Тематична виставка
"Безпека та захист інформаційного простору "

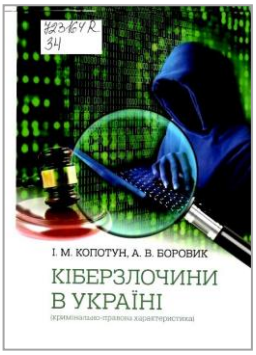
(надходження І півріччя 2020)

Законодавча, нормативно-правова і методична база у сфері інформаційної безпеки

Архипов О. Є. Адаптивний підхід до обробки даних експертного оцінювання при вирішенні завдань у сфері захисту інформації / О. Є. Архипов, С. А. Архіпова // Захист інформації. – 2019. – Т. 21, № 3. – С. 158-167. – Текст рос.

Р/1428

"Адаптивный подход к обработке экспертных данных – целенаправленное формирование (адаптация) процедуры обработки данных, в частности, ее основного элемента – метода, ориентированное на повышение уровня точности обработки".



723164 R
34

Боровик, Андрій Володимирович.
Кіберзлочини в Україні (кримінально-правова характеристика) [Текст] : навч. посіб. / А. В. Боровик, І. М. Копотун. - Луцьк : ВолиньПоліграф, 2019. - 304 с. - Бібліогр.: с. 298-303.

У навчальному посібнику на основі сучасних наукових підходів, структури та змісту кримінологічних знань розглянуто предмет, систему й кваліфікацію злочинів у сфері кіберзлочинності, та перспективи розвитку. Сформульовано низку нових концептуальних положень, висновків і рекомендацій, що мають важливе теоретичне та практичне значення. Для студентів, аспірантів, викладачів юридичних факультетів та вишів, працівників науково-дослідних установ, адвокатів, суддів, працівників правоохоронних органів, усіх, кого цікавлять проблеми запобігання злочинам у сфері кіберзлочинності.

Гайдур Г. І. Теоретичний підхід до визначення змісту поняття "інформація" як основної категорії кібербезпеки / Г. І. Гайдур, С. О. Гахов // Сучасний захист інформації. – 2019. – № 3(39). – С. 51-56.

Р/2300

У статті досліджуються підходи до обґрунтування змісту поняття "інформація". Здійснено обґрунтування змісту поняття "інформація" як основної категорії кібербезпеки. Встановлена функціональна природа інформації в інформаційних системах. Визначено перспективний напрямок подальшого розвитку теорії захищених інформаційних систем.

Євсеєв С. П. Алгоритм оцінювання ступеня ризику інформаційної безпеки, що базується на нечітко-множинному підході / С. П. Євсеєв, О. В. Шматко, Н. В. Ромащенко // Сучасні інформаційні системи. – 2019. – Т. 3, № 2. – С. 73-79. – Текст англ.

Р/543

Метою даної роботи є розробка методики оцінки ступеня ризику інформаційної безпеки, яка б дозволила уникнути фактору невизначеності, що виникає за умови відсутності частини інформації про досліджувану автоматизовану інформаційну систему. Методика заснована на використанні нечіткої логіки та нечітких множин, що передбачає введення терм множин для кожної з характеристик системи та лінгвістичній оцінці показників.

Ємельянов В. М. Кібербезпека як складова національної безпеки та кіберзахист критичної інфраструктури України / В. М. Ємельянов, Г. Л. Бондар // Публічне управління та регіональний розвиток. – 2019. – № 5. – С. 493-523.

Р/662

Стаття присвячена аналізу особливостей кібербезпеки як важливої складової національної безпеки України, законодавчого і нормативно-правового забезпечення даної сфери, реалізації чисельних заходів державою під час боротьби з кібернападами на об'єкти критичної інфраструктури, об'єкти громадянського суспільства та діяльності спеціалізованих державних структур, які забезпечують кіберзахист країни в умовах протидії російській агресії, з використанням сучасних світових практик, зокрема країн НАТО та ЄС в означеній сфері.

721766 R
004

Єсін, Віталій Іванович.
Стислий словник основних термінів з безпеки інформаційних систем, технологій, кібербезпеки [Текст] : словник / [уклад.: В. І. Єсін, С. Г. Рассомахін] ; Харківський національний університет імені В. Н. Каразіна. - Харків : ХНУ ім. В. Н. Каразіна, 2018. - 64 с. - Бібліогр.: с. 59-63. - Уклад. зазнач. на звороті тит. арк.

Словник містить понад 400 найбільш важливих термінів у галузі безпеки інформаційних систем, технологій, кібербезпеки.

Для студентів та аспірантів ВНЗ за спеціальністю підготовки "Кібербезпека", слухачів курсів підвищення кваліфікації, фахівців у галузі інформаційної та кібербезпеки, а також для широкого кола читачів.

Журиленко Б. Є. Метод проектування та оцінка працюючого одиночного технічного захисту інформації за обраним напрямом злому / Б. Є. Журиленко // Захист інформації. – 2019. – Т. 21, № 3. – С. 143-149. – Текст рос.

Р/1428

У даній роботі показана альтернативна відомим способам можливість проектування і оцінки одиночного технічного захисту інформації (ТЗІ) за обраним напрямом злому.

720745 B
004

Інформаційна безпека [Текст] : навч. посіб. / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник [та ін] ; за заг. ред. Ю. Я. Бобала, І. В. Горбатого ; Національний університет "Львівська політехніка". - Львів : Львівська політехніка, 2019. - 580 с. : іл., рис., табл. - Бібліогр. в кінці розд.

Розглянуто основні поняття та визначення в галузі інформаційної безпеки. Описано математичні основи криптології. Розглянуто відомі та сучасні методи криптографії, криптоаналізу, стеганографії. Розглянуто питання ідентифікації, автентифікації та санкціонованого доступу.

Значну увагу в начальному посібнику приділено практичному захисту інформації. Розглянуто питання інформаційної безпеки підприємств та організацій. Особливу увагу приділено проектуванню, побудові та функціонуванню систем інформаційної безпеки.

Для студентів закладів вищої освіти спеціальностей 172 "Телекомунікації та радіотехніка", 125 "Кібербезпека", 163 "Біомедична інженерія" та споріднених спеціальностей, а також для тих, хто цікавиться інформаційною безпекою та захистом інформації.

722463 R
004

Інформаційна безпека держави [Текст] : навч. посіб. / В. М. Рудницький. С. О. Гнатюк, Н. В. Лада, Р. В. Бреус ; Черкаський державний технологічний університет. - Харків : [ДІСА ПЛЮС], 2018. - 359 с. - Бібліогр. в кінці тем.

У навчальному посібнику розкрито концептуальні та нормативно-правові засади інформаційної безпеки держави, загрози інформаційній безпеці та канали витоку інформації. Розглянуто управління інцидентами та ризиками інформаційної безпеки, інформаційне протиборство. Наведено сучасні погляди на стан державної інформаційної політики України та загальнодержавну систему забезпечення інформаційної безпеки України, Національну систему конфіденційного зв'язку та захист державних інформаційних ресурсів в інформаційно-телекомунікаційних системах. Показано широкий спектр засобів інженерно-технічного, криптографічного та стеганографічного захисту інформації, тощо.

Навчальний посібник складається з двох частин: теоретичної та практичної. Теоретична частина містить вісімнадцять ключових тем, що розкривають основний зміст дисципліни "Інформаційна безпека держави". Практична частина складається з відповідних вісімнадцяти практичних занять, що дозволяють закріпити теоретичний матеріал та провести перевірку отриманих знань.

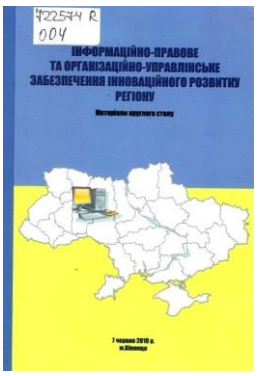
722198 R
004

Інформаційна безпека: сучасний стан, проблеми та перспективи [Текст] : матеріали І міжнар. наук.-практ. конф., 20 вересня 2019 р. / М-во інформ. політики України, Секція правового забезпечення нац. безпеки і оборони НАН України, НДІ інформатики і права Нац. технічного ун-ту України "Київський політехн. ін-т ім. Ігоря Сікорського", Ф-т соціології і права. - Київ : КПІ ім. І. Сікорського , 2019. - 126 с. - Бібліогр. в кінці ст.

Матеріали конференції присвячені теоретичним та практичним засадам державної політики у сфері інформаційної безпеки, проблемам формування, оцінці стану та реалізації Доктрини інформаційної безпеки України.

У конференції брали участь провідні експерти й вчені наукових установ і навчальних закладів, представники державних органів та громадських організацій. Інформаційну підтримку у проведенні заходу надали: журнали "Інформація і право" та Вісник "КПІ ім. Ігоря Сікорського" "Політологія. Соціологія. Право".

Матеріали подано у авторській редакції.



722574 R
004

Інформаційно-правове та організаційно-управлінське забезпечення інноваційного розвитку регіону [Текст] : матеріали круглого столу, 7 червня 2019 р. / Вінницький держ. пед. ун-т ім. Михайла Коцюбинського, Каф. правових наук та філософії, НДІ інформатики і права [та ін.]. - Київ : Вид. дім "Арт-Ек", 2019. - 133 с. - Бібліогр. в кінці ст.

