{0j} + \Delta S_j + F_{Dij \max} \leq f_{0k} - \Delta S_k - F_{Dik \min}, \quad (8)$$



где  $\Delta S$  - ширина спектра сигнала (можно использовать как ширину спектра одиночного импульса, так и их последовательности, рис. 2);  $F_{Dik \min}$ ,  $F_{Dij \max}$  - минимальное и максимальное значение частоты Доплера в различных бистатических парах.

Значения поля доплеровских частот в декартовой системе координат определяются

выражением [3]: 
$$F_{Dik} = \frac{\omega_0}{2c} \left[ \frac{[2\Delta r_i, 3\Delta r_i t - r]}{\|r_i(r) - r\|} + \frac{[2\Delta r_k, 3\Delta r_k t - r]}{\|r_k(r) - r\|} \right],$$
 где  $\Delta r_i = v_i$ ,

$\Delta r_k = v_k$  - векторы скоростей  $i$ -го приемника и  $k$ -го передатчика, соответственно;  $r$  - координаты точки поверхности;  $[\cdot, \cdot]$  - знак скалярного произведения.

Максимальное и минимальное значение  $F_{D \min}$ ,  $F_{D \max}$  отсчитываются по наибольшей ширине следа диаграммы направленности вдоль линий равных доплеровских частот, рис. 1.

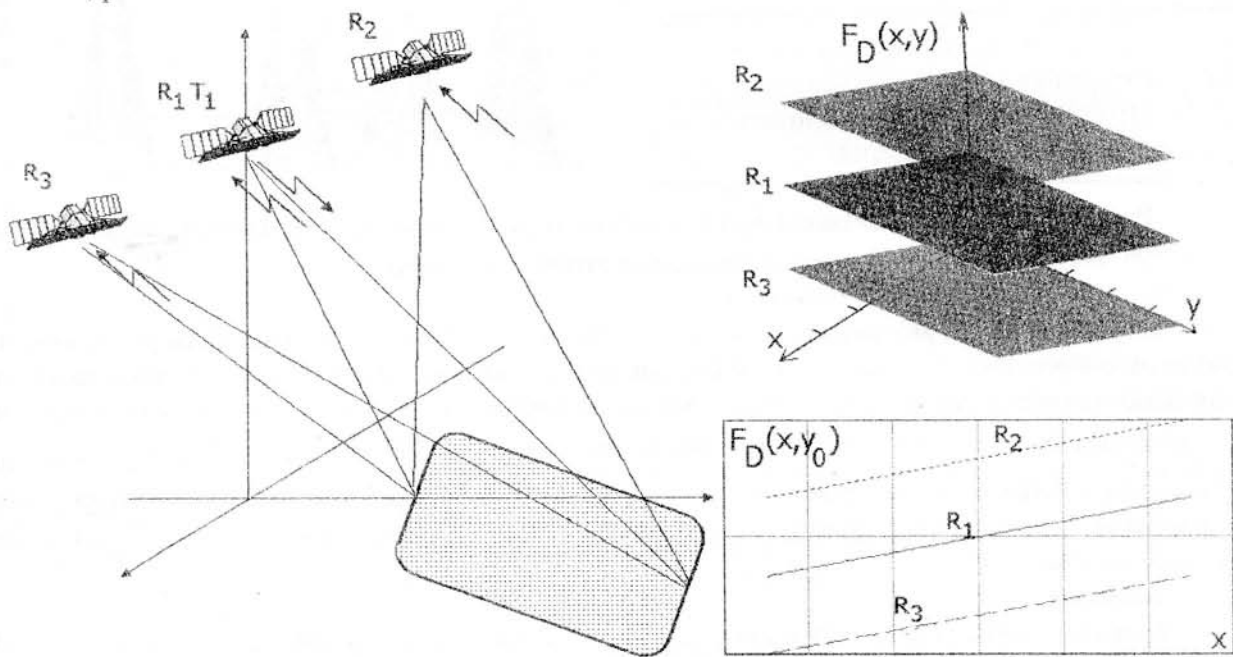


Рис. 1. Пространственная конфигурация МПРСА, обеспечивающая разделение между сигналами по частоте Доплера.

Выполняя разделение доплеровского сдвига частоты на компоненты, вызванные движением приемника  $F_{Di}$  и передатчика  $F_{Dj}$ ,  $F_{Dk}$  относительно зондируемой поверхности, условие (12) можно записать так:

$$F_{Dj \max} - F_{Dk \min} \leq \Delta \omega_{0kj} - \Delta S_{kj} - \Delta F_{Di}, \quad (10)$$

где  $\Delta F_c$  - ширина полосы доплеровских частот, обусловленных движением приемника.

Для случаев кодового разделения условие ортогональности будет определяться шириной спектра комплексной огибающей и полосой доплеровских частот:  $F_{Dk \min} - F_{Dj \max} \geq \Delta S_{kj} + \Delta F_{Di}$ .

