Тематична виставка
"Безпека та захист інформаційного простору "

(надходження II півр. 2019)

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

719341 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 - .
№ 1 (55). - Харків, 2019. - 232 с. : рис., табл. - Бібліогр. наприкінці ст. - Текст кн. укр. та англ.

Зі змісту:
Якимчук О. Ф. **Державне управління кібербезпекою в умовах гібридної війни.** – С. 35-40.
Торічний В. О. **Інформаційне забезпечення державної політики як найважливіший фактор безпеки держави.** – С. 77-85.

Гордеюк А. О. Проблема вдосконалення правового регулювання веб-сайтів і доменних імен в умовах інформатизації суспільства / А. О. Гордеюк // Гуманітарний часопис. – 2019. – № 2. – С. 73-83.

Р/2068

У статті проаналізовано правове становище веб-сайтів і доменних імен в Україні та наукові доробки вчених щодо визначення цих специфічних об'єктів у цивільному законодавстві самостійними об'єктами права інтелектуальної власності. Запропоновано ухвалити спеціальний закон з метою удосконалення правового регулювання веб-сайтів і доменних імен.

Гуцалюк М. В. Оцінка реалізації стратегії кібербезпеки України з урахуванням досвіду європейських і світових практик / М. В. Гуцалюк // Інформація і право. – 2019. – № 2(29). – С. 90-99.

Р/844

У статті аналізується міжнародний досвід проведення оцінки Стратегії кібербезпеки. Акцентується увага на необхідності проведення такої оцінки Стратегії кібербезпеки України.

Дзьобань О. П. Від "інформаційного суспільства" до "інформаційної безпеки": до проблеми концептуалізації сутності понять / О. П. Дзьобань, С. Б. Жданенко // Інформація і право. – 2019. – № 2(29). – С. 60-73.

Р/844

У статті зроблена спроба більш детального заглиблення у проблематику інформаційного суспільства та інформаційної безпеки на основі основоположних праць найбільш яскравих дослідників даної галузі знань.

Довгань О. Д. Концептуальні засади законодавчого забезпечення інформаційної безпеки України / О. Д. Довгань, Т. Ю. Ткачук // Інформація і право. – 2019. – № 1(28). – С. 86-99.

Р/844

У статті досліджуються концептуальні засади правового забезпечення інформаційної безпеки України. На основі теоретичного аналізу запропоновано модель Закону України "Про інформаційну безпеку України" та проаналізовано основні його змістовні частини.

Загальні принципи проведення тестування інформаційної безпеки підприємства / О. А. Курченко, М. В. Бржевський, А. Б. Гребенніков, В. І. Корсун // Сучасний захист інформації. – 2018. – № 4. – С. 27-34.

Р/2300

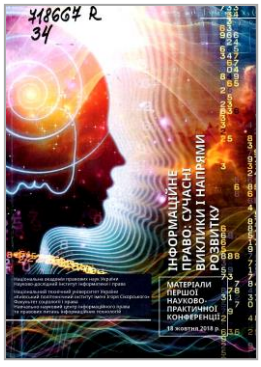
У статті розглянуто технічні методи тестування інформаційної безпеки підприємства та розробка послідовності їх застосування. Також досліджено методи і механізми тестування інформаційної безпеки підприємства. Існуючі методи дослідження інформаційної безпеки підприємства умовно розділені на 3 категорії. Керуючись принципами закладеними у цих методах зовнішній аудитор, за згодою замовника, може на власний розсуд формувати послідовність дій для тестування безпеки. Досі ці методики залишаються лише вказівниками для аудитора і він змушений, в значній мірі, покладатися на свій досвід і експертну думку.

717760 R
004

Інформаційна безпека та інформаційні технології [Текст] : монографія / Альошин Г. В., Герасимов С. В., Засядько А. А. та ін. ; за заг. ред. В. С. Пономаренка. - Харків : ТОВ "Діса Плюс", 2019. - 322 с. : граф., рис., табл. - Бібліогр. в кінц ст. - Авт. зазнач. на звороті тит. арк.

У монографії наведені результати наукових досліджень в галузі розробки і практичного застосування інформаційної безпеки та сучасних інформаційних технологій.

Монографія представляє інтерес як для фахівців, сфера діяльності яких безпосередньо пов'язана з розробкою IT-технологій, способів забезпечення безпеки і передачі в комунікаційних системах, так і для більш широкого кола фахівців. Вона буде корисною викладачам, аспірантам і студентам, що спеціалізуються в області IT-технологій, і всім, хто серйозно цікавиться проблемами взаємодії інформаційних технологій і суспільства.



718667 R
34

Інформаційне право: сучасні виклики і напрями розвитку [Текст] : матеріали першої науково-практичної конференції 18 жовтня 2018 року / упоряд: В. М. Фурашев, С. Ю. Петряєв ; Нац. акад. правових наук. України, НДІ інформатики і права, НТУУ "КПІ ім. Ігоря Сікорського" [та ін.]. - Київ : КПІ ім. Ігоря Сікорського, 2018. - 196 с. : граф., табл. - Бібліогр. в кінці ст. - Упоряд. зазнач. на звороті тит. арк.

Матеріали конференції з нагоди 25-ї річниці створення Національної академії правових наук України та п’ятої річниці створення Навчально-наукового центру інформаційного права та правових питань інформаційних технологій КПІ ім. Ігоря Сікорського присвячені розгляду теоретико-правових та практичних питань розвитку інформаційного права в Україні.

Зі змісту:

Качинський А. Б. Використання інформаційних технологій для розуміння процесів ухвалення колективних рішень Верховною Радою України / А. Б. Качинський, І. В. Стьопочкіна // Безпека інформації. – 2019. – Т. 25, № 1. – С. 30-37.

Р/1408

Стаття присвячена розв'язанню задачі оцінки впливу фракції парламенту, що дозволяє визначити, як політичні сили найбільше впливають на кібернетичну безпеку держави. *Запропоновано методику* автоматизованого збору та обробки даних на основі відкритих результатів голосувань, зібраних з офіційного веб-ресурсу парламенту.

Кіреєнко О. Рекомендації щодо розробки моделі порушника інформаційної безпеки із загальною та спеціалізованою інформацією / О. Кіреєнко // Безпека інформації. – 2019. – Т. 25, № 1. – С. 24-29.

Р/1408

У даній статті надано рекомендації щодо розробки моделі порушника з інформацією, що відрізняється за рівнем спеціалізованості. Розроблена відповідно до наданих рекомендацій модель порушника дозволяє враховувати рівень контролю порушника за проведенням атаки та пріоритет вибору цілей для атаки.

Ковтун В. В. Моделювання доступності інформаційної системи критичного застосування / В. В. Ковтун // Вісник Вінницького політехнічного інституту. – 2019. – № 1. – С. 41-57.

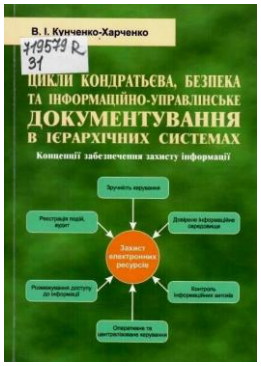
Р/0126

У статті представлено нові математичні моделі управління доступністю ІСКЗ, які, на відміну від існуючих, враховують топологічні особливості ІСКЗ, перебіг її сервісних операцій при управлінні доступом авторизованих суб'єктів до інформаційного середовища системи і формалізують зв'язок множини сервісних операцій з множиною відповідей системи на запити авторизованих суб'єктів у вигляді керованого напівмарковського процесу з резервуванням ресурсів на заходи самоубезпечення.