У збірнику матеріалів круглого столу висвітлено актуальні проблеми інформаційно-правового та організаційно-управлінського забезпечення інноваційного розвитку регіону та шляхи їх вирішення.

Учасниками круглого столу стали провідні експерти і вчені наукових установ і навчальних закладів України, представники зацікавлених державних органів та громадських організацій.

Кальченко В. В. Аналіз існуючої методики проведення аудиту безпеки комп'ютерних систем в державних органах / В. В. Кальченко // Системи управління, навігації та зв'язку. – 2019. – Вип. 3(55). – С. 110-114.

Р/2152

Предметом статті є аналіз існуючих методик проведення аудиту безпеки, які нормативно закріплені в Україні та використовуються посадовими особами Державної служби спеціального зв'язку та захисту інформації.

Концепция внутренней реструктуризации данных для повышения безопасности информационного ресурса / В. В. Баранник, Ю. Н. Рябуха, И. М. Тупица [и др.] // Радиоэлектроника и информатика = Radioelectronics & Informatics. – 2019. – № 2. – С. 67-72.

Р/1138

Разрабатывается концепция внутренней реструктуризации данных по количественному признаку в целях повышения защиты данных информационного ресурса. Исследуется процесс кластеризации элементов сообщения во множестве. Анализируются преимущества применения внутренней реструктуризации данных по сравнению с методами внешней реструктуризации.

Концепція побудови захищеної системи управління ІТ центру / Л. Н. Беркман, Я. О. Прийма, Н. С. Чумак [та ін.] // Сучасний захист інформації. – 2019. – № 3(39). – С. 6-14.

Р/2300

В статті висвітлено шляхи створення ІТ центру, як технологічної системи, що реалізує з необхідною якістю ефективне надання інформаційних послуг, їх захист від несанкціонованого доступу, засекречення потоку даних, що забезпечує захищеність інформації, цілісність з'єднання з відновленням, попередження відмов тощо. Запропоновано до застосування відомий інформаційно-ентропійний метод для визначення одного із основних параметрів системи управління мережами ІТ центру – кількість управляючої інформації, яка забезпечує необхідну точність параметрів мережі, що управляється.

Кочетков О. В. Система оцінки ризиків інформаційної безпеки підприємства на основі нечіткої логіки / О. В. Кочетков, Т. О. Гаур, В. М. Машін // Наукові праці ОНАЗ ім. О.С. Попова. – 2019. – № 1. – С. 97-104.

Р/1485

Запропоновано використання теорії нечіткої логіки для оцінки ризиків.

Для моделювання ризику інформаційної безпеки підприємства запропоновано нечіткі моделі надавати у вигляді нечітких мереж. Модель містить бази правил і дозволяє проводити лінгвістичний аналіз ризиків, які несуть потенційні загрози і збиток організації. Використовуваний в методиці механізм отримання оцінок ризику на основі нечіткої логіки дозволяє отримати чисельне значення ризику, лінгвістичний опис ступеня ризику, а також рівень впевненості експерта у виникненні ризикової події.

Левченко О. В. Трансформація інформаційних загроз у воєнні загрози державі / О. В. Левченко, А. А. Завада // Системи озброєння і військова техніка. – 2019. – № 4(60). – С. 128-133.

Р/1903

У статті розглядається поняття та сутність інформаційних загроз безпеці держави. Визначено найбільш небезпечні інформаційні загрози для України за досвідом протистояння збройній агресії Російської Федерації (РФ).

Петров С. Г. Правові основи взаємодії державних органів та приватних суб'єктів із метою захисту електронних інформаційних ресурсів України / С. Г. Петров // Інформація і право. – 2019. – № 4(31). – С. 107-112.

Р/844

У статті досліджуються питання взаємодії державних органів та приватних суб'єктів із метою забезпечення кібербезпеки і зокрема захисту електронних інформаційних ресурсів України. З цією метою здійснено аналіз підходів в іноземних країнах, а також вітчизняного законодавства.

Попов Г. А. Анализ входных условий в модели информационной безопасности, построенной на основе аппарата редких событий / Г. А. Попов, Е. А. Попова, О. В. Васильева // Научный вестник НГТУ. – 2019. – № 2. – С. 69-88.

Р/882

Рассматривается задача оценки вероятности совершения злоумышленного действия в условиях, когда исходный процесс обеспечения информационной безопасности является регенерирующим. Особый интерес представляет анализ вероятности и возможного момента реализации злонамеренной атаки.

Прав Р. Ю. Роль механізму державно-приватного партнерства у розвитку кібербезпеки України на сучасному етапі / Р. Ю. Прав // Інвестиції: практика та досвід. – 2019. – № 21. – С. 143-88.

Р/2124

Висвітлено завдання державно-приватного партнерства у сфері кібербезпеки та чинники, що впливають на рівень впровадження кібербезпеки у Європейському Союзі. Розглянуто досвід розвинутих країн щодо застосування ДПП у сфері кібербезпеки, виділено основні напрями діяльності громадських інститутів-учасників ДПП у сфері кібербезпеки.

722573 R
34

Радзієвська, О. Г.
Проблеми захисту прав і безпеки дитини в інформаційній сфері [Текст] : монографія / Радзієвська О. Г. ; [за заг. ред. В. Г. Пилипчука] ; Нац. акад. правових наук України, НДІ інформатики і права. - Київ : [Видавничий дім "АртЕк"], 2019. - 238 с. : табл. - Бібліогр. у виносках.

У монографії висвітлено проблемні питання протидії негативним інформаційним впливам на дитину і забезпечення її інформаційної безпеки в умовах інформаційної глобалізації та розбудови інформаційного суспільства. Визначено шляхи і методи захисту інформаційної безпеки дитини з урахуванням стратегічних напрямків розбудови системи забезпечення інформаційної сфери та особливостей дитини, як суб'єкта суспільних відносин.

Тарасюк А. В. Співвідношення інформаційної та кібернетичної безпеки / А. В. Тарасюк // Інформація і право. – 2019. – № 4(31). – С. 73-82.

Р/844

У статті досліджуються концептуальні засади співвідношення інформаційної та кібернетичної безпеки України. На основі теоретичного аналізу запропоновано авторські визначення базових категорій кібернетичної безпеки, а також визначено та проаналізовано стан законодавчого забезпечення та розроблено пріоритетні напрями його вдосконалення.

Програмні системи захисту інформації

722102 R
004

Безпека. Відмовостійкість. Інтелект [Текст] : збірник праць міжнар. наук.-прак. конф. ICSFTI2019, 14-15 травня 2019 р. / Національний технічний університет України "Київський політехнічний інститут ім. Ігоря Сікорського", Ф-т інформатики та обчислювальної техніки, Каф. обчислювальної техніки. - Дод. тит. арк. англ. Текст кн. укр. та англ.

Подано праці міжнародної науково-практичної конференції з комп'ютерної інженерії, інженерії програмного забезпечення та технічної освіти, яка присвячена видатному вченому, викладачу кафедри обчислювальної техніки професору В.П. Широчину.

720883 R
004

Галюк, С. Д.
Програмне забезпечення об'єктів кіберпростору [Текст] : метод. рекомендації до лаб. робіт / уклад.: С. Д. Галюк, О. В. Круліковський, Л. Ф. Політанський ; Чернівецький національний університет імені Юрія Федьковича. - Чернівці : ЧНУ ім. Юрія Федьковича, 2019. - 120 с. - Бібліогр.: с. 120. - Уклад. на обкл. не зазнач.

Лабораторний практикум із об'єктозорієнтованого програмування мовою С++ відповідає навчальному плану дисципліни нормативної підготовки " Програмне забезпечення об'єктів кіберпростору" для студентів бакалаврату спеціальності 125 – "Кібезбезпека".

723030 R
004

Глибовець, М. М.
Моделі обчислень у програмній інженерії [Текст] : навч. посібник / М. М. Глибовець, О. В. Кирієнко, В. С. Проценко ; Національний університет "Києво-Могилянська академія". - Київ : Києво-Могилянська академія, 2019. - 212 с. : іл. - (Серія "Могилянський підручник"). - Бібліогр.: с. 209.

У навчальному посібнику викладено теоретичний базис, який є підґрунтям більшості елементів програмного забезпечення, – головні моделі обчислень, що лежать в основі провідних мов програмування. Розглядаються різні методи конструювання моделей, які утворюють фундамент базових алгоритмів, що використовуються в практиці програмування. Також описано механізми породження та аналізу формальних мов: форми Бекуса-Наура, контекстно-вільні та регулярні граматики. Представлено використання цих теоретичних напрацювань у мові програмування Java. В посібнику наведено велику кількість прикладів.
Для вивчення моделей обчислень описано використання програми ModelComp. Програма має зручний інтенфейс та дозволяє будувати, виконувати й зберігати різні моделі обчислень

722393 B
004

Інформаційні системи та технології. ІСТ-2019 [Текст] : матеріали 8-ї Міжнародної наук.-техн. конф., 9-14 вересня 2019 р., Коблеве-Харків, Україна / НАН України, Люблінський від. Польської АН, Представництво "Польська АН" у Києві, Харків. нац. ун-т радіоелектроніки [та ін.]. - Харків : ХНУРЕ, 2019. - 308 с. : граф., рис., табл. - Бібліогр. в кінці ст. - Паралел. назва англ.

