Тематична виставка
"Безпека та захист інформаційного простору"

(надходження І півріччя 2021)

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

727268 R
34

Артеменко, Олена Вікторівна.
Інформаційне право [Текст] : навч. посібник / Артеменко О. В., Улютіна О. А. ; [Національний університет біоресурсів і природокористування України]. - Київ : [НУБіП України], 2020. - 102 с. : іл. - Бібліогр.: с. 99-101.

У навчальному посібнику викладено практичне висвітлення аспектів регулювання інформаційних відносин, пошук відповідних шляхів удосконалення чинного національного законодавства у сфері інформаційних відносин у вигляді схем.

Бєлєвцева В. В. Адміністративно-правовий захист інформації з обмеженим доступом: визначення та удосконалення / В. В. Бєлєвцева // Бизнес и безопасность. – 2021. – № 1(141). – С. 24-27.

Р/1070

... характерною ознакою надання інформації обмеженого доступу є законодавчо визначена процедура її захисту та охорони як з боку держави, так й іншого власника інформації (суб'єкта).

Бєлєвцева В. В. До питання застосування правових режимів забезпечення кібербезпеки в Україні / В. В. Бєлєвцева // Інформація і право. – 2020. – № 4(35). – С. 106-112.

Р/844

Окреслені правові основи забезпечення кібербезпеки та ознаки правових режимів у цій сфері. У роботі наведені напрями розробки системи правових режимів забезпечення кібербезпеки.

Борисов О. Ю. Нормативно-правова база забезпечення інформаційної безпеки України: сучасні проблеми та відправні точки їх вирішення / О. Ю. Борисов // Інформація і право. – 2020. – № 4(35). – С. 113-118.

Р/844

Дана стаття присвячена питанням актуальності формування в Україні гармонійної і дієвої системи нормативно-правового забезпечення інформаційної безпеки.

Брижко В. М. Приватність, конфіденційність та безпека персональних даних / В. М. Брижко, В. Г. Пилипчук // Інформація і право. – 2020. – № 1(32). – С. 33-46.

Р/844

У статті розглядаються окремі проблеми стану та формування правових основ системи захисту персональних даних в умовах євроінтеграції України у контексті застосування поняття "приватність людини" як фактору, який визначає основу інформаційної безпеки демократичного суспільства. Формулюються окремі позиції в плані можливого вдосконалювання сучасного законодавства.

727833 R
34

Вплив пандемії коронавірусу COVID-19 на права, свободи і безпеку людини в інформаційній сфері [Текст] : матеріали наук.-практ. студ. конференції, 12 травня 2020 р., м. Київ / [упоряд.: В. М. Фурашев, С. Ю. Петряєв] ; Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", Ф-т соціології і права, Каф. інформ. права та права інтелект. власності, НДІ інформатики і права НАПрН України. - Київ : КПІ ім. І. Сікорського , 2020. - 196 с. : граф. - Бібліогр. в кінці ст.

Матеріали конференції присвячені розгляду впливу пандемії коронавірусу COVID-19 на права, свободи і безпеку людини в інформаційній сфері. Участь у конференції взяли виключно студенти, в основному Київського політехнічного інституту імені Ігоря Сікорського різних спеціальностей та спеціалізації.

Гріщенко А. О. Підходи до розуміння категорії "інформаційна безпека" та правові засади її забезпечення / А. О. Гріщенко // Інформація і право. – 2020. – № 4(35). – С. 119-133.

Р/844

Дослідження основних підходів до визначення інформаційної безпеки людини, суспільства та держави в теорії права та правових засад її забезпечення.

Гуцалюк М. В. Шляхи посилення спроможностей правоохоронних та інших державних органів у сфері боротьби з кіберзлочинністю / М. В. Гуцалюк // Інформація і право. – 2020. – № 3(34). – С. 75-87.

Р/844

У статті розглянуто проблеми боротьби з кіберзлочинністю та надаються рекомендації, щодо посилення спроможностей правоохоронних та інших органів у цій сфері.

Довгань О. Д. Протидія загрозам кібербезпеці держави на глобальному рівні / О. Д. Довгань, А. В. Тарасюк // Інформація і право. – 2020. – № 2(33). – С. 85-98.

Р/844

У статті проаналізовано основні тенденції розвитку кіберпростору, а також визначені пов'язані із цим актуальні проблеми забезпечення кібербезпеки на глобальному та національному рівнях, зокрема, у контексті забезпечення безпеки об'єктів критичної інфраструктури, становлення Інтернету речей тощо.

Дудатьєв А. В. Інформаційно-аналітичні центри в управлінні інформаційною безпекою держави / А. В. Дудатьєв, О. П. Войтович, В. В. Миронюк // Вісник Хмельницького національного університету. Серія: Технічні науки. – 2020. – № 1. – С. 105-109.

Р/1055«Т»

Запропоновано модель «інформаційного портрету» об’єкта захисту від локального до держави. Наведена схема інформаційного забезпечення інформаційно-аналітичного центру. На базі отриманих результатів запропонована методологія побудови трьохрівневої політики безпеки, спрямованої на державу, регіон та локальний об’єкт.

727466 В
339

Історико-політичні проблеми сучасного світу [Текст] = Modern historical and political issues : зб. наук. ст. / Чернів. нац. ун-т ім. Юрія Федьковича, Ф-т історії, політології та міжнар. відносин, Каф. міжнар. відносин. - Чернівці : Чернів. нац. ун-т ім Ю. Федьковича, 2005 - .
Т. 41. - Чернівці, 2020. - 284 с. : граф., табл. - Бібліогр. в кінці ст. - Дод. тит. арк. англ. Текст кн. укр., англ.

Зі змісту:

Макух-Федоркова І. **Сучасні інформаційні виклики та формування кібернетичної стратегії Канади.** – С. 29-45.

У статті досліджується питання кібербезпеки Канади, ***характеризується комплекс заходів нормативно-правового,*** військово-політичного характеру щодо формування канадської стратегії інформаційної політики та механізмів захисту системи національної безпеки країни.

727479 В
339

Львівський торговельно-економічний університет.

Вісник Львівського торговельно-економічного університету [Текст] : зб. наук. праць / [редкол.: Куцик П. О., Семак Б. Б., Перепьолкіна та ін.]. - Львів : Вид-во Львів. торг.-екон. ун-ту. - (Економічні науки).

Вип. 59. - Львів, 2020. - 150 с. : граф., табл. - Бібліогр. наприкінці ст. - Текст укр., англ.

Зі змісту:

Боднар І. Р. **Заходи держави в сфері інформаційної безпеки.** – С. 37-41.

Визначено роль держави у формуванні інформаційного суспільства та забезпеченні інформаційної безпеки. Інформаційна безпека розглянута з позиції однієї з суттєвих складових частин національної безпеки країни. Визначені основні напрями діяльності держави в сфері інформаційної безпеки. Запропоновані концептуальні підходи гарантування інформаційної безпеки.

Марущак А. І. Стан розвитку національної системи кібербезпеки (на прикладі СБ України та Держспецзв'язку України) / А. І. Марущак, С. Г. Петров // Інформація і право. – 2020. – № 2(33). – С. 77-84.

Р/844

У статті здійснено аналіз сучасного стану розвитку національної системи кібербезпеки (на прикладі СБ України та Держспецзв'язку України). Сформульовано висновок про необхідність врегулювання окремих відносин, пов'язаних з розвитком національної системи кібербезпеки, з урахуванням міжнародної практики.

Мейш А. В. Методологія інформаційного захисту / А. В. Мейш, О. В. Матвійчук // Вісник Хмельницького національного університету. Серія: Економічні науки. – 2020. – № 4, Т. 1. – С. 130-134.

Р/1055«Е»

У статті проаналізовано та визначено основні загрози інформаційно-комунікативній системі підприємства та їх вплив на діяльність підприємства. Наведено чіткі заходи задля уникнення рейдерства та витоку інформації. Проаналізовані терміни: рейдерство, шахрайство, надана їх характеристика та варіанти зменшення їх на підприємстві.

Петров С. Г. Захист державних електронних інформаційних ресурсів України / С. Г. Петров // Інформація і право. – 2020. – № 3(34). – С. 62-68.

Р/844

У статті здійснено аналіз напрямів удосконалення чинного законодавства України з метою захисту державних електронних інформаційних ресурсів.

Петров С. Г. Організаційні і правові основи вирішення проблем протидії кіберпосяганням в Європейському Союзі / С. Г. Петров // Інформація і право. – 2020. – № 1(32). – С. 99-105.

Р/844

У статті здійснено аналіз організаційних та правових підходів ЄС та окремих держав-членів щодо протидії кіберпосяганням. Запропоновано врахувати в Україні досвід Польщі щодо функціонування установи, яка поєднує наукові дослідження, освітні програми і практичну реалізацію заходів протидії кіберпосяганням, Австрії – щодо існування національного CERTу Австрії для приватного сектору.

Солодка О. М. Забезпечення інформаційного суверенітету держави: правовий дискурс / О. М. Солодка // Інформація і право. – 2020. – № 1(32). – С. 80-87.

Р/844

У статті досліджено поняття "інформаційний суверенітет", його складові та сучасні підходи до розуміння та забезпечення з проекцією на інформаційний простір України.

