Науково-технічна конференція “Інформаційна безпека України”

Report of Contributions

https://indico.knu.ua/e/isu2019

Contribution ID: **224** Type: **Усна**

АНАЛІЗ МЕТОДІВ ПОШУКУ ЗАКЛАДНИХ ПРИСТРОЇВ

Thursday, 25 April 2019 17:40 (15 minutes)

Abstract

.....

Contact Phone

Primary authors: ДОВБНЯ, Іван (ІСЗЗІ НТУУ КПІ ім. І. Сикорського); ДОВБНЯ, Іван

Presenter: ДОВБНЯ, Іван (ІСЗЗІ НТУУ КПІ ім. І. Сикорського)

Session Classification: Загальні питання інформаційної безпеки України

Track Classification: Загальні питання інформаційної безпеки України

Contribution ID: **225** Type: **Усна**

Інформаційна безпека України

Thursday, 25 April 2019 15:10 (15 minutes)

Abstract

…..

Contact Phone

Primary author: ДОВБНЯ , Сергій (КНУ ТШ)

Presenter: ДОВБНЯ , Сергій (КНУ ТШ)

Session Classification: Загальні питання інформаційної безпеки України

Track Classification: Загальні питання інформаційної безпеки України

Contribution ID: **226** Type: **Усна**

МЕТОДИ ЛІКВІДАЦІЇ ЗАГРОЗ КІБЕРБЕЗПЕЦІ ДЕРЖАВИ ПРИ ВИКОРИСТАННІ ЗАХИЩЕНИХ ВУЗЛІВ ІНТЕРНЕТ ДОСТУПУ

Thursday, 25 April 2019 14:00 (15 minutes)

Abstract

…..

Contact Phone

Primary author: ДОВБНЯ , Сергій (ФОП Довбня С.Я.)

Presenter: ДОВБНЯ , Сергій (ФОП Довбня С.Я.)

Session Classification: Програмні та апаратні засоби інформаційної безпеки

Track Classification: Програмні та апаратні засоби інформаційної безпеки

Contribution ID: **227** Type: **Усна**

Аналіз засобів та методів вимірювання струмів та напруг наведень в лініях електроживлення та заземлення

Thursday, 25 April 2019 16:15 (15 minutes)

Abstract

Сучасні методи та засоби технічної розвідки дозволяють виявляти інформаційну складову сигналів на рівні природних завад. Це також актуально для каналів витоку інформації лініями електроживлення та заземлення. У зв'язку з використанням в Україні стандартів ЄС з електроживлення 220 В, актуальним є питання проведення вимірювань диференційних, сумарних струмів та напруг в лініях електроживлення та струму в лінії заземлення в діапазоні від 9 кГц до 1 ГГц та більше.

Contact Phone

Primary author: KYKLA, Volodymyr

Co-author: DOVBNYA, Serghiy

Presenter: KYKLA, Volodymyr

Session Classification: Програмні та апаратні засоби інформаційної безпеки

Track Classification: Програмні та апаратні засоби інформаційної безпеки

Contribution ID: **228** Type: **Усна**

ОЖЕ-СПЕКТРОМЕТРІЯ ЯК МЕТОД РЕВЕРС-ІНЖИНІРИНГУ

Thursday, 25 April 2019 15:45 (15 minutes)

Abstract

В роботі запропоновано використати Оже-електронну спектрометрію для проведення реверс-інжинірингу в галузі напівпровідникової електроніки. Проведено аналіз схемотехнічних рішень, використаних у вимірювальному обладнанні Оже-спектрометра 09-ІОС3 та запропоновано шляхи його модернізації з використанням сучасної елементної бази.

Contact Phone

Primary authors: БЕХ, Ігор Іванович (Київський національний університет імені Тараса Шевченка, факультет радіофізики, електроніки та комп'ютерних систем, кафедра радіотехніки та радіоелектронних систем); СЕРЕБРЕНІКОВ, Сергій Михайлович (Київський національний університет імені Тараса Шевченка, факультет радіофізики, електроніки та комп'ютерних систем, кафедра радіотехніки та радіоелектронних систем, студент); ТКАЧЕНКО, Іван Миколайович (Київський національний університет імені Тараса Шевченка, факультет радіофізики, електроніки та комп'ютерних систем, кафедра радіотехніки та радіоелектронних систем, студент)

Presenter: СЕРЕБРЕНІКОВ, Сергій Михайлович (Київський національний університет імені Тараса Шевченка, факультет радіофізики, електроніки та комп'ютерних систем, кафедра радіотехніки та радіоелектронних систем, студент)

Session Classification: Програмні та апаратні засоби інформаційної безпеки

Track Classification: Програмні та апаратні засоби інформаційної безпеки

Contribution ID: **229** Type: **not specified**

КОНКУРЕНТНА РОЗВІДКА В СИСТЕМІ ТЕХНІЧНГО ЗАХИСТУ ІНФОРМАЦІЇ

Thursday, 25 April 2019 15:25 (15 minutes)

Abstract

Розглянуті основні підходи щодо діяльності та розвитку конкурентної розвідки, її складові та загрози витоку інформації. Проаналізовані форми та методи ефективної роботи бізнесу в Україні. Розглянуті моделі загроз забезпечення безпеки бізнесу.

Contact Phone

Primary author: НІКІТЧИН, Олександр (Київський національний університет імені Тараса Шевченка)

Presenter: НІКІТЧИН, Олександр (Київський національний університет імені Тараса Шевченка)

Session Classification: Загальні питання інформаційної безпеки України

Track Classification: Загальні питання інформаційної безпеки України

Contribution ID: **230** Type: **Усна**

Програмні комплекси розмежування доступу користувачів до інформаційних ресурсів автоматизованих систем

Thursday, 25 April 2019 16:40 (15 minutes)

Abstract

Розглянуто програмні комплекси розмежування доступу до інформаційних ресурсів автоматизованих систем та огляд основних принципів побудови програмних засобів захисту інформації, визначена практична ініціалізація методів і принципів захисту від несанкціонованого доступу до інформації з обмеженим доступом.

Contact Phone

Primary author: НІКІТЧИН, Олександр (ФРЕКС КНУ)

Co-author: ВАСИЛЕНКО, Олександр (студент ФРЕКС КНУ ім.Шевченка)

Presenter: ВАСИЛЕНКО, Олександр (студент ФРЕКС КНУ ім.Шевченка)

Session Classification: Загальні питання інформаційної безпеки України

Track Classification: Загальні питання інформаційної безпеки України

Contribution ID: **231** Type: **Усна**

Організація захисту об’єкту інформаційної діяльності від витоку інформації акустичним каналом

Thursday, 25 April 2019 15:40 (15 minutes)

Abstract

Розглянуті питання організаційних та технічних заходів захисту інформації на об’єктах інформаційної діяльності.

Contact Phone

Primary author: НІКІТЧИН, Олександр (ФРЕКС КНУ)

Co-author: БЛАЩУК, Валентин (ФРЕКС КНУ імені Шевченка)

Presenter: БЛАЩУК, Валентин (ФРЕКС КНУ імені Шевченка)

Session Classification: Загальні питання інформаційної безпеки України

Track Classification: Загальні питання інформаційної безпеки України

Contribution ID: **232** Type: **not specified**

Інтернет-піратство в Україні

Thursday, 25 April 2019 14:40 (15 minutes)

Abstract

Тому піратство завдає шкоди автору тільки тоді, коли забезпечені користувачі, мають змогу придбати ліцензійну продукцію, купують контрафактну. Тільки тоді автор недоодержує законну прибуток. Отже, шкода приносить не піратство саме собою, а недобросовісність, користь деяких людей.