Збірник містить матеріали статей міжнародної науково-технічної конференції з проблем сучасних інформаційних систем та технологій.

Зі змісту:

Секція 1. Сучасні інформаційні системи та технології: проблеми, методи, моделі. Управління проектами та програмами
Секція 2. Математичне та комп'ютерне моделювання у інформаційних системах
Секція 3. Інформаційні технології сталого розвитку. Геоінформаційні системи та технології
Секція 4. Розпізнавання образів, цифрова обробка зображень і сигналів
Секція 5. Інформаційні технології в соціумі, освіті, економіці, медицині, управлінні, поліграфії, екології та юриспруденції
Секція 6. Програмна інженерія
Секція 7. Захист інформації. Інформаційна безпека
Секція 8. Інтелектуальний аналіз даних, Data Mining та Big Data-технології.

Леонов Б. Д. Удосконалення методичного забезпечення експертних досліджень спеціальних програмних засобів у сфері протидії кіберзлочинності / Б. Д. Леонов, В. С. Серьогін // Інформація і право. – 2019. – № 4(31). – С. 98-106.

Р/844

Стаття присвячена аналізу проблем експертного забезпечення правоохоронної діяльності у сфері протидії кіберзлочинності. В межах статті досліджуються проблемні питання розробки методичних матеріалів для проведення експертних досліджень спеціальних програмних засобів. Запропоновані перспективні напрями подальших наукових досліджень протидії кіберзлочинності, модернізації та вдосконалення методик проведення експертних досліджень спеціальних програмних засобів.

Метод захисту модуля програмного забезпечення на основі процедури обфускації / С. Г. Семенов, В. В. Давидов, Д. Г. Волошин, Д. С. Гребенюк // Телекомунікаційні та інформаційні технології. – 2019. – № 4(65). – С. 71-80.

Р/1921

Мета статті: дослідження та розробка методу обфускації коду програмного модуля ліцензування з використанням особливостей презентації строкових виразів, викликів функцій та доступу до ідентифікаторів в байткод-орієнтованих мовах програмування.

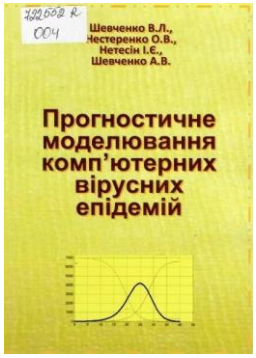
722400 В
621.3

Перспективні напрямки сучасної електроніки, інформаційних і комп'ютерних систем [Текст] : тези доп. на IV Всеукр. наук.-практ. конф. MEICS-2019, м. Дніпро, 27-29 листопада 2019 р. / Дніпровський нац. ун-т ім. Олеся Гончара. - [Кременчук] : [ПП Щербатих О. В.], 2019. - 277 с. : граф., рис. - Бібліогр. наприкінці ст. - Текст кн. укр., рос., англ. мов.

В збірник включені тези доповідей на IV Всеукраїнській науково-практичній конференції, яка відбулася в Дніпровському національному університеті імені Олеся Гончара, 27–29 листопада 2019 р.

Зі змісту:

Секція I. Інформаційні системи і технології
Секція II. Комп'ютерні системи і компоненти
Секція III. Радіотехнічні пристрої й засоби телекомунікації
Секція IV. Функціональна електроніка. Мікро- і нанотехнології
Секція V. Фізичні явища в матеріалах електронної техніки та технологія їх отримання.



722552 R
004

Прогностичне моделювання комп'ютерних вірусних епідемій [Текст] : монографія / Шевченко В. Л., Нестеренко О. В., Нетесін І. Є., Шевченко А. В. ; Український наук. центр розвитку інформ. технологій (УкрНЦ РІТ). - Київ : УкрНЦ РІТ, 2019. - 154 с. : граф., рис., табл. - Бібліогр.: с. 140-152 (106 назв).

Монографію присвячено методам створення прогноз-моделей розвитку комп'ютерних вірусних епідемій. Проаналізовані основні види інцидентів інформаційної безпеки. Надані основні класифікації щодо комп'ютерних атак та способів захисту. Встановлений зв'язок між параметрами математичних моделей та прикладними заходами протидії зараженню інформаційних систем.

Щебланін Ю. М. Розробка програмного забезпечення для захисту інформації від несанкціонованого доступу / Ю. М. Щебланін, О. А. Курченко, Н. А Гончаренко // Сучасний захист інформації. – 2019. – № 4(40). – С. 82-87.

Р/2300

В даній статті проведено детальний аналіз симетричних шифрування. На основі проведеного аналізу розроблено програмне забезпечення з використанням алгоритмів шифрування DES та AES.

Телекомунікаційні мережі та інформаційно-комунікаційні технології

Аналіз загроз під час упровадження технології IMT-2020/5G / Ю. І. Катков, О. В. Зінченко, Ю. В. Березовська, А. С. Ступник // Зв'язок. – 2019. – № 2(138). – С. 3-11.

Р/776

Розглянуто загрози під час упровадження стільникових мереж стандарту IMT-2020/5G. Упровадження і розвиток концепцій "цифрової економіки", хмарних технологій, великих баз даних, Інтернету речей, промислового інтернету речей та технології "розумний пил" потребує розвитку комунікаційного зв'язку нового покоління, яке має забезпечити переміщення цифрової інформації між об'єктами нового технологічного укладу.

Аналіз загроз та вразливостей під час впровадження технології 4G/LTE / Ю. І. Катков, Ю. В. Березовська, Ю. С. Пшеничний [та ін.] // Телекомунікаційні та інформаційні технології. – 2019. – № 4(65). – С. 25-38.

Р/1921

Поставлено завдання: під час розгляду рухомих бездротових широкосмугових стільникових мереж передачі даних стандарту 4G/LTE на основі аналізу функціонування її елементів визначити загрози для потенційно вразливих елементів. Для вирішення завдання виконано опис інноваційних механізмів впровадження мобільного зв'язку 4-го покоління, проаналізовано тенденції розвитку послуг перспективних областей застосування мобільного зв'язку стандарту 4G/LTE, розглянуто загрози для радіоінтерфейсу стільникових мереж стандарту 4G/LTE, що дозволяє визначити потенційну вразливість її окремих елементів.

Ахрамович В. М. Дослідження розподілених соціальних мереж з точки зору специфічних характеристик безпеки / В. М. Ахрамович, Ю. О. Тихонов, В. І. Степаненко // Зв'язок. – 2019. – № 5(141). – С. 13-18.

Р/776

Проведено аналіз розподілених соціальних мереж (ОСМ) (Persona, Safebook, PeerSoN Wie Concentric nodes, Vis-à-Vis) з погляду безпеки конфіденційності, інформаційного самовизначення, довірчих відносин, підтримання мобільності.

Гільгурт С. Методи побудови оптимальних схем розпізнавання для реконфігуровних засобів інформаційної безпеки / С. Гільгурт // Безпека інформації. – 2019. – Т. 25, № 2. – С. 74-81.

Р/1408

Через сталий зріст об'єму мережевого трафіку, кількості та складності атак програмні рішення вже не встигають в реальному часі розпізнавати сигнатури для таких засобів технічного захисту, як мережеві системи виявлення вторгнень, антивірусні сканери, фільтри протидії мережевим хробакам, тощо. Тому розробники все частіше звертають увагу на реконфігуровні (на базі ПЛІС) апаратні рішення, що поєднують в собі продуктивність спецпроцесорів із гнучкістю майже як у програмного забезпечення.

Дібрівний О. А. Сучасний стан мережі мобільного інтернету в Україні / О. А. Дібрівний // Зв'язок. – 2019. – № 6(142). – С. 29-33.

Р/776

Розглянуто стан мережі мобільного інтернету в Україні. Основну увагу приділено порівнянню швидкості підімкнення та щільності покриття в Україні зі світовими лідерами та виокремлено основні здобуті результати такого зіставлення. Також наведено порівняння швидкостей мобільного підімкнення для трьох найбільших мобільних операторів України: Київстар, Vodafone та lifecell, як з урахуванням 2G/3G мереж та окремо 4G мережі. Запропоновано статистику використання 4G мережі абонентами даних операторів. Сформульовано основні проблеми становлення 100-відсоткового покриття України мережею 4G.

721902 R
004

Захист систем електронних комунікацій [Текст] : навч. посіб. / [В. О. Хорошко, О. В. Криворучко, М. М. Браіловський та ін.] ; Київський національний торговельно-економічний університет. - Київ : Київ. нац. торг.-екон. ун-т, 2019. - 164 с. : рис., табл. - Бібліогр.: с. 160-163. - Авт. зазнач. на звороті тит. арк.

У навчальному посібнику розглядаються основи організації та порядок виконання робіт із захисту інформації в системах електронних комунікацій, порядок прийняття рішень щодо складу комплексної системи захисту інформації в залежності від умов функціонування СЕК і видів оброблюваної інформації, визначення обсягу і змісту робіт, етапності робіт, основних завдань та порядку виконання робіт кожного етапу.

Зубок В. Ю. Особливості моделі порушника при аналізі атак на глобальну маршрутизацію в Інтернеті / В. Ю. Зубок // Електронне моделювання. – 2019. – Т. 41, № 5. – С. 59-69.