Костенко О. В. Проблеми правового регулювання та розвиток кібернетичної безпеки України на сучасному етапі / О. В. Костенко // Інформація і право. – 2019. – № 3(30). – С. 96-104.

Р/844

У статті проаналізовано проблеми законодавчого регулювання сфери кібернетичної безпеки України на досвіді сучасних кібернетичних загроз та кібератак, що здійснювалися на державні інформаційні ресурси протягом останніх років. Висвітлено проблему понятійно-категоріального апарату основних нормативно-правових актів сфери кібернетичної безпеки.



719579 R
31

Кунченко-Харченко, В. І.
Цикли Кондратьєва, безпека та інформаційно-управлінське документування в ієрархічних системах. Концепції забезпечення захисту інформації [Текст] : наук.-навч. посібн. / В. І. Кунченко-Харченко ; Черкаський держ. технологічний ун-т. - Львів : Укр. акад. друкарства, 2019. - 420 с. : граф., рис., табл. - Бібліогр.: с. 296-320.

"... велике значення на сьогодні, здобули комп'ютерні технології і засоби, що забезпечують на базі діючого законодавства та інших нормативно-правових норм оперативність фіксації, збору, обробки, пошуку і передачі інформації, надійність її збереження; вилучений доступ надання інформації на потрібному носії у визначеній формі та т. п. Доступ до світових інформаційних ресурсів переходить на електронне документування та збереження, що відкриває принципово нові способи організації інформації і доступу до неї. Але тим самим, ставить принципово нові вимоги до документознавства, до документалістики, архівознавства та спеціальних історичних дисциплін і визначає їм одне із провідних місць серед наукових дисциплін, та їх об'єкту дослідження – документу. Вирішення цієї проблеми вимагає від науковців вивчення історичного досвіду, еволюції документа, як провідника інформації. Зміна носіїв і технологій, створення відповідних умов для розвитку як загального

документознавства, документології треба розглядати як цілісну науку, що вивчає історію, теорію створення документа, впливає на роботу апарату управління і документознавства в цілому. Тісний зв'язок документознавства з практикою роботи дає додаткові можливості для науково-дослідної роботи в даній галузі".

Лаптєв О. А. Модель інформаційної безпеки на основі марковських випадкових процесів / О. А. Лаптєв // Зв'язок. – 2018. – № 6. – С. 45-49.

Р/776

Обґрунтовано та запропоновано математичний апарат, в якому за елемент інформаційної безпеки беруть не загрози несанкціонованого знімання інформації (атаки), а загрози – можливість знімання інформації уразливості.

Розглянуто математичний апарат для моделювання систем із відмовами і відновленням (виявлення каналів витоку інформації і запобігання знімання інформації по цих каналах), з характеристиками безпеки. Виконано розрахунки за зазначеною методикою для різних значень ρ (де ρ = λ/μ, λ–виникнення уразливості і μ–усунення уразливості).

Литвин Н. А. Сучасний стан правового забезпечення інформаційної безпеки органів Державної фіскальної служби України / Н. А. Литвин // Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика). Серія: Право. – 2018. – Вип. 1–2. – С. 81-86.

Р/653

У статті розглянуто сучасний стан рівня інформаційної безпеки в податкових та митних органах України, а також висвітлено напрями вдосконалення правового забезпечення інформаційної безпеки зазначених органів.

Ліпінський В. В. Застосування стандартів НАТО при створенні систем захисту інформації в сфері національної безпеки / В. В. Ліпінський // Телекомунікаційні та інформаційні технології. – 2018. – № 3. – С. 88-93.

Р/1921

Проведено аналіз стандартів НАТО, розглянуті питання можливого їх застосування при створенні та впровадженні комплексних систем захисту інформації на стадіях життєвого циклу інформаційних систем в сфері національної безпеки. Використання окремих положень стандартів НАТО допомогло б звузити фокус національного законодавства щодо підвищених вимог до інформаційних систем.

719304 R
070

Любовець, Григорій Вікторович.
Комунікаційно-контентна безпека: проблематика, підходи, етапи становлення [Текст] : наук. розвідки інформ. простору України за період 2002 – 2017 рр. ; [монографія] / Любовець Г. В., Король В. Г. - Дніпро : Середняк Т. К., 2018. - 462 с. : табл. - Бібліогр.: с. 454-461 (110 назв).

Останні події, пов'язані з гібридно-месіанськими агресіями путінського режиму проти України і світу загалом, примусили провідні країни по-іншому подивитись на проблематику інформаційної безпеки. Інформаційний простір країн світу в умовах сучасних динамік перманентної публічності перетворився на арену жорсткого міждержавного суспільно-ментального протистояння цивілізаційного поступу глобального світу. Від постійних різновекторних та різноформатних комунікаційно-контентних агресій з боку глобального гібридного терориста, яким є нині політико-корпоративний режим путінської Росії, потерпають не лише окремі країни, а й уся загальносвітова демократична система.

Читачу пропонуються до уваги попередні результати-практики досліджень інформаційного простору України, зокрема такого аспекту, як комунікаційно-контентна безпека, які проводились авторами протягом останніх п'ятнадцяти років. Пропонується нове бачення цієї проблематики та авторський глосарій, який розроблявся в процесі потоково-лабораторного дослідження протягом зазначеного часу та робота над яким триває. Дається також порівняльний аналіз розвитку окремих сегментів інформпростору.

Марущак А. Європейський досвід з питань боротьби з правопорушеннями в інформаційній сфері / А. Марущак // Безпека інформації. – 2019. – Т. 25, № 1. – С. 13-17.

Р/1408

У статті здійснено аналіз найбільш поширених правопорушень в інформаційній сфері: кіберправопорушень і дезінформування, проаналізовано європейський досвід з питань боротьби із такими правопорушеннями. Запропоновано рекомендації для правоохоронних органів України.

Марченко В. В. GDPR – зброя, а не захист / В. В. Марченко, В. І. Кучер, Г. І. Гайдур // Сучасний захист інформації. – 2018. – № 4. – С. 35-39.

Р/2300

В статті розглянуті основні відомості про GDPR, регламент, що змінив відношення до регулювання даних в Європі та його основні проблеми. На конкретних прикладах наведені яскраво виражені недоліки створеного регламенту, з якими має зіштовхнутись кожен, хто відтепер хоче співпрацювати з ЄС. Особлива увага приділена проблемам практичної реалізації регламенту, а також використанню явних недоліків регламенту на користь зловмисника.

718835 R
35

Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України [Текст] : аналітична доповідь / [Суходоля О. М., Бобро Д. Г., Іванюта С. П., Кондратов С. І.,]; [за заг. ред. О. М. Суходолі] ; Нац. ін-т стратегічних досліджень. - Київ : НІСД, 2019. - 224 с. : табл. - Бібліогр. у виносках. - Авт. зазнач. на звороті тит. арк.

У виданні висвітлено теоретичні та нормативно-правові засади створення системи безпеки і стійкості критичної інфраструктури в Україні, запропоновано методологічні засади виокремлення критичної інфраструктури та формалізації діяльності залучених суб'єктів з питань захисту критичної інфраструктури.

Проаналізовано передовий зарубіжний досвід у галузі захисту критичної інфраструктури, ситуацію із запровадження концепції захисту критичної інфраструктури в Україні, окреслено можливі напрями та інструменти щодо здійснення державної політики у цій сфері, сформульовано низку конкретних рекомендацій і пропозицій.