В многопозиционной системе с синтезированием апертуры антенны возможно разделение сигналов, путем выбора пространственного положения ее элементов даже при идентичности сигналов, излучаемых различными передатчиками. В качестве примера ниже приведены результаты определения спектров сигналов в системе с синтезированием апертуры антенны при идентичности кодов различных передатчиков, рис. 2.

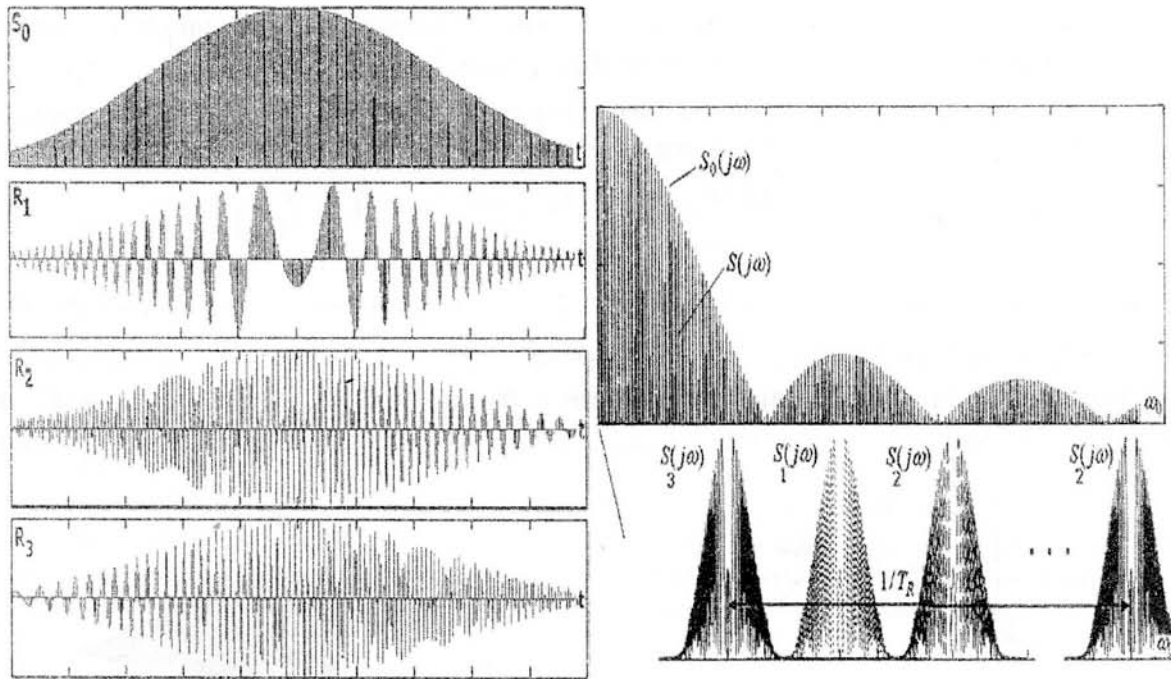


Рис. 2. Излученный сигнал ( $S_0$ ) и сигналы, отраженные от центральной точки синтеза в различных бистатических парах.

С учетом преобразования пространственных координат функций неопределенности различное пространственное положение бистатических пар может быть интерпретировано как использование различных несущих частот. В линейной аппроксимации закона движения согласованных элементов эквивалентный разнос частот составит  $\Delta\omega_0 = F_{Dk \min} - F_{Dj \min}$ . Однако при использовании такого способа уменьшения взаимных помех необходимо учесть увеличение расстояния между элементами как фактор уменьшения отношения сигнал/помеха.

**Выводы.**

Использование групп сигналов, отличающихся комплексной огибающей (кодовое разделение для дискретных систем) позволяет достичь высокой помехозащищенности и скрытности, обеспечивая при этом необходимый уровень качественных показателей системы дистанционного зондирования.

Выбор основных параметров групп сигналов необходимо осуществлять с учетом особенностей функционирования систем с синтезированием апертуры антенны.

Дальнейшим развитием работы может являться исследование определенных групп дискретных кодов и основных характеристик PCA, а также выбор и обоснование методов кодирования с учетом особенностей передаваемой информации.

**Список литературы.**

*Ксендзук А.В.* Использование спутниковых навигационных систем ГЛОНАСС/GPS для дистанционного зондирования поверхности. - Электромагнитные волны и электронные системы, 2003, т.8, № 5, с. 8-15.

*Фалькович С.Е. Хомяков Э.Н.* Статистическая теория измерительных радиосистем. -М.: Радио и связь, 1981. - 288 с.

*Ksendzук, V.K. Volosyuk, N.S. Sologub* Space Ambiguity Functions of the Optimal Processing Algorithm for the Stochastic Surface // EUSAR 2004. - Vol 1. - PP 191-194.

*Поступила 22.12.2004г.*