Contact Phone

Primary author: ТОМИН, Оксана

Presenter: ТОМИН, Оксана

Session Classification: Загальні питання інформаційної безпеки України

Track Classification: Загальні питання інформаційної безпеки України

Contribution ID: **235** Type: **not specified**

ВИКОРИСТАННЯ КІБЕРФІЗИЧНИХ ПІДХОДІВ ДЛЯ КОНТРОЛЮ СТАНУ ФІЗИЧНОЇ ІНФРАСТРУКТУРИ

Thursday, 25 April 2019 16:30 (15 minutes)

Abstract

У даний час дослідниками багатьох країн ведуться дослідження можливостей кіберфізичних систем в багатьох галузях економіки. В розвиток цих досліджень розвинуті країни вкладають значні ресурси, розраховуючи отримати як економічний так і соціальний ефект.
Під кіберфізичною системою (КФС) розуміють поєднання фізичних процесів та кібернетичних компонентів, які забезпечують організацію вимірювально-обчислювальних процесів, захищене зберігання та обмін вимірювальною і службовою інформацією, організацію та здійснення впливів на фізичні процеси.

У даний час дослідниками багатьох країн ведуться дослідження можливостей кіберфізичних систем в багатьох галузях економіки. В розвиток цих досліджень розвинуті країни вкладають значні ресурси, розраховуючи отримати як економічний так і соціальний ефект.
Під кіберфізичною системою (КФС) розуміють поєднання фізичних процесів та кібернетичних компонентів, які забезпечують організацію вимірювально-обчислювальних процесів, захищене зберігання та обмін вимірювальною і службовою інформацією, організацію та здійснення впливів на фізичні процеси.

Метою цієї роботи є дослідження можливості використання КФС для контролю стану фізичної інфраструктури.
У епоху КФС пристрої стають дедалі «розумнішими», що дає нам додаткові можливості для та моніторингу систем та контролю ресурсів (наприклад, вода та електрика). Це стає можливим завдяки вбудованим розширеним можливостям зв'язку та обчислення, що в кінцевому підсумку формує КФС. Нова складна та гнучка інфраструктура створюється завдяки оснащенню датчиками та виконавчими елементами, а також здатності передавати виміряні спостережувані дані, приймати розумні рішення та діяти відповідно до них.
КФС все більше відслідковує та контролює фізичні активи в реальних інфраструктурах таких як системи життєзабезпечення, управління безпекою руху, сучасні автомобільні системи, управління виробничими процесами, , екологічний контроль, контроль та управління критичною інфраструктурою, оборонні систем, виробництво та ін. КФС не тільки спираються на розробки в інших технологічних областях, а й доповнюють їх, виступаючи в ролі сприятливого чинника для формування великомасштабних комплексних Систем Систем. Зрозуміло, що КФС виходить за межі кожної окремої галузі та покликані зменшити складність, паралельно знизити витрати та підвищити ефективність.
Завдяки даним, що збираються та за потреби аналізуються кіберфізичною системою є можливість значно спростити всеохоплююче обстеження та аналіз існуючого стану підприємства. У разі інцидентів зібрана інформація допоможе незалежному інспектуванню, проведенню розслідування при встановленні причин, джерел та осіб які завдали збитки, формуванні доказової бази
Таким чином кіберфізичні підходи для контролю стану фізичної інфраструктури дозволяють

надавати складні послуги не лише кінцевим користувачам, а й всім зацікавленим сторонам, інтегрованим в ціннісний ланцюжок, а також позиціонує зміну правил гри та зміну шляху, для створення більш інтелектуальної інфраструктури.

Contact Phone

Primary authors: RUDNITSKA, Olena (Kyiv National University of Construction and Architecture); KHLAPONIN, Dmytro

Presenter: KHLAPONIN, Dmytro

Session Classification: Програмні та апаратні засоби інформаційної безпеки

Track Classification: Програмні та апаратні засоби інформаційної безпеки

Contribution ID: **236** Type: **not specified**

ПІДХОДИ ДО ОРГАНІЗАЦІЇ ІНФРАСТРУКТУРИ ВІДДАЛЕНИХ РОБОЧИЙ МІСЦЬ

Thursday, 25 April 2019 14:15 (15 minutes)

Abstract

У нинішній час користувачі переходять на роботу з новими технологіями – мобільними пристроями та хмарними сервісами, при цьому для адміністраторів стає все далі складніше організувати доступ до додатків в IOS, Android пристроях, а також можливість доступу до операційних систем Windows, Linux. Питання захисту даних стає номером один при проектуванні IT інфраструктурі як в локальних ЦОД так і в хмарах.
Метою цієї роботи є дослідження підходу до організації, управління та захисту інфраструктури з використанням мобільних пристроїв та хмарних сервісів.
Одним з основних рішень цієї проблеми є використання технології – інфраструктури віртуальних робочих місць (VDI).
Чому саме VDI? Використання інфраструктури віртуальних робочих місць дозволяє отримувати користувачам доступ до необхідних додатків або операційних систем будь-де та з будь-якого пристрою безпечним способом.
При використанні технології VDI можливо налаштування шифрованого з'єднання клієнтського пристрою та серверу з VDI чи хмари, таким чином користувачі завжди мають доступ до даних по надійним каналам зв'язку, а дані при цьому залишаються в ЦОД чи хмарі підприємства, тобто не залишають захищеного периметру. Це дозволяє компанія захищати свої дані від витоку через копіювання на змінні носії чи відправлення даних через пошту шляхом використання програмного забезпечення (data loss prevention) DLP, яке контролює всю діяльність користувача з робочим місцем в цілому.
Дані, які зберігаються на системах збереження даних в локальному ЦОД чи хмарі також обов'язково підлягають шифруванню до запису цих даних на носії.
Якщо порівнювати VDI технології з такими рішеннями як Remote Desktop Services (RDS), то сучасні системи VDI мають багато переваг в застосуванні. Технологія RDS обмежена в використанні і підтримує роботу тільки Windows операційних систем, VDI же може працювати з Windows, Linux, MacOS, Android, IOS, включаючи мобільні пристрої. Інфраструктура VDI працює з декількома віртуальними та фізичними машинами, що дає змогу забезпечити відмово стійкість сервісу, RDS же працює з однією операційною системою, при відмові якої користувачі не зможуть продовжувати роботу.
Таким чином розмістивши віртуальне робоче місце користувача в локальному ЦОД чи хмарі з забороною по політикам безпеки зберігати дані на локальних пристроях ми забезпечуємо всеохоплюючу безпеку даних - безпечна передача даних, безпечне зберігання даних, захист від витоку інформації.

Contact Phone

Primary authors: RUDNITSKA, Olena (Kyiv National University of Construction and Architecture); BOYKO, Ganna (Kyiv National University of Construction and Architecture); KAMYANOV, Sergey (Kyiv National University of Construction and Architecture)

Presenter: KAMYANOV, Sergey (Kyiv National University of Construction and Architecture)

Session Classification: Програмні та апаратні засоби інформаційної безпеки

Track Classification: Програмні та апаратні засоби інформаційної безпеки

Contribution ID: **237** Type: **Усна**

Підхід до оцінки ризику інформаційної безпеки на основі аналізу факторів загроз та вразливостей

Thursday, 25 April 2019 14:00 (15 minutes)

Abstract

…..

Contact Phone

Primary author: ЇЗМАЙЛОВА, Ольга (КНУ БА)

Presenter: ЇЗМАЙЛОВА, Ольга (КНУ БА)

Session Classification: Загальні питання інформаційної безпеки України

Track Classification: Загальні питання інформаційної безпеки України

Contribution ID: **238** Type: **Усна**

SECURITY VULNERABILITIES OF IOT

Thursday, 25 April 2019 16:55 (15 minutes)

Abstract

…..

