Наукова школа кібербезпеки Національного авіаційного університету: теоретичні та практичні результати діяльності

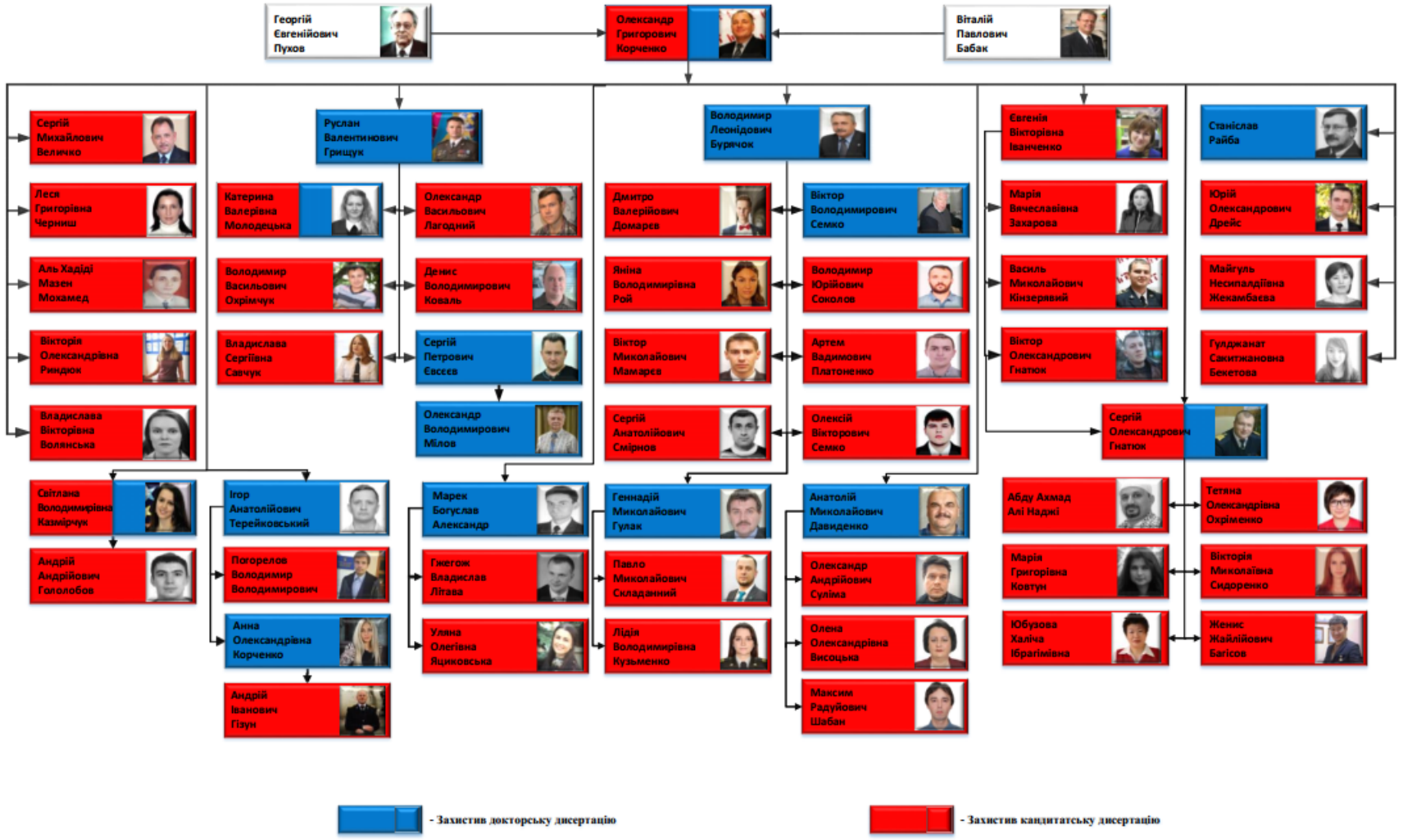
ДОСВІД НАУ

13 березня 2018 року було затверджено **наукову школу «Кібербезпека»** Національного авіаційного університету, до складу якої входить більше 40 фахівців вищої кваліфікації (включаючи закордонних).

Засновник та науковий керівник

д.т.н., проф. Корченко О. Г.

ДЕРЕВО НАУКОВОЇ ШКОЛИ «КІБЕРБЕЗПЕКА» НАУ



БАЗОВІ НАПРЯМКИ НАУКОВИХ ДОСЛІДЖЕНЬ

1) оцінювання ризиків інформаційної безпеки;
2) виявлення вторгнень в інформаційних системах;
3) ідентифікація аномальних станів для систем виявлення вторгнень;
4) побудова симетричних криптосистем;
5) стеганографічні методи приховування даних;
6) виявлення, ідентифікація та оцінювання впливу кризових ситуацій в ІТ-сфері;
7) виявлення та ідентифікація порушників в ІКСМ;
8) оцінювання шкоди національній безпеці у разі витоку державної таємниці;
9) технології квантової криптографії;
10) захист цивільної авіації від кіберзагроз;
11) методи управління кіберінцидентами;
12) захист від шкідливих інформаційно-психологічних впливів.

ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

НАУКОВІ РЕЗУЛЬТАТИ:

1. Розроблено низку методів для оцінювання ризиків безпеки ресурсів інформаційних систем, з можливістю оперування одночасно чіткими і нечіткими величинами з варіативним числом терм-множин,
2. Розроблено методи оцінювання ризиків безпеки ресурсів інформаційних систем на основі значень CVSS (Common Vulnerability Scoring System) показників, які дозволяють автоматизувати та реалізувати в реальному часі процес оцінювання ризиків без залучення експертів необхідної предметної області.

ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

НАУКОВІ РЕЗУЛЬТАТИ:

3. Розроблено методологію процесу синтезу систем оцінювання ризиків, яка дозволяє формалізувати процес створення адаптивних інструментальних засобів з гнучкими можливостями щодо перетворення заданих множин оброблюваних величин, а також експорту та імпорту еталонів параметрів при оцінюванні ризиків безпеки ресурсів інформаційних систем.

ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

ПРАКТИЧНІ РЕЗУЛЬТАТИ:

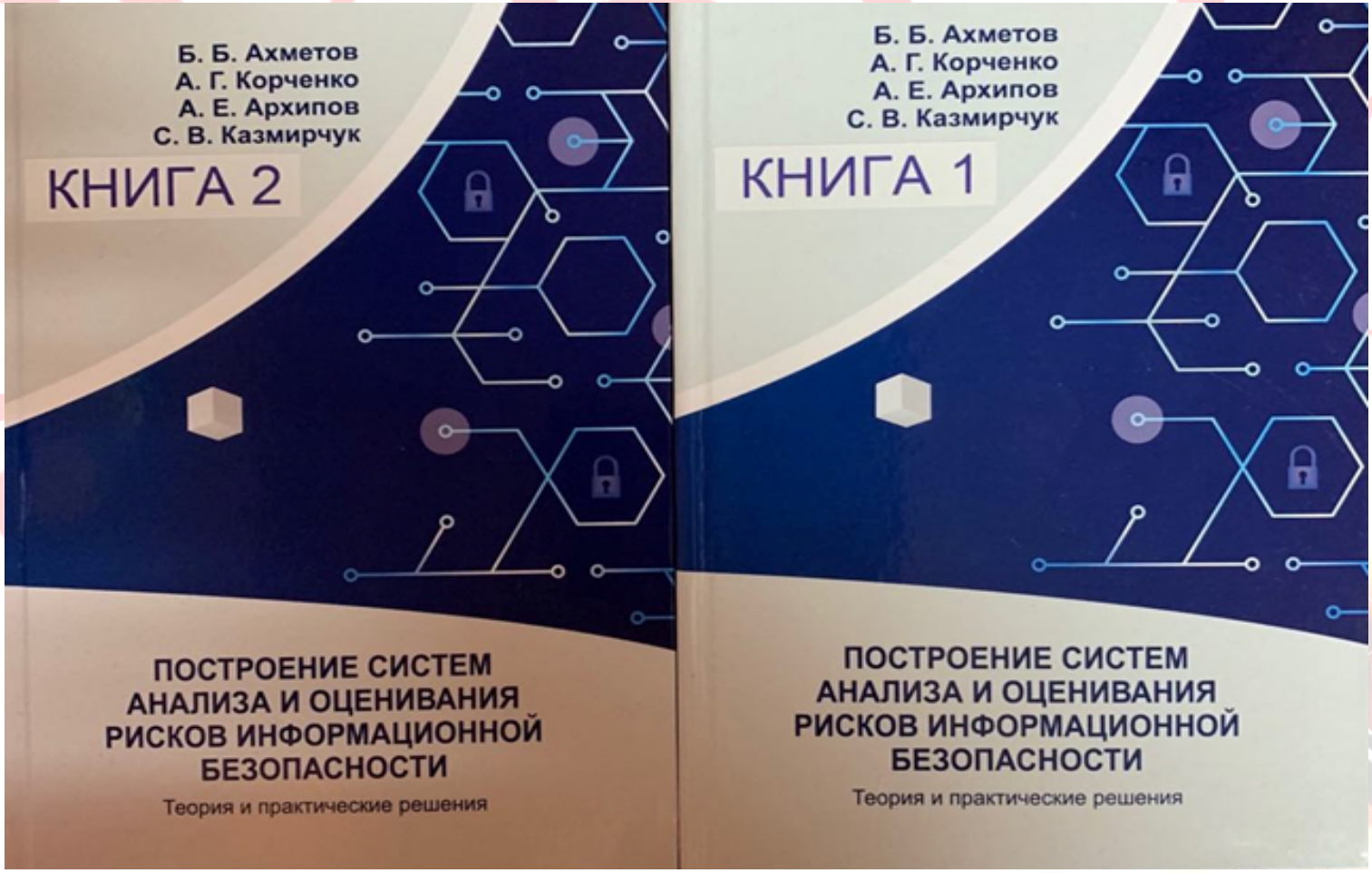
На базі запропонованої методології синтезу та структурно-функціональних моделей, розроблено алгоритмічне забезпечення та прикладні програмні моделі систем оцінювання ризиків, в яких досягнута висока інтеграція функціональних можливостей, адаптивність, гнучкість і зручність їх використання для ефективного вирішення відповідних завдань оцінювання ризиків як в детермінованому, так і в нечіткому, слабоформалізованому середовищі з можливістю функціонування в реальному часі за рахунок використання бази уразливостей NVD (National Vulnerability Database).

ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Основні наукові результати відображені у монографіях:

ОЦІНЮВАННЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Основні наукові результати відображені у монографіях:



ВИЯВЛЕННЯ ВТОРГНЕНЬ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

НАУКОВІ РЕЗУЛЬТАТИ:

1. Розроблені методи, моделі нечітких та нейромережевих засобів виявлення вторгнень з можливістю адаптації до типу кібератак, умов застосування, навчання за допомогою експертних даних, які дозволяють визначити похибку класифікації та реалізувати верифікацію отриманих рішень.

2. Розроблено метод визначення ефективності розробки нейромережевих засобів оцінювання параметрів безпеки, який дозволяє обрати найбільш ефективний засіб.

ВИЯВЛЕННЯ ВТОРГНЕНЬ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

ПРАКТИЧНІ РЕЗУЛЬТАТИ:

Розроблено та впроваджено програмні засоби оцінювання параметрів безпеки Інтернет-орієнтованих інформаційних систем для розпізнавання кібератак, які мають підвищену оперативність, адаптованість до умов застосування, нових видів кібератак та низьку обчислювальну ресурсоємність

ВИЯВЛЕННЯ ВТОРГНЕНЬ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Основні наукові результати відображені у монографіях:

ІДЕНТИФІКАЦІЯ АНОМАЛЬНИХ СТАНІВ ДЛЯ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

НАУКОВІ РЕЗУЛЬТАТИ:

1. Розроблено низку моделей та методів для ідентифікації аномальних станів, що застосовуються при побудові систем виявлення вторгнень та дозволяють розширити їх функціональні можливості щодо виявлення кібератак в m-вимірному гетерогенному параметричному довкіллі.
2. Розроблено методологію побудови систем виявлення аномалій, породжених кібератаками, яка дозволяє будувати системи, що використовуються для визначення у режимі реального часу рівня аномального стану в *m*-вимірному гетерогенному параметричному довкіллі.

ІДЕНТИФІКАЦІЯ АНОМАЛЬНИХ СТАНІВ ДЛЯ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

ПРАКТИЧНІ РЕЗУЛЬТАТИ:

На базі запропонованої методології та структурного рішення розроблено, алгоритмічне забезпечення та відповідна програмна модель системи для виявлення аномальних станів, яка може використовуватися автономно або бути розширювачем функціональних можливостей сучасних систем виявлення вторгнень, а також дозволить здійснити в режимі реального часу необхідну адаптацію (під зміни атакуючого довкілля) до виявлення аномалій, породжених модифікованими або раніше невідомими кібератаками.

ІДЕНТИФІКАЦІЯ АНОМАЛЬНИХ СТАНІВ ДЛЯ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

Основні наукові результати відображені у монографії:

ПОБУДОВА СИМЕТРИЧНИХ КРИПТОСИСТЕМ

НАУКОВІ РЕЗУЛЬТАТИ:

Розроблені методи побудови блокових шифрів, що дозволяють будувати шифри із підвищеними вимогами стійкості відносно методів лінійного та диференціального криптоаналізу при заданих обмеженнях щодо швидкості шифрування.

ПОБУДОВА СИМЕТРИЧНИХ КРИПТОСИСТЕМ

ПРАКТИЧНІ РЕЗУЛЬТАТИ:

1. Розроблено два нові блокові шифри Luna та Neptun, які забезпечують високу швидкість шифрування електронних інформаційних ресурсів, а також практичну стійкість відносно методів лінійного та диференціального криптоаналізу.
2. Розроблено структури криптографічних обчислювачів на основі підходу конвеєризації процесу обчислень, що дають можливість підвищити швидкість обробки електронних інформаційних ресурсів.