Р/518

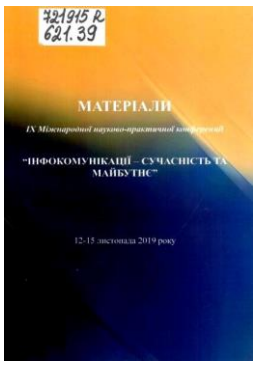
Запропоновано модель порушника безпеки інформації.

Через аналіз загроз та методів проведення атак на глобальну маршрутизацію встановлено, що джерелом таких загроз є зовнішні порушники. Наведено класифікацію таких порушників та розроблено неформальну модель порушника безпеки.

Іванченко Н. О. Основні проблеми безпеки IOT в умовах цифровізації економіки України / Н. О. Іванченко, О. М. Густера // Економіка та держава. – 2019. – № 11. – С. 50-54.

Р/1829

У статті виділено законодавчі, організаційні та технічні групи проблем безпеки, які нині є найбільш актуальними для світового і вітчизняного ринку інформаційних технологій. Також було проаналізовано кожен окремий тип загрози безпеки IoT.



721915 R
621.39

Інфокомунікації – сучасність та майбутнє, Міжнар. наук.-практ. конф. (9 ; 2019 ; Одеса).

Матеріали IX Міжнародної науково-практичної конференції "Інфокомунікації – сучасність та майбутнє" [Текст] : [тези], м. Одеса, 12-15 листопада 2019 р. / Одеська нац. акад. зв'язку ім. О. С. Попова. - Одеса : ОНАЗ ім. О. С. Попова, 2019. - 454 с. : іл. - Бібліогр. в кінці ст.

Даний збірник містить тези матеріалів, що представлені на дев'ятій міжнародній науково-практичній конференції "Інфокомунікації – сучасність та майбутнє", що проводилась 12–15 листопада 2019 р. в Одеській національній академії зв'язку ім. О.С. Попова.

У збірник включені тези доповідей за такими напрямками:

– сучасні системи мобільного зв'язку та широкосмугового радіодоступу;
– мультисервісні засоби телекомунікацій та телекомунікаційних мереж;
– інформаційні мережі та технології;
– телекомунікаційні системи;
– інформаційна безпека;
– програмна інженерія та комп'ютерні науки;
– проблеми економіки та управління у сфері інфокомунікацій.

Корольков Р. Особливості реалізації атаки деавтентифікації в мережах стандарту 802.11 / Р. Корольков, С. Куцак // Захист інформації. – 2019. – Т. 21, № 3. – С. 175-181.

Р/1428

У статті досліджено і продемонстровано практичну реалізацію спеціального типу атаки – "відмова в обслуговуванні" Denial of Service (DoS) в мережах на основі стандарту 802.11, а саме атаку деавтентифікації. Дане дослідження ілюструє можливу схему дії зловмисника і сценарій атаки на клієнта. Можливість реалізації атаки деавтентифікації безпосередньо пов'язана з особливостями механізму встановлення зв'язку в бездротовій мережі стандарту 802.11.

Корченко О. Модель параметрів для ідентифікації функціонального профілю захисту у комп'ютерних системах / О. Корченко, А. Давиденко, М. Шабан // Безпека інформації. – 2019. – Т. 25, № 2. – С. 122-126.

Р/1408

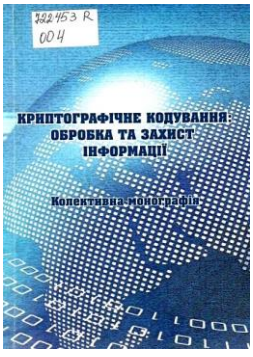
... пропонується модель параметрів для ідентифікації опису ФПБ в комп'ютерних системах (КС). Визначені множити критеріїв, їх елементів та рівнів. Все це дозволило у формальному вигляді сформувати необхідний набір величин для реалізації процесу ідентифікації ФПЗ в КС.

Кривкін А. В. Еволюція захисту безпроводової технології Wi-Fi / А. В. Кривкін // Зв'язок. – 2019. – № 2(138). – С. 35-38.

Р/776

Обговорено перспективи впровадження інформаційних та телекомунікаційних технологій в Україні та світі, де мережі потребують технічних знань та допомоги стосовно правильного налаштування повністю надмірних Wi-Fi вирішень із використанням переваг найсучасніших функцій безпроводових технологій.

722453 R
004



Криптографічне кодування: обробка та захист інформації [Текст] : кол. монографія / під ред. В. М. Рудницького ; Черкаський державний технологічний університет. - Харків : Діса Плюс, 2018. - 139 с. : рис., табл. -Ред. зазнач. на звороті тит. арк.

Колективна монографія містить матеріали актуальних напрямків криптографічного захисту та обробки інформації, а також соціальної інженерії щодо прогнозування та проведення оцінки якості та ефективності діяльності людства.

Лисенко С. М. Методи виявлення бот-мереж в комп'ютерних системах / С. М. Лисенко, К. Ю. Бобровнікова, В. С. Харченко // Сучасні інформаційні системи. – 2019. – Т. 3, № 4. – С. 87-95.

Р/543

Запропоновано новий підхід до виявлення бот-мереж в корпоративних мережах на основі аналізу поведінки ботів.

721959 В
629.7

Проблеми інформатизації та управління [Текст] : зб. наук. пр. / Нац. авіац. ун-т, Ін-т комп'ютерних інформаційних технологій. - Київ : [НАУ].
Вип. 1 (61). - Київ, 2019. - 109 с. : іл., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., рос., англ.

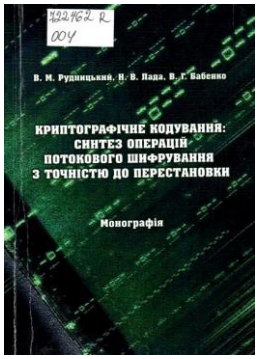
Зі змісту:

Балакін С. В. **Оптимізація діагностування несанкціонованих дій в комп'ютерній мережі.** – С. 7-11. – Текст рос.

Р/908
Радиотехника : всеукр. межвед. науч.-техн. сб. / Харьк. нац. ун-т радиоэлектроники. – 2019. – Вып. 198: **Информационная безопасность.** – 233 с.

Разделы сборника:

- Перспективные криптологические преобразования и их применение
- Анализ и использование криптографических методов в децентрализованных технологиях.



722462 R
004

Рудницький, В. М.
Криптографічне кодування: синтез операцій потокового шифрування з точністю до перестановки [Текст] : монографія / В. М. Рудницький, Н. В. Лада, В. Г. Бабенко ; Черкаський державний технологічний університет. - Харків : [ДІСА ПЛЮС], 2018. - 184 с. : рис., табл. - Бібліогр.: с. 155-173.

Монографія присвячена підвищенню якості систем потокового шифрування конфіденційної інформації за рахунок підвищення стійкості та надійності перетворення на основі використання модифікованих операцій додавання за модулем два з точністю до перестановки. Монографія містить матеріали конкретних інженерних методик, алгоритмів, моделей та варіантів функціональних схем спеціалізованих дискретних пристроїв криптографічного перетворення і можливих варіантів їх реалізації.

Сальник С. Модель порушення захищеності інформаційних ресурсів комунікаційних систем / С. Сальник, А. Сторчак, А. Микитюк // Information Technology and Security. – January-June 2019. – Vol. 7, Iss. 1(12). – P. 25-34.

Р/1212

Представлено модель порушення захищеності інформаційних ресурсів, що обробляються в комунікаційних системах. Описано основні функції системи забезпечення безпеки як одного з елементів комунікаційної системи.

Соболєв А. М. Виявлення в глобальній мережі Інтернет інформаційних джерел, які розповсюджують недостовірну інформацію / А. М. Соболєв // Реєстрація, зберігання і обробка даних. – 2019. – Т. 21, № 3. – С. 56-68.

Р/1346

Наведено метод, який базується на значеннях дисперсії і показника Херста в часових рядах, що утворюють масиви публікацій в інформаційних джерелах глобальної мережі Інтернет.

Ступень П. В. Моделювання характеристик обладнання комп'ютерних мереж у ракурсі інформаційної безпеки / П. В. Ступень, К. В. Дікусар, А. А. Рябой // Вісник Черкаського державного технологічного університету. Серія: Технічні науки. – 2019. – № 4. – С. 42-48.

Р/1308

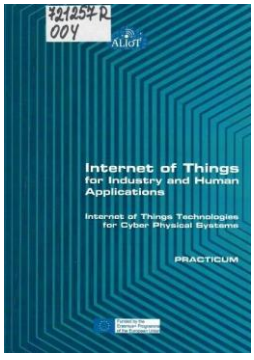
Дослідження присвячене розвитку моделей аналізу та оцінювання ризиків інформаційної безпеки в комп'ютерних мережах, які використовуються при розробці систем захисту інформаційних ресурсів підприємств та при аудиті рівня захисту інформаційних систем, які вже функціонують, розробленню сімейства моделей безпеки комунікаційного обладнання комп'ютерних мереж.

Розроблені алгоритми та моделі були реалізовані в системі аналізу та виправлення порушень інформаційної безпеки, використання якої дало можливість скоротити час виправлення наслідків таких порушень.