Contact Phone

Primary author: СЛАБКОВСЬКА, Марія (КНУБА)

Presenter: СЛАБКОВСЬКА, Марія (КНУБА)

Session Classification: Загальні питання інформаційної безпеки України

Track Classification: Загальні питання інформаційної безпеки України

Contribution ID: **240** Type: **Усна**

Сценарій реалізації захищеної системи оцінки інноваційних рішень техногенної безпеки

Thursday, 25 April 2019 18:10 (15 minutes)

Abstract

Доповідь присвячена аналізу базового сценарію системи оцінки інноваційних рішень техногенної безпеки

Contact Phone

Primary authors: ПОТЬОМКІНА, Валерія; СИДОРЕНКО, Валерій; ІЗМАЙЛОВА, Ольга

Presenter: ПОТЬОМКІНА, Валерія

Session Classification: Загальні питання інформаційної безпеки України

Track Classification: Загальні питання інформаційної безпеки України

Contribution ID: **241** Type: **Усна**

SECURITY VULNERABILITIES OF IOT

Thursday, 25 April 2019 18:10 (15 minutes)

Abstract

Analysis of up-to-date IoT solutions, standarts and requirements, revealing of vulnerabilities and overall solution according to protection of weak points.

Contact Phone

Primary author: СЛАБКОВСЬКА, Марія (Київський національний університет будівництва і архітектури)

Presenter: СЛАБКОВСЬКА, Марія (Київський національний університет будівництва і архітектури)

Session Classification: Програмні та апаратні засоби інформаційної безпеки

Track Classification: Програмні та апаратні засоби інформаційної безпеки

Contribution ID: **242** Type: **not specified**

ОБҐРУНТУВАННЯ НАПРЯМУ УДОСКОНАЛЕННЯ ЗАСОБУ ПРОСТОРОВОГО ЕЛЕКТРОМАГНИТНОГО ЗАШУМЛЕННЯ

Thursday, 25 April 2019 15:55 (15 minutes)

Abstract

В сучасних умовах все більш використовуються засоби обчислювальної техніки та носії інформації які працюють на тактових частотах в діапазоні від 750 МГц до 3 ГГц та більше. Відповідно до цього змінився частотний діапазон побічних електромагнітних випромінювань (далі ПЕМВ) які мають інформаційні ознаки. Одним із методів технічного захисту інформації є застосування маскуючого електромагнітного шуму спектр якого повинен відповідати спектру сигналів, які приховуємо від засобів технічних розвідок.

Contact Phone

Primary author: САВОСІК, Олександр

Presenter: САВОСІК, Олександр

Session Classification: Загальні питання інформаційної безпеки України

Track Classification: Загальні питання інформаційної безпеки України

Contribution ID: **243** Type: **not specified**

Актуальні та найбільш «популярні» методи захисту серверів

Thursday, 25 April 2019 16:00 (15 minutes)

Abstract

Доповідь присвячена одному з найголовніших етапів захисту автоматизованої системи - серверного обладнання, на якому знаходяться бази даних.

Contact Phone

Primary author: DOUMENKO, Yulia

Presenter: DOUMENKO, Yulia

Session Classification: Програмні та апаратні засоби інформаційної безпеки

Track Classification: Програмні та апаратні засоби інформаційної безпеки

Contribution ID: **244** Type: **not specified**

Підхід до оцінки ризику інформаційної безпеки на основі аналізу факторів загроз та вразливостей

Thursday, 25 April 2019 17:10 (15 minutes)

Abstract

Запропонований сценарій оцінки факторів ризику даних в інформаційних системах та технлогіях, що базується на методах експертного оцінювання.

Contact Phone

Primary authors: ШИМАНСЬКИЙ, Максим; ІЗМАЙЛОВА, Ольга

Presenter: ШИМАНСЬКИЙ, Максим

Session Classification: Загальні питання інформаційної безпеки України

Track Classification: Загальні питання інформаційної безпеки України

Contribution ID: **245** Type: **not specified**

ДЕСТРУКТИВНИЙ ІНФОРМАЦІЙНИЙ ВПЛИВ НА КЕРОВАНИЙ НАТОПІВ ЯК ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ДЕРЖАВИ

Thursday, 25 April 2019 18:25 (15 minutes)

Abstract

Останнім часом з'явилася велика кількість оголошень про тимчасову роботу: «потрібні розносщики газет», «потрібні розклеювачі оголошень», «робота на дому». За цими оголошеннями зручно можуть ховатися будь-які деструктивні сили. На жаль, вони можуть використовувати такі технології в антиукраїнських і антидержавних цілях, виконуючи замовлення держави-агресора. Такі піраміди важко визначити, до того ж вони ховають в собі елемент раптовості, що підвищує ризики, пов'язані із загрозою організації антидержавних заходів, що призводять до захоплення адміністративних будівель, передусім відділків поліції та СБУ.

Contact Phone

Primary author: ДАШКЕВИЧ, Олександр (КНУБА)

Presenter: ДАШКЕВИЧ, Олександр (КНУБА)

Session Classification: Загальні питання інформаційної безпеки України

Track Classification: Загальні питання інформаційної безпеки України

Contribution ID: **246** Type: **Усна**

Правило обробки надлишкових даних для обґрунтування захищеності джерел від витоку інформації в рамках імплементації міжнародних стандартів з менеджменту інформаційної безпеки

Thursday, 25 April 2019 14:15 (15 minutes)

Abstract

….

Contact Phone

Primary author: ІВАНЧЕНКО, Сергій (ІСЗЗІ НТУУ КПІ імені І. Сікорського)

Presenter: ІВАНЧЕНКО, Сергій (ІСЗЗІ НТУУ КПІ імені І. Сікорського)

Session Classification: Загальні питання інформаційної безпеки України

Track Classification: Загальні питання інформаційної безпеки України

Contribution ID: **247** Type: **Усна**

ХМАРНІ ОБЧИСЛЕННЯ VSAAS В РІШЕННІ ПРОБЛЕМ БЕЗПЕКИ

Thursday, 25 April 2019 17:55 (15 minutes)

Abstract

Існуючі системи відеоспостереження мають два основні види реалізацій – локальні програмні системи, що обслуговують послуги клієнтів на строго визначеній території (VMS), а також хмарні сервіси, які використовують для проведення віддаленої роботи в галузі відеоспостереження (VSaaS).

VMS (Video Management System, Video Management Software або Video Management Server) – це повнофункціональний комплекс програмного забезпечення для управління системою відеоспостереження на місцях. Існують рішення, що забезпечують більшу надійність, наприклад Video Surveillance as a Service, скорочено VSaaS, перекладається словосполученням «відеоспостереження як послуга». Тобто це певний сервіс, що надається користувачам, головне призначення якого – записувати, зберігати, відтворювати та управляти даними відеоспостережень. VSaaS є пріоритетною технологією в сфері відеоспостереження, оскільки вона не має вразливостей кібербезпеки, властивих традиційним системам. В таких системах немає відкритих портів, вразливих брандмауерів, а програмне забезпечення сервісу віртуалізується, через що зловмисник не може отримати доступ до фізичної машини.

Очікується, що зростання VSaaS на глобальному ринку відеоспостереження буде відповідати 16,6% у період між 2017 і 2025 роками. При такому темпі оцінка цього ринку до кінця 2025 року сягне 101, 7025,11 млрд. у 2017 році [1].

Основними місцями, що підлягають застосуванню технології VSaaS є громадські місця, такі, як залізниці, дороги, аеропорти, мережі зв'язку, житлові, торгові, комерційні, організації, транспорт, урядові будівлі, промислові та інші сегменти.

Хмарний підхід та віддалений доступ до відеокамер мають деякі відмінності. VSaaS забезпечує провайдер, що бере на себе всі задачі з обслуговування програмної та апаратних частин, такі як обслуговування інфраструктури, налагодження та оновлення програмного забезпечення, підтримка його надійності та оплата роботи персоналу, що займається супроводом всієї системи. Клієнт може розподіляти права доступу до камер, змінювати їх кількість та налаштування, звертатися до архіву і підключати модулі відеоаналітики віддалено, використовуючи інтерфейс, наданий VSaaS-провайдером.