ПОБУДОВА СИМЕТРИЧНИХ КРИПТОСИСТЕМ

ПРАКТИЧНІ РЕЗУЛЬТАТИ:

3. Запропоновано спосіб підвищення швидкодії блокових шифрів для організації більш ефективних криптосистем.

4. Розроблено низку програмних засобів, що дозволяють моделювати роботу систем квантового розподілу ключів на основі пінг-понг протоколу, шифрувати електронні інформаційні ресурси, генерувати таблиці замін для блокових шифрів із високими показниками стійкості відносно методів лінійного та диференціального криптоаналізу та ін.

СТЕГАНОГРАФІЧНІ МЕТОДИ ПРИХОВУВАННЯ ДАНИХ

НАУКОВІ РЕЗУЛЬТАТИ:

1. Розроблено метод побітового приховування інформації у точково-задані криві векторних зображень, який, за рахунок впливу послідовності даних на процес сегментації кривих з фіксованим кроком зміни параметра побудови заданих кривих (розбиття кривих на сегменти відбувається лише при вбудовуванні нульового/одиничного біта приховуваної послідовності даних), забезпечує високу швидкодію приховування, вилучення секретного повідомлення та підвищує стійкість до активних атак на основі афінних перетворень.

СТЕГАНОГРАФІЧНІ МЕТОДИ ПРИХОВУВАННЯ ДАНИХ

НАУКОВІ РЕЗУЛЬТАТИ:

2. Розроблено метод шаблонного приховування інформації у точково-задані криві векторних зображень, який, за рахунок впливу послідовності даних на процес сегментації кривих згідно визначеної таблиці співвідношень значень елементів шаблону різним крокам зміни параметра побудови заданих кривих (при розбитті кривої на два сегменти вбудовується блок даних), на відміну від побітового методу, дозволяє зменшити розміри стеганоконтейнерів, підвищити швидкість вбудовування та стійкість до активних атак на основі афінних перетворень.

СТЕГАНОГРАФІЧНІ МЕТОДИ ПРИХОВУВАННЯ ДАНИХ

ПРАКТИЧНІ РЕЗУЛЬТАТИ:

1. Розроблено два нових стеганографічні алгоритми приховування інформації у криві Без'є третього ступеня StegoBIT та StegoTEMPL, що можуть бути використані в стеганографічних системах для підвищення стійкості до активних атак на основі афінних перетворень.

2. Розроблено програмні засоби, що реалізують запропоновані алгоритми приховування інформації та дозволяють вбудовувати інформацію у криві Без'є векторних зображень. Також, розроблено програмний засіб, що дозволяє спотворювати векторні зображення на основі виконання до них афінних перетворень.

ВИЯВЛЕННЯ, ІДЕНТИФІКАЦІЯ ТА ОЦІНЮВАННЯ ВПЛИВУ КРИЗОВИХ СИТУАЦІЙ В ІТ-СФЕРІ

НАУКОВІ РЕЗУЛЬТАТИ:

1. Розроблена інтегрована модель представлення інцидентів / потенційних кризових ситуацій (ІПКС) на базисі теорії нечітких множин, в якій інтегруються ідентифікатори ІПКС, базові оціночні та ідентифікуючі компоненти та набір евристичних правил, що дозволила виявлення кризових ситуацій в нечіткому середовищі,
2. Розроблено методи виявлення ІПКС та оцінки критичності ситуації, що за рахунок обробки нечітких ідентифікуючих та оціночних параметрів, моделей лінгвістичних еталонів та евристичних правил, дозволяють виявити інциденти/потенційні кризові ситуації та оцінити критичність ситуації, яка склалася внаслідок впливу зазначених інцидентів в інформаційному середовищі, відображеного у вигляді індикатора.

ВИЯВЛЕННЯ, ІДЕНТИФІКАЦІЯ ТА ОЦІНЮВАННЯ ВПЛИВУ КРИЗОВИХ СИТУАЦІЙ В ІТ-СФЕРІ

ПРАКТИЧНІ РЕЗУЛЬТАТИ:

На базі запропонованої моделі представлення ІПКС та методів виявлення ІПКС та оцінки критичності ситуації, розроблено алгоритмічне забезпечення та прикладні програмні моделі та комп'ютерні програми «Система виявлення ІПКС» та «Система оцінки критичності ситуації», які дозволили підвищити ефективність та рівень автоматизації процесів управління кризовими ситуаціями, і використовуються для ідентифікації і раннього виявлення інцидентів різного характеру в нечітких слабоформалізованих середовищах для підтримки прийняття рішень в умовах дії КС, а також оцінки рівня критичності ситуації, що є наслідком впливу ІПКС.