721888 R
621.3

Сучасні проблеми інфокомунікацій, радіоелектроніки та наносистем, Міжнар. наук.-техн. конф. (1 ; 2019 ; Вінниця).
Матеріали І Міжнародної науково-технічної конференції "Сучасні проблеми інфокомунікацій, радіоелектроніки та наносистем (СПРІН-2019)" [Text] : збірка доп., м. Вінниця, 14-16 листопада 2019 р. / Вінницький нац. технічний ун-т, Нац. техн. ун-т "Київський політехн. ун-т ім. І. Сікорського", Харківський нац. ун-т радіоелектроніки [та ін.]. - Вінниця : ВНТУ, 2019. - 189 р. : іл. - Бібліогр. в кінці ст.
З нагоди 50-річчя ф-ту інфокомунікацій, радіоелектроніки та наносистем. Дод. тит. арк. англ. Текст кн. укр., англ.

Збірка містить матеріали доповідей І Міжнародної науково-технічної конференції з сучасних проблем інфокомунікацій, радіоелектроніки, телекомунікацій, наносистем та приладобудування за такими основними напрямками: обробка сигналів і зображень в радіоелектронних, телекомунікаційних та біотехнічних системах; радіотехнічні, телекомунікаційні комплекси та системи та їх інфокомунікаційне забезпечення; інформаційні, біотехнічні системи та штучні імпланти в біоінженерії; мікро- та наносистемна техніка; сучасні напрямки розвитку електроніки.



721257 R
004

Технології Інтернету речей для кіберфізичних систем [Text] : практикум / Г. І. Воробець, В. С. Харченко, Р. К. Кудерметов [та ін.] ; за ред. Г. І. Воробця та В. С. Харченко ; Чернівецький національний університет імені Юрія Федьковича, Нац. аерокосмічний ун-т "ХАІ", Запорізький нац. техн.ун-т. - [Київ] : [ЮСТОН], 2019. - 172 р. : рис., табл. - (Інтернет речей для промисловості та гуманітарних застосувань. Проект Erasmus+ALIOT" Інтернет речей: нові навчальні програми для промисловості та гуманітарних застосунків" (573818-EPP-1-2016-1-UK-EPPKA2-CBHE-JP)). - Бібліогр. в кінці ст. - Обкл., дод. тит. арк. та текст кн. англ. Авт. на обкл. не зазнач.

Наведено структуру курсу, навчальні матеріали, приклади завдань для семінарів, практичних і лабораторних робіт, а також методичні рекомендації для самопідготовки і перевірки знань з дисципліни, та критерії їх оцінювання.

Матеріал подається послідовно для формування цілісної картини сучасного стану, синергії, перспектив розвитку та досліджень технологій інтернету речей і кіберфізичних систем. Увага акцентується на концептуальних питаннях моделювання, аналізу, синтезу і практичного впровадження КФС, та ролі IoT на всіх етапах життєвого циклу складних комп'ютерних систем.

721950 В
621.39

"Український науково-дослідний інститут зв'язку", державне підприємство.
Наукові записки Українського науково-дослідного інституту зв'язку [Текст] : науковий журнал / Державний університет телекомунікацій. - Київ : [Вид. центр Держ. ун-ту телекомунікацій] .
№ 3 (55). - Київ, 2019. - 92 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., рос., англ.

Зі змісту:

Макаренко А. О., Лавренко А. С., Козлов Б. С., Андрюк О. М., Казмирчук М. Г. **Методи підвищення ефективності роботи безпроводових телекомунікаційних мереж.** – С. 74-79.
У статті наведені дослідження про методи множинної передачі сигналу в системах MIMO. Такі як мультиплексування, рознесення сигналу на прийом та передачу, адаптивну передачу, а також описано який приріст вони можуть дати. Розглянуто роботу з точки зору 802.11 Wi-Fi, зазначені методи використовуються і в інших бездротових стандартах (LTE, 802.16 WiMAX).

722082 R
004

Швиденко, Михайло Зіновійович.
Інформаційні технології [Текст] : навч. посіб. для студ. ОС "Бакалавр" спец. "Публічне управління", "Готельно-ресторанний бізнес" та "Туризм" / Швиденко М. З., Касаткіна О. М., Швиденко О. М. ; Національний університет біоресурсів і природокористування України, Каф. інформаційних систем. - Київ : Компринт, 2019. - 572 с. : іл. - Авт. на тит. арк. не зазнач.

Навчальний посібник призначений для підготовки здобувачів вищої освіти ступеню "Бакалавр" за спеціальностями "Публічне управління", "Готельно- ресторанний бізнес" та "Туризм" з дисциплін "Інформаційні системи і технології" та "Інформатика". Посібник містить необхідний теоретичний та практичний матеріал, який надає можливість студентам сформувати відповідні компетентності у сфері інформаційно-комунікаційних технологій.

Шемаєв В. М. Соціальні мережі в аспекті інформаційної безпеки / В. М. Шемаєв, М. М. Присяжнюк, А. П. Онофрійчук // Наука і оборона. – 2019. – № 3. – С. 36-39.

Р/810

У статті розглядається забезпечення інформаційної безпеки в соціальних мережах. Досліджуються соціальні мережі як середовище маніпулятивного впливу та розкриваються причини й наслідки негативного впливу в соціальних мережах.

722089 R
339

Шиндировський, Ігор Миколайович.
Інтернет у бізнесі [Текст] : навч. посіб. / І. М. Шиндировський ; Центральна спілка споживчих товариств України, Львівський торг.-екон. ун-т. - Львів : Вид-во ЛТЕУ, 2019. - 200 с. : граф., табл. - Бібліогр.: с. 187-190.

В українські економіці неабиякого значення набуває використання глобальної мережі Інтернет в діяльності суб'єктів господарювання. Тому виникла потреба запровадження курсу "Інтернет у бізнесі" в навчальний план підготовки бакалаврів галузей знань 24 "Сфера обслуговування" (спеціальність 241 "Готельно-ресторанна справа") та 07 "Управління та адміністрування" (спеціальності 073 "Менеджмент", 075 "Маркетинг", 076 "Підприємництво, торгівля та біржова діяльність"). У посібнику розглядаються теоретичні основи застосування мережі Інтернет в бізнесі, організація та технологія, використання можливостей Інтернету для вирішення конкретних завдань.

Інформаційне протиборство у воєнних конфліктах. Інформаційно-психологічна безпека

Антонов А. М. Павутиння соцмереж / А. М. Антонов // Оборонний вісник. – 2019. – № 12. – С. 14-19.

Р/1134

"Попередні покоління медіа використовували горизонтальну модель впливу, коли власник визначав основний зміст наративу, що доносився до читачів, слухачів, глядачів. А зараз швидкість комунікаційного обміну в соцмережах, відсутність просторово-часових обмежень, посилюють вплив на користувача".

Білобородов О. О. Технології інформаційно-психологічних війн та інформаційно-психологічна зброя / О. О. Білобородов, А. С. Довгополий // Озброєння та військова техніка. – 2019. – № 4(24). – С. 93-99.

Р/1126

У статті проаналізовані технології інформаційно-психологічного впливу на людину і суспільну свідомість. Розглянуто погляди на методичні та організаційні основи ведення інформаційно-психологічних війн. Проаналізовано застосування методів впливу на підсвідомість і методи прямого впливу на психофізіологічний стан людини. Розглянуто методи і засоби інформаційно-психологічної боротьби, що використовуються ворожими режимами по відношенню до України і власного населення.

722557 R
35

Головко, О. М.
Медіабезпека людини : засади інформаційно-правової політики [Текст] : монографія / Головко О. М. ; НДІ інформатики і права Нац. акад. правових наук України. - Київ : [Видавничий дім "АртЕк"], 2019. - 168 с. - Бібліогр.: с. 146-167 (331 назва).

В монографії здійснено міждисциплінарне дослідження феномену медіабезпеки людини.

Проаналізовано політичні, філософські та правові проблеми забезпечення медіабезпеки людини з огляду на становлення інформаційного суспільства, розширення спектру інформаційно-психологічних небезпек та утвердження нового формату ведення війни згідно концепції DIME wars.

721951 В
623

Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки.
Збірник наукових праць Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки [Текст] : науково-теоретичний та науково-практичний збірник наукових праць. - Чернігів : ФОП Брагинець О. В., 2019 - .
Вип. 1 (1). - Чернігів, 2019. - 177 с. : граф., рис., табл. - Бібліогр. в кінці ст.

Зі змісту:

Камак Д. О., Скиба О. В., Троцик С. М., Доманов І. О., Богучарський В. В. **Використання хибних мікробазових станцій та фемтосот в інтересах підрозділів інформаційно-психологічних операцій Збройних Сил України.** – С. 82-86.

Калініченко Б. М. Новітні засоби інформаційного протиборства в умовах техногенної цивілізації / Б. М. Калініченко // Держава і право. – 2019. – Вип. 86. – С. 296-305.

Р/788

Наводиться перелік новітніх засобів інформаційного протиборства, до яких віднесено: фальсифікацію мови, хибну ідентифікацію, нав'язування ірраціоналізму, масові розсилки, віруси, логічні бомби тощо. Також охарактеризовані прийоми, які застосовуються на їхній основі: вкидання, тролінг, дискредитація, продукування віртуальних особистостей та ін.