З точки зору зберігання відео є кілька видів архітектури хмарного відеоспостереження – публічна, приватна і гібридна хмара [2].

Публічний VSaaS – найпопулярніший і найпростіший тип підключення, що потребує встановлення камер і підключення сервісу. Відеозаписи з камер зберігаються і обробляються на сервері VSaaS-провайдера. Часто такий підхід застосовується для приватних осіб і бізнес-клієнтів малих і середніх компаній.

Приватний VSaaS – тип підключення, при якому відео зберігається і обробляється на стороні клієнта, використовуючи корпоративні сервери організації, і дані не виходять за межі організації. Такий варіант підходить для організацій, в яких не допустимий витік інформації назовні і які мають кошти для створення власної локальної системи. Часто такий підхід застосовується в державній і фінансовій сфері.

До локального зберігання даних вдаються із міркувань безпеки, але насправді, це рішення може бути хибним, оскільки дата-центри, що оброблюють інформацію мають хороші рівні захищеності. Наприклад, сервери Ivideon розташовуються в центрах рівня Tier 3 і Tier 4, які відповідають найголовнішим показникам захисту даних і сервісів. Це режимні об'єкти і доступ сторонніх осіб туди обмежений.
Гібридний VSaaS комбінує попередні два підходи до зберігання даних. Наприклад, він дозволяє підтримувати локальний архів резервних копій всередині компанії і звертатися за розширеними функціями відеоаналітики і іншими хмарними сервісами до провайдера.
Найбільш істотним бар'єром розширення послуг VSaaS в світі є недостатня пропускна здатність каналів зв'язку за межами локальної мережі.
В світі щорічне зростання обсягів відеоданих, що реєструються камерами, становить понад 50%, а зростання пропускної здатності каналів – тільки 20%. Таким чином, розрив між потребами VSaaS і можливостями каналів зв'язку щорічно збільшується на 30% в рік.[3]
Питання зниження навантаження на канали зв'язку вирішується за допомогою використання відеоаналітики на стороні клієнта, буферизації даних на локальних носіях, ранжирування відеоданих (пріоритетна передача інформації за ступенями важливості), причому пріоритет фрагментів відео автоматично визначається відеоаналітикою.
Отже, VSaaS має ряд переваг над VMS, що полягають в кращій захищеності даних, віддаленому управлінні доступом та автоматизації процесів стеження за допомогою відеоаналітики.

Contact Phone

Primary author: SAVELENKO, Natasha

Presenter: SAVELENKO, Natasha

Session Classification: Програмні та апаратні засоби інформаційної безпеки

Track Classification: Програмні та апаратні засоби інформаційної безпеки

Contribution ID: **248** Type: **Усна**

СПОСІБ ТРЬОХВИМІРНОЇ КОЛЬОРОВОЇ ФОРМАЛІЗАЦІЇ РІВНЯ РИЗИКУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Thursday, 25 April 2019 16:10 (15 minutes)

Abstract

Запропоновано спосіб формалізації рівня ризику інформаційної безпеки з використанням тривимірної кольорової моделі HSV. Використання моделі HSV дає можливість відображення рівня ризику ІБ з урахуванням просторово-часових характеристик APT атак.

Contact Phone

Primary author: ДАВИДЮК, Андрій (Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України)

Co-author: МОХОР, Володимир (Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України)

Presenter: ДАВИДЮК, Андрій (Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України)

Session Classification: Загальні питання інформаційної безпеки України

Track Classification: Загальні питання інформаційної безпеки України

Contribution ID: **249** Type: **Усна**

Основні підходи до визначення захищеності комп'ютерних систем

Thursday, 25 April 2019 17:25 (15 minutes)

Abstract

Безпека інформації, що опрацьовується у комп'ютерних системах, завжди була актуальною, незважаючи на неминучі затрати фінансових та інших ресурсів. У процесі розробки будь-яких засобів захисту інформації, при побудові систем захисту інформації (СЗІ), а також при проведенні оцінок рівня захищеності СЗІ завжди постає питання поєднання інтересів виробника, споживача і експерта, до того ж інтереси кожного досить суттєво відрізняються один від одного. Саме для вирішення таких питань потрібна система нормативних документів із захисту інформації в комп'ютерних системах (КС) або, простіше кажучи, стандарти із захисту інформації.

Contact Phone

Primary authors: ТКАЧЕНКО, Володимир (Інститут проблем моделювання в енергетиці ім. Г.Є.Пухова НАН України, м.Київ); Mr ГОНЧАР, Сергій (Ін-т проблем моделювання в енергетиці ім. Г.Є.Пухова НАН України); Mr БУРЛАКОВ, Володимир (НТУУ «Київський політехнічний інститут імені Ігоря Сікорського»)

Presenter: ТКАЧЕНКО, Володимир (Інститут проблем моделювання в енергетиці ім. Г.Є.Пухова НАН України, м.Київ)

Session Classification: Загальні питання інформаційної безпеки України

Track Classification: Загальні питання інформаційної безпеки України

Contribution ID: **250** Type: **Усна**

Особливості вибору системи виявлення вторгнень

Thursday, 25 April 2019 18:55 (15 minutes)

Abstract

На сьогоднішній день існує велика різноманітність IDS як комерційних, так і вільно розповсюджуваних. Що б описати технології IDS необхідно відповісти на 4 питання, які майже в повній мірі охоплюють всі аспекти даної технології.

Contact Phone

Primary author: ШЕЛЮК , Максим (КНУБА)

Co-author: ХЛАПОНІН, Юрій (КНУБА)

Presenter: ШЕЛЮК , Максим (КНУБА)

Session Classification: Програмні та апаратні засоби інформаційної безпеки

Track Classification: Програмні та апаратні засоби інформаційної безпеки

Contribution ID: **251** Type: **Усна**

Захищена система миттєвого обміну повідомленнями

Thursday, 25 April 2019 19:45 (15 minutes)

Abstract

Проблема приватності і захисту даних в інтернеті є однією з найактуальніших. Вона досить загострилася з масовим поширенням смартфонів, які сильніше схильні до злому, ніж стаціонарні комп'ютери та ноутбуки.

Contact Phone

Primary author: ЧОБАНЯН, Георгій (КНУБА)

Co-author: ХЛАПОНІН, Юрій (КНУБА)

Presenter: ЧОБАНЯН, Георгій (КНУБА)

Session Classification: Програмні та апаратні засоби інформаційної безпеки

Track Classification: Програмні та апаратні засоби інформаційної безпеки

Contribution ID: **252** Type: **not specified**

Використання нейронних мереж для виявлення атак в телекомунікаційних мережах критичного застосування

Thursday, 25 April 2019 14:30 (15 minutes)

Abstract

У зв'язку з постійно наростаючим використанням комп'ютерних систем у різних сферах науки, техніки, технологій, бізнесу, а також життя людей, інформаційні телекомунікаційні мережі піддаються різного роду загрозам, і користувач не може бути впевнений у захищеності важливої інформації, оскільки кіберзлочинці продовжують масово удосконалювати і розробляти методи і засоби організації кібератак (зловмисний код, мережеві вторгнення і т.д.). Тому дана тема є актуальною в наш час.

