Міністерство освіти і науки України
Одеська національна академія зв'язку ім. О.С. Попова

Друга всеукраїнська науково-практична конференція

"ПЕРСПЕКТИВНІ НАПРЯМИ ЗАХИСТУ ІНФОРМАЦІЇ"

03-07 вересня 2016 року

Збірник тез

Одеса
ОНАЗ
2016

Програмний комітет

Воробієнко П.П.	голова, д.т.н., проф., ректор ОНАЗ ім. О.С. Попова
Каптур В.А.	заступник голови, к.т.н., с. н. с., проректор з наукової роботи ОНАЗ ім. О.С. Попова
Василіу Є.В.	д.т.н., проф., директор Навчально-наукового інституту Радіо, телебачення та інформаційної безпеки ОНАЗ ім. О.С. Попова;
Корченко О.Г.	д.т.н., проф., зав. каф. безпеки інформаційних технологій, Національний авіаційний університет
Оксіюк О.Г.	д.т.н., проф., зав. каф. кібербезпеки та захисту інформації, КНУ ім. Тараса Шевченка;
Рудницький В.М.	д.т.н., проф., зав. каф. системного програмування, Черкаський державний технологічний університет;
Захарченко М.В.	д.т.н., проф., зав. каф. інформаційної безпеки та передачі даних, ОНАЗ ім. О.С. Попова;
Корчинський В.В.	д.т.н., проф. каф. інформаційної безпеки та передачі даних, ОНАЗ ім. О.С. Попова;
Гнатюк С.О.	к.т.н., доц. каф. безпеки інформаційних технологій, Національний авіаційний університет;
Ніколаєнко С.В.	к.т.н., доц. каф. інформаційних технологій, ОНАЗ ім. О.С. Попова;
Стайкуца С.В.	к.филос.н., доц. каф. інформаційної безпеки та передачі даних, ОНАЗ ім. О.С. Попова;
Онацький О.В.	к.т.н., доц. каф. інформаційної безпеки та передачі даних, ОНАЗ ім. О.С. Попова;
Кільдішев В.Й.	к.т.н., доц. каф. інформаційної безпеки та передачі даних, ОНАЗ ім. О.С. Попова

Організаційний комітет

Василіу Є.В.	д.т.н., проф., директор навчально-наукового інституту радіо, телебачення та інформаційної безпеки, ОНАЗ ім. О.С. Попова;
Ніколаєнко С.В.	к.т.н., доц. каф. інформаційних технологій, ОНАЗ ім. О.С. Попова;
Пилявський В.В.	к.т.н., відповід. за навчальну та наукову роботу навчально-наукового інституту радіо, телебачення та інформаційної безпеки, ОНАЗ ім. О.С. Попова;
Михайлова Л.В.	викл. каф. інформаційної безпеки та передачі даних, ОНАЗ ім. О.С. Попова;
Кишмар І.Б.	пров. фахівець каф. інформаційної безпеки та передачі даних, ОНАЗ ім. О.С. Попова
Лімарь І.В.	аспірант каф. інформаційної безпеки та передачі даних, ОНАЗ ім. О.С. Попова

$$\Phi_{ij}^{n+1} = \begin{cases} \Phi_{ij}^{n} & \text{якщо} \quad 0 < \Phi_{ij}^{n} < \tau_{ij}^{e} + \tau_{ij}^{n}, \\ 0 & \text{якщо} \quad \Phi_{ij}^{n} = \tau_{ij}^{e} + \tau_{ij}^{r}, \\ 0 & \text{якщо } \Phi_{ij}^{n} = 0 \text{ й } u_{ij}^{n+1} < h_{ij}, \\ 0 & \text{якщо } \Phi_{ij}^{n} = 0 \text{ й } u_{ij}^{n+1} \geq h_{ij}. \end{cases} \quad (1)$$

Можна вважати, що вплив кожного члена групи на будь-якого іншого є однакові. Тоді кожен елемент отримує активатор від усіх збуджених елементів.

$$u_{ij}^{n+1} = g_{ij} u_{ij}^{n} + \sum_{k,l} C_{kl} I_{i+k,j+l}, \quad (2)$$

де матриця Cu описує величину взаємного впливу елементів один на одного. У нашому випадку $C_{kl} = 1$;

$$I_{ij}^{n} = \begin{cases} 1, & \text{якщо} \quad 0 < \Phi_{ij}^{n} \leq \tau_{ij}^{e}, \\ 0, & \text{якщо} \quad \tau_{ij}^{e} < \Phi_{ij}^{n} \leq \tau_{ij}^{e} + \tau_{ij}^{r} \quad \text{або} \quad \Phi_{ij}^{n} = 0. \end{cases}$$

У рівнянні (1) перший доданок описує розпад активатора поточного елемента. Другий доданок – це активатор, який поступає від інших елементів групи.