Петров С. Г. Повноваження СБ України як суб'єкта національної системи кібербезпеки / С. Г. Петров // Інформація і право. – 2019. – № 2(29). – С. 100-105.

Р/844

У статті досліджуються питання визначення повноважень Служби безпеки України як суб'єкта національної системи кібербезпеки з урахуванням процесів реформування державного органу спеціального призначення з правоохоронними функціями, що забезпечує державну безпеку.

718563 В
34

Повітряне і космічне право. Юридичний вісник [Текст] : наук. пр. Нац. авіац. ун-ту / Нац. авіац. ун-т. - Київ : [НАУ]. -

№ 1 (50). - Київ, 2019. - 208 с. : табл. - Бібліогр. наприкінці ст. - Текст укр., англ.

Зі змісту:

Салаєв Т. Г. **Особливості адміністративно-правового регулювання інформаційної безпеки при застосуванні інформаційних технологій та автоматизованих систем у митній сфері у контексті запровадження механізму "єдиного вікна".** – С. 85-91.

Прав Р. Ю. Інноваційні методи реалізації державної політики протидії зовнішнім інформаційним загрозам / Р. Ю. Прав // Інвестиції: практика та досвід. – 2019. – № 16. – С. 113-118.

Р/2124

Досліджено питання сучасних інформаційних загроз та інформаційної безпеки України на сучасному етапі в рамках реалізації пріоритетних завдань державної політики забезпечення інформаційної безпеки. Наведено методи протидії держави зовнішнім інформаційним загрозам. Наведено оперативні методи протидії зовнішнім інформаційним загрозам.

Самохвалов Ю. Я. Оцінка інформаційної безпеки організації за критерієм впевненості / Ю. Я. Самохвалов, М. М. Браіловський // Захист інформації. – 2019. – Т. 21, № 1. – С. 13-24. – Текст рос.

Р/1428

… виникає необхідність в розробці методичного апарату оцінки ІБ організації з урахуванням об'єктивних і суб'єктивних аспектів безпеки. У статті пропонується підхід до оцінки ІБ на основі критерію впевненість в тому, що в організації реалізується прийнята політика безпеки.

717221 В
33

Стратегічні пріоритети [Текст] = Strategic priorities : науково-аналітичний щокварт. зб. / Національний ін-т стратегічних досліджень. - [К.] : [НІСД]. -
№ 2 (47). - [К.], 2018. - 160 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., рос., англ.

Зі змісту:

Сніцаренко П. М. **Термінологічний нігілізм в інформаційній сфері та його наслідки для інформаційної безпеки України.** – С. 31-38.
У статті розглядається та аналізується проблема неусталеності термінології в інформаційній сфері, зокрема в законодавстві України, показано наслідки цієї ситуації для інформаційної безпеки держави та подальших шляхів її забезпечення.

719342 В
33

Стратегічні пріоритети [Текст] = Strategic priorities : науково-аналітичний щокварт. зб. / Національний ін-т стратегічних досліджень. - [Київ] : [НІСД].
№ 1 (49). - [Київ], 2019. - 136 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., рос., англ.

Зі змісту:

Бойко В. О. **Європейський досвід державно-приватного партнерства: підходи до формування нормативно-правових засад.** – С. 28-36.
У статті проаналізовано ініціативи ЄС щодо державно-приватного партнерства у сфері кібербезпеки, відзначено наскрізне акцентування на полегшенні доступу підприємств малого та середнього бізнесу, що працюють у галузі кібербезпеки, до нових ринків. Досліджено пріоритетні напрями стратегії співпраці приватного та державного сектору в галузі кібербезпеки.

Ткачук Н. А. Стан та проблемні питання реалізації Стратегії кібербезпеки України / Н. А. Ткачук // Інформація і право. – 2019. – № 1(28). – С. 129-134.

Р/844

У статті досліджено стан і проблемні питання реалізації Стратегії кібербезпеки України та запропоновано шляхи удосконалення стратегічного планування у сфері кібербезпеки держави.

Турчак А. В. Основні засади державної політики забезпечення інформаційної безпеки в Україні / А. В. Турчак // Інвестиції: практика та досвід. – 2019. – № 11. – С. 123-127.

Р/2124

З'ясовано основні засади державної політики забезпечення інформаційної безпеки в Україні. Визначено, що інформаційну безпеку підтримують, проводячи виважену та збалансовану державну політику в інформаційній галузі. Держави, що мають потужний потенціал в інформаційному середовищі, можуть впливати на держави, в яких інформаційний простір та кіберпростір є незахищеними.

Формалізована модель оцінки гарантій інформаційної безпеки комплексної системи захисту інформації / Д. С. Комін, О. В. Чечуй, М. А. Левченко [та ін.] // Системи озброєння і військова техніка. – 2018. – № 4. – С. 92-99.

Р/1903

Розглянуті особливості проведення оцінювання гарантій інформаційної безпеки для комплексної системи захисту інформації у відповідності до державних та міжнародних стандартів. Запропоновано застосування формалізованої моделі процесу оцінювання вимог гарантій інформаційної безпеки суб'єктів експертизи із застосуванням аксіоматичних конструкцій.

Програмні системи захисту інформації

Гільгурт С. Я. Побудова асоціативної пам'яті на цифрових компараторах реконфігуровними засобами для вирішення задач інформаційної безпеки / С. Я. Гільгурт // Електронне моделювання. – 2019. – Т. 41, № 3. – С. 59-80.

Р/518

... швидко набувають популярності апаратні прискорювачі на основі ПЛІС. Один з найпоширеніших підходів до побудови швидкодіючих схем розпізнавання на програмованій логіці заснований на застосуванні асоціативної пам'яті та цифрових компараторів, з яких вона складається. З метою підвищення ефективності створюваних реконфігуровних засобів інформаційної безпеки проаналізовано переваги та недоліки такого підходу, особливості його реалізації на ПЛІС, проблеми, що виникають, та шляхи їх вирішення.

Дегтярьова Л. М. Аналіз структури системи захисту інформації / Л. М. Дегтярьова, М. В. Мірошникова, С. В. Волошко // Системи управління, навігації та зв'язку. – 2019. – Вип. 2. – С. 78-82.

Р/2152

У статті виконаний аналіз пріоритетних елементів архітектури системи захисту інформації з позиції ефективності її роботи. Система включає в себе модулі для реєстрації, обліку та обмеження доступу з урахуванням затверджених норм та правил, шифрування інформації, що передається або зберігається, резервування інформаційних ресурсів та забезпечення цілісності.

Дєлобоско О. П. Вразливість PATH TRAVERSAL архіватор WINRAR до версії 5.61 / О. П. Дєлобоско, Н. О. Савеленко, Ю. І. Хлапонін // Бизнес и безопасность. – 2019. – № 3. – С. 27-28.

Р/1070

WINRAR – це програмне забезпечення для архівації та управління архівами, розроблений для операційних систем Windows, Linux, FreeBSD, Mac OS X, Android. Розповсюджується як умовно-безкоштовне програмне забезпечення.

Помилка, про яку вперше повідомила компанія Check Point Research, знаходиться у мало використовуваній DLL (Dynamic Linked Library), яка декодує архіви ACE і була написана ще в 2005 році без механізму захисту на кшталт ASLR, DEP та інших[1]. Назви даної вразливості, яку ще називають експлойтами: CVE-2018-20250, CVE-2018-20251, CVE-2018-20252 і CVE-2018-20253[2].

