

«Технологія створення, експлуатації та експертизи комплексних систем захисту інформації»

Основні наукові результати

1. Розроблено нові математичні моделі, методи, методики та технології створення, експлуатації та експертизи КСЗІ, у т.ч. розроблено відповідні специфікації цих технологій, що дозволяють на практиці здійснювати оптимальний динамічний перерозподіл між рівнями ефективності та гарантованості захисту в залежності від потреб прикладних застосувань. В процесі створення вищеназваних моделей, методів, методик та технологій враховано сучасні тенденції щодо розробки та організації експлуатації ІТКС (зокрема, вимоги нових міжнародних стандартів - ISO 15408, ISO/IEC 17799:2005, ISO/IEC 27001:2005, ГОСТ Р ИСО/МЭК 15408 тощо), а також нові функціональні можливості сучасного телекомунікаційного обладнання з точки зору забезпечення технічного захисту інформації (нові механізми пріоритизації та класифікації пакетного трафіку, механізми служби *QoS*, механізми *VPN* тощо).

2. Розроблено нову модель вузькосмугового авіаційного радіоканалу, заснованого на використанні некогерентних методів приймання, що забезпечує можливість передавання мовного трафіку на швидкостях, більших ніж 6,2 кбіт/с при відношенні «сигнал/шум» не менше 25 дБ. Реалізація цієї моделі представляє компромісне технічне рішення, що забезпечує необхідний для авіаційних застосувань рівень захисту мовного трафіку без втрати якості зв'язку.

3. Розроблено нову модель системи інформаційного протиборства для фізичного рівня спеціальних широкосмугових ТКС з ЧФМ сигналами за допомогою якої проаналізовано ефективність

від звісних методів запропонований СМ-метод дозволяє забезпечити абсолютну гарантованість захисту із параметрами так званих досконало секретних систем.

6. Розроблено нову технологію створення комплексних систем захисту інформації (КСЗІ) в ІТКС. Надано технічні специфікації усіх технологічних етапів створення КСЗІ. Вперше запропоновано новий порядок здійснення технологічних етапів і нова схема організації робіт під час створення КСЗІ в ІТКС, що суттєво відрізняються від відомих технологій розробки КСЗІ. Розроблена технологія відповідає вимогам вітчизняних стандартів у сфері ТЗІ (зокрема, стандартам ДСТУ 3396.0-96 та ДСТУ 3396.1-96) і дозволяє забезпечити тонку структуру потреб прикладних застосувань користувачів ресурсів ІТКС щодо гарантованості та ефективності захисту інформації з оптимальним використанням ресурсів. Розроблена технологія створення КСЗІ апробована на практиці, зокрема при організації захисту інформаційної системи контролю і управління доступом ДП МА «Бориспіль».

7. Розроблено нову технологію оцінювання (експертизи) КСЗІ в ІТКС. Ця технологія на практиці реалізує запропоновану у даній роботі парадигму довіри, тобто реалізує довірчий принцип оцінки якості КСЗІ. Розроблено також нову методику оцінювання захищеності інформаційних ресурсів ІТКС, що відображає запропоновану концептуальну модель оцінювання систем захисту інформаційних ресурсів сучасних авіаційних інформаційно-телекомунікаційних систем. Надано технічні специфікації усіх технологічних етапів оцінювання КСЗІ. Отримано аналітичні залежності ефективності захисту від вартості організаційно-технічних заходів щодо ТЗІ. Розроблена технологія оцінювання КСЗІ апробована на практиці, при експертизі систем захисту інформаційних систем.

8. Запропоновано концептуальну модель експлуатації комплексних систем захисту інформаційних ресурсів (КСЗІ) сучасних (у т.ч., авіаційних) інформаційно-телекомунікаційних систем (ІТКС), що базується на моделі *TMN*, яка підтримується *ISO*, *ANSI*, а також Рекомендації *ITU-T* та міжнародного стандарту *ISO 7498-4*. Використання цієї моделі дозволило стандартизу-

вати експлуатаційні процеси щодо КСЗІ і, отже, підвищити надійність експлуатації ІТКС та мінімізувати експлуатаційні витрати.

Із застосуванням моделі *TMN* розроблено нову технологію експлуатації КСЗІ в ІТКС. Надано технічні специфікації усіх технологічних етапів експлуатації КСЗІ. Розроблена технологія експлуатації КСЗІ впроваджена у практику використання КСЗІ інформаційних систем ДП МА «Бориспіль». Зокрема, для цих систем розроблено та впроваджено відповідні пакети настанов, інструкцій з експлуатації та інших організаційно-розпорядчих документів.