Стефурак О. Р. Удосконалення стохастичної моделі з метою визначення загроз пошкодження або несанкціонованого витоку інформації / О. Р. Стефурак, Ю. О. Тихонов, О. А. Лаптєв, С. А. Зозуля // Сучасний захист інформації. – 2020. – № 2(42). – С. 19-26.

Р/2300

Ключову роль при побудові систем безпеки інформаційних ресурсів, як складових національних інформаційних ресурсів держави, відіграє теорія та практика, в якій науково-методологічна база є основою для прийняття обґрунтованих та ефективних управлінських рішень суб'єктами забезпечення інформаційної безпеки держави на усіх рівнях.

У статті на основі аналітичного аналізу загроз пошкодження або несанкціонованого витоку інформації на об'єктах інформаційної діяльності визначаються критичні складові безпеки інформаційного простору.

726619 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 (69). - Київ, 2020. - 154 с. : граф., рис., табл. - Бібліогр. наприкінці ст. Текст кн. укр., англ., рос.

Зі змісту:

Алексєєв М. М. **Методика кількісного оцінювання інформаційних ризиків із застосуванням онтології факторного аналізу.** – С. 72-78.

У статті розглянуто методику кількісного оцінювання інформаційних ризиків. У системі забезпечення кібернетичної безпеки ризик, головним чином, асоціюється з «втратою даних».

Запропоновано модель ризику під час використання онтології факторного аналізу інформаційних ризиків. У процесі побудови моделі ризику використано такі складові, як частота події, що викликає втрати, та магнітуда втрати.

Горбенко О. В., Горбенко Ю. Л., Горбенко А. Ю., Сівоха О. М. **Захист інформаційних систем за допомогою використання методів автентифікації.** – С. 79-85.

Мета статті – аналіз існуючих методів автентифікації користувачів інформаційних систем та визначення перспективного напряму розвитку методів автентифікації, використовуючи тест Люшера.

Шопіна І. М. Стратегічні комунікації як правова категорія: поняття та розвиток / І. М. Шопіна // Наука і правоохорона. – 2020. – № 2(48). – С. 158-165.

Р/2256

Стаття присвячена визначенню сутності стратегічних комунікацій у правовому аспекті. Обґрунтовано, що завдання правової науки мають включати формулювання визначення поняття "стратегічні комунікації" в аспекті інформаційної діяльності суб'єктів публічного адміністрування і підготовку пропозицій щодо відповідних змін та правових актів, в яких закріплено їх правовий статус.

728045 R
327

Яковенко, Наталя Леонідівна.
Міжнародні організації у сфері безпеки . НАТО, ОБСЄ [Текст] : навч. посібник / Н. Л. Яковенко ; Київський національний університет імені Тараса Шевченка. - [Київ] : ВПЦ Київський ун-т, 2020. - 367 с. - Бібліогр. в кінці розд. та у виносках.

Висвітлено основні проблеми сучасного розвитку євроатлантичних відносин, досліджено роль і внесок НАТО й ОБСЄ у створення надійних механізмів гарантування європейської та євроатлантичної безпеки та співпрацю України із цими ключовими організаціями. Доведено, що НАТО й ОБСЄ відіграють важливу роль в успішному протистоянні України агресивній політиці Росії. Наголошено, що активна взаємодія України з Північноатлантичним альянсом та її участь у діяльності ОБСЄ позиціонує нашу державу як вагомого гравця на міжнародній арені у сфері безпеки.

Зі змісту:

Розділ 1.9. **Кіберзахист НАТО.** – С. 105-115.

Програмні системи захисту інформації

Бобровнікова К. Ю. Метод виявлення шкідливого програмного забезпечення шляхом аналізу мережного трафіку та поведінки програмного забезпечення в комп'ютерних системах / К. Ю. Бобровнікова, Д. О. Денисюк // Вісник Хмельницького національного університету. Серія: Технічні науки. – 2020. – № 4, Т. 1. – С. 7-11.

Р/1055«Т»

Метод ґрунтується на класифікації множин API-викликів, вилучених з побудованих графів потоків керування для програмних додатків, та використовує аналіз DNS-трафіку комп'ютерної мережі. В якості класифікатора застосована комбінація глибокої нейронної та рекурентної нейронної мереж.

Використання програмного забезпечення IBM i2 Analyst's Notebook під час підготовки фахівців з розвідувально-інформаційної роботи / Д. Ю. Шаршаткін, Г. Д. Братченко, В. В. Маміч, О. П. Розмазнін // Збірник наукових праць Військової академії (м. Одеса). Серія: Технічні науки. – 2020. – Вип. 1(13), Ч. ІІ. – С. 167-172.

Р/431

У статті розглядаються проблеми щодо здійснення інформаційно-аналітичної діяльності під час роботи з великими інформаційними масивами. Розглянуте сучасне бачення та інноваційні підходи під час підготовки фахівців з розвідувально-інформаційної роботи у навчальних закладах Збройних Сил України. Здійснено огляд основних можливостей програмного продукту – спеціалізованої аналітичної системи "IBM i2 Analyst's Notebook". Розглянуті конкретні приклади застосування системи візуалізації "IBM i2 Analyst's Notebook".

Горюк Н. В. Засоби інтеграції технології статичного аналізу безпеки вихідного коду у середовище розробки програмного забезпечення / Н. В. Горюк // Сучасний захист інформації. – 2020. – № 3(43). – С. 54-58.

Р/2300

У статті досліджуються методи автоматизації та засоби інтеграції технології статичного аналізу безпеки вихідного коду. Досліджено процес аналізу безпеки програмного забезпечення, який реалізується технологією статичного аналізу безпеки вихідного коду, та запропоновані методи вирішення проблеми автоматизації та інтеграції технології у середовище розробки вихідного коду. Встановлено перспективний напрямок подальшого розвитку технології статичного аналізу вихідного коду.

728438 В
37

"Києво-Могилянська академія", національний університет.
Наукові записки НаУКМА [Текст] : [зб. наук. ст.]. - К. : [НУ НаУКМА]. - (Комп'ютерні науки).
Т. 3. - Київ, 2020. - 162 с. : рис., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., англ.

Зі змісту:

Торба Т. В., Вовк Н. Є. **Віртуальна кімната даних як сховище конфіденційних корпоративних документів.** – С. 56-61.
У роботі розглянуто основні характеристики віртуальних кімнат даних, проведено аналіз конкурентів для визначення ключових недоліків і переваг наявних продуктів. "*Постановка завдання.* Дослідити та використати найбільш доречний архітектурний стиль для проектування програмного забезпечення для віртуальної кімнати даних".

728930 В
004

Компьютерное моделирование в наукоемких технологиях [Текст] : сб. науч. трудов междунар. научно-технической конф., Харьков, 22-24 апреля 2020 г. / Харьковский нац. ун-т им. В. Н. Каразина, Ф-т компьютерных наук. - Харьков : [ХНУ им. В. Н. Каразина], 2020. - 312 с. : рис., табл., ил., граф. - Загол. обкл.
: Комп'ютерне моделювання в наукоємних технологіях. - Обкл. укр. Текст кн. укр. рос., англ. мов.

Доповіді, що увійшли до збірника, висвітлюють такі напрямки: математичне моделювання фізичних процесів, моделювання інформаційних процесів в складних та розподілених системах, системи автоматизованого збору та когнітивного подання наукових даних, аналіз процесів в радіаційних, плазмових та інших сучасних технологіях, моделювання транспортних процесів і систем, ***безпека інформаційних систем і технологій, верифікація та оцінка надійності програмного забезпечення.***

Лисенко С. М. Метод ідентифікації шпигунського програмного забезпечення в комп'ютерних системах / С. М. Лисенко, В. Ю. Омельяненко, Р. В. Щука // Вісник Хмельницького національного університету. Серія: Технічні науки. – 2020. – № 3. – С. 43-49.

Р/1055«Т»

У роботі представлено подальший розвиток методу ідентифікації шпигунського програмного забезпечення в комп'ютерних системах, який дозволяє виявляти усі типи, і відрізняється від відомих тим, що забезпечує принцип проактивності та базується на механізмах машинного навчання з підкріпленням.

728162 В
004

Мартін, Роберт Сесіл.
Чистий код: створення і рефакторинг за допомогою Agile [Текст] : [науково-популярне вид.] / Роберт С. Мартін ; [перекл. з англ. Ігоря Бондаря-Терещенка]. - [Харків] : Вид-во "Ранок", Фабула, 2021. - 448 с. : іл. - Бібліогр. в кінці розд. - Алф.-Предм. покажч.: с. 441-446. - Текст кн. укр. та англ.

Роберт Мартін, також відомий як дядечко Боб, – знакова постать у світі розробки ПЗ, блискучий професіонал, міжнародний консультант, один із тих, хто створив у 2001 році всесвітньо відомий Agile-маніфест. "Чистий код" – мабуть, найвідоміша й найпопулярніша книжка цього автора.
Навіть поганий програмний код може працювати. Однак якщо він не є "чистим", це заважатиме розвитку проєкту, відтягуючи значні ресурси на його підтримку та "приборкання". Книжка Р. Мартіна присвячена саме гарному програмуванню і насичена реальними прикладами коду. Із нею ви навчитеся відрізняти

хороший код від поганого, дізнаєтеся, як писати гарний код і як перетворити поганий код на по-справжньому чистий. Автор наводить принципи, патерни і прийоми написання чистого коду, практичні сценарії зростаючої складності, перелік евристичних правил і "запахів коду". Загалом це першокласна база знань і прикладів, що описують хід нашої думки в процесі читання, написання та чищення коду.