Довбешко С. В. Застосування методів інтелектуального аналізу даних для побудови систем виявлення атак / С. В. Довбешко, С. В. Толюпа, Я. В. Шестак // Сучасний захист інформації. – 2019. – № 1(37). – С. 6-15.

Р/2300

Безліч параметрів для виявлення мережевих атак становить значний обсяг даних, що визначає можливість їх обробки саме методами інтелектуального аналізу. На сьогодні системи виявлення вторгнень і атак зазвичай являють собою програмні або апаратно-програмні рішення, які автоматизують процес контролю подій, що відбуваються в інформаційній системі або мережі, а також самостійно аналізують ці події в пошуках ознак проблем безпеки.

Князєв О. А. Програмне забезпечення адаптивної комплексної системи фільтрації контенту / О. А. Князєв // Вісник Хмельницького національного університету. Серія: Технічні науки. – 2019. – № 3. – С. 208-214.

Р/1055«Т»

На основі запропонованої адаптивної комплексної системи фільтрації контенту (АКСФК), що відрізняється від існуючих тим, що завдяки постійному оновленню списків та профілю користувачів має більш високу якість фільтрації контенту, розроблено програмний продукт "Проксі Блокер", для якого в якості платформи розробки було обрано програмну оболонку Debian. Наведено послідовність проходження процедури фільтрації контенту. Виконано тестування програмного продукту "Проксі Блокер".

Конявский В. А. Защищенные компьютеры новой гарвардской архитектуры / В. А. Конявский // Вопросы защиты информации. – 2019. – № 1. – С. 18-29.

Р/0171

Рассматривается построение архитектуры компьютера, позволяющей обеспечить высокую защищенность и достаточную универсальность за счет динамического изменения структуры.

Лисенко С. М. Метод та програмне забезпечення виявлення шкідливих запитів в комп'ютерних мережах на основі протоколу DNS / С. М. Лисенко, В. О. Лісовий // Вісник Хмельницького національного університету. Серія: Технічні науки. – 2019. – № 3. – С. 173-179.

Р/1055«Т»

В роботі представлено метод, спрямований на виявлення і блокування доменів, які запитуються в потоковому трафіку DNS і використовуються для зловмисного видалення даних DNS.

Лисецкий Ю. М. Комплексна інформаційна безпека корпоративних інформаційних систем / Ю. М. Лисецкий // Управляющие системы и машины. – 2019. – № 1. – С. 68-75. – Текст рос.

Р/487

Інформація в електронному вигляді, до якої має доступ корпоративна система, повинна мати такі властивості: конфіденційність, цілісність; автентичність; досяжність. Ці властивості і повинна забезпечувати корпоративна система інформаційної безпеки.

Лисецькій Ю. М. Резервне копіювання як інструмент захисту інформації / Ю. М. Лисецькій // Управляющие системы и машины. – 2019. – № 2. – С. 80-87. – Текст рос.

Р/487

Із зростанням об'ємів інформації, що знаходяться на різних носіях, ускладняється завдання надійності їх зберігання. Один із інструментів захисту інформації – резервне копіювання і створення інформаційних архівів для швидкого доступу до даних.

Основні виробники сучасних систем резервного копіювання (СРК) – *IBM* з *Tivoli Storage Manager, EMC* з *Neworker і Avamar, Veritas* з *Backup Exec* і *Net Backup.*

Москвитин Г. И. Механизмы анализа и синтеза систем защиты от несанкционированного доступа к данным в информационных системах / Г. И. Москвитин // Вопросы защиты информации. – 2019. – № 2. – С. 3-5.

Р/0171

Рассматриваются процедурные методы защиты информации, которые обеспечивают доступ к данным только пользователям, имеющим соответствующие разрешения. Механизмы защиты предназначены для обеспечения доступа и допуска к информации только обладающих соответствующими полномочиями пользователей.

719347 В
63

Національний лісотехнічний університет України.
Науковий вісник НЛТУ України [Текст] = Scientific Bulletin of UNFU : збірник наук.-техн. праць. - Львів : [РВВ НЛТУ України].
Вип. 29, № 5. - Львів, 2019. - 156 с. : граф., рис., табл. - Бібліогр. наприкінці ст. -Текст кн. укр., рос., англ. Дод. тит. арк. англ.

Зі змісту:

Яковина В. С., Угриновський Б. В. **Старіння програмного забезпечення в контексті його надійності: огляд проблематики.** – С. 123-128.

719336 В
623

Сучасна спеціальна техніка [Текст] : науково-практичний журнал / Державний н.-д. ін-т МВС України. - Київ : [Видавець ФОП Горбенко Ю. В.].
№ 3 (54). - Київ, 2018. - 158 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., англ.

Зі змісту:

Опірський І. Р., Тишик І. Я. **Оцінювання ймовірності реалізації загроз інформаційній системі на різних рівнях стеку TCP/IP.** – С. 51-60.

Сучасні тенденції та методологія захисту персональних даних засобами RASPBERRY PI / С. Лавченчук, С. Костючко, А. Возняк, А. Булік // Комп'ютерно-інтегровані технології: освіта, наука, виробництво. – 2019. – № 35. – С.141-145. – Текст англ.

Р/2346

У даній статті досліджено аспекти розвитку процедури захисту інформації на базі розробки програмного забезпечення. В процесі розробки за основу береться платформа RASPBERRY PI та система Raspbian. Розглянуто основні вразливі місця та можливості впливу сторонніми засобами на керування досліджуваного об'єкту, як приклад «розумний дім».

Тецький А. Г. Аналіз проблем і можливостей забезпечення безпеки WEB-застосунків, створених за допомогою систем керування вмістом / А. Г. Тецький // Системи управління, навігації та зв'язку. – 2019. – Вип. 1. – С. 133-136.

Р/2152

"Системи керування вмістом є програмним забезпеченням, за допомогою якого можна досить швидко і легко створити WEB-сайт в мережі Інтернет.

Зростання кількості сайтів в мережі Інтернет супроводжується зростанням інтересу зловмисників в даній сфері [1]. Таким чином, дослідження процесів отримання несанкціонованого доступу в систему керування вмістом являє науковий інтерес і дає можливість розробляти ефективні способи захисту від вторгнень [2]".

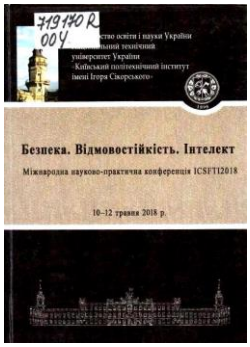
Телекомунікаційні мережі та інформаційно-комунікаційні технології

719496 R
34

Актуальні питання забезпечення службово-бойової діяльності сил сектору безпеки і оборони [Текст] : матеріали регіонального круглого столу (м. Харків, 19 квітня 2019 року) / Служба безпеки України, Національний юридичний університет імені Ярослава Мудрого, Інститут підготовки юридичних кадрів для Служби безпеки України. - Харків : ФОП Бровін О. В.
Вип. 3. - Харків, 2019. - 307 с. : табл. - Бібліогр. наприкінці ст.