Практична цінність

Отримані результати можуть знайти застосування при створенні, оцінюванні та експлуатації КСЗІ будь-яких ІТКС, де виникає необхідність захисту інформації.

Розроблені технології оптимізовані за критеріями мінімуму затрат і можуть бути використані тільки на вітчизняних підприємствах, оскільки вони узгоджені із вітчизняною нормативною базою.

Розроблені технології впроваджені в чотири інформаційно-телекомунікаційні системи ДП МА «Бориспіль».

За розробленими технологіями виконано 9 Договорів на загальну суму 398 тис. грн.. Зокрема:

- № 653-X10 (02.2-4/7.1) Надання консультативних послуг з конфігурації комп'ютерних технічних засобів (технічний захист інформації, контроль доступу) «Розробка та введення в експлуатацію комплексної системи захисту інформації системи контролю та управління доступом (СКУД)»;

- № 654-X10 Проведення додаткової експертизи штатної системи захисту обладнання цифрової телефонної автоматичної станції «КВАНТ-Є», що належать АТЗТ «Українська цифрова телефонна компанія»;

- № 650-X10 Проведення додаткової експертизи комплексної системи захисту інформації мережі надання послуг Інтернет у складі центрального вузла доступу (м. Славутич) та віддалених вузлів доступу (м. Чернігів, м. Чорнобиль), що належать ПрАТ «МАКЕТ»;

- № 679 –X10/ 802640-107 Проведення додаткової державної експертизи комплексної системи захисту інформації мережі надання послуг Інтернет ВАТ "Укртелеком";

- № 690-X10 Проведення атестації комплексної системи захисту інформації в автоматизованих системах класу «1» режимно-секретного органу Головного управління охорони здоров'я та медичного забезпечення ВО КМР (КМДА);

- № 684-X10 Проведення державної експертизи комплексної системи захисту інформації автоматизованої системи класу «1» Міністерства транспорту та зв'язку України;

- № 750-X11 Проведення атестації комплексної системи захисту інформації в автоматизованій системі класу «1» Міністерства інфраструктури України;

- № 747-X11 Проведення атестації двох комплексних систем захисту інформації в автоматизованих системах класу «1» режимно-секретного сектору Державної авіаційної служби України;

- № 770-X11 Проведення атестації комплексної системи захисту інформації в автоматизованій системі класу «1» режимно-секретного органу Київської обласної митниці.

Розроблено 10 методик проведення Експертизи телекомунікаційного обладнання та комплексних систем захисту інформації:

- Програма та методика проведення експертизи комплексної системи захисту інформації в автоматизованій системі класу «1» режимно-секретного сектору Міністерства транспорту та зв'язку України створеної на основі сервісів безпеки ОС Windows XP SP2 на відповідність вимогам нормативно-правових актів та нормативних документів системи технічного захисту інформації;

- Програма та методика проведення експертизи комплексної системи захисту інформації в автоматизованій системі класу «1» режимно-секретного сектору Державної авіаційної адміністрації створеної на основі сервісів безпеки ОС Windows XP SP2 на відповідність вимогам нормативно-правових актів та нормативних документів системи технічного захисту інформації;

- Програма та методика проведення експертизи комплексної системи захисту інформації в автоматизованій системі класу «1» Головного управління охорони здоров'я та медичного забезпечення Київської міської державної адміністрації створеної на основі сервісів безпеки ОС Windows XP SP2 на відповідність вимогам нормативно-правових актів та нормативних документів системи технічного захисту інформації;

- Програма та методика проведення експертизи комплексної системи захисту інформації в автоматизованій системі класу «1» режимно-секретного органу Київської обласної митниці Державної митної служби України створеної на основі сервісів безпеки ОС Windows XP SP2 на відповідність вимогам нормативно-правових актів та нормативних документів системи технічного захисту інформації;

- Програма та методика проведення експертизи комплексної системи захисту інформації в автоматизованій системі класу «1» режимно-секретного сектору Міністерства інфраструктури України створеної на основі сервісів безпеки ОС Windows XP SP2 на відповідність вимогам нормативно-правових актів та нормативних документів системи технічного захисту інформації;

- Програма та методика додаткових експертних випробувань штатних програмно - технічних засобів технічного захисту інформації у цифровій автоматичній телефонній станції «КВАНТ-Є» за критеріями технічного захисту інформації на рівні довіри ЕЗ;

- Програма та методика випробувань комплексної системи захисту інформації центрального вузла доступу мережі надання послуг Internet ПрАТ «Макег»;

- Програма та базова методика випробувань комплексної системи захисту інформації типового віддаленого вузла доступу Internet ПрАТ «Макег»;

- Програма та методика додаткових експертних випробувань комплексної системи захисту інформації мережі надання послуг Інтернет ВАТ "Укртелеком»;

- Програма та методика оціночних випробувань комплексної системи захисту інформації автоматизованої системи контролю та управління доступом ДП МА "Бориспіль".