Contact Phone

Primary author: ЮРЧУК, Лілія (студент)

Presenter: ЮРЧУК, Лілія (студент)

Session Classification: Програмні та апаратні засоби інформаційної безпеки

Track Classification: Програмні та апаратні засоби інформаційної безпеки

Contribution ID: **253** Type: **not specified**

РОЗРАХУНОК КУТОВОГО РОЗНЕСЕННЯ МІЖ РУХОМИМИ ПРИЙМАЧАМИ ЛОКАЦІЙНОЇ ІНФОРМАЦІЇ В УМОВАХ РАДІОМОНІТОРИНГУ НЕСАНКЦІОНОВАНИХ ДЖЕРЕЛ ВИПРОМІНЮВАННЯ

Thursday, 25 April 2019 16:45 (15 minutes)

Abstract

Анотація.
Розглянуто ключові моменти роботи мобільних засобів пасивної системи РМ на базі ДПЛА які дозволяють отримувати необхідну інформацію щодо НДРВ. Висвітлено алгоритм знаходження кутової поправки при пеленгації НДРВ двома ДПЛА.
Ключові слова: пеленгація, ДПЛА, радіомоніторинг, пасивна локація, джерела радіовипромінювання, радіочастотний ресурс.
Abstract.
The key moments of the work of mobile devices of the passive system of the radio monitoring on the basis of the UAVs are considered, which allow get the necessary information about the not authorized radio emission sources. The algorithm of finding the angular correction in the process of direction-finding the not authorized radio emission sources of two UAVs is shown.
Key words: direction-finding, UAV, radio monitoring, passive location, radio emission sources, Radio-Frequency Resources.

Contact Phone

Primary author: СОКОЛОВ, Кирило

Presenter: СОКОЛОВ, Кирило

Session Classification: Програмні та апаратні засоби інформаційної безпеки

Track Classification: Програмні та апаратні засоби інформаційної безпеки

Contribution ID: **254** Type: **not specified**

ПРИНЦИПИ БОРОТЬБИ ІЗ МЕРЕЖЕВОЮ АТАКОЮ ARP-SPOOFING

Thursday, 25 April 2019 18:25 (15 minutes)

Abstract

Сучасні комп'ютерні мережі є вразлими до різноманітних атак з боку зловмисників. ARP-spoofing є одним із видів мережевих атак, що, в даний момент, широко використовується. Отже, необхідно знати, якими методами можна запобігти даних атак в майбутньому.

Contact Phone

Primary author: КАМЛУК, Іван

Presenter: КАМЛУК, Іван

Session Classification: Програмні та апаратні засоби інформаційної безпеки

Track Classification: Програмні та апаратні засоби інформаційної безпеки

Contribution ID: **255** Type: **Усна**

Застосування аналогової моделі штучного нейрона для моделювання динамічних систем.

Thursday, 25 April 2019 18:40 (15 minutes)

Abstract

Дана робота окреслює перспективи застосування аналогової моделі штучного нейрона як у пристроях інформаційної безпеки, так і для моделювання роботи динамічних систем.

Contact Phone

Primary authors: БЕХ, Ігор Іванович (Київський національний університет імені Тараса Шевченка, факультет радіофізики, електроніки та комп'ютерних систем, кафедра радіотехніки та радіоелектронних систем); НОВАК, Сергій Олександрович (Київський національний університет імені Тараса Шевченка, факультет радіофізики, електроніки та комп'ютерних систем, кафедра радіотехніки та радіоелектронних систем); ВЕРКАЛЕЦЬ, Дмитро Васильович. (Київський національний університет імені Тараса Шевченка, факультет радіофізики, електроніки та комп'ютерних систем, кафедра радіотехніки та радіоелектронних систем); МАРЧЕНКО, Євген Андрійович (Київський національний університет імені Тараса Шевченка, факультет радіофізики, електроніки та комп'ютерних систем, кафедра радіотехніки та радіоелектронних систем); ШВАБ, Леонід Валерійович (Київський національний університет імені Тараса Шевченка, факультет радіофізики, електроніки та комп'ютерних систем, кафедра радіотехніки та радіоелектронних систем)

Presenter: ВЕРКАЛЕЦЬ, Дмитро Васильович. (Київський національний університет імені Тараса Шевченка, факультет радіофізики, електроніки та комп'ютерних систем, кафедра радіотехніки та радіоелектронних систем)

Session Classification: Програмні та апаратні засоби інформаційної безпеки

Track Classification: Програмні та апаратні засоби інформаційної безпеки

Contribution ID: **257** Type: **Усна**

Методика створення криптовалюти

Thursday, 25 April 2019 17:55 (15 minutes)

Abstract

Криптовалюти, або віртуальні валюти, є потужним двигуном валютного ринку, зручним та технологічним засобом здійснення платежів і захисту інформації, який сьогодні використовують мільйони людей у світі
У переважній своїй більшості криптовалюти, які розробляються сьогодні, недосконалі, недостатньо популярні та мало досліджені.
За таких умов об'єктивно виникає необхідність застосування комплексного підходу та створення дієвого методичного апарату створення криптовалюти.

Contact Phone

Primary authors: КУХАР, Дана (КНУ ім. Тараса Шевченка); РЄЗНІКОВ, Михайло (КНУ ім. Тараса Шевченка)

Presenter: КУХАР, Дана (КНУ ім. Тараса Шевченка)

Session Classification: Загальні питання інформаційної безпеки України

Track Classification: Загальні питання інформаційної безпеки України

Contribution ID: **258** Type: **not specified**

Оцінка захищеності інформації криптографічними засоба

Thursday, 25 April 2019 18:40 (15 minutes)

Abstract

Оцінка захищеності інформації криптографічними засобами

Contact Phone

Primary authors: VASYLENKO, Oleksandr; NIKITCHYN, Aleksandr

Presenter: NIKITCHYN, Aleksandr

Session Classification: Загальні питання інформаційної безпеки України

Track Classification: Загальні питання інформаційної безпеки України

Contribution ID: **260** Type: **Усна**

Аналіз особливостей проведення додаткових експертиз комплексних систем захисту інформації в автоматизованих системах в сучасних умовах

Thursday, 25 April 2019 16:25 (15 minutes)

Abstract

.....

Contact Phone

Primary author: ПАВЛЮЧЕНКО, Сергій (ДержНДІ спецзв'язку)

Presenter: ПАВЛЮЧЕНКО, Сергій (ДержНДІ спецзв'язку)

Session Classification: Загальні питання інформаційної безпеки України

Track Classification: Загальні питання інформаційної безпеки України

Contribution ID: **261** Type: **Усна**

ВИЗНАЧЕННЯ КУТОВОЇ ПОПРАВКИ ПРИ ЗНАХОДЖЕННІ МІСЦЯ РОЗТАШУВАННЯ НЕСАНКЦІОНОВАНОГО ДЖЕРЕЛА РАДІОВИПРОМІНЮВАННЯ В УМОВАХ БАГАТОПОЗИЦІЙНОГО ПРИЙОМУ ІНФОРМАЦІЇ

Thursday, 25 April 2019 19:45 (15 minutes)

Abstract

….

Contact Phone

Primary author: СОКОЛОВ, К.А. (НТУУ КПІ імені Ігоря Сікорського)

Presenter: СОКОЛОВ, К.А. (НТУУ КПІ імені Ігоря Сікорського)

Session Classification: Програмні та апаратні засоби інформаційної безпеки

Track Classification: Програмні та апаратні засоби інформаційної безпеки

Contribution ID: **262** Type: **Усна**

СТАН НАЦІОНАЛЬНОЇ СИСТЕМИ КОНТРОЛЮ ЗА КОСМІЧНИМИ АПАРАТАМИ ТА ОБГРУНТУВАННЯ НАПРЯМКУ РОЗВИТКУ НАЗЕМНИХ ЗАСОБІВ СПОСТЕРЕЖЕННЯ

Thursday, 25 April 2019 14:45 (15 minutes)

Abstract

…..

Contact Phone

Primary author: СКУРЕНКО, Павло (КНУ ім Т.Шевченка)

Presenter: СКУРЕНКО, Павло (КНУ ім Т.Шевченка)

Session Classification: Програмні та апаратні засоби інформаційної безпеки

Track Classification: Програмні та апаратні засоби інформаційної безпеки

Contribution ID: **263** Type: **Усна**

Аналіз загроз витоку інформації по віброакустичному каналу та методи боротьби

Thursday, 25 April 2019 19:10 (15 minutes)

Abstract

Одним з видів загроз діяльності державних і комерційних підприємств, організацій, фірм є несанкціоноване знімання службової, комерційної й особистої інформації. Існує і більш проста назва - підслуховування, однак останнім часом зловмисники або конкуренти не обмежуються використанням різного роду апаратури, що підслухує конфіденційні розмови.