Стецюк М. В. Архітектура спеціалізованих інформаційних систем з врахуванням вимог живучості та відмовостійкості в умовах впливів зловмисного програмного забезпечення / М. В. Стецюк, А. С. Каштальян, В. І. Грибинчук // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2020. – № 2(66). – С. 69-77.

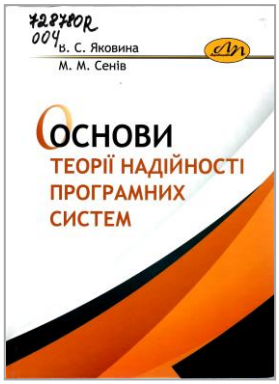
Р/1051

У результаті використання розроблених заходів було отримано архітектуру ІС вузькоспеціалізованого використання для різних сфер застосування, де супроводжуванні процеси відносяться до ірреального або нереального часу із досить високими параметрами відмовостійкості, живучості та загалом резилентності.

Стецюк М. В. Модель забезпечення живучості та відмовостійкості спеціалізованих інформаційних технологій в умовах руйнуючого впливу зловмисного програмного забезпечення / М. В. Стецюк, А. В. Горошко, Б. О. Савенко // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2020. – № 1(65). – С. 97-103.

Р/1051

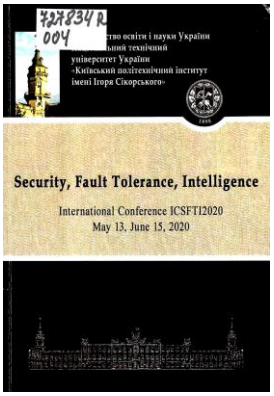
Для забезпечення відмовостійкості та живучості ІТ розроблено систему заходів, в результаті виконання яких отримано ІТ вузькоспеціалізованого використання для різних сфер застосування, де супроводжуванні процеси відносяться до ірреального часу із досить високими параметрами відмовостійкості, живучості та загалом резилентності і, в той же час, прийнятним рівнем фінансових витрат та її експлуатацією в умовах руйнуючого впливу зловмисного програмного забезпечення.



728780 R
004

Яковина, Віталій Степанович.
Основи теорії надійності програмних систем [Текст] : навч. посібник / В. С. Яковина, М. М. Сенів ; Національний університет "Львівська політехніка". - Львів : Вид-во Львів. політехніки, 2020. - 248 с. : граф., рис., табл. - Бібліогр.: с. 239-244.

Висвітлено основні поняття і визначення теорії надійності, загальну характеристику надійності ПЗ, критерії надійності невідновлюваних та відновлюваних систем, найпоширеніші в теорії надійності закони розподілу часу до відмови. Наведено методи розрахунку надійності технічних систем, розкрито характеристики надійності програмних і апаратних засобів та наведено класифікацію моделей надійності ПЗ. Ґрунтовно висвітлено моделі надійності ПЗ на основі неоднорідного пуассонового процесу, на основі недосконалого відлагодження та компонентних. Описано засоби інженерії програмних систем з урахуванням вимог до надійності ПЗ.



727834 R
004

Security, Fault Tolerance, Intelligence [Text] : International Conference ICSFTI2020, Kyiv, Ukraine, May 13, June 15, 2020 / National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Faculty of Informatics and Computer Science, Department of Computer Engineering . - Kyiv : Igor Sikorsky Kyiv Polytechnic Institute, 2020. - 300 p. : il. - Бібліогр. в кінці ст. - Текст кн. англ.

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

Телекомунікаційні мережі та інформаційно-комунікаційні технології

Виявлення атак в корпоративній мережі за допомогою правил нечіткої логіки / С. В. Толюпа, Р. С. Одарченко, І. І. Пархоменко, С. Ю. Даков // Наукоємні технології. – 2020. – № 4(48). – С. 470-477.

Р/2289

Розглянуто задачу виявлення можливих атак на ресурси корпоративної мережі. Виконано аналіз підходів до виявлення порушень інформаційної безпеки з використанням теорії нечітких множин.

Виявлення атак на комп'ютерну мережу на основі використання комплексу нейронних мереж / І. В. Жуковицький, В. М. Пахомова, Д. О. Остапець, О. І. Циганок // Наука та прогрес транспорту. – 2020. – № 5(89). – С. 68-79. – Текст англ.

Р/1815

Мета. За основну мету дослідження ми ставимо розвиток методики визначення атак на комп'ютерну мережу. Досягнення поставленої мети передбачає вирішення таких завдань: розробити методику виявлення атак на комп'ютерну мережу на основі ансамблю нейронних мереж із використанням нормалізованих даних відкритої бази KDDCup99; під час виконання машинного навчання виявити оптимальні параметри нейронної мережі, що забезпечить достатньо високий рівень достовірності виявлення вторгнень у комп'ютерну мережу.

Галата Л. П. Дослідження системи захисту інформації корпоративної мережі на основі GNS3 / Л. П. Галата, Б. Я. Корнієнко // Наукоємні технології. – 2020. – № 2(46). – С. 172-179.

Р/2289

Розроблена імітаційна модель системи захисту корпоративної мережі на базі GNS3 із використанням цифрового підпису мінімального розміру із забезпеченням заданого рівня стійкості. Проаналізовано статистичні дані щодо реакції системи захисту інформації. Зроблено висновки щодо ефективності розробленої системи захисту інформації в корпоративній мережі.

Гвоздьов Р. Ю. Метод і методика формального проектування комплексної системи захисту інформації в інформаційно-телекомунікаційних системах / Р. Ю. Гвоздьов, Р. В. Олійников // Радіотехніка. – 2020. – Вип. 203. – С. 91-96.

Р/908

На даний момент не існує методик для формального проектування комплексної системи захисту інформації в інформаційно-телекомунікаційних системах, тому розробка такої методики є актуальною задачею. В статті розглядаються методи формалізованого моделювання політики безпеки інформації та методи формалізованого опису інформаційно-телекомунікаційної системи та процесів обробки інформації.

728184 В
004

Глибовець, А. М.
Агентно-базовані програмні системи пошуку та аналізу інформації [Текст] : [монографія] / Глибовець А. М. ; Національний університет "Києво-Могилянська академія". - Київ : Вид. дім "Києво-Могилянська акад.", 2019. - 284 с. : іл. - Бібліогр.: с. 262-274.

У монографії висвітлено дослідження розв'язку проблеми підвищення якості пошукових систем шляхом розробки комплексного підходу до пошуку, аналізу та

обробки інформації в мережі Інтернет, зокрема представленої української мовою в колекціях наукових матеріалів і судженнях (висловлюваннях) користувачів соціальних мереж (СМ), а також вибір моделей, архітектурних і технологічних рішень для реалізації ефективного програмного прототипу обробки великих обсягів інформації в реальному часі з акцентом на використання агентного підходу й удосконалення відповідного математичного забезпечення створенням багатофункціональної моделі інтелектуальної мультиагентної системи пошуку наукових матеріалів українською мовою із соціальним складником. Об'єктом дослідження є пошук та аналіз даних у Світовій павутині (WWW). Предметом дослідження є агентне моделювання, методи машинного навчання та статистичної обробки великих обсягів даних, методи онтологічного аналізу й моделі створення гнучких архітектур програмних систем, технології аналізу висловлювань користувачів соціальних мереж та програмний інструментарій обробки великих обсягів даних на базі агентного моделювання. Вибір методів дослідження зумовлений сучасним станом технологій інтелектуальної обробки текстової інформації великої розмірності. Ефективність запропонованих підходів продемонстровано на прикладах програмних систем.

Дубровін В. І. Виявлення DOS-атак в мережевому трафіку методом вейвлет-перетворення / В. І. Дубровін, Б. В. Петрок, Г. В. Неласа // Сучасний захист інформації. – 2020. – № 2(42). – С. 37-46.

Р/2300

Аналіз даних мережевого трафіку дуже важливий для виявлення DOS-атак і шкідливої аномалії. У цій статті пропонується аналіз атаки деавтентифікації та локалізація даних аномалії методом вейвлет-перетворення.

Єгоров С. Методи приховування особистості користувача в мережі Інтернет / С. Єгоров, Т. Шкварницька // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2019. – Вип. 1(37). – С. 71-77.

Р/2287

Під час використання мережі Інтернет ми обов'язково залишаємо деякі сліди. Не зважаючи на всі ці факти можна використовувати методи, які дозволяють максимально ускладнити великим корпораціям, або зловмисникам збір персональної інформації про себе і зробити цей процес нерентабельним. Для досягнення максимальної анонімності на деяких сервісах потрібно робити складні налаштування. Слід пам'ятами, що особу користувача можна розкрити навіть у випадку повної надійності сервісу анонімізації. Для цього можна використати загрози нульового дня, різноманітні віруси, відбитки браузера, аналіз поведінки користувача в Мережі.