Додатково розроблено та виготовлено дослідні зразки:

- Пристій захисту технічних каналів цифрових ліній «ПЗТК-ЦЛ»;

Прилад оперативного контролю роботи пристроїв захисту «ПОКР-ПЗ».

Перелік основних наукових

9. В.М. Бабенко, А.В. Карпов, В.І. Г.Ф. Конахович, В.І. Корчук / Методика визначення контрольованої зони приміщення за допомогою модифікованої моделі Хата // Сборник научных трудов НАУ «Защита информации» - К.: НАУ, 2010 – Выпуск № 17 – с. 35-40.
10. В.М. Бабенко, А.В. Карпов, В.І. Г.Ф. Конахович, В.І. Корчук / Методика модернізації моделі хата та моделі COST 231 // Сборник научных трудов НАУ «Защита информации» - К.: НАУ, 2010 – Выпуск № 17 – с. 100-105.
11. Г.Ф. Конахович, М.Г. Луцький, Р.С. Одарченко / Методика визначення радіусу зони обслуговування точки доступу стандарту IEEE 802.11g // Сборник научных трудов НАУ «Защита информации» - К.: НАУ, 2010 – Выпуск № 17 – с. 269-277.
12. А.В. Карпов, Г.Ф. Конахович, Г.С. Конахович, Р.С. Одарченко / Розробка пристрою для визначення еквівалентного шкідливого електромагнітного випромінювання // Наукоємні технології, Науковий журнал НАУ – К.:НАУ, 2010 – Выпуск № 2 – с.112-115.
13. А.В. Карпов, Г.Ф. Конахович, Г.С. Конахович, Р.С. Одарченко / Методика визначення загального рівня опромінення персоналу в сучасному інформаційному просторі // Наукоємні технології, Науковий журнал НАУ – К.:НАУ, 2010 – Выпуск № 2 – с.116-121.
14. И.А. Мачалин / Выбор оптимального варианта эксплуатации авионики в период гарантийного обслуживания // Проблемы транспорта: Сб. научных праць, Вип.8.-Київ: НТУ, 2011.- с. 50-55.
15. I.A. Machalin, V.V. Ulanskyi / Mathematical models for evaluation of operational readiness of periodically inspected electronic systems.- Математичні машини і системи.-Вип.4, 2011.- с. 45-52.
16. О.Ю. Пузиренко / Система обробки додаткової інформації в мережі цифрового звукового мовлення // Проблеми інформатизації та управління : зб. наук. праць. — К. : НАУ, 2011. — Вип. 2 (34). - с. 111-119.
17. Андрухович П.О., Шевченко А.О., Одарченко Р.С., Одарченко М.С. Обчислення контрольованої зони радіозакладних пристроїв// Захист інформації: Зб. наук.пр. – Вип.1(29) - К: НАУ, 2010 : с. 302-306.
18. В. В.Антонов, О. П. Нечипорук, Р.С. Одарченко, Ю.О. Петрова / Багатокритеріальний підхід до визначення доцільності використання технології кабельних мереж // Електроніка та системи управління : зб. наук. праць. — К. : НАУ, 2010. — Вип. 3 (25). — с. 89-94.
19. О.Г. Голубничий / Моделювання та аналіз роботи широкосмугових радіосистем // Комп'ютерні системи та мережні технології: III міжнар. наук.-техн. конф. 15 – 17 червня 2010 р.: тези доп. – К.: НАУ, 2010. – с. 15.
20. О.Г. Голубничий, Г.Ф. Конахович, А.В. Степанов / Параметри вибору архітектури внутрішньої інформаційно-комунікаційної системи // Захист інформації в інформаційно-комунікаційних системах: наук.-практ. конф., 7–10 червня 2011 р.: тези доп.–К.: НАУ, 2011.–с. 34.
21. А.Н. Афанасьев, О.О.Горбунов, И.В. Харламов / Методы взлома и защита данных пользователей на веб-серверах // «Проблеми навігації і управління рухом»: всеукраїнська науково практична конф. 21-22 листопада 20011 р.: зб.тез доповідей – К., 2011. – с. 99.
22. Р.С. Одарченко, Ю.О. Петрова / Перспективи технології LTE в світі // «Проблеми навігації і управління рухом» Всеукраїнська науково-практична конференція молодих учених і студентів, НАУ, м. Київ – К.: Інноваційно-видавничий центр «Холтех», 2010- с. 150.
23. О.П. Нечипорук, Р.С. Одарченко, В.Г. Потапов, В.Г. Тараненко, О.П. Ткаліч / Кодирование речи с линейным предсказанием // Захист інформації: науково-технічний журнал № 4 (49), Київ: НАУ, 2010- с. 106.
24. А.С.Муранов, В.М. Чуприн / Моделі диференційованого обслуговування з гарантованим сервісом // Проблеми інформатизації та управління: Зб.наук. праць НАУ К.: НАУ, випуск № 1 (27), 2010 – с. 5.
25. В.В.Заєць, В.М. Чуприн / Дослідження семантичного методу захисту табличних даних // Захист інформації: Зб.наук. праць. НАУ К.: НАУ, випуск №1, 2010 – с. 12.
26. В.В.Заєць, В.О. Лобок, В.М. Чуприн / Розроблення досконало секретної системи для семантичного захисту табличних даних // «Проблеми навігації і управління рухом» Всеукраїн-