Висновки.

На слайдах презентації доповіді показані деякі результати моделювання. Застосування математичної моделі процесу інформаційно-психологічного впливу на цільову групу дає потужний інструмент для вивчення складних механізмів синхронізації поведінки людей у групі, перевіряти заходи по захисту від деструктивного впливу. Розроблена модель дозволить удосконалити та підвищити ефективність формування та професійної виучки членів служби кібербезпеки.

Література

1. Петрик В.М. Информационно-психологическая безопасность в эпоху глобализации: учебное пособие / В.М. Петрик, В.В. Остроухов, А.А. Штоквиш // Под ред. В.В. Остроухова. – К., 2008. – 544 с.

2. Минаев В.А. Как управлять массовым сознанием: современные модели : монография [Текст] / В.А. Минаев, А.С. Овчинский, С.В. Скрыль, С.Н. Тростянский Т.В – М., 2012. – 213 с.

3. Тарасевич Ю.Ю. Академическая сеть как возбудимая середа [Текст] / Ю.Ю. Тарасевич, В.А. Зеленухина // Компьютерные исследования и моделирование. Модели экономических и социальных систем. Т. 7 № 1. – Астрахань: АГУ, – 2015. – С. 177-183.

УДК 621.395.7

Ганшин Д.Г.
Харьковский национальный университет радиоэлектроники.
d.hanshyn@gmail.com
Научный руководитель – д.т.н., проф. Цопа О.І.

ОЦЕНКА ЗАЩИЩЕННОСТИ СИСТЕМЫ СВЯЗИ С ПСЕВДОСЛУЧАЙНЫМ СКАЧКООБРАЗНЫМ ИЗМЕНЕНИЕМ ЧАСТОТЫ *OFDM* СИГНАЛА

Аннотация. *Предложен один из вариантов построения системы связи с использованием псевдослучайной перестройки частот OFDM сигнала. На основе концепции отводного канала получены данные скрытности беспроводных широкополосных систем связи с использованием OFDM модуляции, а так же проведена оценка скрытности предложенной системы связи с использованием псевдослучайной перестройкой частоты.*

Для построения производительных ведомственных систем связи, работающих в каналах с частотно-селективными замираниями, приняты целый ряд стандартов передачи мультимедийной информации *ADSL, WLAN, WiMAX, LTE, DAB, DVB-T* на основе технологии с ортогональным частотным разделением каналов *OFDM* (*Orthogonal Frequency-Division Multiplexing*), которая может успешно противостоять межсимвольной интерференции [1].

В тоже время псевдослучайная перестройка рабочей частоты (ППРЧ) является одним из двух основных распространенных методов расширения спектра сигналов, которые также позволяют повысить эффективность работы в частотно-селективных каналах, и имеет низкую вероятность перехвата (*LPI - low probability of interception*). Этот метод широко применяется в системах военной связи для работы в условиях сильных преднамеренных помех, а также используется в некоторых беспроводных стандартах передачи информации, таких как *GSM*, *Bluetooth* и др. [2].

Сочетание технологии *OFDM* и ППРЧ, позволяет существенно увеличить спектральную эффективность, повысить защищенность системы связи от перехвата, снизить влияние многолучевости, а также существенно уменьшить влияние помех.

В докладе рассматривается один из вариантов построения системы связи с псевдослучайным скачкообразным изменением частоты *OFDM* сигнала (рис. 1).