Зі змісту:

Голубничий Д. Ю., Ільїна І. В., Семеренко Ю. О., Радівілова А. С. **Активний захист інформації при протидії кіберзагрозам в інформаційно-телекомунікаційній мережі.** – С. 251-254.
Білоус І. А. **Інформаційна війна в мережах Інтернет, як метод сучасного протиборства.** – С. 282-284.
Рибалка Г. В., Бзот В. Б., Луковський О. Я., Сметана Є. А., Пилипенко В. Г., Булай А. М. **Аналіз підходів до вирішення проблем інформаційної безпеки для організації безпечного функціонування бездротових корпоративних мереж.** – С. 297-301.



719170 R
004

Безпека. Відмовостійкість. Інтелект. [Текст] : Міжнародна науково-практична конференція ICSFTI2018, 10-12 травня 2018 р. : [зб. пр.] / Нац. техн. ун-т України "Київ. політехн. ін-т ім. Ігоря Сікорського", Ф-т інформатики та обчислюв. техніки, Каф. обчислюв. техніки. - Київ : Політехніка КПІ ім. Ігоря Сікорського, 2018. - 378 с. : рис., табл. - . - Бібліогр. в кінці ст. - Дод. тит. арк. англ. Текст кн. укр., рос., англ. мов.

Зі змісту:

Секція 1.SEC **(Безпека комп'ютерних систем та мереж. Відмовостійкі розподілені обчислення).** – С. 26-98.

719048 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. - К. : [ВІКНУ].
Вип. № 61. - Київ, 2018. - 216 с. : іл. - Бібліогр. наприкінці ст. - Текст кн. укр., рос., англ.

Зі змісту:

Чорненький В. І., Сєлюков О. В., Осипа В. О., Глінський О. В., Щерба В. І. **Вдосконалення методу підвищення інформаційної безпеки комп'ютерних мереж на основі формування правил політики безпеки.** – С. 157-168.
У статті розглянуто підхід, який об'єднує множину моделей і методику, для реалізації детального аналізу захищеності комп'ютерних мереж на етапах експлуатації і проектування, який базується на імітації дій порушника, побудові і аналізу графу загроз.

719040 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. - К. : [ВІКНУ].
Вип. № 62. - Київ, 2018. - 142 с. : іл. - Бібліогр. наприкінці ст. - Текст кн. укр., рос., англ.

Зі змісту:

Горбенко І. Д., Замула О. А., Вдовенко С. Г. **Оцінка показників захищеності сучасних бездротових систем зв'язку широкосмугового доступу на основі врахування особливостей технології OFDM.** – С. 67-76.

Гейдарова О. В. Захист інформаційних систем та технологій в управлінні готельно-ресторанним бізнесом / О. В. Гейдарова, В. П. Паюк // Вісник Хмельницького національного університету. Серія: Економічні науки. – 2019. – № 1. – С. 115-118.

Р/1055«Е»

Розглянуто можливість захисту інформаційних систем управління готельно-ресторанним бізнесом в сучасних умовах. Запропоновано інформаційну технологію виявлення помилок у комп'ютерних системах та мережах. Обґрунтовано впровадження поетапного здійснення технічного захисту інформації з урахуванням динаміки зміни можливих загроз.

Джулій В. М. Метод виявлення та протидії розподіленим атакам, спрямованим на відмову в обслуговуванні / В. М. Джулій, В. І. Чорненький, О. О. Савіцька // Вісник Хмельницького національного університету. Серія: Технічні науки. – 2019. – № 2. – С. 122-127.

Р/1055«Т»

В роботі запропоновано актуальний метод та інструментарій для раннього виявлення розподілених атак, спрямованих на відмову в обслуговуванні, і подальшого виявлення шкідливого трафіку на стороні ресурсу, що атакується і його блокування власними силами.

Дмитренко Ю. Безопасность Wi-Fi сетей / Ю. Дмитренко // Бизнес и безопасность. – 2019. – № 4. – С. 18-22.

Р/1070

Европейские специалисты обнаружили очередную уязвимость Wi-Fi. Причем такую, что она потенциально угрожает не только роутерам, но и вообще всем гаджетам, которые используют Wi-Fi. А ведь это – только одно из несовершенств беспроводной связи.

Донцов О. Ю. Застосування моделі ARMA для прогнозування навантаження комп'ютерних мереж / О. Ю. Донцов, В. С. Ситніков // Наукові праці Чорноморського національного університету імені Петра Могили. Серія: Комп'ютерні технології. – 2018. – Т. 317, Вип. 305. – С. 97-101.

Р/1886

Більшість локальних комп'ютерних мереж не застраховані від раптових навантажень, які можуть спричинити втрату даних, порушення їх цілісності, безпеки мережі і безліч інших проблем. Запропоновано застосовувати модель ARMA для прогнозування у реальному часі пікового навантаження, що може допомогти системним адміністраторам локальних мереж вжити необхідних заходів, або надати інформацію автоматизованим системам моніторингу та адміністрування мереж для подальшої обробки.

Зеліско І. М. Розвиток інформаційного суспільства як домінанта інноваційного зростання / І. М. Зеліско, О. О. Сосновська, Ху Сунцзе // Економіка. Менеджмент. Бізнес. – 2019. – № 1. – С. 33-39.

Р/2331

У статті проаналізовано динаміку індексу розвитку інформаційно-комунікаційних технологій (IDI) як основного показника моніторингу глобального інформаційного суспільства для виявлення тенденцій інноваційного зростання у національному, регіональному та світовому масштабах.

Зідан А. М. Забезпечення захисту інформації від загроз профілю Facebook в комп'ютерних та телефонних мережах / А. М. Зідан // Сучасний захист інформації. – 2018. – № 3. – С. 58-70.

Р/2300

Проведено детальний аналіз можливих загроз інформації профілю Facebook як в комп'ютерних, так і в телефонних мережах. Наведені приклади заходів та засобів, що може використовувати зловмисник для реалізації атак. Розглянуті сучасні методи забезпечення захисту для інформації профілю Facebook.

719601 В
004

Інтелектуальні системи та інформаційні технології [Текст] = Intellectual systems and information technologies : праці міжнар. наук.-практ конф., 19-24 серпня 2019 р., Одеса, Україна / Одеська міськрада, Одеський держ. екол. ун-т, Одеський нац. ун-т ім. І. І. Мечникова [та ін.]. - Одеса : ТЕС, 2019. - 269 с. : іл.

Збірка містить праці Міжнародної науково-практичної конференції з інформаційних технологій, систем та засобів штучного інтелекту, обчислювальних машин, систем, мереж та їх компонентів, автоматизації систем та процесів керування, систем захисту інформації, кібернетики, управління проектами, електротехніки та телекомунікацій, інтелектуальних приладів та систем.

717368 В
004

"Інформаційні технології в сучасному світі: дослідження молодих вчених", міжнар. наук.-практ. конф. мол. учених, асп. та студ. (2019 ; Харків).

Тези доповідей Міжнародної науково-практичної конференції молодих учених, аспірантів та студентів "Інформаційні технології в сучасному світі: дослідження молодих вчених" [Текст] : тези доп., 21 - 22 березня 2019 р. / Харківський нац. екон. ун-т ім. Семена Кузнеця. - Х. : [ФОП Бровін О. В.], 2019. - 85 с. : іл. - Бібліогр. в кінці ст. - Текст кн. укр., рос.

Наведені тези пленарних та секційних доповідей за теоретичними та практичними результатами наукових досліджень і розробок. Представлені результати теоретичних досліджень в галузях проектування інформаційних систем, технологій захисту інформації, використання сучасних інформаційних технологій в управлінні системами, моделювання бізнес-процесів, застосування геоінформаційних технологій в дистанційній освіті та електронному навчанні, інформаційних технологій у видавничо-поліграфічній галузі, а також розроблення інструментальних засобів прикладної статистики.

