УДК 378.162.33+65.012.8

В.С. Блінцов, професор
С.М. Нужний, кандидат технічних наук
Д.А. Баша, інженер
(Національний університет кораблебудування, м. Миколаїв, Україна)

КОНЦЕПЦІЯ СТВОРЕННЯ ЛАБОРАТОРНОГО КОМПЛЕКСУ «ОСНОВИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В ВТКМ»

В роботі проведено аналіз та визначені основні вимоги до лабораторного комплексу по підготовці студентів в галузі знань «інформаційна безпека». Запропонована структура лабораторного комплексу та визначені основні принципи його побудови.

Постійне збільшення кількості і якості пристроїв передачі інформації по відкритим телекомунікаційним мережам (ВТКМ), необмежена можливість вільного виходу в Internet, як зі стаціонарного так і з мобільного телефонного апарату (ноутбуку, смартфону та інших), використання супутникових інформаційних систем і т.д. призвело до зростання об'ємів конфіденційної інформації, яка циркулює в ВТКМ.

Широке застосування в світовій практиці персоніфікованої інформації набуло і в інших формах. Так, наприклад, в країнах Балтії вже декілька років функціонують державні системи електронного голосування на виборах всіх рівнів. До таких систем відноситься також міжнародні кадрові інформаційні системи обліку (наприклад, моряків), пошуково-криміналістична система Interpol та багато інших.

До специфічних умов України необхідно віднести широке залучення для створення вказаних вище систем як державних так і приватних підприємств, в тому числі для забезпечення функціонування ліній передачі інформації. При цьому специфікою України є створення таких систем на фоні приватизації одного з найважливіших з її учасників – Укртелекому. Тобто, на деякий час, рівень захищеності конфіденційної інформації, як приватного так і державного характеру, значно знизиться. Цьому буде сприяти системна перебудова в самому Укртелекомі і відтік висококваліфікованих кадрів, в тому числі в тіньові і кримінальні структури.

Все вище сказане ставить задачу необхідності підвищення кваліфікаційного рівня студентів, які навчаються в галузі знань «інформаційна безпека», за рахунок більш широкого використаннях сучасних методик розрахунку та проектування систем ТЗІ, застосовування пристроїв протидії НСД до ІзОД в ВТКМ та визначення демаскуючих факторів технічних каналів витоку інформації.

Для вирішення поставленої задачі на кафедрі електрообладнання суден та інформаційних технологій планується створення лабораторного комплексу «Основи технічного захисту інформації в ВТКМ», яка повинна забезпечити комплексну підготовку бакалаврів та спеціалістів в галузі знань «інформаційна безпека», за трьома напрямами підготовки.

Задача створення як окремих дослідницьких лабораторних стендів так і спеціалізованих лабораторій з метою підготовки кваліфікованих спеціалістів для відділів ТЗІ державних та приватних організацій і підприємств розглянута в [1-5] та інші. Однак, аналіз показує, що в більшості випадків ставиться задача дослідження вузькоспеціалізованих технічних засобів перетворення та передачі інформації по ВТКМ. Яскравим прикладом такого підходу є лабораторії дослідження захищеності інформації в АС першого – третього рівнів. Такі лабораторії оснащені сучасними програмними, апаратними та програмно-апаратними комплексами, які забезпечують заданий рівень безпеки інформації. Однак, в більшості випадків, в них концептуально не передбачено наявність інших каналів несанкціонованого доступу до інформації (візуально-оптичного, акустичного, ПЕМВН і т.д.), що циркулює в контрольованій зоні (зоні розміщення АС), по ВТКМ, які використовуються для штатної роботи системи.

Одночасно з цим, аналіз науково-технічної літератури показав відсутність матеріалів, пов’язаних зі створенням сучасних лабораторій для дослідження захищеності інформації при комплексному використанні декількох різнотипних ВТКМ. Так, наприклад, в наш час є широко застосованим метод створення локальної мережі організації з використанням Wi-Fi, Wimax чи Bluetooth та використання електропровідних (UTP-5+ та UTP-6) чи оптоволоконних для ліній зв’язку для зовнішнього підключення. При цьому вимоги до захисту інформації від витоку по каналу ПЕМВН для таких систем фактично не виконуються, в першу чергу, із-за відсутності відповідного теоретичного обґрунтування та практичних наробітків спеціалістів і як наслідок цього – відсутності методик розрахунків і проведення досліджень.

Метою роботи є розробка концепції лабораторного комплексу для дослідження сучасних методів побудови КСЗІ для інформації, яка передається по ВТКМ любої конфігурації, в тому числі за умови використання зловмисником комплексних методів для отримання несанкціонованого доступу до ІзОД.

Лабораторний комплекс планується до використання в учбовому процесі при підготовці фахівців за напрямком «Інформаційна безпека» по спеціальностях 170101…03, а також для проведення перепідготовки фахівців відділів «ТЗІ» чи їх аналогів та проведення науково-дослідних робіт і експертиз обладнання.