Contact Phone

Primary author: ЯЦУХ, Юрій (Сергійович)

Presenter: ЯЦУХ, Юрій (Сергійович)

Session Classification: Програмні та апаратні засоби інформаційної безпеки

Track Classification: Програмні та апаратні засоби інформаційної безпеки

Contribution ID: **264** Type: **Усна**

Дезорієнтація систем супутникової навігації як засіб електронної протидії

Thursday, 25 April 2019 18:55 (15 minutes)

Abstract

Технології з дезорієнтації системи супутникової навігації GPS були використані більше 10 000 разів російським устаткуванням електронної війни, починаючи з лютого 2016 року. Про це йдеться у новому звіті американської неурядової організації C4ADS.

Contact Phone

Primary authors: АНДРІЙЧУК, Роман; ШИФРУК, Анастасія (КНУ ім. Тараса Шевченка)

Presenter: АНДРІЙЧУК, Роман

Session Classification: Загальні питання інформаційної безпеки України

Track Classification: Загальні питання інформаційної безпеки України

Contribution ID: **265** Type: **Усна**

ВАРІАНТИ ПРАКТИЧНОГО ЗАСТОСУВАННЯ ХЕШ-ФУНКЦІЙ

Thursday, 25 April 2019 15:00 (15 minutes)

Abstract

Доповідь присвячена варіантам використання хеш-функцій. Особлива увага приділяється класу криптозахищених хеш-функцій.Під час досліджень хеш-функцій створено триланковий веб-застосунок автентифікації захищений SHA256.

Contact Phone

Primary author: ЄРШИКОВ, Максим (КНУ імені Тараса Шевченка)

Co-author: ЧЕТВЕРІКОВ, Іван (КНУ імемі Тараса Шевчека)

Presenter: ЄРШИКОВ, Максим (КНУ імені Тараса Шевченка)

Session Classification: Програмні та апаратні засоби інформаційної безпеки

Track Classification: Програмні та апаратні засоби інформаційної безпеки

Contribution ID: **266** Type: **Усна**

ЯК ОБДУРИТИ НЕЙРОННУ МЕРЕЖУ?

Thursday, 25 April 2019 14:55 (15 minutes)

Abstract

За останні декілька десятиліть різко зріс рівень автоматизації у всіх сферах життя. Це призвело до підвищення рівня продуктивності праці, якості продукції і захисту населення. Одним із найбільш прогресивних способів автоматизації є використання машинного навчання. Найчастіше нейромережі використовуються в системах розпізнавання обличь, системах безпеки і системах прийняття рішення. Загалом, нейромережі використовуються там, де необхідно опрацьовувати велику кількість даних.
Оскільки, нейромережа використовує алгоритми для узагальнення і аналізу даних, то можливо знайти такі конфігурації вхідних даних при яких навіть натренована нейромережа буде давати збої. Розглянемо найпоширеніші випадки "злому" на прикладі нейромереж розроблених для розпізнавання образів.

Contact Phone

Primary authors: OLIFIROVICH, Mykola; BORETSKIJ, Viacheslav (Taras Shevchenko National University of Kyiv)

Presenter: OLIFIROVICH, Mykola

Session Classification: Загальні питання інформаційної безпеки України

Track Classification: Загальні питання інформаційної безпеки України

Contribution ID: **267** Type: **Усна**

АНАЛІЗ МОЖЛИВОСТІ БЛОКУВАННЯ АТАКИ ДЕАВТЕНТИФІКАЦІЇ В МЕРЕЖАХ WI-FI

Thursday, 25 April 2019 17:00 (15 minutes)

Abstract

Актуальність блокування атак в мережах Wi-Fi на сьогодні обґрунтовується широким використанням різноманітних засобів, що можуть працювати одночасно в мережах GSM, bluetooth та інших. Аналіз стандарту IEEE 802.11 показує, що «службові» дані не шифруються тобто передача MAC-адресу абонента та точки доступу відбувається у відкритому вигляді. Тому у таких бездротових мережах є можливість здійснити підміну MAC – адреси.

Contact Phone

Primary authors: USTENKO, Ivan; DOVBNYA, Serghiy

Presenters: USTENKO, Ivan; DOVBNYA, Serghiy

Session Classification: Програмні та апаратні засоби інформаційної безпеки

Track Classification: Програмні та апаратні засоби інформаційної безпеки

Contribution ID: **268** Type: **Усна**

МЕХАНІЗМИ ПРОТИДІЇ ІНФОРМАЦІЙНІЙ АГРЕСІЇ В МЕДІАПРОСТОРІ УКРАЇНИ: КАРНАВАЛЬНІ ФОРМИ ВПЛИВУ

Abstract

Жорстке інформаційно-психологічне протистояння у медіа- та інтернет-просторі, яке розгортається на тлі складних геополітичних процесів у сучасному світі, отримало назву консцієнтальної війни, або війни за свідомість, семантичної війни, війни смислів. Гібридна війна вже спричинила, за коментарем В.П. Горбуліна, відчутне «руйнування світового порядку». Усе це активізувало експертне середовище щодо розробки механізмів протидії інформаційній агресії.

Contact Phone

Primary author: Dr СНИТКО, Олена (Інститут філології Київського національного університету імені Тараса Шевченка)

Presenter: Dr СНИТКО, Олена (Інститут філології Київського національного університету імені Тараса Шевченка)

Session Classification: Інформаційна війна в парадигмах лінгвістики впливу

Track Classification: Інформаційна війна в парадигмах лінгвістики впливу

Contribution ID: **269** Type: **Усна**

МОВА ЯК ЗБРОЯ КОНСЦІЄНТАЛЬНОЇ ВІЙНИ: НАРАТИВНИЙ ІНСТРУМЕНТАРІЙ

Abstract

Російська агресія проти України є гібридною, оскільки поєднує мілітарний та немілітарний (інформаційний, психологічний, культурний, мовний, комунікаційний) складники. Певні прояви агресії немілітарного типу пов'язані з концепцією консцієнтальної війни, мета якої – ураження людської свідомості та руйнування способів і форм ідентифікації особистості та суспільства за допомогою розповсюдження комунікативними каналами певних образів і текстів. Консцієнтальна зброя руйнує стійку систему світоглядних цінностей, родову і культурну пам'ять, традиційні механізми самоідентифікації задля цивілізаційного перевербування етносів і народів. До типів такої зброї дослідники відносять зокрема мову та наративи.

Contact Phone

Primary author: ГРЕЧКА, Станіслав (Київський національний університет імені Тараса Шевченка)

Presenter: ГРЕЧКА, Станіслав (Київський національний університет імені Тараса Шевченка)

Session Classification: Інформаційна війна в парадигмах лінгвістики впливу

Track Classification: Інформаційна війна в парадигмах лінгвістики впливу

Contribution ID: **270** Type: **Усна**

СТРУКТУРА ІДЕОЛОГІЧНОЇ МАТРИЦІ РОСІЙСЬКИХ МЕДІА

Abstract

Світоглядні війни зумовлені контрадикторними ідеологічними матрицями, або провідними поняттєвими системами, кожна з яких на інформаційному рівні визначає теми, об'єкти обговорення, наративи, які складаються в дискурси, і кожна обумовлює вибір конотованих вербальних і невербальних об'єктиваторів думки, які просувають інтенції. «Поняттєвий апарат – це зброя масового світоглядного ураження», – цілком справедливо твердить один з активних авторів російських медіа. Тому осмислення дискурсу російських медіа крізь призму системи панівних ідеологем є нагальним питанням, зокрема, для організації ефективної системи інформаційного контрзахисту з боку українського соціуму.