Лепіхов А. В. Стратегія непрямих дій / А. В. Лепіхов, Г. С. Храпач // Оборонний вісник. – 2019. – № 12. – С. 8-13.

Р/1134

"Вітчизняні науковці та іноземні дослідники вважають, що образ сучасної війни носить локальний характер, визначається таким явищем, як поєднання обмеженого силового впливу на супротивника із застосуванням стратегії непрямих дій. Характер цього сценарію може об'єднувати широкий діапазон ворожих обставин і намірів, а саме: дестабілізацію суспільно-політичної обстановки в країні, застосування іррегулярних військ, кібервійну ...".

Метод виявлення деструктивно інформаційно-психологічного впливу на підсвідомість особового складу та населення України / В. В. Бараннік, С. О. Сідченко, Т. В. Белікова, Ю. О. Олійник // Системи озброєння і військова техніка. – 2019. – № 4(60). – С. 120-127.

Р/1903

Визначено, що запропонований метод лінгвістичного процесору дає можливість для визначення в текстовому повідомленні головних слів, що характеризують текст, та визначити їх спрямованість щодо впливу на підсвідомість особистості. Проведені практичні дослідження показали працездатність даного методу для виявлення сугестивного деструктивного ІПВ на підсвідомість військовослужбовців сектору оборони безпеки України та населення України.

Мужанова Т. М. Досвід Європейського Союзу з протидії деструктивній інформаційній діяльності в мережі Інтернет / Т. М. Мужанова, Ю. М. Якименко // Сучасний захист інформації. – 2019. – № 2(38). – С. 37-41.

Р/2300

У статті окреслено передумови розширення масштабів деструктивної інформаційної діяльності в мережі Інтернет, розглянуто сутність та види заходів інформаційно-психологічного впливу в Інтернеті. Автори проаналізували діяльність Європейського Союзу зі стратегічних комунікацій (2015-2019 рр.), спрямовану на запобігання та протидію небезпечному для ЄС інформаційно-психологічному впливу у всесвітній мережі.

Науменко Н. Ю. Теоретико-методологічні аспекти інформаційно-психологічної безпеки в послідовності держава – регіон – суспільство – людина / Н. Ю. Науменко // Економічний вісник Донбасу. – 2019. – № 3(57). – С. 49-62.

Р/1932

Мета статті. Завдання даного дослідження – уточнити сутнісні характеристики інформаційно-психологічної безпеки в сфері економічної безпеки регіону за допомогою аналізу взаємозв'язків з іншими складовими феномену безпеки через розгляд ролі та місця інформаційно-психологічної безпеки в трьох системах більш високого ієрархічного рівня: безпека людини, інформаційна безпека регіону, інформаційна безпека держави.

Семенова К. О. Запобігання загрозам медіа-пропаганди в умовах розвитку електронної демократії / К. О. Семенова // Економіка та держава. Серія: Державне управління. – 2019. – № 1(9). – С. 63-68.

Р/1829

У статті досліджено сутність пропагандистського впливу в сучасному світі в умовах мережевої війни. Основна увага приділяється особливостям медіа-пропаганди в умовах розвитку електронної демократії, що здійснюється в системах горизонтальних масових комунікацій, прикладом яких можуть слугувати соціальні мережі. Охарактеризовано методи маніпуляції масовою свідомістю у ЗМІ, в тому числі мережі Інтернет. Проаналізовано тролінг як основний засіб Інтернет-пропаганди, запропоновано класифікацію тролінгу, що включає в себе т. зв. "товстий" і "тонкий" тролінг.

Структурно-логічна послідовність та принципи організації протидії інформаційно-психологічним впливам з боку недружньої держави / В. Ю. Богданович, О. В. Дублян, О. В. Передрій, П. Пацек // Наука і техніка Повітряних Сил Збройних Сил України. – 2019. – № 4(37). – С. 13-19.

Р/2266

Розглядається системно-логічна послідовність організації асиметричної протидії інформаційно-психологічним впливам з боку недружніх держав, яка посилює можливості політичного керівництва держави щодо функціонування в умовах гібридних загроз, зокрема при здійсненні проти нього інформаційно-психологічних впливів в зовнішньополітичній та внутрішньополітичній сферах.

Тарасенко Я. Визначення координат семантичної частки в англомовному тексті при відомому психолінгвістичному портреті пропагандиста / Я. Тарасенко // Захист інформації. – 2019. – Т. 21, № 3. – С. 168-174.

Р/1428

Існуючі засоби протидії інформаційній пропаганді, як і власне засоби інформаційного впливу, базуються на використанні методів нейро-лінгвістичного програмування. Відомий інструментарій недостатньо ефективний при протидії інформаційні пропаганді. Одним з можливих рішень є підвищення ефективності приховування цільового впливу на пропагандиста з використанням квантово-семантичного дослідження при формуванні чи модифікації тексту за індивідуальною семантичною функцією.

Тарасенко Я. Використання принципів квантової лінгвістики в інформаційному протиборстві / Я. Тарасенко // Безпека інформації. – 2019. – Т. 25, № 2. – С. 96-103.

Р/1408

В статті проводиться огляд існуючих підходів квантово-лінгвістичного дослідження тексту та суміжних методів, що реалізують принципи квантової лінгвістики та можуть бути використані для отримання теоретичного підґрунтя в подальших дослідженнях технічного аспекту використання квантової лінгвістики в забезпеченні інформаційної безпеки держави в умовах можливої ворожої пропагандистської діяльності як однієї особи, так і групи осіб за умови як відомого, так і невідомого психологічного портрету зловмисника.

723021 R
32

Фейки, пропаганда, дезінформація та виборчий процес: як нам захистити демократичні практики [Текст] : аналітична доповідь / Дубов Д. В., Корецька І. О., Баровська А. В. [та ін.] ; за заг. ред. Дубова Д. В. ; Школа Політичної Аналітики НаУКМА, НІСД (Нац. ін-т стратегічних досліджень). - Київ : Сталь, 2019. - 249 с. - Бібліогр. у виносках. - Авт. зазнач. на с. 3.

Підготовка до виборів, сам день виборів і період, що триває безпосередньо після виборів (потрібний для підрахунку голосів, оголошення результатів тощо) зазвичай регламентується особливим законодавством, що закріплює ролі, можливості та обмеження як безпосередніх учасників, так і дотичних суб'єктів (передусім медіа). Водночас законодавство, як і державні інституції, чия діяльність спрямована на захист виборів, та громадська думка багатьох країн виявилися "не готовими" до нових інформаційних реалій проведення сучасних виборів.

Вибори в Україні традиційно є точкою найвищого політичного протиборства, в якому використовуються всі можливі засоби. Виборчі кампанії 2019 року не стали винятком: відповідно до звіту ENEMO у більшості областей України фейкові новини з метою підриву авторитету та гідності кандидатів використовувалися під час агітації, зокрема між двома турами голосування за президента. Україна на п'ятому році гібридного протистояння досі слабко адаптована до таких деструктивних дій.

Ця доповідь – спроба окреслити ключові напрями вдосконалення нормативно-правової та організаційної моделі захисту виборчого процесу від деструктивного впливу дезінформації, а також створити основу для більш широкого діалогу між державою та професійною спільнотою в пошуках рішень для ефективного інформаційного захисту демократичного процесу в Україні загалом.

721718 В
355

Центр воєнно-стратегічних досліджень Національного університету оборони України.
Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського [Текст] : [наук. вид.] / [гол. ред. Загорка Олексій Миколайович]. - Київ : [ЦВСД НУОУ].
Вип. 2 (66). - Київ, 2019. - 146 с. : граф., рис., табл. - Бібліогр. наприкінці ст.

Зі змісту:

Циганок В. Використання даних з відкритих джерел для прийняття рішень в умовах інформаційної боротьби / В. Циганок, С. Каденко, О. Андрійчук // Information Technology and Security. – January-June 2019. – Vol. 7, Iss. 1(12). – P. 35-48.

Р/1212

Оглянуто методи, засоби та інструменти, що дозволяють використовувати дані з відкритих джерел для підтримки рішень у слабко структурованих предметних областях. Як приклад слабко структурованої предметної області розглянуто інформаційне протистояння, зокрема, виявлення інформаційних операцій. Для даної сфери запропоновано гібридну методику підтримки прийняття рішень, що використовує як експертні дані, так і дані з відкритих джерел. За основу методики взято принцип ієрархічної декомпозиції головної мети інформаційної операції.

Кібербезпека – проблема XXI століття

Аналіз та оцінка методів і засобів знищення інформації з магнітних носіїв як елементу сучасної інформаційної безпеки / О. М. Семененко, Ю. Б. Добровольський, Р. В. Лукаш [та ін.] // Збірник наукових праць Військової академії (м. Одеса). Серія: Технічні науки. – 2019. – Вип. 1(11). – С. 99-112.

Р/431

У статті проведено аналіз та оцінку ефективності існуючих методів і засобів знищення інформації з магнітних носіїв як важливого елементу сучасної інформаційної безпеки з метою вироблення практичних рекомендацій щодо вибору найбільш ефективних та економічно вигідних методів та засобів знищення конфіденційної інформації в оборонній сфері.

Барабаш О. В. Математичне моделювання інтенсивності кібератак підприємства з урахуванням еластичності часового періоду проведення аудиту / О. В. Барабаш, Є. М. Галахов // Сучасний захист інформації. – 2019. – № 4(40). – С. 12-21.