Забезпечення безпеки зв'язку в безпроводових сенсорних мережах на основі багаторівневої архітектури захисту / Р. М. Боярчук, М. С. Пуха, А. П. Маковський [та ін.] // Сучасний захист інформації. – 2020. – № 3(43). – С. 39-43.

Р/2300

Ця стаття є дослідженням аспектів комунікаційної безпеки цих мереж. Наш підхід полягає у класифікації типів даних, що існують у сенсорних мережах, та виявленні можливих загроз безпеці зв'язку відповідно до цієї класифікації. Ми пропонуємо схему захисту зв'язку, де для кожного типу даних ми визначаємо відповідний механізм захисту.

Зубок В. Ю. Аналіз захищеності інтернет-вузлів від кібератак типу "перехоплення маршруту" / В. Ю. Зубок // Реєстрація, зберігання і обробка даних. – 2020. – Т. 22, № 3. – С. 58-67.

Р/1346

Кібератаки на глобальну маршрутизацію в глобальній комп'ютерній мережі Інтернет (перехоплення маршруту, витік маршруту) призводять до масштабних наслідків з порушенням цілісності, доступності та конфіденційності інформації під час міжмережевого обміну. Запропоновано новий, ризик-орієнтований підхід до підвищення захищеності інформації під час міжмережевого обміну, націлений на вдосконалення топології міжмережевих зв'язків.

726578 R
004

Інформаційні технології та системи [Текст] : монографія / [В. П. Бурдаєв, О. Г. Руденко, О. О. Безсонов та ін.] ; за заг. ред. Пономаренка В. С. ; Харк. нац. екон. ун-т імені Семена Кузнеця. - Харків : [ФОП Бровін О. В.], 2020. - 173 с. : граф., рис., табл. - Бібліогр. в кінці глав. - Авт. зазнач. на звороті тит. арк.

В монографії розглянуті сучасний стан та перспективи розвитку інформаційних технологій та систем різних видів і різного прикладного характеру.

Каштальян А. С. Моделі приманок в корпоративних комп'ютерних мережах з врахуванням типів зловмисних атак / А. С. Каштальян, Б. О. Савенко, Р. Е. Бельфер // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2020. – № 1(65). – С. 104-110.

Р/1051

Організація експериментальних досліджень представлена на основі побудови багаторівневої системи з приманками, яка динамічно змінюватиме свою конфігурацію та матиме систему прийняття рішень для оперативного реагування на події, що протікатимуть в мережі.

Представлено використання приманок як перспективний напрям у здійсненні захисту комп'ютерних мереж від зловмисних втручань, інформація про які обмежена або відсутня.

Каштальян А. С. Покращення безпеки та модель антивірусних інтелектуальних приманок у корпоративних комп'ютерних мережах / А. С. Каштальян, О. С. Савенко // Вісник Хмельницького національного університету. Серія: Технічні науки. – 2020. – № 4, Т. 1. – С. 33-38.

Р/1055«Т»

У статті запропоновано модель та концепцію побудови мережі інтелектуальних приманок, розгорнутої в комп'ютерній мережі. Запропонована мережа представляє собою багаторівневу систему, що включає множину інтелектуальних приманок.

Киричок Р. В. Метод контролю послідовності реалізації атакуючих дій під час активного аналізу захищеності корпоративних мереж / Р. В. Киричок, Г. В. Шуклін, З. М. Бржевська // Сучасний захист інформації. – 2020. – № 2(42). – С. 52-58.

Р/2300

У статті запропоновано підхід щодо підвищення ефективності валідації вразливостей під час автоматичного активного аналізу захищеності корпоративних мереж на основі контролю послідовності реалізації атакуючих дій (експлойтів) згідно стратегії вибору дій softmax з використанням ймовірнісного розподілу Гіббса.

Киричок Р. В. Методика аналізу якості роботи механізму валідації вразливостей корпоративних мереж / Р. В. Киричок, Г. В. Шуклін // Телекомунікаційні та інформаційні технології. – 2020. – № 2(67). – С. 29-39.

Р/1921

... було запропоновано методику аналізу якості роботи механізму валідації вразливостей корпоративних мереж, яка дозволяє кількісно оцінити якість роботи досліджуваного механізму валідації, що в свою чергу дозволить в режимі реального часу відслідковувати та контролювати хід валідації виявлених вразливостей. Також, в дослідженні було отримано залежності визначених ключових показників якості роботи механізму валідації вразливостей від часу раціонального циклу, що надає змогу будувати функції належностей для нечітких множин.

726785 R
004

Лисецкий, Юрий Михайлович.
Инновационные информационные технологии. Опыт интеграции и внедрения [Текст] : монография / Ю. М. Лисецкий ; НАН Украины, Ин-т проблем математических машин и систем. - Киев : Изд-во ЛАТ&К, 2020. - 276 с. : карты, рис. - Библиогр.: с. 262-275.

Монография посвящена инновационным информационным технологиям в области хранения и управления данными, сетей, конвергентных и гиперконвергентных инфраструктур, виртуализации, облачных коммуникационных платформ, Интернета вещей, информационной безопасности, систем поддержки операционных процессов и мониторинга. Разработаны инструментальные средства обеспечения информационной безопасности Security Operation System и Центр оперативного реагирования для организации эффективной защиты информационно-технологической инфраструктуры предприятий и организаций от кибератак и киберугроз, за счет получения информации о событиях и инцидентах безопасности из различных источников и их корреляционного анализа. Также предложен инструментарий автоматизации работы с инцидентами, позволяющий ускорить проведение базовой диагностики и поиска корневой аварии в системе мониторинга.

Значительное внимание уделено практическим аспектам интеграции и внедрения инновационных информационных технологий для различных отраслей экономики: металлургии, топливно-энергетического комплекса, финансового сектора и отрасли связи.

Литвин П. В. Безопасность 5G / П. В. Литвин // Бизнес и безопасность. – 2020. – № 6(140). – С. 28-30.

Р/1070

Одна из самых популярных тем в последнее время: безопасен ли 5G для здоровья людей. Однако, в этой статье речь пойдет совсем не об этом, а об архитектуре безопасности этой сети. Насколько надежные технологии скрываются внутри?

Маслов О. Г. Методика підвищення захищеності Інтернет речей на базі технологій блокчейна / О. Г. Маслов, О. В. Кітура // Сучасний захист інформації. – 2020. – № 2(42). – С. 32-36.

Р/2300

Показані шляхи несанкціонованого отримання інформації у інформаційно-телекомунікаційних системах. Показані три етапи процесу запобігання та зниження ризиків небезпек в інформаційно-телекомунікаційних системах. Розглянуто загрози інформаційній безпеці у інформаційно-телекомунікаційних системах, та їх класифікація. Приведені методи та технології протидії загрозам інформації в інформаційно-телекомунікаційних системах.

Метод виявлення DDoS атак на IoT мережі / А. О. Нічепорук, А. А. Нічепорук, О. В. Фегир [та ін.] // Вісник Хмельницького національного університету. Серія: Технічні науки. – 2020. – № 1. – С. 184-191.

Р/1055«Т»

В роботі представлено метод виявлення DDoS атак на IoT-мережі, що заснований на використанні логістичної регресії. Запропонований метод складається з двох етапів: offline та online. Головною метою offline етапу є створення моделі класифікатора, яка буде в подальшому використана в процесі виконання online етапу. Шляхом моніторингу мережевого трафіку в режимі реального часу етап online здійснює виявлення DDoS атак на основі використання сформованої на етапі offline моделі класифікатора. Висновок про наявність DDoS атаки здійснюється на основі порівняння середнього значення серед всіх проміжних результатів класифікації з пороговим значенням виявлення. У випадку перевищення порогового значення робиться висновок про наявність DDoS атаки.

Мішак Р. Розробка засобу стеганографічного захисту інформації / Р. Мішак, Я. Ковівчак // Технічні вісті. – 2020. – № 1(51), 2(52). – С. 41-42.

Р/728

У даній роботі для приховування інформації використано методи стеганографії. Зі швидким розвитком інформаційно-комунікаційних технологій найбільш активно розвиваються комп'ютерні методи стеганографії та можливості їх застосування в кіберпросторі.

Розглянемо існуючі системи стеганографічного захисту, а саме: Steganos Privacy Suite 11, S-Tools, ImageSpyer 2009, JSTEG, Gifshuffle.

Питання побудови перспективної захищеної інформаційної інфраструктури науково-дослідної установи на основі впровадження хмарних технологій / Р. В. Лукаш, І. В. Симоненкова, В. М. Симоненков, О. П. Григор'єв // Збірник наукових праць Військової академії (м. Одеса). Серія: Технічні науки. – 2020. – Вип. 1(13), Ч. ІІ. – С. 122-133.

Р/431

На основі аналізу сучасного досвіду застосування технологій доставки додатків до кінцевого користувача запропоновано шляхи побудови перспективної захищеної інформаційної інфраструктури науково-дослідної установи з використанням технологій і хмарних рішень.