ВИЯВЛЕННЯ ТА ІДЕНТИФІКАЦІЯ ПОРУШНИКІВ В ІКСМ

НАУКОВІ РЕЗУЛЬТАТИ:

Розроблено методи виявлення та ідентифікаціїї порушника в ІКСМ, які за рахунок використання теорії нечітких множини та заданих параметрів ідентифікації з використання евристичних підходів, дозволяють виявити та категоризувати порушника інформаційної безпеки, зокрема ідентифікувати тип порушника в аспекті їх реалізації безпосередньо людиною чи з використанням автоматизованих ботів.

ВИЯВЛЕННЯ ТА ІДЕНТИФІКАЦІЯ ПОРУШНИКІВ В ІКСМ

ПРАКТИЧНІ РЕЗУЛЬТАТИ:

На базі запропонованих методів виявлення та ідентифікаціїї порушника в ІКСМ, розроблено алгоритмічне забезпечення та прикладні програмні моделі на основі застосування технологій Honeypot, які дозволили здійснити виявлення порушника в ІКСМ та здійснити його категоризацію за такими видами як «Порушник-людина» (Хакер, Крекер, Спамер, Дезінформатор) та «Порушник-бот» в нечітких слабоформалізованих середовищах, при цьому підвищивши рівень автоматизації моніторингу компютерних систем та мереж.

ОЦІНЮВАННЯ ШКОДИ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ У РАЗІ ВИТОКУ ДЕРЖАВНОЇ ТАЄМНИЦІ

НАУКОВІ РЕЗУЛЬТАТИ:

1. Розроблено моделі засобів та базову модель інтегрованого представлення параметрів шкоди, яка дозволяє використовувати необхідну множину наборів параметрів існуючих засобів забезпечення сфери ОДТ для оцінювання величини можливої шкоди національній безпеці;

2. Розроблено метод аналізу і оцінки величини можливої шкоди національній безпеці у сфері ОДТ, який розраховує показники економічної шкоди та інший тяжкий наслідок у кількісному і вартісному значенні, що дозволило визначити величину можливої сукупної шкоди національній безпеці у разі розголошення ДТ чи втрати МНСІ;

ОЦІНЮВАННЯ ШКОДИ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ У РАЗІ ВИТОКУ ДЕРЖАВНОЇ ТАЄМНИЦІ

НАУКОВІ РЕЗУЛЬТАТИ:

3. Розроблено метод оцінювання важливості відомостей за сферами ДТ, який дозволив провести порівняльний аналіз важливості статей, існуючих сфер і ЗВДТ у цілому;

4. Удосконалено метод визначення рівня компетентності членів експертної комісії при державних експертах з питань таємниць;

5. Розроблено методологію синтезу системи оцінювання шкоди національній безпеці України у сфері ОДТ, яка дозволяє використовуючи існуючі інструментальні засоби забезпечення сфери ОДТ встановити й обґрунтувати шкоду національній безпеці у разі витоку ДТ.