Р/2300

Виокремлено чинники, які впливають на тривалість часу між аудитами: інвестування підприємства у кібербезпеку, рівень складності систем, конфіденційні дані. Розглянуто плановий автоматизований аудит на підприємстві у розрізі кібер-загроз типу Спаму і розрахувати середнє значення ефекту. Змодельовано функціональну залежність інтенсивності кібератак, що описується нелінійним диференціальним рівнянням Бернуллі, яке згідно з гіпотезою, що інтегральна функція інтенсивності кібератак підлягає логістичному закону, описує процес часового ряду інтенсивності кібератак.

Барченко Н. Л. Методи теорії прийняття рішень в кібербезпеці / Н. Л. Барченко, В. К. Ободяк, В. Р. Татарінов // Вісник Інженерної академії України. – 2019. – № 2. – С. 71-74.

Р/1139

Розглянуто можливість застосування методів теорії прийняття рішень, а саме, методу аналізу ієрархій, для вирішення завдання вибору програмного забезпечення для управління інформаційною безпекою.

Біленчук П. Космічна і електронна кіберзлочинність третього тисячоліття: новітні виклики та загрози для людини, суспільства, держави, цивілізації / П. Біленчук, М. Малій // Бизнес и безопасность. – 2019. – № 5. – С. 18-21.

Р/1070

"... глобальна електронна комп'ютерна мережа інтернет надає можливість увійти до будь-якої американської відомчої комп'ютерної системи, у тому числі і військової. У порівнянні з США, національна кібербезпека України поки що залежить від електронних комп'ютерних мереж значно менше. На сьогодні ми стикаємось з комп'ютерними злочинами, в основному, у економічній та фінансово-кредитній сфері. Але у недалекому майбутньому такі злочини можуть привести до глобальних катастроф...".

Біленчук П. Новітні засоби забезпечення кібербезпеки / П. Біленчук, М. Малій // Бизнес и безопасность. – 2019. – № 5. – С. 27-28.

Р/1070

Серед чотирьох основних способів ідентифікації особистості користувача в процесі електронного документознавства (за предметом, яким володіє людина; за паролем або особистим ідентифікаційним кодом, який вводиться в ЕОМ з клавіатури; за фізичними характеристиками особистості, притаманними індивідуально лише їй; за електронним цифровим підписом) найбільш перспективними та надійними вважаються останні два способи.

720762 В
355

Військовий інститут Київського національного університету імені Тараса Шевченка.
Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка [Текст] : збірник наукових праць. - Київ : [ВІКНУ].
Вип. № 64. - Київ, 2019. - 172 с. : іл. - Бібліогр. наприкінці ст. - Текст кн. укр., рос., англ.

Зі змісту:

Даник Ю. Г., Вдовенко С. Г. **Ланцюгові ефекти в кібердіях.** – С. 71-90.
У статті представлені результати досліджень особливостей гібридної війни, яка відбувається в Україні та інших державах в кіберпросторі. У зв'язку з тим, що на цей час енергетика є базовою галуззю національної економіки та національної безпеки будь-якої держави, особливості комплексних деструктивних кібер-, інформаційних та когнітивних дій та впливів в кіберпросторі та через кіберпростір розглянуті на прикладі енергетичної сфери з урахуванням загроз, ризиків та особливостей кібервпливів на системи і об'єкти критичної інфраструктури паливо-енергетичного комплексу.

722395 В
621.39

Військовий інститут телекомунікацій та інформатизації.
Збірник наукових праць [Текст] = Collection of Scientific Papers / Міноборони України. - Київ : [ВІТІ].
Вип. № 3. - Київ, 2019. - 112 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст укр., та англ.

Зі змісту:

Куцаєв В. В., Радченко М. М., Терещенко Т. П. **Модель оцінки готовності інформаційно-телекомунікаційного вузла зв'язку в умовах кібернетичних атак.** – С. 43-50.
Чередниченко О. Ю., Процюк Ю. О., Шемендюк О. В., Мальцева І. Р. **Способи вдосконалення схем захисту від кібернетичних атак в інформаційно-телекомунікаційних системах.** – С. 103-109.

Гайдур Г. І. Механізм функціонування цілісної інформаційної системи в умовах кібернетичного впливу / Г. І. Гайдур, С. О. Гахов // Сучасний захист інформації. – 2019. – № 4(40). – С. 22-26.

Р/2300

Відповідно до запропонованої концепції аналізу зв'язків запропоновано аналіз системи та визначення ефективності роботи інформаційної системи як при цілісному підході, так і при аналізі ефективності складових різних рівнів інформаційної системи в умовах кібернетичного впливу.

Галахов С. М. Розвиток моделей кібератак у площині інформаційної безпеки підприємства / С. М. Галахов, В. В. Собчук // Телекомунікаційні та інформаційні технології. – 2019. – № 4(65). – С. 12-24.

Р/1921

Проблеми інформаційної безпеки обумовлюють дослідження уразливостей, моделей кібератак, які складаються з чотирьох груп: моделі кібератак на стандартне програмне забезпечення і пропрієтарні додатки; моделей кібератак на конфігурацію сервера, рівень виправлень сервера та моделей кібератак на мережеву інфраструктуру. Представлено відповідні уразливості і проблеми усіх груп кібератак на підприємство.

Жилін А. Функціональна модель оцінювання рівня зрілості SOC на основі моделі зрілості / А. Жилін, Г. Голич, М. Худинцев // Захист інформації. – 2019. – Т. 21, № 3. – С. 182-193.

Р/1428

Розвинуті сучасні організації, що у своїх бізнес-процесах застосовують передові технології, потребують висококласного підходу до управління процесом кіберзахисту, незалежно від призначення застосовуваних технічних засобів – інформаційних технологій (IT), систем промислового управління (ICS), кібер-фізичних систем (CPS) або пристроїв IoT.

"Метою даної роботи визначено створення функціональної моделі оцінювання рівня зрілості SOC на основі обраної моделі зрілості, а також аналіз ролі самих моделей оцінки зрілості у загальному фреймворку з ІБ організації".

Киберпреступники все активнее атакуют мобильные устройства на iOS // Технології безпеки. – 2019. – № 5-6. – С. 34-35.

Р/1115

"По данным исследования компании Eset, в первом полугодии количество обнаруженных уязвимостей на Android уменьшилось. В частности, за весь 2018 г. их было обнаружено 611, тогда как в 2019 г. опубликована информация только о 86 уязвимостях в системе безопасности мобильных устройств Android.

Надежность и безопасность считаются основными преимуществами смартфонов и планшетов на базе операционной системы iOS. Однако уязвимости в системе безопасности и угрозы для этой платформы все равно существуют".

Кібербезпека України: аналіз сучасного стану / О. Трофименко, Ю. Прокоп, Н. Логінова, О. Задерейко // Захист інформації. – 2019. – Т. 21, № 3. – С. 150-157.

Р/1428

За умов стрімкого зростання кіберризиків і кіберзагроз важливим є моніторинг сучасного стану кібербезпеки нашої країни, висвітлення основних проблем розбудови національної системи кіберзахисту та визначення напрямів їх вирішення. У статті визначено політичні, науково-технічні, організаційні та просвітницькі питання, вирішення яких є необхідним у рамках комплексної протидії кіберзагрозам задля випереджального реагування на динамічні змінення, що відбуваються у кіберпросторі.

Клиен А. Обнаружение кибервторжений на цифровой подстанции / А. Клиен // Енергетика та електрифікація. – 2019. – № 8. – С. 2-7.

Р/464

"Подстанции являются потенциальным объектом для кибератак. Если злоумышленник может повлиять на одну или несколько подстанций, это может иметь серьезные последствия для сети.

В системе обнаружения вторжений для подстанций МЭК 61850 StationGuard реализован подход, который обеспечивает небольшое количество ложных срабатываний тревоги и все еще низкие издержки конфигурации благодаря возможностям SCL".

Комп'ютерна безпека інформаційних та керуючих систем АЕС: документи, що обґрунтовують комп'ютерну безпеку / А. А. Симонов, О. Л. Клевцов,С. О. Трубчанінов, О. П. Лазуренко // Ядерна та радіаційна безпека. – 2019. – № 4(84). – С. 73-81. – Текст рос.

Р/1232

У статті розглянуті підходи до створення та керування документами, що обґрунтовують комп'ютерну безпеку, такими як: політика, програма та план комп'ютерної безпеки, план реагування на комп'ютерні інциденти, звітні документи з комп'ютерної безпеки.

Лисенко С. М. Метод забезпечення резильєнтності комп'ютерних систем в умовах кіберзагроз на основі самоадаптивності / С. М. Лисенко // Радіоелектронні і комп'ютерні системи. – 2019. – № 4(92). – С. 4-16.

Р/1769

У статті представлена самоадаптивна система для забезпечення резильєнтності корпоративних мереж за наявності кібератак-мереж. Резильєнтність забезпечується адаптивним переконфігуруванням мережі.

Механізми кібербезпеки: проблема концептуалізації / О. Мілов, Н. Казакова, П. Мільчарський, О. Король // Безпека інформації. – 2019. – Т. 25, № 2. – С. 110-116. – Текст англ.