Князєв Д. Інтернет загрози: новітні реалії / Д. Князєв, С. Князєв // Бизнес и безопасность. – 2019. – № 3. – С. 5-8.

Р/1070

Унікальні якості Інтернету забезпечують широкі можливості для реалізації прав громадян на доступ та поширення інформації «незалежно від кордонів»… Разом з тим, поряд з позитивними можливостями, які суттєво збільшили та збагатили можливості людини, у тому числі щодо комунікації та отримання інформації, динамічно розвиваються й специфічні загрози пов’язані із використанням такої мережі.

Конредди Р. Встраиваемая защита для интернета вещей / Р. Конредди // Chip news. Инженерная микроэлектроника. – 2019. – № 6. – С. 68-70.

Р/1070

В статье описаны общие проблемы безопасности интернета вещей. Приведены примеры атак злоумышленников и способы борьбы с ними. Кратко описан микроконтроллер SAM L11 с ядром ARM Cortex-M23 и архитектурой ARM TrustZone, предназначенный для использования во встраиваемых системах интернета вещей.

Концепція безпеки інформації в системі IoT / О. А. Серков, В. О. Кравець, О. В. Касілов [та ін.] // Сучасні інформаційні системи = Advanced Information Systems. – 2019. – Т. 3, № 1. – С. 136-139. – Текст англ.

Р/543

Мета – розробка концепції організації широкосмугового доступу до Інтернету та реалізація ключових компетенцій безпеки під час виконання проектів IoT. В основі моделі покладено еталонну модель DigComp 2.0, яку створено в рамках системи цифрової компетентності громадян. Причому, основною сферою компетентності цієї моделі є безпека.

Ларін В. В. Аналіз можливості підвищення конфіденційності відеоінформаційного ресурсу в умовах забезпечення заданої якості в інфокомунікаційних системах / В. В. Ларін, Д. В. Єрема, Ю. О. Болотська // Наука і техніка Повітряних Сил Збройних Сил України. – 2019. – № 2. – С. 158-162. – Текст англ.

Р/2266

Відеоконференцзв'язок знаходить широке застосування в бойовій підготовці й практиці повсякденного життя Збройних Сил. Як показує досвід останніх військових конфліктів, кризової ситуації в Автономній Республіці Крим і на сході країни реалізація властивостей системи керування військами досягається за рахунок впровадження сучасних технологій обробки й передачі відеоінформації в режимі реального часу з якістю не нижче заданої для керування військами і контролю виконання поставлених задач.

Мусиенко Д. Защита информации. Атаки по сторонним каналам / Д. Мусиенко // Бизнес и безопасность. – 2019. – № 5. – С. 29-35.

Р/1070

Безопасность давно является серьезной проблемой в вычислительных и коммуникационных системах и значительная часть научных исследований была посвящена ее изучению. Криптографические алгоритмы, в том числе симметричные шифры с открытыми ключами и хэш-функции образуют множество примитивов, которые могут быть использованы в качестве строительных блоков для построения механизмов безопасности, которые нацелены на конкретные цели.

718910 В
004

Наукоємні технології в інфокомунікаціях, Міжнар. наук.-практ. конф. (3 ; 2019 ; Харків / Кам'янець-Подільський).

Міжнародна науково-практична конференція "Наукоємні технології в інфокомунікаціях" [Текст] : матеріали III Міжнар. наук.-практ. конф., 23-25 травня 2019 р. / Харківський нац. ун-т Повітряних Сил імені І. Кожедуба, Кам'янець-Подільський нац. ун-т імені І. Огієнка, Харківський нац. ун-т радіоелектроніки. - Харків : [Друкарня Мадрид], 2019. - 158 с. : рис., граф. - Бібліогр. наприкінці ст. - Обкл. англ. Текст кн. укр., рос., англ. мов.

Зі змісту:

Секція 2. Інформаційна безпека та захист інформації

Бараннік В. В., Гаврилов Д. С., Рябуха Ю. М. **Загрози та шляхи захисту інформації у відомчих структурах.** – С. 43-44.

В роботі проведено аналіз можливих загроз та шляхів захисту інформації, що циркулює в мобільних системах відомчих структур.

Бараннік В. В., Слоблодянюк О. В., Бараннік Н. В. **Архітектурні особливості систем захисту веб-ресурсів від несанкціонованого доступу.** – С. 45-46.

Та ін.

Нитья В. Обнаружение и предотвращение атак с проверкой ввода в веб-приложениях с использованием детерминированных автоматов с магазинной памятью / В. Нитья, С. Сентилкумар // Проблемы управления и информатики. – 2019. – № 5. – С. 73-91.

Р/677

Оскільки зловмисники стрімко набувають навиків та здібностей, вони зосереджені на вивченні вразливостей у веб-додатках та намагаються наразити на небезпеку конфіденційність, цілісність та доступність інформаційної системи. Використовуючи атаки з перевіркою коду, хакери можуть викрасти конфіденційні дані, що знижують ринкову вартість організації. У цьому проекті досліджено проблему виявлення та усунення похибок перевірки як клієнтського, так і серверного коду з використанням даного підходу. Запропоновано нову ідею, що сприяє виявленню та усуванню атаки з перевіркою коду з використанням статичного та динамічного аналізу.

Патрікей А. В. Аналіз можливих загроз безпроводовим мережам на базі мікроконтролера ESP8266 / А. В. Патрікей, С. С. Романчук, М. О. Карпець // Зв'язок. – 2018. – № 4. – С. 55-57.

Р/776

У статті виконано аналіз основних технічних засобів і систем, застосовуваних для організації атаки на Wi-Fi мережу. Розкрито структуру мікрочіпа та дано пояснення щодо призначення його компонентів. Наведено технічні характеристики приладу, який слугує для атак на Wi-Fi мережу. Запропоновано варіанти основних і допоміжних видів мікрочіпа. Проаналізовано можливості їх застосування як за допомогою комп'ютера, так і з використанням планшетів, смартфонів чи іншої мобільної техніки.

Підвищення захищеності інформаційно-телекомунікаційних систем шляхом використання TPM-модулів / Г. І. Гайдур, В. А. Козачок, Р. М. Хмелевський, В. Є. Дмітрієв // Сучасний захист інформації. – 2019. – № 1(37). – С. 28-35.

Р/2300

В статті обґрунтована необхідність комплексних систем захисту інформації в інформаційно-телекомунікаційних системах, в яких обробляється інформація з обмеженим доступом. Розглянуті питання забезпечення збереження інформації, що накопичується в окремих файлах і базах даних. Розглянуті основні принципи захисту ресурсних та фізичних об'єктів інформаційних систем.

Підходи до вимірювання та моніторингу мережі для забезпечення перевірки керуючих повідомлень OpenFlow / Г. О. Гринкевич, К. О. Домрачева, С. В. Шелудько, Д. П. Коновалов // Зв'язок. – 2018. – № 5. – С. 30-35.

Р/776

У статті визначено методи моніторингу мережі, на основі яких запропоновано нові схеми виявлення несправностей для SDN і докладний розгляд головних принципів технології OpenFlow. Також представлено концепцію Software-Defined-Networking.

Польгуль Т. Д. Інформаційна технологія побудови інтелектуальних систем виявлення шахрайства при інсталюванні мобільних додатків / Т. Д. Польгуль // Інформаційні технології та комп'ютерна інженерія. – 2019. – № 1. – С. 4-16.