Створення сучасних телекомунікаційних систем неможливе без комплексного використання різнотипних мереж. Їх різноманітність останнім часом збільшується кожні декілька років. Особливо швидкими темпами йде розвиток цифрових технологій з передачею великої кількості інформації по радіоканалу та використання аналогових систем на понад високих частотах. Одночасно з цим йде й подальший розвиток електропровідних та оптиковолоконних технологій передачі інформації.

Така різноманітність сприяє зловмисникам, даючи можливість використання як моноканалів для доступу до ІзОД, так і комбінованих. При цьому необхідно враховувати можливість виникнення як природніх так і штучно створюваних каналів витоку інформації.

На рис. 1 наведено структурна схема лабораторного комплексу для дослідження методів протидії несанкціонованому доступу до інформації, яка передається по ВТКМ. Схема складається з трьох базових блоків:

– блок 1 «Дослідження принципів протидії НСД до ІзОД, яка передається по провідним ВТКМ»

– блок 2 «Моделювання перехоплення інформації (СМПІн), що передається по дротяних і радіочастотним ВТКМ»

– блок 3 «Дослідження принципів протидії НСД до конфіденційної інформації, яка передається по дротяних і радіочастотним ВТКМ (зв'язок через Інтернет)»

Блок "Дослідження принципів протидії НСД "Телефон"" складається з телефонного апарату, засобу контролю фізичних параметрів лінії і захисту інформації від НСД. Призначений - для моделювання обміну інформацією між абонентами по дротяній ВТКМ, контролю фізичних параметрів дротяної ВТКМ і захисту інформації, яка передається по лініям в мережі, від НСД інженерно-технічними і криптографічними методами [7]. До складу блоку входить два модуля «Дослідження принципів протидії НСД «Телефон»».

Блок "Дослідження принципів протидії НСД "Інтернет"" складається з ПЕОМ і пристроїв підключення Інтернет-ресурсів. Призначений - для моделювання обміну інформацією між абонентами (АС2), у тому числі, з виходом в Інтернет (АС3), контролю фізичних параметрів радіочастот і захисту інформації, яка передається в мережі, від НСД інженерно-технічними і криптографічними методами.

Блок "Моделювання перехоплення інформації" складається з моделей пристроїв НСД до ВТКМ. Призначений - для моделювання пристроїв знімання інформації з дротяних і радіочастотних ВТКМ. Кількість модулів визначається переліком задач, дослідження яких виконується. Модулі також використовуються для моделювання комплексного впливу фізичних параметрів середовища на канал передачі інформації.