Contact Phone

Primary author: Dr СЛУХАЙ, Наталія (Інститут філології Київського національного університету імені Тараса Шевченка)

Presenter: Dr СЛУХАЙ, Наталія (Інститут філології Київського національного університету імені Тараса Шевченка)

Session Classification: Інформаційна війна в парадигмах лінгвістики впливу

Track Classification: Інформаційна війна в парадигмах лінгвістики впливу

Contribution ID: **271** Type: **Усна**

КОНТРАСТИВНІ СУБКОНЦЕПТИ «ВІЙНА / МИР» В УКРАЇНСЬКОМУ ВИМІРІ: АСОЦІАТИВНИЙ СКЛАДНИК

Abstract

Стрімке зростання наративів агресивного дискурсу російських медіа, активне використання ресурсів мови ворожнечі (hate speech) та технологій замаскованого впливу на свідомість споживачів мас-медійної інформації сьогодні обумовлює інтерес сучасних когнітивістів до вивчення національних мілітарних концептосфер та їх складових, зокрема субконцептів «Війна в Україні», «Мир в Україні» та ін.

Contact Phone

Primary author: Mrs ГИЛЮН, Ольга (Інститут філології Київського національного університету імені Тараса Шевченка)

Presenter: Mrs ГИЛЮН, Ольга (Інститут філології Київського національного університету імені Тараса Шевченка)

Session Classification: Інформаційна війна в парадигмах лінгвістики впливу

Track Classification: Інформаційна війна в парадигмах лінгвістики впливу

Contribution ID: **272** Type: **Усна**

ОПТИМІЗАЦІЯ ЗАВАНТАЖЕНОСТІ КАНАЛУ РАДІОЗВ'ЯЗКУ В СИСТЕМАХ ДИНАМІЧНОГО МОНІТОРИНГУ

Thursday, 25 April 2019 17:15 (15 minutes)

Abstract

Новітні системи та засоби радіозв'язку забезпечують великий обсяг передавання інформації. Це, в свою чергу, потребує вдосконалення систем моніторингу мереж радіозв'язку та вирішення проблем надлишкової завантаженості каналів радіозв'язку.

Contact Phone

Primary authors: МІЩЕНКО, Володимир (ТОВ "ДЕПС СОЛЮШЕНЗ"); КОВАЛЕВСЬКА, Ганна (Департамент забезпечення діяльності НКРЗІ)

Presenter: МІЩЕНКО, Володимир (ТОВ "ДЕПС СОЛЮШЕНЗ")

Session Classification: Програмні та апаратні засоби інформаційної безпеки

Track Classification: Програмні та апаратні засоби інформаційної безпеки

Contribution ID: **273** Type: **Усна**

МАТЕМАТИЧНІ ФУНКЦІОНАЛЬНО-СТАТИСТИЧНІ МОДЕЛІ ОБ'ЄКТІВ КОНТРОЛЮ І УПРАВЛІННЯ МЕРЕЖ РАДІОЗВ'ЯЗКУ

Thursday, 25 April 2019 19:45 (15 minutes)

Abstract

Об'єктом контролю і управління мереж радіозв'язку може бути будь-яке активне устаткування ядра мережі, а також уся мережа радіозв'язку в цілому. При цьому мережа радіозв'язку розглядається як складна система, що підлягає управлінню. Складність процесу контролю і управління обумовлюється, в основному, складністю об'єктів. Для опису функціонування об'єкту доцільно побудувати його математичну модель. Якнайповніший стан об'єкту характеризує математична функціонально-статична модель – це система рівнянь або операторів, які описують залежність вихідних параметрів об'єкту, системи або блоку від зовнішніх і внутрішніх впливів під час функціонування. На основі аналізу зазначеної моделі можливо сформулювати основні завдання, які вирішуються автоматичною системою контролю і управління, а також синтезувати оптимальну систему управління мережею радіозв'язку, визначаючи міру автоматизації та її ефективність.

Contact Phone

Primary authors: МІЩЕНКО, Володимир (ТОВ "ДЕПС СОЛЮШЕНЗ"); МІЩЕНКО, О.В. (ПП "Авто-Актив")

Presenter: МІЩЕНКО, Володимир (ТОВ "ДЕПС СОЛЮШЕНЗ")

Session Classification: Програмні та апаратні засоби інформаційної безпеки

Track Classification: Програмні та апаратні засоби інформаційної безпеки

Contribution ID: **274** Type: **Усна**

РОЗРОБКА АЛГОРИТМІВ ОПТИМАЛЬНОГО ПРИЙНЯТТЯ СИГНАЛІВ ІЗ ФАЗОРІЗНИЦЕВОЮ МОДУЛЯЦІЄЮ ВИСОКОЇ КРАТНОСТІ

Thursday, 25 April 2019 15:15 (15 minutes)

Abstract

Новітні системи та засоби радіозв'язку забезпечують великий обсяг передавання інформації. Це, в свою чергу, вимагає вдосконалення та оптимізації радіоприймальних пристроїв з різноманітними видами модуляції сигналів.

Contact Phone

Primary authors: МІЩЕНКО, Володимир (ТОВ "ДЕПС СОЛЮШЕНЗ"); ГАРІФОВА, Л.М. (Відділення технічних наук КПНЗ "Київська Мала академія наук учнівської молоді")

Presenter: МІЩЕНКО, Володимир (ТОВ "ДЕПС СОЛЮШЕНЗ")

Session Classification: Програмні та апаратні засоби інформаційної безпеки

Track Classification: Програмні та апаратні засоби інформаційної безпеки

Contribution ID: **275** Type: **Усна**

ГУМАНІТАРНИЙ ІНСТРУМЕНТАРІЙ ГІБРИДНОЇ ВІЙНИ

Abstract

Війни супроводжують людство упродовж усієї історії. Феномен війни є предметом наукового аналізу здавна, починаючи з давніх часів, і до нашого часу кількість таких досліджень постійно збільшується. Наука сьогодні надає полі дисциплінарний опис феномену війни, використовуючи інструментарій філософії, політології, лінгвістики, психології, історії, дискурс-аналізу, семіотики, сугестології.

Сьогодні, коли постійно підвищується градус гібридної війни, яку веде Росія проти України і світу в цілому, стає особливо актуальним чітке розуміння суті подій, які описуються українськими та міжнародними аналітиками, науковцями, військовими, політиками та громадськими діячами в рамках концепції гібридної війни.

Contact Phone

Primary author: БОНДАРЕНКО, Олександр (Інститут філології Київського національного університету імені Тараса Шевченка)

Presenter: БОНДАРЕНКО, Олександр (Інститут філології Київського національного університету імені Тараса Шевченка)

Session Classification: Plenary Lectures

Track Classification: Інформаційна війна в парадигмах лінгвістики впливу

Contribution ID: **276** Type: **Усна**

Автоматизація бототизацією: від моніторингу радіоелектронної обстановки до торгівлі криптовалютами

Thursday, 25 April 2019 19:45 (15 minutes)

Abstract

Автоматизація бототизацією: від моніторингу радіоелектронної обстановки до торгівлі криптовалютами

Contact Phone

Primary author: LUBIN, Vlad

Co-authors: КУХАР, Дана (КНУ ім. Шевченка); ЧЕТВЕРІКОВ, Іван (КНУ ім. Шевченка)

Presenter: LUBIN, Vlad

Session Classification: Програмні та апаратні засоби інформаційної безпеки

Track Classification: Програмні та апаратні засоби інформаційної безпеки

Contribution ID: **277** Type: **Усна**

АНАЛІЗ МОЖЛИВОСТІ БЛОКУВАННЯ БЕЗДРОТОВИХ МЕРЕЖ ЗВ’ЯЗКУ

Thursday, 25 April 2019 15:30 (15 minutes)