Р/1954

Здійснено інтелектуальну обробку наявних даних по користувачу, на основі якої запропоновано шкалювання не по значенню ознаки, а по кінцевій інформації, яку несе ознака по користувачу. Запропоновано систему з інтелектуальною складовою – формування бази знань, яка дозволить визначити шахраїв, та в яку включатимуться правила аналізу аномалій, при чому так, щоб поява нової аномалії в даних дозволила створити нове правило.

Торошанко О. С. Діагностика та ідентифікація несправностей в телекомунікаційних мережах з розпізнаванням типу відмови / О. С. Торошанко // Телекомунікаційні та інформаційні технології. – 2018. – № 4. – С. 62-70.

Р/1921

Запропоновані методики вибору контрольованих параметрів для досягнення необхідного рівня достовірності перевірки стану телекомунікаційної мережі, визначення їх кількості і послідовності контролю. Розроблено алгоритм ідентифікації завад в лінійних динамічних системах.

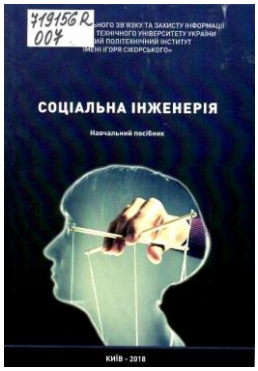
720120 В
621.39

"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] .
№ 2 (54). - Київ, 2019. - 70 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., рос., англ.

Зі змісту:

В статті розглянуто питання підвищення надійності телекомунікаційних мереж майбутнього за рахунок вибору оптимальної побудови телекомунікаційної мережі.

Інформаційне протиборство у воєнних конфліктах. Інформаційно-психологічна безпека



719156 R
007

Богданов, Олександр Михайлович.
Соціальна інженерія (сучасні технології та шляхи захисту) [Текст] : навч. посіб. для курсантів і асп., що навч. за спец. 172 Телекомунікації та радіотехніка, 122 Комп'ютерні науки та інформ. технології, 125 Кібернетика / Богданов О. М., Петрик В. М. ; за заг. ред. В. М. Петрика ; Ін-т спец. зв'язку та захисту інформації НТУ України "КПІ ім. І. Сікорського". - Київ : ІСЗЗІ КПІ ім. І. Сікорського, 2018. - 78 с. : табл. - Бібліогр. в кінці розд. - Авт. зазнач. на звороті тит. арк.

У навчальному посібнику розглядаються сучасне застосування, основні методи, головні вектори та види атак з використанням соціальної інженерії. Також розкриваються базові методи і заходи захисту від атак, які проводяться за допомогою соціальної інженерії.

Богданович В. Ю. В павутинні інформаційних технологій / В. Ю. Богданович, Б. А. Воровich // Оборонний вісник. – 2019. – № 8. – С. 10-15.

Р/1134

Для успішного протистояння зовнішнім і внутрішнім ризикам та забезпечення надійного захисту національних інтересів держави необхідно ретельно вивчати вплив глобальної інформаційної системи на воєнну безпеку суспільства як найважливішої складової безпеки країни.
"Поняття "мирний і воєнний стан" переплелося в віртуальному просторі, породивши страшне явище "інформаційна війна", яка здатна втягнути в ареал воєнно-інформаційних дій мільйони людей за стислий період часу".

719048 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. - К. : [ВІКНУ].
Вип. № 61. - Київ, 2018. - 216 с. : іл. - Бібліогр. наприкінці ст. - Текст кн. укр., рос., англ.

Зі змісту:
Нікіфоров М. М., Пампуха І. В., Лоза В. М. **Аналіз загроз воєнної безпеки в інформаційній сфері та протидії в умовах ведення гібридної війни.** – С. 135-142.

Гребенюк М. В. Актуальні проблеми забезпечення інформаційної безпеки електоральних процесів: аналіз зарубіжного досвіду / М. В. Гребенюк, Б. Д. Леонов // Інформація і право. – 2019. – № 1(28). – С. 100-107.

Р/844

У статті аналізується зарубіжний досвід забезпечення інформаційної безпеки електоральних процесів. Висвітлюються проблеми боротьби з фейковими аккаунтами та деструктивною пропагандою у вітчизняному інформаційному просторі. Аналізуються законодавчі ініціативи США та окремих країн ЄС у сфері забезпечення інформаційної безпеки.

Гребенюк М. В. Проблеми протидії поширенню деструктивної пропаганди та дезінформації напередодні виборів: аналіз досвіду ЄС / М. В. Гребенюк, Б. Д. Леонов // Інформація і право. – 2019. – № 2(29). – С. 82-89.

Р/844

У статті аналізується досвід ЄС із забезпечення протидії деструктивній пропаганді та дезінформації під час електоральних процесів. Висвітлюються проблеми боротьби з деструктивною пропагандою у вітчизняному інформаційному просторі. Аналізуються законодавчі ініціативи окремих країн ЄС у сфері інформаційного забезпечення протидії деструктивній пропаганді та дезінформації.

Дослідження моделі міжнародного інформаційного простору з метою пошуку ефективних механізмів захисту національного інформаційного простору/ О. В. Серпухов, О. А. Макогон, С. А. Новік [та ін.] // Системи управління, навігації та зв'язку. – 2018. – Вип. 6. – С. 116-121.

Р/2152

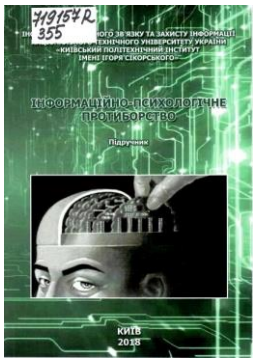
У роботі проведено дослідження моделі міжнародного інформаційного простору з метою аналіза деструктивних впливів та пошуку шляхів протидії дискредитації України на міжнародному рівні.

718984 R
355

Информационное противоборство в современных условиях [Текст] : монография / Л. Г. Пирцхалава, В. А. Хорошко, Ю. Е. Хохлачева, М. Е. Шелест ; под ред. В. А. Хорошко. - Киев : Компринт, 2019. - 226 с. : іл. - Бібліогр.: с. 218-225 (127 назв).

В монографии рассматривается широкий круг проблем, связанных с формированием определенных идеологических взглядов, представлений, убеждений, которые вызывают у людей одновременно положительные или отрицательные эмоции, чувства и бурные массовые реакции.

В современных условиях информационное противоборство превратилось в одно из наиболее эффективных средств войны между государствами.



719157 R
355

Інформаційно-психологічне протиборство [Текст] : підручник для курсантів і асп., що навч. за спец. 172 Телекомунікації та радіотехніка, 122 Комп'ютерні науки та інформ. технології, 125 Кібернетика / [В. М. Петрик, М. М. Присяжнюк, Я. М. Жарков та ін. ; за заг. ред. В. М. Петрика] ; Ін-т спец. зв'язку та захисту інформації НТУ України "КПІ ім. І. Сікорського". - Київ : ІСЗЗІ КПІ ім. І. Сікорського, 2018. - 387 с. : іл. - Бібліогр.: с. 370-378. - Імен. покажч.: с.379-380. - Предм. покажч.: с. 381-382. - Авт. зазнач. на звороті тит. арк.

У підручнику розкриваються концептуальні основи інформаційної безпеки держави та еволюція інформаційно-психологічного протиборства. Розглядаються особливості сучасного етапу інформаційно-психологічного протиборства.