Праворська Н. І. Забезпечення безпечного обміну інформації в мережі елементів Інтернету речей / Н. І. Праворська // Вісник Хмельницького національного університету. Серія: Технічні науки. – 2020. – № 1. – С. 219-224.

Р/1055«Т»

Пристрої Інтернету речей дозволяють передавати інформацію від малих до великих обсягів даних. Однією з типових проблем речей Інтернету є необхідність захисту інформації від втручання в канал зв'язку. Зростання обчислювальної потужності обмежується доступним енергоспоживанням. Тому важливим є забезпечення надійної аутентифікації та захисту даних із застосуванням простих та ефективних алгоритмів.

727861 В
629.7

Проблеми інформатизації та управління [Текст] : зб. наук. пр. / Нац. авіац. ун-т, Ф-т кібернетики, комп'ютерної та програмної інженерії. - Київ : [НАУ].
Вип. 3 (63). - Київ, 2020. - 98 с. : іл., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., рос., англ.

Зі змісту:

Зубок В. Ю. **Поводження з ризиками від перехоплення маршруту в мережі інтернет з використанням ризик-орієнтованої моделі глобальної маршрутизації.** – С. 34-41.
"*Метою роботи* є розробка методології поводження з ризиками на основі оцінки ефективності міжмережевих зв'язків та удосконалення топології мережі".

727393 R
004

Русин, Володимир Богданович.
Безпека інформаційно-комунікаційних мереж [Текст] : навч. посібник / уклад. : В. Б. Русин, Л. Ф. Політанський ; Чернівецький національний університет імені Юрія Федьковича. - Чернівці : Чернів. нац. ун-т ім Ю. Федьковича, 2020. - 136 с. : рис., табл., фот. - Бібліогр. в кінці розд. - Уклад. на обкл. не зазнач.

У посібнику наведені основні терміни і визначення стосовно інформаційної безпеки та правові аспекти захисту інформації. Розглянуті основні вузли персонального комп'ютера, вірусні та антивірусні програми, принципи побудови мереж електронних обчислювальних машин та технічні засоби забезпечення захисту.

Савченко В. А. Оцінювання параметрів безпеки персональних даних у степеневих соціальних мережах на основі їх топології / В. А. Савченко, В. М. Ахрамович, М. В. Акулінічева // Сучасний захист інформації. – 2020. – № 3(43). – С. 6-13.

Р/2300

У статті досліджується модель степеневої соціальної мережі, яка, на відміну від класичних підходів, дозволяє аналізувати динамічні процеси взаємодії окремих агентів всередині мережі, зокрема щодо поширення інформації соціального впливу.

726621 В
62

Технічна інженерія [Текст] : науковий журнал / Державний університет "Житомирська політехніка". - Житомир : [Держ. ун-т "Житомирська політехніка"], 2020 - .
1(85). - Житомир, 2020. - 295 с. : іл., граф., рис., табл. - Бібліогр. в кінці ст. - Текст кн. укр., рос., англ. мов.

Зі змісту:

Бойченко О. С., Гуменюк І. В., Сметанін К. В., Некрилов О. В. **Метод блокування доступу до інформаційно-телекомунікаційних систем на основі біометричної ідентифікації/аутентифікації користувачів.** – С. 171-176.
Мета статті полягає в удосконаленні методу біометричної ідентифікації/аутентифікації та його застосування при вирішенні завдань блокування доступу до ІТС користувачами.

Черненко П. Р. Вразливості системи безпеки в додатках ОС ANDROID / П. Р. Черненко, М. М. Орлова // Вісник Вінницького політехнічного інституту. – 2020. – № 3(150). – С. 43-50.

Р/0126

Більшість мобільних додатків для ОС Android ініціюють з'єднання з мережею, іншими додатками або сторонніми сервісами, що робить необачного користувача більш вразливим до атаки зловмисників.
В роботі продемонстровано деякі стандартні засоби для проведення статичного аналізу додатків для ОС Android без запуску на пристрої користувача. Позаяк соціальні мережі в наш час є найзначущим медіа-місцем у світі і найпоширенішим каналом для передачі даних, відео та аудіо, за допомогою вищезгаданих методів статичного аналізу, перевірено вісім додатків популярних соціальних мереж, якими на сьогоднішній день користуються мільйони користувачів, та продемонстровано типи вразливостей, які виявлено в цих додатках. Також в роботі проаналізовано загрози з найбільшим потенційним впливом на бізнес-середовище та сформульовано рекомендації щодо зменшення ризиків їх виникнення.

Інформаційне протиборство у воєнних конфліктах. Інформаційно-психологічна безпека

Батиргареєва В. С. Основні напрями протидії поширенню дезінформації (на прикладі пандемії COVID-19) / В. С. Батиргареєва // Інформація і право. – 2020. – № 2(33). – С. 121-131.

Р/844

У статті на прикладі гуманітарної кризи світового масштабу, пов'язаної із пандемією COVID-19, представлені основні напрями протидії поширенню дезінформації, яка нерідко створює загрозу національній безпеці держав. До таких напрямів віднесено організаційно-інституційний, правовий та просвітницько-виховний.

Грицюк В. В. Алгоритм процесу автоматизованої класифікації подій в інформаційному просторі / В. В. Грицюк // Штучний інтелект. – 2020. – № 2(88). – С. 42-52.

Р/1075

"*Метою дослідження* є розробка алгоритму процесу автоматизованої класифікації подій в інформаційному просторі для виконання функції розподілу інформаційних подій (повідомлень) різної природи на категорії (класи). Цей алгоритм автоматизації слугуватиме підвищенню оперативності загального процесу протидії негативному інформаційному впливу".

До питання типових сценаріїв проведення інформаційних операцій / С. В. Абрамов, О. І. Кондратенко, В. А. Полюга [та ін.] // Збірник наукових праць Військової академії (м. Одеса). Серія: Технічні науки. – 2020. – Вип. 1(13), Ч. ІІ. – С. 44-51.

Р/431

Використання різних засобів і технологій інформаційно-комунікаційного впливу, застосування інформаційних технологій у сфері комунікацій, які надають можливість охоплювати чисельну аудиторію стало досить звичайним явищем в повсякденному житті. Об'єктом цих впливів є перш за все колективна людська свідомість. Вплив інформаційних факторів, які, трансформуючись через поведінку людини, її дію (або бездіяльність), змінюють сприйняття соціальних суб'єктів різного рівня спільності, різної системно-структурної і функціональної організації, що в силу різних причин сприяє неадекватному відображенню навколишнього світу.

Копан О. В. Інформаційно-психологічна війна як засіб маніпулювання людською свідомістю / О. В. Копан, В. І. Мельник // Бизнес и безопасность. – 2021. – № 1(141). – С. 2-4.

Р/1070

"На жаль, в Україні має місце інформаційне протистояння, яке чинить деструктивний дестабілізуючий вплив на національну безпеку і вже переросло в інформаційну війну".

Підхід до моделювання поведінкових проявів у соціальному інжинірингу в інтересах захисту інформації / Н. М. Баландіна, М. Д. Василенко, В. М. Слатвінська, С. В. Сисоєнко // Вісник Черкаського державного технологічного університету. Серія: Технічні науки. – 2020. – № 4. – С. 57-66.

Р/1308

Розглянуто проблеми побудови кількісної теорії людських систем. Доведено потребу в новому методологічному підході до побудови моделі поведінки людини в цифровій сфері, спрямованої на захист інформації в соціальному інжинірингу. Запропоновано синергійно-криптографічний підхід до побудови моделі поведінкових проявів в умовах соціального інжинірингу та в інтересах захисту інформації.

727164 В
681

Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем [Текст] : зб. наук. пр. / Міноборони, Житомирський військовий інститут імені С. П. Корольова . - Житомир : [ЖВІ]. -
Вип. 17. - Житомир, 2019. - 188 с. : іл., граф., табл. - Бібліогр. наприкінці ст. - Текст укр., англ.

Зі змісту:

Манько О. В., Наумчак О. М. **Підхід до організації захисту військовослужбовців від негативного інформаційного впливу.** – С. 110-120.
У роботі проаналізовано досвід, отриманий у ході моніторингу інформаційного простору, та описано основні способи створення й розповсюдження матеріалів із негативним інформаційним впливом на особовий склад Збройних Сил. Наведено рекомендації для забезпечення захисту військовослужбовців від деструктивного впливу та сформовано загальний підхід до його організації.

Прокофьєв М. Інформаційна війна як форма ведення інформаційного протиборства. Частина 1 / М. Прокофьєв, Л. Скачек, В. Хорошко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2018. – Вип. 2(36). – С. 15-26.

Р/2287

Розглядається пряма та зворотна оптимізація розподілу інформаційного простору між країнами та державами. Викладено концепцію стратегії інформаційної війни першого та другого поколінь і доведено, що настає новий етап – перехід від стратегії ядерного стримування до високоточної контрсилової інформаційної зброї, головне завдання якої полягає в маніпулюванні масами.

Прокофьєв М. Інформаційна війна як форма ведення інформаційного протиборства. Частина 2 / М. Прокофьєв, Л. Скачек, В. Хорошко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2019. – Вип. 1(37). – С. 7-23.

