рез крайние элементы эквивалентного линейного раскрыва этой ФАР, изменяются на постоянную величину, что позволяет упростить и ускорить процесс формирования провала.

Сущность предлагаемого фазового способа формирования провала в ДН плоской ФАР состоит в оценке уровня исходной диаграммы направленности N-элементной ФАР в направлении помехи, выделении в раскрыве двух М-элементных подрешеток, расположенных на краях исходной, и введении фазовых поправок, со знаком минус для элементов одной подрешетки и со знаком плюс для элементов другой подрешетки [4].

Данный способ свободен от недостатков, присущих предыдущему способу, поскольку формирование провала осуществляется в ДН плоской ФАР в направлении помехи, имеющей угловые координаты (θ_n, ϕ_n) в сферической системе координат, причем фазы сигналов, проходящих через крайние элементы эквивалентного линейного раскрыва этой ФАР, изменяют на постоянную величину, что позволяет упростить и ускорить процесс формирования провала.

Выводы

Рассмотренный метод позволяет устранить взаимное влияние преднамеренных и не преднамеренных помех, что в совокупности со всеми другими вышеперечисленными методами позволяет повысить помехозащищённость сетей мобильной связи и беспроводной передачи данных.

ЛИТЕРАТУРА

1. Широкополосные беспроводные сети передачи информации / [Вишневский В. М., Ляхов А. И., Портной С. Л., Шахович И. В.]. – М. : Техносфера, 2005 – 592 с.

2. The Path to 4G Mobile // Communications Week International. – Issue 260. – 5 March 2001. – P. 16–17.

3. Сети мобильной связи LTE. Технологии и архитектура / Тихвинский В. О., Терентьев С. В., Юрчук А. Б. – М. : Эко-Трендз, 2010. – 284 с.

4. Фазовый способ формирование провала в диаграммы направленности плоской фазированной антенной решетки [Электронный ресурс] / [Грибанов А. Н., Мосейчук Г. Ф., Гаврилова С. Е, Павленко Е. А.,Чубанова О. А.]. – Режим доступа : http://www. freepatent. ru

В. Царюк,
студент 5 курсу факультету
комп'ютерних наук та інноваційних технологій,
Міжнародний гуманітарний університет;
керівник – канд. техн. наук, доц. В. В. Сергеєв

ІДЕНТИФІКАЦІЯ ЗАГРОЗ ТА ВРАЗЛИВОСТЕЙ ІНФОРМАЦІЙНОЇ СИСТЕМИ БАНКУ

Загрози безпеки інформаційній системі (ІС) банку при їх реалізації можуть завдати значної шкоди бізнес-процесам/банківським продуктам, клієнтам, обладнанню, процесам і програмно-технічним засобам, та, відповідно, банку [1]. Загрози можуть мати природні та людські джерела і можуть бути випадковими або навмисними.

При складанні політики інформаційної безпеки (ІБ) повинні бути ідентифіковані усі джерела загроз у загальному вигляді чи за типами (наприклад, неавторизовані дії, фізичне пошкодження обладнання, вплив на інформаційні ресурси, та ін.) [2].

До процесу ідентифікації загроз слід залучати спеціалістів з інформаційної безпеки, представників юридичної служби, власників бізнес-процесів/банківських продуктів, фахівців з управління персоналом тощо.

Реалізація загроз здійснюється зловмисниками через використання вразливостей ІС банку.

Процес ідентифікації вразливостейІС слід здійснювати у наступних областях:

− інформаційна система у цілому;

− фізичне середовище;

− характеристика та конфігурація програмно-технічних засобів, програмного забезпечення,технологічного та телекомунікаційного обладнання;

− характеристика системи управління інформаційною безпекою (СУІБ);

− характеристика персоналу ІС та служби захисту інформації (СЗІ);

− характеристика постачальників програмного забезпечення та апаратних засобів ІС;

− характеристика організації, що надає послуги з аудиту ІБ інформаційної системи банку.

Для виявлення вразливостей в залежності від вимог до захисту інформації та бізнес-процесу/банківського продукту, а також від застосованої інформаційно-телекомунікаційної технологіїслід застосовувати різні методи аналізу захищеності ІС [3]. До них належать:

− спеціальні програмні засоби сканування вразливостей;

− засоби тестування та поточної оцінки інформаційної безпеки;

− тести на проникнення;

− перегляд коду програмно-технічних комплексів;

− аналіз відомих та виявлених вразливостей та порушень ІБ, що досліджені та систематизовані СЗІ банків;

− моніторинг процесів ІС та дій її персоналу.

Перелічені методи не тільки дають змогуідентифікувати вразливості, але й ліквідувати певну загрозу.

ЛІТЕРАТУРА

1. SO/IEC 27005 «Information technology – Security techniques – Information security risk management» (Управління ризиками інформаційної безпеки).

2. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України.

3. Сізова Н. Д., Здановський Я. В. Захист інформації в банківських та комерційних системах : навчальний посібник. – Х. : ХДТУБА, 2009. – 112 с.

К. Чоговадзе,
К. Чоговадзе, студентка 5 курса
факультета Компьютерных наук и инновационных технологий;
Международный гуманитарный университет

РАЗРАБОТКА АРХИТЕКТУРНОЙ МОДЕЛИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ И СЕТЕЙ

Обеспечение безопасности компьютерных систем (КС) в наши дни становится все более актуальным в связи с постоянным развитием информационных технологий и появлением новых способов хищения, искажения информации, нарушения работоспособности КС. При этом штатное функционирование государственных и коммерческих КС становится невозможным без постоянного поддержания их конфиденциальности и целостности.