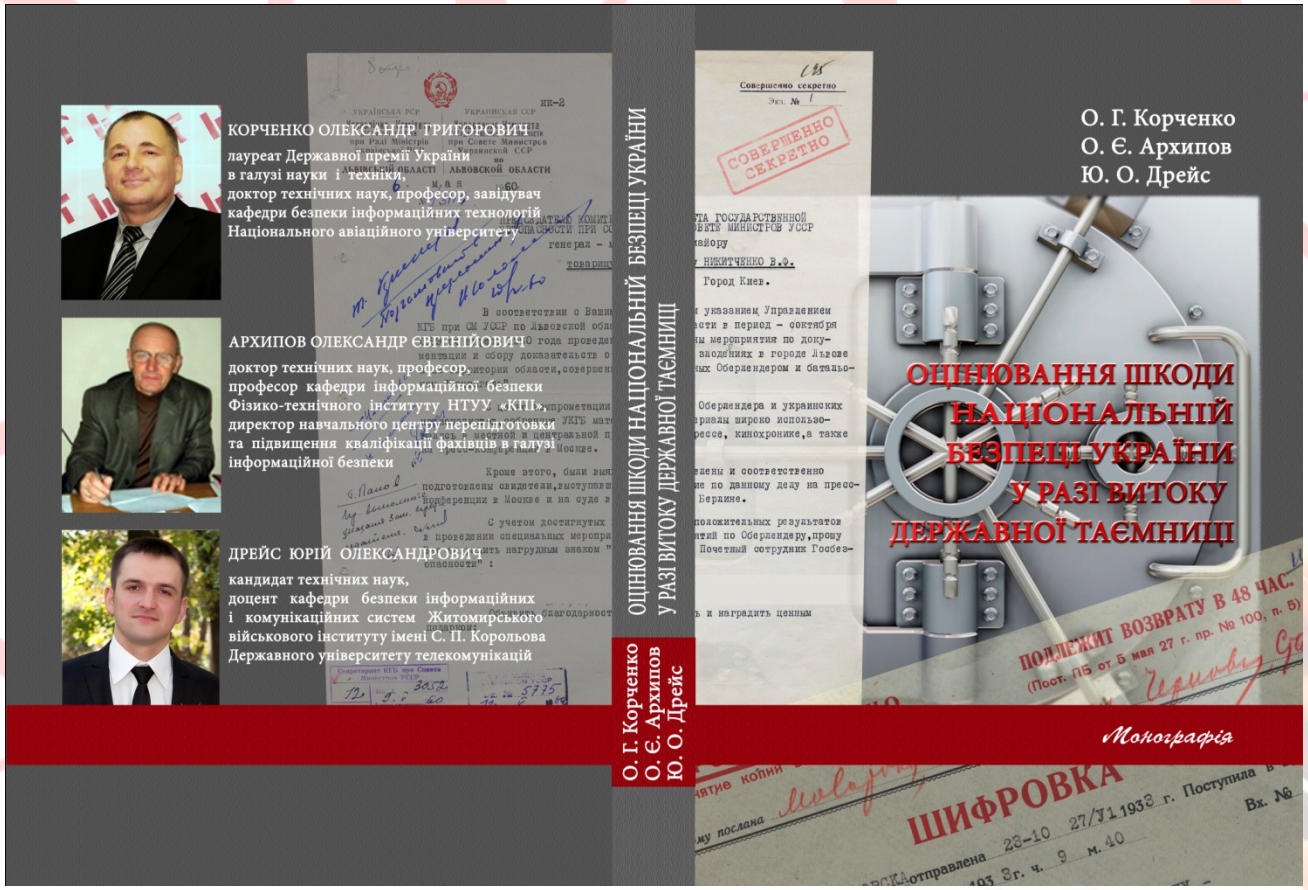
ОЦІНЮВАННЯ ШКОДИ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ У РАЗІ ВИТОКУ ДЕРЖАВНОЇ ТАЄМНИЦІ

ПРАКТИЧНІ РЕЗУЛЬТАТИ:

На базі запропонованої методології синтезу та структурно-функціональних моделей, розроблено алгоритмічне забезпечення систем оцінювання шкоди національній безпеці, в яких досягнута висока інтеграція функціональних можливостей, адаптивність, гнучкість і зручність їх використання для ефективного вирішення відповідних завдань оцінювання шкоди національній безпеці у разі витоку ДТ з можливістю функціонування в реальному часі з формуванням експертного висновку за рахунок використання ЗВДТ та у відповідності до існуючих методик для державних експертів з питань таємниць.

ОЦІНЮВАННЯ ШКОДИ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ У РАЗІ ВИТОКУ ДЕРЖАВНОЇ ТАЄМНИЦІ

Основні наукові результати відображені у монографії:



ТЕХНОЛОГІЇ КВАНТОВОЇ КРИПТОГРАФІЇ

НАУКОВІ РЕЗУЛЬТАТИ:

1. Розроблено низку нових більш ефективних протоколів квантового розподілу ключів та квантового прямого безпечного зв'язку, які дозволяють збільшити швидкість роботи протоколів при збереженні стійкості до деяких видів атак;

2. Розроблено нові криптостійкі протоколи шифрування даних для систем захисту на базі квантових технологій;

3. Розроблено методи і процедури підвищення рівня безпеки квантових протоколів, що дозволяють використовувати системи з більшою інформаційною ємністю (використання кудитів).