Р/2287

Запропоновано модель інформаційної війни та розглянуто методи психологічного впливу на свідомість людей та суспільства в цілому. Розроблено концепцію інформаційно-психологічного протиборства у суспільстві, значну увагу приділено процесам маніпулювання інформацією у суспільстві.

На прикладі агресії Росії відносно України досліджено особливості трирівневої концепції мережі, яка поєднує усі допустимі види інформаційного впливу на противника та являє собою комплексну стратегію інформаційно-психологічного протиборства.

Улічев О. Моделювання процесів поширення та нейтралізації інформаційних впливів у сегменті соціальної мережі / О. Улічев, Є. Мелешко // Захист інформації. – 2020. – Т. 22, № 3. – С. 166-176.

Р/1428

У даній роботі проведено дослідження існуючих методів генерації структури соціальних мереж, запропоновано метод генерації сегменту соціальної мережі з можливістю вибору різної кількості та типів кластерів, а також здійснено моделювання процесів поширення та нейтралізації інформаційних впливів в сегменті соціальної мережі з наперед заданими особливостями топології мережі.

728413 В
62

Центральноукраїнський науковий вісник. Технічні науки [Текст] = Central ukrainian scientific bulletin. Technical sciences : зб. наук. праць / Центральноукраїнський нац. технічний ун-т ; за заг. ред. М. І. Черновола. - Кропивницький : [ЦНТУ], 2019 - .

Вип. 3(34). - Кропивницький, 2020. - 391 с. : граф., рис., табл. - Бібліогр. в кінці ст. - Текст кн. укр. та англ.

Зі змісту:

Марченко К. М., Оришака О. В., Марченко А. К. **Проблеми інформаційної безпеки людини в умовах епідемії.** – С. 22-31.

У статті розглянуті інформаційні причини захворювань, особливості впливу засобів масової інформації на свідомість людини під час епідемій. Розглянуто особливості інформаційних атак та зараження інформаційними вірусами. Дано рекомендації по індивідуальному захисту та підтриманню інформаційного здоров'я людини.

Штефанюк Є. Ф. Аналіз застосування існуючих технік розпізнавання фейкових новин для протидії інформаційній пропаганді / Є. Ф. Штефанюк, І. Р. Опірський, О. І. Гарасимчук // Безпека інформації. – 2020. – Т. 26, № 3. – С. 139-144.

Р/1075

В цій статті розглянуто особливості інформаційної пропаганди та підходів до боротьби з нею; ефективність роботи декількох відомих технік розпізнавання фейкових новин; проведено аналіз ефективності цих технік в контексті можливості їхнього застосування для протидії цілеспрямованим інформаційним впливам.

728188 В
34

Юридичні науки [Текст] : зб. наук. пр. Vol. 7 № 2 (26) / голова РВР Наталія Чухрай. - Львів : Вид-во Львів. політехніки, 2020. - 300 с. - (Вісник Національного університету "Львівська політехніка" : наук. журнал / Національний університет "Львівська політехніка"). - Бібліогр. наприкінці ст. - Текст кн. укр., рос. та англ.

Зі змісту:

Жаровська І., Ортинська Н. **Інформаційна війна як сучасне глобалізаційне явище.** – С. 56-61.

Вказано, що особливістю інформаційної війни є не тільки те, що вплив здійснюється з використанням новітніх засобів, а й те, що це непідконтрольний ресурс, який дуже слабо піддається правовій регламентації, тому активно застосовує неправдиву, перекручену інформацію як засіб маніпуляції свідомістю.

727496 В
31

Digital media: становлення новітньої комунікації [Текст] : колективна монографія / за ред. М. М. Поплавського, Л. О. Кочубей ; Київ. нац. ун-т культури і мистецтв. - Київ : Вид. центр КНУКІМ, 2020. - 244 с. : табл., фот. кол. - Бібліогр. у виносках.

Колективна монографія кафедри зв'язків із громадськістю і журналістики містить розділи, присвячені новітнім тенденціям сучасних комунікацій в інформаційному суспільстві; ***психологічним впливам у інформаційному просторі;*** новітнім трендам журналістики та мережевим особливостям digital media. ***Зокрема, у роботі висвітлюються питання, присвячені*** новітнім технологіям у виборчих кампаніях, електронній демократії, міжнародним стратегічним комунікаціям у діджитал-епоху, сучасним геобрендинговим комунікаціям, ***інформаційним війнам, інформаційному тероризму, психологічним трендам глобальної діджиталізації,*** новітнім трендам журналістики тощо.

Кібербезпека – проблема XXI століття

728411 В
35

Актуальні проблеми державного управління [Текст] = Pressing problems of public administration : зб. наук. пр. / Нац. акад. держ. упр. при Президентові України, Харківський регіон. ін-т держ. упр. - Харків : [Магістр], 2008 - .
Вип. 2 (58). - Харків, 2020. - 244 с. : граф., табл. - Бібліогр. наприкінці ст. - Текст кн. укр. та англ.

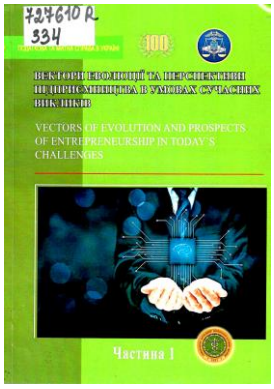
Зі змісту:

Довбиш А. С., Котух Є. В. **Сучасний стан та проблеми "цифровізації" в Україні.** – С. 25-31.
У статті досліджено особливості цифровізації в публічному управлінні, сформульовано основні напрями забезпечення кібербезпеки при цьому. Проаналізовано сучасний стан кібербезпеки, а також визначено шляхи підвищення її рівня в сфері публічного управління та в цілому в Україні.

728908 В
004

Бобало, Юрій Ярославович.
Стратегічна безпека системи "об'єкт-інформаційна технологія" [Текст] : монографія / Ю. Я. Бобало, В. Б. Дудикевич, Г. В. Микитин ; Національний університет "Львівська політехніка". - Львів : Вид-во Львівської політехніки, 2020. - 260 с. : рис., табл. - Бібліогр.: с. 247-258.

Висвітлено взаємозв'язок завдань програм інформатизації та інтелектуалізації для забезпечення стратегічної безпеки системи "об'єкт – інформаційна технологія" у контексті роботоздатності об'єктів та гарантоздатності інформаційних технологій.
Викладено парадигму побудови інформаційних технологій відбирання різнорідних даних та аналітичну платформу безпеки "об'єкт – інформаційна технологія" у контексті інфраструктури інформатизації.
Синтезовано квінтесенцію безпеки багаторівневих кіберфізичних систем "кібернетичний простір – комунікаційне середовище – фізичний простір".
Розглянуто парадигму, концепцію та універсальну платформу побудови комплексних систем безпеки у просторі "загрози – профілі – інструментарій", які цілісно спрямовані на забезпечення гарантоздатності кіберфізичних систем.



727610 R
334

Вектори еволюції та перспективи підприємництва в умовах сучасних викликів [Текст] = Vectors of evolution and prospects of entrepreneurship in today's challenges : зб. матеріалів IV Міжнар. наук.-практ. конф. "Економічні перспективи підприємництва" : у 2-х ч., 8-9 жовтня 2020 р. / орг. ком.: Пашко П. В. (голова), Шевчук С. В., Драган О. В. [та ін.] ; Мінфін України, Ун-т держ. фіскальної служби України, Спілка підприємців малих, середніх і приватиз. підприємств України, ДУ "Ін-т економіки та прогнозування НАН України [та ін.]. - Ірпінь : [Ун-т ДФС України].

Ч. 1. - Ірпінь, 2020. - 242 с. : граф., табл. - (Серія "Податкова та митна справа в Україні" ; т.160). - Бібліогр. в кінці ст. - Дод. тит. арк. англ. Текст кн. укр., рос., англ. мов.

У збірнику опубліковано матеріали IV Міжнародної науково-практичної конференції, присвячені питанням осмислення економічних проблем та перспектив розвитку підприємництва. Основними напрямами досліджень є: теорія підприємництва та вектори її еволюції в умовах сучасних викликів; держава і бізнес: цілі, моделі, засоби взаємодії; ***цифровізація і кіберзахист підприємницького простору;*** правове регулювання підприємництва; економічна безпека підприємницької діяльності: нові загрози; малий, середній і великий бізнес: інституційні особливості становлення та розбудови; маркетинг і логістика ефективного бізнесу; фінанси підприємництва та виклики його фінансовізації; Україна – територія можливостей для розвитку бізнесу: погляд молоді.

Веселова Л. Ю. Актуалізація інформаційної безпеки та глобальної кібернетичної загрози / Л. Ю. Веселова // Наука і правоохорона. – 2020. – № 1(47). – С. 347-355.

Р/2256

У статті досліджені актуальні питання кібернетичної безпеки як загрози у глобальному кіберпросторі. Проаналізовано інформацію щодо нових атак у кібернетичній сфері та визначено головні тенденції розвитку кібернетичних загроз.

Гапоненко О. І. Переваги та недоліки Honeypot – приманки для хакерів / О. І. Гапоненко, В. В. Марченко, Г. І. Гайдур // Сучасний захист інформації. – 2020. – № 2(42). – С. 59-63.