ська науково-практична конференція молодих учених і студентів, НАУ К.: Інноваційно-видавничий центр «Холтех», 2010 - с. 122.

27. В.О. Лобок, В.М. Чуприн, Ю.В.Чуприна / Перспективи розвитку вітчизняної нормативної бази у сфері створення комплексних систем захисту інформації // «Проблеми навігації і управління рухом» Всеукраїнська науково-практична конференція молодих учених і студентів, НАУ К.: Інноваційно-видавничий центр «Холтех», 2010 - с. 123.

28. В.В. Антонов, Г.Ф. Конахович, В.Г. Потапов, О.П. Ткаліч, В.М. Чуприн / «Експлуатація телекомунікаційних систем» // Навчальний посібник - підготовлено до друку, 750 с.

29. І.О. Мачалін / Методи підвищення ефективності експлуатації радіоелектронних систем в періоди гарантійного та післягарантійного обслуговування повітряних кораблів // Дисертація на здобуття наук. ступ. д.т.н., Наук. спец. 05.22.20 - експлуатація та ремонт засобів транспорту, захищена 2010 р.

30. О.Г. Голубничий / Методи забезпечення прихованості передавання інформації у широкосмугових радіосистемах // Дисертація на здобуття наук. ступ. к.т.н., ДСК, Наук. спец. 05.13.21 – системи захисту інформації, спец. вч. рада Д 26.062.01 НАУ, захищена 2010 р.

31. О.С. Муранов / Розробка методів прогнозування пульсацій трафіку для вузлового обладнання комп'ютерних мереж // Дисертація на здобуття наук. ступ. к.т.н., Наук. спец. 05.13.05 – комп'ютерні системи та компоненти, захищена 2010 р.

32. Р.С. Одарченко / Оптимізація структури бездротового сегменту комп'ютерних мереж // Дисертація на здобуття наук. ступ. кандидат технічних наук НАУ, Наук. спец. 05.12.17 – Радіотехнічні та телевізійні системи, атестат НК №000097 2011 р.

ПІДГОТОВЛЕНІ ДИСЕРТАЦІЇ

1. О.Ю. Пузиренко / Комп'ютерні системи стеганографічної обробки і захисту інформації у цифровому звуковому мовленні // Дисертація на здобуття наук. ступ. к.т.н. за спеціальністю 05.13.05 – комп'ютерні системи та компоненти.

2. В.В. Антонов / Удосконалення технології передавання захищеного мовного трафіка в авіаційних системах радіозв'язку // Дисертація на здобуття наук. ступ. к.т.н. за спеціальністю 05.13.06 – інформаційні технології.

3. А.С. Муранов / Дослідження телекомунікаційних технологій диференційованого обслуговування з гарантованим сервісом // Дисертація на здобуття наук. ступ. к.т.н. за спеціальністю 05.12.02 – телекомунікаційні системи та мережі.

4. П.О. Андрухович / Розробка математичної моделі апроксимації розповсюдження побічних електромагнітних випромінювань // Дисертація на здобуття наук. ступ. к.т.н. за спеціальністю 05.13.21 – системи захисту інформації.

Охоронні документи

1. Патент на корисну модель «Детектор шкідливого електромагнітного випромінювання» № 63174 від 26.09.2011.

2. Патент на корисну модель «Вузол керування комутаційним пристроєм» № 43630 від 25.08.2009.

3. Свідоцтво про реєстрацію авторського права на твір «Комп'ютерна програма "Програма оптимізації обмінного фонду комплектуючих виробів повітряних кораблів і розрахунку експлуатаційних витрат ("МАЙНТОРТ")»» № 32435 від 19.03.2010.