Р/1408

У статті розглянуто загальні підходи, пов'язані з використанням поняття "механізм" в системі кібербезпеки. Представлено первинне визначення механізму в системах аналітичної динаміки. Простежено трансформацію поняття "механізм" від механічних систем до економічних, соціальних і організаційно-технологічних. Сформульовано визначення механізму, яке може бути використано при аналізі і проектуванні систем прийняття рішень, розглянуті особливості використання цього поняття в системах кібербезпеки.

Моделювання кібератак засобами теорії графів / В. А. Савченко, О. Й. Мацько, С. В. Легомінова [та ін.] // Сучасний захист інформації. – 2019. – № 4(40). – С. 6-11.

Р/2300

У статті розглядається комплексна модель кібератаки на основі теорії графів, яка поєднує класичні уявлення щодо моделювання складних атак з розширеннями, що враховують залежності уразливостей окремих компонентів системи та мережевий статус компонентів. Наведено приклад оцінювання сценарію атаки та зроблено висновки щодо можливості застосування моделі для прогнозування наслідків атаки.

723438 R
004

Моделювання та інформаційні технології [Текст] : зб. наук. пр. / НАН України, Ін-т проблем моделювання в енергетиці імені Г. Є. Пухова. - Київ : [ПП "Системи, технології, інформаційні послуги"].
Вип. 86. - Київ, 2019. - 145 с. : рис., табл. - Бібліогр. наприкінці ст.

Зі змісту:

Зубок В. Ю. **Ретроспективний аналіз інцидентів кібербезпеки, пов'язаних з атаками на глобальну маршрутизацію.** – С. 42-49.

Мохор В. В. Оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури / В. В. Мохор, С. Ф. Гончар // Електронне моделювання. – 2019. – Т. 41, № 6. – С. 65-76.

Р/518

Обґрунтовано поняття комплексного ризику кібербезпеки інформаційних систем об'єктів критичної інфраструктури (ІСОКІ). Запропоновано векторну модель ризику та модель комплексного ризику. Розроблено структурні рішення обчислювальних систем для розрахунку сумарного ризику кібербезпеки ІСОКІ з використанням запропонованих методів.

Попівняк Ю. М. Кібербезпека та захист бухгалтерських даних в умовах застосування новітніх інформаційних технологій / Ю. М. Попівняк // Бізнес Інформ. – 2019. – № 8. – С. 150-157.

Р/610

Стрімкий розвиток інформаційних технологій та впровадження їх у практику ведення бухгалтерського обліку поставили під загрозу безпеку облікових даних, які циркулюють у кіберсередовищі, та вивели на передній план проблеми визначення заходів щодо підвищення їх кібербезпеки. Ґрунтуючись на аналізі статистичних даних, опублікованих у вітчизняних та іноземних дослідженнях, описано стан кібербезпеки у світі за різними показниками, основні джерела кіберзагроз для облікової інформації на підприємстві, яка базується на застосуванні загальних та специфічних засобів захисту організаційного, технічного, кадрового та юридичного характеру.

Савченко В. А. Управління ризиками кібербезпеки на основі теоретико-ігрового підходу / В. А. Савченко, О. Й. Мацько // Сучасний захист інформації. – 2019. – № 2(38). – С. 6-16.

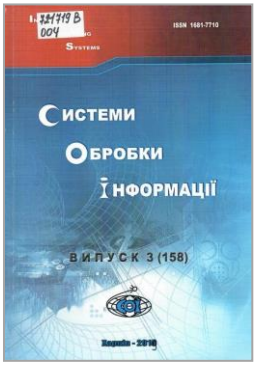
Р/2300

У статті розглядається концепція побудови Ігрової Моделі Кібербезпеки, як засобу, який кількісно ідентифікує ризики кібербезпеки та використовує цю метрику для визначення оптимального пакету засобів захисту відповідно до вкладених інвестицій.

Савчук М. М. Захист інформаційних технологій та кібербезпека : стенограма наукової доповіді на засіданні Президії НАН України 25 вересня 2019 року / М. М. Савчук // Вісник Національної академії наук України. – 2019. – № 11. – С. 23-28.

Р/250

У доповіді висвітлено низку найважливіших досліджень з розроблення методів захисту інформації, інформаційних технологій, математичного апарату криптології, стеганографії, а також технічних засобів та правових засад кібернетичної безпеки.



721719 В
004

Системи обробки інформації [Текст] = Information Processing Systems : щоквартальне наукове видання / Міноборони, Харківський нац. ун-т Повітряних Сил імені Івана Кожедуба. - Харків : Видавництво ХНУПС імені Івана Кожедуба.
Вип. 3 (158). - Харків, 2019. - 134 с. : іл., табл. - Бібліогр. наприкінці ст. - Алф. покажч.: с. 134. - Текст укр., рос., англ. Дод. тит. арк. англ.

Зі змісту:

Сторчак А. С., Сальник С. В. **Метод оцінювання рівня захищеності мережевої частини комунікаційної системи спеціального призначення від кіберзагроз.** – С. 98-109.

Сорокін Д. В. Інфраструктура промислових мереж IoT та кіберзагрози в доступі при використанні IoT рішень / Д. В.Сорокін, А. П. Бондарчук, К. П. Сторчак // Телекомунікаційні та інформаційні технології. – 2019. – № 4(65). – С. 120-127.

Р/1921

Підняте питання кібербезпеки в мережах IoT. Проведено аналіз інцидентів несанкціонованих втручань в мережу, які призвели до тимчасової відмови сервісів та заподіяли значної шкоди кінцевим споживачам услуг. Розглянуто методи перешкоджання кібератакам в мережах IoT.

Проведено аналіз використання рішень на основі стандарту NB-IoT та рішень на базі IoT для автоматизації промислових сервісів та з точки зору забезпечення безпеки в приватних мережах. Запропоновано методику вибору рішення з урахуванням вимог до бізнес-процесів кінцевих споживачів сервісів та технічних можливостей оператора. Розглянуто переваги приватних NB-IoT-мереж порівняно з LPWAN.

Ткаченко В. Киберугрозы и как с ними бороться / В. Ткаченко // Сети и бизнес : Телекоммуникации и сети – технологии и рынок. – 2019. – № 5(108). – С. 38-41.

Р/1698

Преступники изощряются в техниках атак, но не брезгуют и использованием известных уязвимостей.

Ткаченко В. Кібератаки в автоматичному режимі / В. Ткаченко // Сети и бизнес : Телекоммуникации и сети – технологии и рынок. – 2019. – № 6(109). – С. 52.

Р/1698

Найближче майбутнє кіберзлочинності: роботи-хакери і невловимі віруси.

Ткаченко В. В. Основні аспекти інформаційної безпеки в Smart Grid системах на основі стандартів ISO/IES 27001 та 27005 / В. В. Ткаченко, Ю. М. Щебланін // Сучасний захист інформації. – 2019. – № 3(39). – С. 36-41.

Р/2300

Наведено результати огляду основних загроз інформаційної безпеки, які притаманні Smart Grid системам. Надано перелік керівних вимог інформаційної безпеки які необхідно враховувати при проектуванні інтелектуальних мереж.

Ткаченко І. В. Спосіб організації оцінки стану кіберзахисту критичної інформаційної інфраструктури в режимі реального часу з урахуванням індикаторів кіберзагроз / І. В. Ткаченко, В. А. Козачок // Сучасний захист інформації. – 2019. – № 4(40). – С. 88-93.

Р/2300

Оцінку стану кіберзахисту запропоновано здійснювати за рахунок використання різних типів даних, диференційованих джерел інформації, та програмних платформ, що здатні здійснювати обробку великих даних.

Фактори створення стратегії безпеки інформаційних технологій сучасного підприємства / О. М. Шушура, С. В. Довбешко, О. А. Золотухіна, Л. А. Асєєва // Телекомунікаційні та інформаційні технології. – 2019. – № 2(63). – С. 5-13.

Р/1921

В роботі проведено аналіз стану інформаційної безпеки сучасного підприємства та розглянуті проблеми, що виникають у роботі інформаційних систем. Надано рекомендації фахівцям підрозділів інформаційних технологій щодо побудови стратегії інформаційної безпеки.

Шевченко А. Аналіз застосування методів машинного навчання на основі штучних нейронних мереж для виявлення кіберзагроз / А. Шевченко, Г. Застело, Є. Шпачинський // Information Technology and Security. – January-June 2019. – Vol. 7, Iss. 1(12). – P. 79-90.

Р/1212

Проаналізовано застосування методів машинного навчання на основі штучних нейронних мереж у прикладних задачах виявлення та класифікації кіберзагроз. Актуальність тематики статті обумовлена значними обсягами впровадження технологій машинного навчання в системі захисту інформації та забезпечення кібербезпеки.

Шуклін Г. В. Динамічна модель діагностики станів кіберзахисту систем інформатизації з використанням Fuzzy-технологій / Г. В. Шуклін, А. М. Правдивий, О. Ю. Котомчак // Сучасний захист інформації. – 2019. – № 2(38). – С. 17-24.

Р/2300

У роботі запропоновано підхід отримання миттєвого розрахунку ймовірностей негативних наслідків від успішної реалізації кібератак на об'єкти інформаційної діяльності на основі теорії диференціальних рівнянь із запізненням і механізму побудови логічної Fuzzy-функції.