Р/2300

Розглянуто історію виникнення Honeypot та проаналізовано переваги і недоліки використання "Приманки для хакерів", як інструмент для статистичного моделювання, аналізу дій, виявлення нападів або дослідження поведінки зловмисників.

Гуцалюк М. В. Загрозливі тенденції організованої кіберзлочинності / М. В. Гуцалюк // Інформація і право. – 2020. – № 1(32). – С. 88-98.

Р/844

У статті досліджуються сучасні тенденції кіберзлочинності, у тому числі її організовані форми, надаються пропозиції щодо посилення протидії цьому явищу.

Даник Ю. Г. Від кібербезпеки до кібероборони / Ю. Г. Даник, С. Г. Вдовенко // Оборонний вісник. – 2020. – № 10. – С. 10-15.

Р/1134

Більшість країн світу, а також країни ЄС, НАТО та ОБСЄ зосереджують значні зусилля щодо забезпечення спроможностей зі своєчасного виявлення, запобігання, нейтралізації і ліквідації загроз в кіберпросторі, зокрема у сфері оборони.

Даник Ю. Г. Від кібербезпеки до кібероборони / Ю. Г. Даник, С. Г. Вдовенко // Оборонний вісник. – 2020. – № 11. – С. 10-15. *(Продовження. Початок у "ОВ" № 10 (2020 р.))*.

Р/1134

Сучасні високі технології змінюють процеси організації бойових дій та операцій і методи управління ними, і тому вимагають розробки та впровадження нових концепцій та стратегій оборони.

Даник Ю. Г. Від кібербезпеки до кібероборони / Ю. Г. Даник, С. Г. Вдовенко // Оборонний вісник. – 2020. – № 12. – С. 12-17. *(Закінчення. Початок у "ОВ" №№ 10, 11 (2020 р.))*.

Р/1134

В Україні вкрай необхідно створювати дієздатну систему кібероборони з урахуванням досвіду провідних країн світу, особливо держав-членів НАТО.

Живучість системи кібербезпеки держави / В. О. Хорошко, Ю. Є. Хохлачова, А. Аясрах, А. Аль-Далваш // Інформатика та математичні методи в моделюванні. – 2020. – Т. 10, № 1-2. – С. 84-89. – Текст рос.

Р/2357

Одним з найважливіших питань при проектуванні і експлуатації систем захисту інформації є питання забезпечення і оцінки її живучості. У роботі було проведено дослідження, які показали, що критерії ймовірності оцінки якості функціонування засобів захисту і оцінки надійності (живучості) системи захисту в цілому можна використовувати. До узагальненому процесу захисту застосовані критерії теорії надійності, що дозволяють в ході проектування і експлуатації системи захисту оперативно оцінювати її надійність (живучість, готовність).

Иванов М. Кибербезопасность бизнеса / М. Иванов // Бизнес и безопасность. – 2021. – № 1(141). – С. 12-17.

Р/1070

Разделы статьи:

- Киберпреступность 2020
- Основные правила защиты компании от киберугроз
- Как помочь компаниям лучше организовать реагирование на киберинциденты?

728002 R
004

Інформаційні технології і безпека. Матеріали XX Міжнародної науково-практичної конференції ІТБ-2020 [Текст] : збірник матеріалів доп., 10 грудня 2020 р., м. Київ, Україна / редкол.: О. Г. Додонов, В. В. Голенков, Д. В. Ланде [та ін.] ; НАН України, Інститут проблем реєстрації НАН України. - Київ : Інжиніринг, 2020 - .

Вип. 20. - Київ, 2020. - 174 с. : граф., рис., табл. - Бібліогр. в кінці ст. -Текст кн. укр. та англ. мов.

У збірнику представлені матеріали, присвячені питанням створення і впровадження інформаційних технологій, актуальним проблемам забезпечення інформаційної та кібербезпеки, протидії інформаційним операціям і кібертероризму, проведенню аналітичних досліджень на основі аналізу контенту мережі Інтернет.

Кібербезпека в проявах ризиків у період пандемії: стан та генеза / М. Д. Василенко, В. П. Новіков, В. О. Рачук, В. М. Слатвінська // Вісник Черкаського державного технологічного університету. – 2020. – № 3. – С. 30-39.

Р/1308

Зокрема, проаналізовано та надано оцінку проявам кіберризиків у контексті кібербезпеки як нової проблеми, пов'язаної з появою COVID-19, а також з'ясовано її стан та генезу.

Кількісно-якісна оцінка та визначення рівня кібербезпеки інформаційних систем держави / І. В. Пискун, Ю. М. Ткач, В. О. Хорошко [та ін.] // Безпека інформації. – 2020. – Т. 26, № 3. – С. 131-138.

Р/1075

В статті розроблено методику кількісно-якісного аналізу та визначення рівня кібербезпеки інформаційних систем держави. Отримані результати достатньо чітко визначають критерій кібербезпеки, який виходить із чисельних значень індексу кібербезпеки або кіберзагрози. Критерій оцінки рівня кіберзагрози має опиратися на характер кіберзагрози з обов'язковим урахуванням її масштабу.

Колісник Д. Р. Системна архітектура IoT-Fog-Cloud для систем аналізу великих даних і кібербезпеки: огляд туманних обчислень, впровадження аудиту інтернету речей / Д. Р. Колісник, К. С. Місевич, С. В. Коваленко // Сучасний захист інформації. – 2020. – № 3(43). – С. 34-38.

Р/2300

В статті розглянуто питання щодо системної архітектури IoT-Fog-Cloud, розглянуто взаємодію між трьома рівнями IoT, Fog і Cloud для ефективного впровадження програм для аналізу великих даних і кібербезпеки. В статті також розглядаються проблеми безпеки, рішення та направлення майбутніх досліджень в галузі Інтернету речей та туманних обчислень.

Кононович В. Г. Старіння інформації в моделях категоріювання та вплив на матриці цінності суб'єкта у системі кібербезпеки / В. Г. Кононович, О. В. Сєвєрінов, М. Г. Романюков // Прикладна радіоелектроніка = Applied Radio Electronics. – 2019. – Т. 18, [№ 3, 4]. – С. 182-189.

Р/1944

Досліджуються впливи процесів старіння інформації в моделях категоріювання матриць цінностей та маніпулювання інформаційним обміном у системі кіберпростору держави на індивідуальну та колективну свідомість суб'єктів. Отримано залежності між матрицями цінностей та цілей, розраховано очікувані ймовірності досягнення цілей від обраних цінностей для поставлених цілей.

Котух Є. В. Основні підходи до забезпечення кібербезпеки: досвід країн Вишеградської четвірки / Є. В. Котух // Інвестиції: практика та досвід. – 2021. – № 3. – С. 68-74.

Р/2124

У статті виокремлено базові стратегії у сфері кібербезпеки загалом, розглянуто конкретні стратегії країн Вишеградської четвірки (Польща, Словаччина, Угорщина, Чехія). Досліджено як співвідносяться державницька та економічна парадигма з реальним процесом реалізації стратегій кібербезпеки.

Метод виявлення кіберзагроз та ШПЗ для забезпечення живучості комп'ютерних систем в корпоративних мережах на основі самоадаптивності / С. М. Лисенко, Т. М. Кисіль, Ю. О. Нічепорук, А. В. Горошко // Вісник Хмельницького національного університету. Серія: Технічні науки. – 2020. – № 4, Т. 1. – С. 39-43.

Р/1055«Т»

У роботі представлено метод забезпечення живучості комп'ютерних систем в умовах кіберзагроз на основі самоадаптивності, який дозволяє здійснювати адаптивне реконфігурування компонентів КС шляхом сценаріїв безпеки та забезпечує здатність системи до стійкого її функціонування в ситуації наявності кібератак.

Мужанова Т. М. Геопросторовий підхід до забезпечення кібербезпеки / Т. М. Мужанова // Сучасний захист інформації. – 2020. – № 2(42). – С. 27-31.

Р/2300

У статті розглянуто роль та функції геоінформаційних технологій у забезпеченні кібербезпеки організації. Проаналізовано концепцію застосування ГІС у галузі кібербезпеки компанії-виробника ГІС-платформ ESRI, яка пропонує впроваджувати геопросторову модель захисту периметру з метою виявлення й оцінювання спроб компрометації ІТКС та формувати лінії кіберпідтримки для виконання критичних місій організації.

Особливості розповсюдження ризико-орієнтованого підходу до оцінки вразливості об'єктів кіберзахисту / І. Рубан, В. Тютюнник, В. Заболотний, О. Тютюнник // Безпека інформації. – 2020. – Т. 26, № 3. – С. 145-155.

Р/1075

Представлено результати розповсюдження ризико-орієнтованого підходу для оцінки ефективності функціонування системи інформаційної безпеки об'єкту кіберзахисту (ОКЗ) в умовах можливого розголошення та витоку інформації, її блокування та модифікації.

Певнєв В. Я. Кібербезпека безпроводових смарт-систем: канали втручань та радіочастотні вразливості / В. Я. Певнєв, В. В. Торяник, В. С. Харченко // Радіоелектронні і комп'ютерні системи. – 2020. – № 4(96). – С. 79-92.