Abstract

АНАЛІЗ МОЖЛИВОСТІ БЛОКУВАННЯ БЕЗДРОТОВИХ МЕРЕЖ ЗВ’ЯЗКУ

Contact Phone

Primary author: ЮШТА, Захар

Presenter: ЮШТА, Захар

Session Classification: Програмні та апаратні засоби інформаційної безпеки

Track Classification: Програмні та апаратні засоби інформаційної безпеки

Contribution ID: **278** Type: **Усна**

Реєстратор електронно-захватного детектора з диференціальним каналом передачі даних

Thursday, 25 April 2019 17:30 (15 minutes)

Abstract

Одним з найбільш перспективних напрямків розвитку цифрової техніки є побудова систем обробки цифрової інформації на основі спеціально сформованих диференціальних сигналів. Для передачі диференціального сигналу використовується два виходи з метою передачі сигналів по двох лініях передачі. Перший канал передає один біт інформації, а другий канал передає його інверсну форму. Інформаційний сигнал є саме різниця напруги у цих лініях. [1]
У двох канальній лінії передачі диференціайна напруга d визначається як різниця між миттєвими напругами «a» та «b» на обох провідниках

Contact Phone

Primary author: ПОЗЮБАН, Костянтин (ФРЕКС КНУ студент)

Co-author: ОЛЬШЕВСЬКИЙ, Сергій

Presenter: ПОЗЮБАН, Костянтин (ФРЕКС КНУ студент)

Session Classification: Програмні та апаратні засоби інформаційної безпеки

Track Classification: Програмні та апаратні засоби інформаційної безпеки

Contribution ID: **279** Type: **Усна**

Антенний модуль з апаратною функцією формування променя для базових станцій стільникового зв’язку малого і середнього радіусу покриття

Thursday, 25 April 2019 19:25 (15 minutes)

Abstract

…..

Contact Phone

Primary authors: КЛІМОВ, Олександр; КВАЧЕНОК, Ігор

Presenter: КВАЧЕНОК, Ігор

Session Classification: Програмні та апаратні засоби інформаційної безпеки

Track Classification: Програмні та апаратні засоби інформаційної безпеки

Contribution ID: **280** Type: **Усна**

АНАЛІЗ ЗАХИЩЕНОСТІ ЗМІШАНИХ МІКРОСХЕМ

Thursday, 25 April 2019 14:30 (10 minutes)

Abstract

Популяризація змішаних мікросхем створює загрози витоку інформації.

Contact Phone

Primary authors: SHVAB, Andrii; BORETSKIJ, Viacheslav (Taras Shevchenko National University of Kyiv)

Presenter: SHVAB, Andrii

Session Classification: Загальні питання інформаційної безпеки України

Track Classification: Загальні питання інформаційної безпеки України

Contribution ID: **281** Type: **Усна**

ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ПЕРЕДАЧІ ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ, ЯКІ ВИКОРИСТОВУЮТЬ ТЕХНОЛОГІЮ ”FIBER TO THE HOME”

Thursday, 25 April 2019 19:40 (15 minutes)

Abstract

При побудові сучасних інформаційно-телекомунікаційних систем і мереж все більше уваги приділяється питанню захисту інформації, що передається. Враховуючи численну кількість методів та засобів технічного захисту інформації варто зазначити й фізичний захист. Прикладом якого є використання волоконно-оптичних ліній зв’язку.

Contact Phone

Primary authors: HONENKO, Serhii; REZNIKOV, Mykhailo (Taras Shevchenko National University of Kyiv); FELINSKYI , G. (Taras Shevchenko National University of Kyiv); KORCHAK, Oleksandr

Presenter: HONENKO, Serhii

Session Classification: Програмні та апаратні засоби інформаційної безпеки

Track Classification: Програмні та апаратні засоби інформаційної безпеки

Contribution ID: **282** Type: **Усна**

Достовірність даних станції моніторингу PM2.5 частинок в атмосферному повітрі

Thursday, 25 April 2019 17:45 (10 minutes)

Abstract

В даній роботі для статистичної обробки даних датчика PM2.5 запропоновано використати фільтр високої частоти на основі швидкого перетворення Фур'є. Це дозволить відкинути флуктуації пов'язані з високочастотними (наводки, тактування АЦП та мікроконтролера) та впливами на середніх частотах внаслідок тимчасового потрапляння в вимірювальний канал крупних пилинок.

Contact Phone

Primary authors: ANTONENKO, Andrii; BORETSKIJ, Viacheslav (Taras Shevchenko National University of Kyiv)

Presenters: ANTONENKO, Andrii; ZAGARIA, Olexandr

Session Classification: Програмні та апаратні засоби інформаційної безпеки

Track Classification: Програмні та апаратні засоби інформаційної безпеки

Contribution ID: **283** Type: **Усна**

ТРАНЗАКЦІЇ ВЗАЄМОДІЇ СИСТЕМИ РОЗУМНОГО ДОМУ НА ОСНОВІ ТЕХНОЛОГІЇ БЛОКЧЕЙН

Thursday, 25 April 2019 19:50 (10 minutes)

Abstract

Contact Phone

Primary authors: REZNIKOV, Mykhailo (Taras Shevchenko National University of Kyiv); БРАТАНИЧ, Дмитро (КНУ)

Presenter: БРАТАНИЧ, Дмитро (КНУ)

Session Classification: Програмні та апаратні засоби інформаційної безпеки

Track Classification: Програмні та апаратні засоби інформаційної безпеки

Contribution ID: **284** Type: **not specified**

АНАЛІЗ КЕРУЮЧИХ СИСТЕМ ЕЛЕКТРОЖИВЛЕННЯ, ЯКІ ВИКОРИСТОВУЮТЬСЯ У ШТУЧНИХ СУПУТНИКАХ ЗЕМЛІ

Thursday, 25 April 2019 19:50 (10 minutes)

Abstract

АНАЛІЗ КЕРУЮЧИХ СИСТЕМ ЕЛЕКТРОЖИВЛЕННЯ,
ЯКІ ВИКОРИСТОВУЮТЬСЯ
У ШТУЧНИХ СУПУТНИКАХ ЗЕМЛІ

Contact Phone

0633495635

Primary authors: Mr ГАЛИНОВСЬКИЙ, Олександр; ДОВБНЯ, Сергій (КНУ Тараса Шевченка)

Presenter: Mr ГАЛИНОВСЬКИЙ, Олександр

Session Classification: Програмні та апаратні засоби інформаційної безпеки

Track Classification: Програмні та апаратні засоби інформаційної безпеки

Contribution ID: **285** Type: **Усна**

ПЕРСПЕКТИВИ ПОСТКВАНТОВОЇ КРИПТОГРАФІЇ

Abstract

Сучасна криптологія виділяє проблемні задачі повного розкриття, пов'язані з можливостями використання методів та алгоритмів квантового криптоаналізу [1]. Особливість квантових комп'ютерів полягає в тому, що для виконання обчислень вони використовують такі фізичні ефекти, як суперпозиція станів і сплутування. В даний час їх продуктивність набагато нижче, ніж у стандартних комп'ютерів. Однак деякі алгоритми перевершили стандартні комп'ютери у швидкодії в 100 млн. разів [2]. Важливою властивістю квантових об'єктів є можливість здійснювати паралельні операції. Так, для системи із N кубітів, що перебуває в переплутаному стані, ефективно кодується відразу 2N чисел. Тому операція над такою системою, завдяки когерентності станів різних кубітів, впливає на всі доданки в сумі і це дозволяє обробляти відразу всі 2N чисел. Це може привести до злому протоколів безпеки, заснованих на криптографічних алгоритмах.

Contact Phone

Primary authors: ТЕЛІЖЕНКО, О.Б. (Інститут СЗРУ); CHETVERIKOV , Ivan

Presenter: ТЕЛІЖЕНКО, О.Б. (Інститут СЗРУ)

Session Classification: Загальні питання інформаційної безпеки України

Track Classification: Загальні питання інформаційної безпеки України