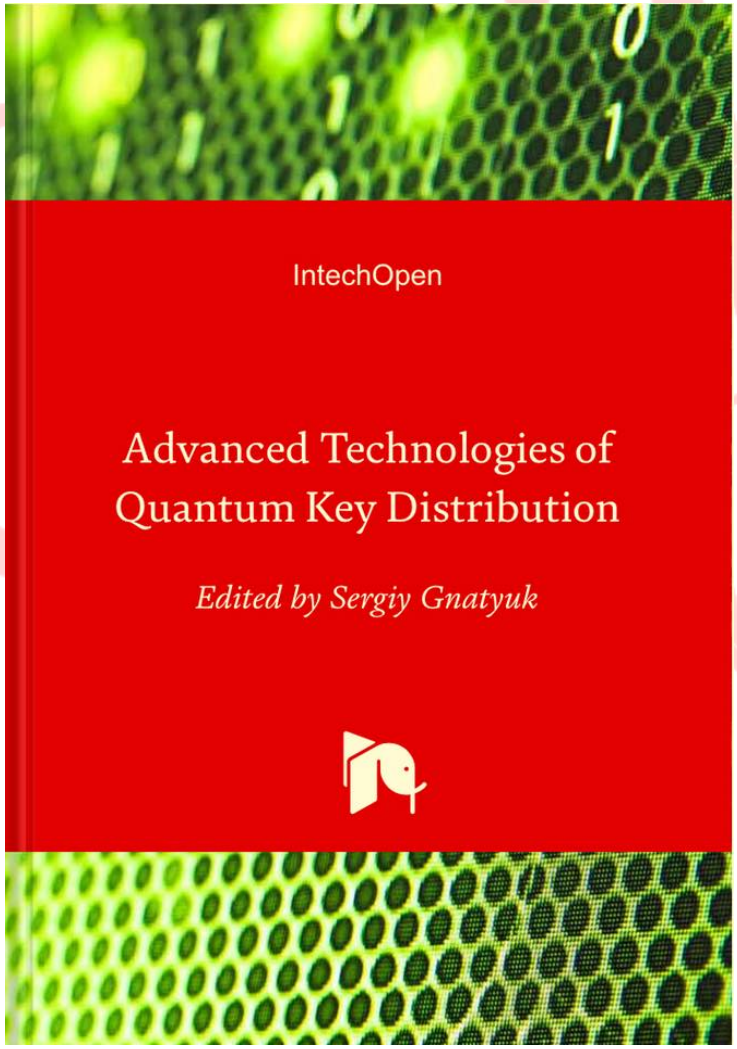
ТЕХНОЛОГІЇ КВАНТОВОЇ КРИПТОГРАФІЇ

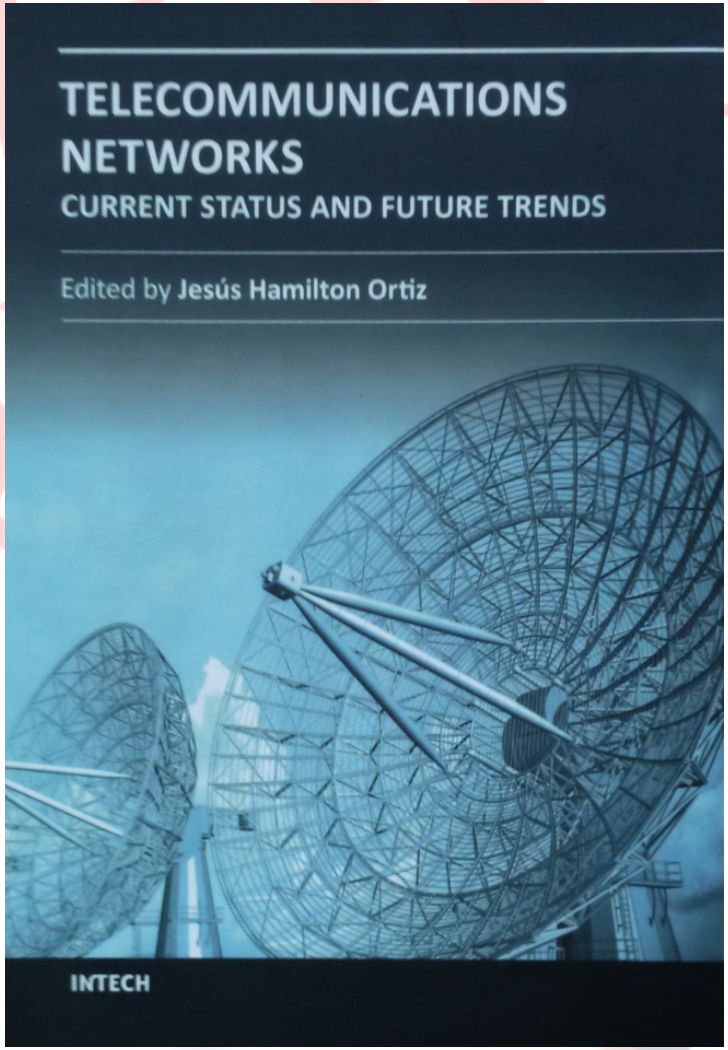
ПРАКТИЧНІ РЕЗУЛЬТАТИ:

Розроблено низку комп'ютерних програм, захищених свідоцтвами про реєстрацію авторського права на твір, зокрема «Імітаційна модель пінг-понг протоколу в квантовому каналі з шумом» (№ 36373 від 04.01.2011 року), «GenSBOX3» (№ 48037 від 26.02.2013 року), «TrytTon 2012» (№ 48040 від 26.02.2013 року) та «Model ping-pong protocol» (№ 48041 від 26.02.2013 року), а також отримано патент України на корисну модель «Спосіб підсилення стійкості квантових протоколів прямого безпечного зв'язку» №108520 України, МПК H04K 1/06 (2006.01). – № u201512445; Заявл. 16.12.2015; Опубл. 25.07.2016.