Р/1769

Предметом даного дослідження є кіберуразливість радіочастотної технології інформаційно-управляючої взаємодії в безпроводових смарт-системах (БСС). БСС - це кіберфізичні системи, що функціонують у рамках моделі OSI. Специфіка і спеціалізація таких систем визначається радіотехнологіями фізичного рівня, наприклад, видами БСС є Інтернет Речей (IoT, зокрема, медичний IoMT, Інтернет Дронів (IoD), системи авіамоніторингу ADS-B і управління трафіком ATM, а в перспективі – системи Інтернету Всього (IoE).

728435 В
34

Повітряне і космічне право. Юридичний вісник [Текст] : наук. пр. Нац. авіац. ун-ту / Нац. авіац. ун-т. - Київ : [НАУ].
№ 4(57). - Київ, 2020. - 204 с. : табл. - Бібліогр. наприкінці ст. - Текст укр., англ.

Зі змісту:

Філінович В. В. **Кібербезпека та Інтернет речей: правовий аспект.** – С. 122-127.
Мета: дослідити особливості та сутність Інтернету речей та правові можливості захисту такої системи. *Методи дослідження:* дослідження було проведено із застосуванням загальновизначених методів наукового пізнання, таких як: аналітичний, порівняльно-правовий, системно-структурний та інші.

Савченко В. А. Основні напрями застосування технологій штучного інтелекту у кібербезпеці / В. А. Савченко, О. Д. Шаповаленко // Сучасний захист інформації. – 2020. – № 4(44). – С. 6-11.

Р/2300

У якості ключової ідеї застосування засобів штучного інтелекту у кібербезпеці запропоновано використання технологій та методів, які полегшують виявлення та реагування на загрози, використовуючи набори статистичних даних про кібератаки. Пріоритетні сфери застосування штучного інтелекту – забезпечення безпеки мереж і захист даних.

Салієва О. В. Дослідження достовірності впливу загроз на рівень захищеності системи захисту інформації та об'єкта критичної інфраструктури за результатами когнітивного моделювання / О. В. Салієва, Ю. Є. Яремчук // Вісник Черкаського державного технологічного університету. – 2020. – № 3. – С. 85-93.

Р/1308

... застосовано апарат множинного регресійного аналізу, який дає можливість простежити зв'язок між загрозами та захищеністю досліджуваних систем, оцінивши ступінь ймовірного впливу. Сформовано аналітичні вирази лінійної кореляції залежності між найвагомішими концептами кожної когнітивної моделі та захищеністю відповідної досліджуваної системи. З метою порівняння впливу загроз на захищеність об'єкта критичної інфраструктури та системи захисту інформації, отриманого за результатами когнітивного моделювання, визначено стандартизовані коефіцієнти регресії та коефіцієнти еластичності. Проведений аналіз отриманих значень цих показників дав змогу підтвердити достовірність впливу загроз на рівень захищеності досліджуваних систем.

Салієва О. В. Дослідження імпульсних процесів на когнітивній карті для визначення зміни рівня захищеності системи захисту інформації / О. В. Салієва, Ю. Є. Яремчук // Вісник Вінницького політехнічного інституту. – 2020. – № 5(152). – С. 56-62.

Р/0126

... у роботі пропонується провести дослідження імпульсних процесів на нечіткій когнітивній карті для визначення зміни рівня захищеності системи захисту інформації. Ця методика базується на розповсюдженні імпульсу, введеного у концепт (або декілька концептів) когнітивної карти, який, поширюючись по системі, посилюється або ж згасає.

728620 В
623

Сучасна спеціальна техніка [Текст] : науково-практичний журнал / Державний н.-д. ін-т МВС України. - Київ : [Видавець ФОП Горбенко Ю. В.].
№ 1 (60). - Київ, 2020. - 186 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., англ.

Зі змісту:

Зибін С. В. **Алгоритм пошуку множини рішень, оптимальних за Парето і Слейтером, за інформаційно-аналітичної підтримки процесів системи інформаційної безпеки.** – С. 5-15.
Статтю присвячено розробці алгоритму звуження множини Парето-оптимальних рішень в досить вузький набір альтернатив, призначених для остаточного вибору особою, яка приймає рішення.

728621 В
623

Сучасна спеціальна техніка [Текст] : науково-практичний журнал / Державний н.-д. ін-т МВС України. - Київ : [Видавець ФОП Горбенко Ю. В.].
№ 2 (61). - Київ, 2020. - 162 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., англ.

Зі змісту:

Ткач Ю. М. **Моделі систем захисту інформаційної сфери держави.** – С. 59-66.
У статті проведено аналіз основних завдань захисту інформації. Побудовано моделі впливів на інформацію, оцінки вразливості інформації, що захищається, та запропонована модель нейтралізації загроз.

728937 В
63

Таврійський державний агротехнологічний університет імені Дмитра Моторного.
Збірник наукових праць Таврійського державного агротехнологічного університету імені Дмитра Моторного [Текст] / за ред. С. В. Кальченка ; Таврійський держ. агротехнол. ун-т ім. Дмитра Моторного, Ф-т економіки та бізнесу. - Мелітополь : Вид-во Мелітопольська типографія "Люкс". - (Економічні науки).
№1 (41). - Мелітополь, 2020. - 227 с. : іл., табл. - Бібліогр. наприкінці ст. - Текст укр. та англ. Дод. тит. арк. англ.

Зі змісту:

Баханова М. В., Синяєва Л. В. **Кібершахрайства та кібербезпека у банківській сфері .** – С. 27-33.
Статтю присвячено проблемі незаконного використання інформаційних систем у банківській сфері. Розглянуто основні популярні кібершахрайські атаки у фінансовій сфері і принципи протидії їм. Даються рекомендації щодо захисту від кібератак як фізичним особам, так і превентивно в масштабах державного адміністрування.

728407 В
35

Теорія та практика державного управління [Текст] = Theory and Practice of Public Administration : зб. наук. пр. / Нац. акад. держ. упр. при Президентові України, Харк. регіон. ін-т держ. упр. - Харків : [Магістр], 2009 .
Вип. 3 (70). - Харків, 2020. - 216 с. : граф., табл. - Бібліогр. наприкінці ст. - Текст кн. укр. та англ.

Зі змісту:

Мялковський Д. В., Семенченко А. І. **Розвиток інституційних спроможностей суб'єктів забезпечення системи кібербезпеки та кіберзахисту України.** – С. 40-54.
Визначено поняття, сутність, структуру інституційних спроможностей суб'єктів забезпечення системи кібербезпеки та системи кіберзахисту України, проведено аналіз та оцінювання їхнього стану, обґрунтовано пріоритетні напрями їхнього вдосконалення, спрямовані на підвищення ефективності та результативності публічної політики у сфері кібербезпеки та кіберзахисту України.
Обґрунтовано пріоритетні напрями удосконалення правового механізму інституційних спроможностей для ієрархічної моделі правового забезпечення на законодавчому, підзаконному та нормативно-технічному (нормативно-правовому) рівнях.

728408 В
35

Теорія та практика державного управління [Текст] = Theory and Practice of Public Administration : зб. наук. пр. / Нац. акад. держ. упр. при Президентові України, Харк. регіон. ін-т держ. упр. - Харків : [Магістр], 2009 - .
Вип. 4 (71). - Харків, 2020. - 216 с. : граф., табл. - Бібліогр. наприкінці ст. - Текст кн. укр. та англ.

Зі змісту:

Ободяк В. К., Котух Є. В. **Основні виклики урядування у сфері кібербезпеки.** – С. 38-46.
Проаналізовано характеристики урядування у сфері кібербезпеки, виявлено низку проблем, які суттєво ускладнюють урядування ("безкоштовне використання", відносні вигоди, шахрайство).

Ткач Ю. М. Метод вибору функціонального профілю захищеності / Ю. М. Ткач // Інформатика та математичні методи в моделюванні. – 2020. – Т. 10, № 1-2. – С. 68-74.

Р/2357

... метод вибору функціонального профілю захищеності дозволяє здійснити оптимальний вибір при виконанні умови максимізації відверненого збитку та неперевищення допустимих витрат за рахунок ймовірно-вартісної оцінки показників кількості й частоти появи загрози, ймовірних збитків від реалізації визначених загроз й вартості послуги захисту. Розроблений метод може бути використаним при створенні системи захисту інформації в кіберпросторі.

Ткаченко В. Найбільш нищівна кібератака в історії США / В. Ткаченко // Сети и бизнес. – 2020. – № 6(115). – С. 80-82.

Р/1698

Ніколи такого не було, і от знову: росіяни проникли у комп'ютерні мережі уряду США.

Функціональна модель Оперативного центру кіберзахисту / В. Г. Бушков, Є. В. Соловйов, О. О. Бобровський [та ін.] // Сучасний захист інформації. – 2020. – № 3(43). – С. 44-48.

Р/2300

У статті розглядається функціональна модель Оперативного центру кіберзахисту (SOC – Security Operation Center), яка поєднує основні політики, процедури та технологічні засоби для протидії кібервпливам на організацію. Визначено основні функції SOC, завдання та способи реалізації. Наведено приклади практичного застосування моделі. Запропонована архітектура типової інфраструктури SOC.