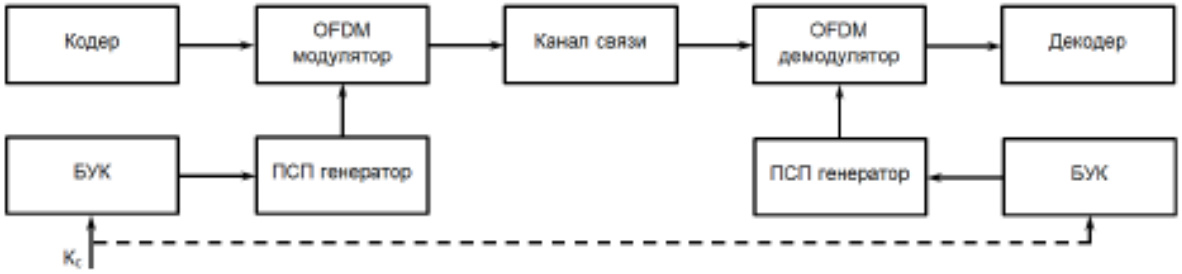

Рисунок 1 – Упрощенная стуркурная схема системы связи с псевдослучайной перестройки частоты *OFDM* сигнала

В данном примере формирования псевдослучайной перестройки частоты происходит после цифроаналогового преобразователя, который подключен к смесителю (рис. 2).

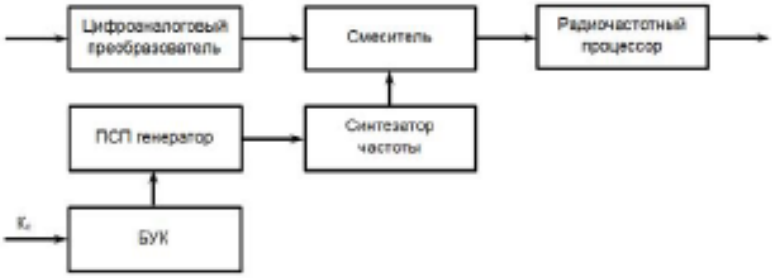

Рисунок 2 – Формирование псевдослучайной перестройки частоты *OFDM* сигнала

На выходе смесителя формируеться *OFDM* сигнал с псевдослучайной перестойкой частоты (рис. 3). Синтезатор частоты управляется генератором псевдослучайной последовательности, который в свою очередь управляеться блоком управления ключем (БУК).

Ключ *Кс* поступает в блок управления ключем в котором формируеться новый ключ. Для формировании нового ключа в данном блоке может использоваться М-последовательность. Ново сформированный ключ поступает в генератор псевдослучайной последовательности. В ПСП генераторе используеться М-последовательность.

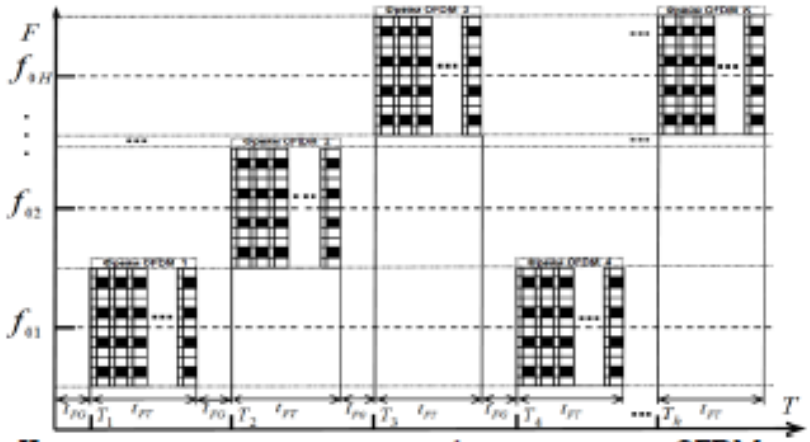

Рисунок 3 – Частотно временная диаграмма сформированного OFDM сигнала с псевдослучайной перестройкой по частоте

Оценка потенциальной структурной скрытности системы связи, является одним из важнейших параметров систем связи. Противостояние системы против радиотехнической разведки, которая предполагает выполнения трех основных задач таких как: выявления факта работы системы связи (обнаружения сигнала); определение структуры обнаруженного сигнала и его основных параметров; раскрытие передаваемой информации.

При оценке скрытности сигналов используются два основных подхода. В первом скрытность определяется как вероятность успешного выявления сигнала в заданное время. Во втором оценивают скрытность сигнала через затраты на выявления его состояния с заданной достоверностью (вероятность правильного решения).

Потенциальная скрытность является характеристикой собственно объекта исследования (в нашем случае сигнала), его выраженным в числовой форме качеством, способностью противостоять выявлению текущего состояния. Потенциальная скрытность сигнала не зависит от действий системы выявления его состояний, так как предполагает использование оптимального алгоритма поиска. Фактически она является наиболее «*осторожной*» оценкой скрытности.