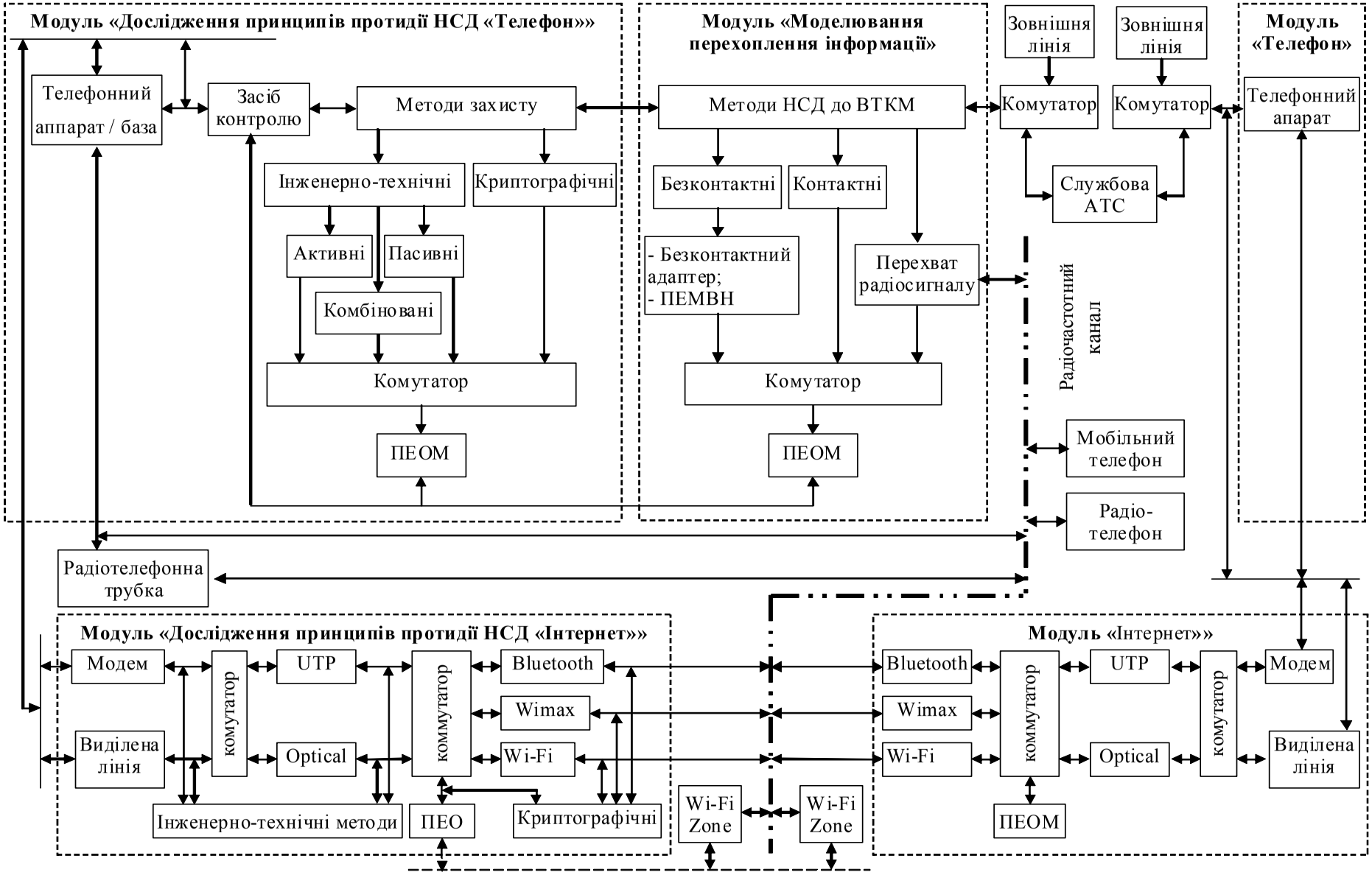

Рис. 1. Структурна схема лабораторії по дослідженню методів протидії НСД до ІзОД, яка передається по ВТКМ

На основі вищесказаного, формуються рекомендації по забезпеченню лабораторії лініями ВТКМ :

- 2 виділених телефонних лінії з міськими номерами (2 номери);
- 2 лінії від службової АТС (2 номери);
- WiFi Zone (може входити до складу стенду "Дослідження принципів протидії НСД "Інтернет"");
- Wimax Zone (може входити до складу стенду "Дослідження принципів протидії НСД "Інтернет"");
- мобільний телефон (може входити до складу стенду "Дослідження принципів протидії НСД "Телефон"");
- радіотелефон (може входити до складу стенду "Дослідження принципів протидії НСД "Телефон"");
- комплект "телефонний апарат (база) з радіотелефонною трубкою" (може входити до складу стенду "Достти лідження принципів протидії НСД "Телефон"");
- телефонний апарат (може входити до складу стенду "Дослідження принципів протидії НСД "Телефон"").

Висновки

В роботі проаналізовано сучасний стан розвитку технічних засобів і умов їх використання при побудовах ВТКМ, що дозволило визначити основні напрями вирішення поставленої задачі – побудови лабораторного комплексу по дослідженню методів захисту ІзОД, яка передається по ВТКМ.

В якості базового підходу прийнято модульний метод побудови комплексу, що дає змогу виконувати дослідження як окремих частин (модулів), так і дослідження багаторівневих мереж.

Такий підхід дозволить вирішити наступні задачі:

– розвиток теоретичних основ проектування комплексних систем захисту інформації (КСЗІ) при використанні різнотипних розгалужених мереж передачі інформації в АС–1, 2 і 3;

– розробка методик розрахунку взаємовпливу різнотипних мереж передачі інформації з метою визначення оптимальних умов для її обробки та передачі за умови забезпечення заданого рівня захищеності, цілісності та доступності;

– розробка моделей загроз для конфіденційної інформації, яка циркулює в інформаційній мережі, за умови заданої вірогідності використання зловмисником комбінованих атак та сучасних засобів і методів перехоплення інформації;

– підвищення рівня підготовки спеціалістів, які навчаються за напрямом «Інформаційна безпека», та підвищення кваліфікації на курсах перепідготовки.

Список літератури

1. *Торокин А.А.* Инженерно-техническая защита информации. – М.: Гелиос АРВ, 2005. – 960 с.

2. *Зайцев А.П., Шелупанов А., Мещеряков Р. и др.* Техническая защита информации: Учебник для вузов. – М.: Горячая линия-Телеком, 2009. – 615 с.

3. *Сидорин Ю.С.* Технические средства защиты информации: Учеб. пособие. СПб.: Изд-во Политехн. ун-та, 2005. 141 с.

4. Технические средства и методы защиты информации: Учебник для вузов / *Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.*; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009 – 508 с.

5. *Ленков С.В.* Методы и средства защиты информации. В 2-х томах / Ленков С.В., Перегудов Д.А., Хорошко В.А. Под ред. В.А. Хорошко. – К.: Арий, 2008.

6. НД ТЗІ 2.3-003-2001 – Технічний захист мовної інформації в симетричних абонентських аналогових телефонних лініях. Засоби активного приховування мовної інформації. Генератори спеціальних сигналів. Методика випробувань