ТЕХНОЛОГІЇ КВАНТОВОЇ КРИПТОГРАФІЇ

Основні наукові результати відображені у монографіях:





ЗАХИСТ ЦИВІЛЬНОЇ АВІАЦІЇ ВІД КІБЕРЗАГРОЗ

НАУКОВІ РЕЗУЛЬТАТИ:

1. Розроблено базову модель формування вимог до забезпечення кібербезпеки цивільної авіації (ЦА), яка за рахунок введення базової множини вимог, які містяться у різних керівних документах щодо безпеки ЦА, та відповідних підмножин, що характеризують базову множину, дає можливість формалізувати процес створення повної множини вимог, які необхідно забезпечити для захисту ЦА від кіберзагроз;
2. Розроблено мультирівневу модель даних, яка за рахунок використання базової моделі формування вимог до забезпечення кібербезпеки ЦА, конкатенації та бінарно-шістнадцяткового кодового представлення характеристик безпеки, а також введення множини розширених моделей безпеки та підмножин характеристик безпеки, дозволяє формалізувати процес ідентифікації забезпеченості вимог та визначення режимів безпеки критичних авіаційних інформаційних систем;

ЗАХИСТ ЦИВІЛЬНОЇ АВІАЦІЇ ВІД КІБЕРЗАГРОЗ

НАУКОВІ РЕЗУЛЬТАТИ:

3. Розроблено метод оцінювання повноти виконання вимог, який за рахунок введення множини коефіцієнтів важливості, ініціалізації множин, визначення значень повноти, нормалізації параметрів та перемасштабування, дає можливість визначити кількісні параметри, що характеризують повноту виконання множини вимог щодо кібербезпеки ЦА та окремих вимог відповідних керівних органів;

4. Розроблено методологію формування та забезпечення державної системи кібербезпеки в галузі ЦА, яка за рахунок розроблених базової моделі формування і мультирівневої моделі ідентифікації виконання вимог до забезпечення кібербезпеки ЦА, теоретичних положень щодо кібербезпеки ЦА, низки методів забезпечення відповідних вимог, а також методу оцінювання повноти виконання вимог, дозволяє забезпечити підтримку процесів формування державної системи кібербезпеки в галузі ЦА з урахуванням вимог керівних органів, а також забезпечити захист ЦА від кіберзагроз.

МЕТОДИ УПРАВЛІННЯ КІБЕРІНЦИДЕНТАМИ

НАУКОВІ РЕЗУЛЬТАТИ:

1. Розроблено метод мережево-центричного моніторингу кібер-інцидентів (КбІ), який за рахунок класифікації кібератак та порівняння їх параметрів з еталонними, формування множини базових правил і встановлення зв'язків між підкласом кібератаки та категорією КбІ на базі обробки їх статистики, ідентифікації об'єктів захисту та експертного оцінювання впливу на них КбІ, узгодження суджень експертів та ранжування ступенів небезпеки КбІ, дозволяє визначити найбільш важливі об'єкти захисту, прогнозувати категорії КбІ, які виникнуть внаслідок реалізації кібератаки, та їх рівень небезпеки (критичності).

2. Розроблено метод оцінювання ефективності обробки КбІ центрами CSIRT, який за рахунок визначення показників функціонування CSIRT, виділення серед них ключових показників ефективності використовуючи багаточинниковий кореляційно-регресійний аналіз, побудови панелі індикаторів та візуалізації залежності KPI та ефективності, дає можливість проводити аудит діяльності CSIRT.

ЗАХИСТ ВІД ШКІДЛИВИХ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ВПЛИВІВ

НАУКОВІ РЕЗУЛЬТАТИ:

1. Розроблено класифікацію методів медіа маніпулятивного впливу на свідомість та підсвідомість людей, яка за рахунок часткових узагальнень теоретичних положень та практичних досягнень у галузі, дозволяє розширити можливості щодо вибору певних методів для реалізації інформаційних операцій та розробки превентивних заходів.

2. Розроблено модель оцінювання маніпулятивного впливу мас медіа, яка дає можливість кількісно оцінювати негативні інформаційно-психологічні впливи на громадян, суспільство та державу у цілому. Отримали подальший розвиток структурно-аналітичні моделі маніпулятивного впливу, які за рахунок синтезу формалізованих представлень мас медіа, каналу впливу та інформаційного середовища і кортежу коефіцієнтів якості інформації, дають можливість оцінити ефективність впливу мас медіа на особу та соціальну групу.