Потенциальная структурная скрытность зависит от ансамбля (арсенала) A реализаций сигнала и определяется числом двоичных измерений (диз), которые необходимо осуществить для раскрытия структуры широкополосного сигнала. Общее выражение для потенциальной структурной скрытности имеет вид [1]:

$$S_P = \log_2 A \ \ [\text{диз}], \tag{1}$$

где A – ансамбль (арсенал) реализаций, определяемый количеством всех возможных значений каких-либо параметров сигнала.

Такими параметрами сигнала могут быть несущая частота, амплитуда, вид модуляции, структура линейного кода, параметры формы и временные характеристики сигнала, а также другие специфические параметры, зависящие от физического уровня конкретной технологии передачи сигналов. В общем случае скрытность зависит от способа построения конкретного вида сигнала, используемого для переноса информации.

Оценка структурной скрытности *OFDM* сигналов с учетом возможных ансамблей значений параметров данного сигнала можно провести, используя формулу (2):

$$S_P = S_{OFDM} + S_{QAM} \tag{2}$$

На основе этого подхода можно дать оценку потенциальной скрытности предложенной нами системы связи с псевдослучайной перестройки частоты *OFDM* сигнала.

$$S_P = S_{OFDM} + S_{QAM} + S_{ППРЧ} \tag{3}$$

В табл. 1 приведены данные о потенциальной структурной скрытности сигналов современных беспроводных систем связи: *Wi-Fi, WiMAX, LTE, DBV*.

Таблица 1

Данные о структурной скрытности сигналов *OFDM* для различных систем связи

Вид технологии	Тип сигнала	Количество поднесущих частот *N*	Уровень модуляции *M-QAM*	Длина *L* фрейма *OFDM*	ППРЧ *B*	Скрытность *S*, диз
Wi-Fi IEEE.802.11	*OFDM*	64	16	80	-	10
WiMAX IEEE.802.16d	*OFDM*	256	256	40	-	16
WiMAX IEEE.802.16e	*OFDM*	512	256	40	-	17
LTE	*OFDM*	1024	256	120	-	18
DBV-T	*OFDM*	6800	64	40	-	18
DBV-T2	*OFDM*	32000	256	40	-	23
Система FH-OFDM	*OFDM*	2048	256	120	100	482

С табл.1 видно, что в системах с использованием псевдослучайной перестройки частоты *OFDM* сигнала существенно повышается скрытность системы связи.

Література

1. Методы прогнозирования защищенности ведомственных систем связи, основанные на концепции отводного канала. / Под редакцией А. И. Цопы и В. М. Шокало. – Харьков: КП «Городская типография», 2011. – 502 с.

2. Борисов В. И. Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты. / В. И. Борисов, В. М. Зинчук, А. Е. Лимарев. – М.: Радио и связь, 2000. – 384 с.

3. Ганшин Д. Г. Исследование защищенности системы связи с многочастотными сигналами. / Д. Г. Ганшин, В. В. Маслий, А. И. Цопа // Радиотехника. Всеукраинский межведомственный научно-технический сборник. – 2013. – Выпуск № 173. – С. 195-203.

УДК 004.056.53:004.492.3

Гізун А.І.
Національний авіаційний університет.
andriy.gizun@gmail.com

СИСТЕМИ УПРАВЛІННЯ КРИЗОВИМИ СИТУАЦІЯМИ ЯК СКЛАДОВА СИСТЕМИ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Анотація. *Концепція управління безперервністю бізнесу як перспективний напрям оперативного та стратегічного менеджменту визначає важливість захисту інформаційних ресурсів в умовах впливу кризових ситуацій. У цій роботі проведений аналіз систем управління кризовими ситуаціями і обґрунтоване їх віднесення до окремого класу в структурі системи менеджменту інформаційної безпеки, визначені їх функціональні взаємозв'язки з іншими захисними системами, такими як системи виявлення та попередження вторгнень, системи аналізу та оцінки ризиків, системи антивірусного захисту, системи управління інцидентами інформаційної безпеки.*

Внаслідок розвитку можливостей ІТ у сучасному світі пріоритетним напрямом є автоматизація управлінських, технологічних, виробничих та інших процесів. Інформаційні системи займають провідні ролі в системі функціонування бізнесу та держави, причому взаємозв'язок ІТ та бізнес-процесів стає настільки тісним, що життєздатність підприємств