Методичний підхід до кластеризації інформаційних повідомлень в ході протидії інформаційно-психологічним впливам противника / Г. В. Пєвцов, С. В. Залкін, С. О. Сідченко, К. І. Хударковський // Наука і техніка Повітряних Сил Збройних Сил України. – 2019. – № 2. – С. 39-46.

Р/2266

У статті запропонований методичний підхід до кластеризації інформаційних повідомлень, використання якого під час виконання заходів з протидії інформаційно-психологічним впливам противника дозволить прискорити виконання циклу Джона Бойда (петлі OODA – Observation, Orientation, Decision, Action).

Мороз Л. Критичність мислення як чинник зниження рівня тривоги в умовах інформаційно-психологічної війни / Л. Мороз, С. Яковенко // Вісник Київського національного університету імені Тараса Шевченка. Серія: Військово-спеціальні науки. – 2018. – № 3(40). – С. 33-38.

Р/1276

З'ясовується можливість та доцільність застосування екологічного підходу для розуміння психічного стану населення, яке вважає себе потерпілим внаслідок інформаційно-психологічної війни, яку ведуть проти України ЗМІ РФ.

Писарчук А. А. Особенности информационного воздействия, реализуемого в киберпространстве / А. А. Писарчук, О. В. Мороз, А. М. Баланчук // Вісник Інженерної академії України. – 2019. – № 1. – С. 65-70.

Р/1139

В статье рассмотрены особенности информационного воздействия, вызванные развитием современных информационных технологий и поляризацией киберпространства. Выявленные особенности позволяют сделать предположение о бифуркационной модели отклика социума на информационное воздействие.

Планування інформаційно-психологічної операції на основі реалізації циклів Бойда / Г. В. Пєвцов, С. В. Залкін, С. О. Сідченко, К. І. Хударковський // Наука і техніка Повітряних Сил Збройних Сил України. – 2019. – № 1. – С. 23-29.

Р/2266

У статті представлені результати аналізу керівних і доктринальних документів збройних сил провідних країн світу, визначено, що типовою моделлю циклу прийняття рішень в системах управління є цикл Джона Бойда або петля OODA (Observation, Orientation, Decision, Action), яка задовольняє вимогам оптимальності та обґрунтованості. Запропоновано методологічний підхід до планування і управління інформаційно-психологічною операцією (інформаційно-психологічними впливами) на основі реалізації циклів Дж. Бойда.

Принципи, методи і технології ведення збройної боротьби, управління силами і засобами в умовах активного інформаційного протиборства конфліктуючих сторін / Д. А. Гриб, Б. О. Демідов, Ю. Ф. Кучеренко [та ін.] // Наука і техніка Повітряних Сил Збройних Сил України. – 2019. – № 1. – С. 12-22.

Р/2266

У статті розглядаються проблемні питання ведення активного інформаційного протиборства конфліктуючих сторін в динаміці антагоністичного конфлікту при реалізації конфліктно-сталого управління силами і засобами угруповань збройних сил, а також питання управління структурною динамікою складних систем військового призначення.

Рекунков И. С. Разрушающие программные воздействия на информационно-телекоммуникационные системы – новая форма информационной войны / И. С. Рекунков // Вопросы защиты информации. – 2019. – № 2. – С. 41-44.

Р/0171

Описывается применение разрушающих программных воздействий для поражения информационно-телекоммуникационных систем как новой формы информационной войны.

719342 В
33

Стратегічні пріоритети [Текст] = Strategic priorities : науково-аналітичний щоквартальний зб. / Національний ін-т стратегічних досліджень. - [Київ] : [НІСД].
№ 1 (49). - [Київ], 2019. - 136 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., рос., англ.

Зі змісту:

Ауліна О. В. **Специфіка застосування асиметричних підходів в інформаційному протиборстві.** – С. 37-43.
У сучасних умовах асиметричні алгоритми активно використовуються під час проведення інформаційно-психологічних операцій (ІПСО). За допомогою порівняно невеликої кількості інформаційних технологій під час ІПСО здійснюється обернено пропорційний вплив на колективну та індивідуальну свідомість. У результаті потенційно можливою стає кардинальна зміна ситуації навіть в цілому у сфері глобальної безпеки.

716749 В
623

Сучасна спеціальна техніка [Текст] : науково-практичний журнал / Державний н.-д. ін-т МВС України. - К. : [Видавець ФОП Горбенко Ю. В.].
№ 2 (53). - К., 2018. - 140 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., англ.

Зі змісту:

Пирцхалава Л. Г., Хорошко В. А., Хохлачова Ю. Е. **Информационные атаки и модель рисков в информационном противоборстве.** – С. 44-50.
«Проблема информационного противоборства в связи с агрессивными действиями России против Украины и Грузии вызывает особый интерес. Это информационно-психологическая война нового типа, объектом которой является сознание людей и общества».

Фурашев В. М. Маніпуляції свідомістю людини як основний спосіб ведення передвиборчих кампаній / В. М. Фурашев, О. А. Самчинська // Інформація і право. – 2019. – № 3(30). – С. 119-125.

Р/844

Дослідження сутності маніпуляцій як основного способу ведення політичної кампанії на виборах.

Хорошко В. Інформаційна війна. Захист від деструктивних інформаційно-психологічних впливів. Частина 2 / В. Хорошко, Ю. Хохлачова // Безпека інформації. – 2019. – Т. 25, № 1. – С. 18-23.

Р/1408

У ході проведеного дослідження було сформовано рекомендації щодо протистояння інформаційній війні. Проведено аналіз факторів інформаційних впливів та протидія інформаційній зброї.

Кібербезпека – проблема XXI століття

Алексєєв М. М. Небезпечний бік кіберпростору / М. М. Алексєєв, О. В. Устименко // Оборонний вісник. – 2019. – № 4. – С. 10-13.

Р/1134

Кіберзагрози стали повсякденним атрибутом сучасного життя та серйозним викликом національній безпеці будь-якої країни, тож необхідні інвестиції в кібербезпеку для забезпечення надійного захисту критичної інформаційної інфраструктури держави.

716900 В
004

Безпека соціально-економічних процесів в кіберпросторі [Текст] : матеріали Всеукр. наук.-практ. конф., Київ, 27 березня 2019 р. / Київський нац. торг.-екон. ун-т, Департамент кіберполіції Нац. поліції України, Майкрософт Україна, Чернів. нац. ун-т ім. Федьковича. - К. : [КНТЕУ], 2019. - 244 с. - БІбліогр. в кінці ст. - Текст кн. укр., англ.

Збірник матеріалів учасників Всеукраїнської науково-практичної конференції «Безпека соціально-економічних процесів в кіберпросторі» присвячений актуальним питанням у сфері економічного, соціального, нормативно-правового, адміністративного безпечного функціонування кіберпростору, технічного забезпечення кібербезпеки, боротьби із кіберзлочинністю, захисту інформації в комп'ютерних системах і мережах.

Біленчук П. Д. Сучасні комп'ютерні злочинці та кібертерористи: новітні технології на службі організованого злочинного світу / П. Д. Біленчук, М. І. Малій // Бизнес и безопасность. – 2019. – № 4. – С. 2-4.

Р/1070

Світова спільнота на світанку XXI століття остаточно вступила в епоху нового інноваційного цивілізаційного розвитку "Індустрії 4.0", "Четвертої промислової революції" та "Суспільства знань". Новітні ідеї, інновації, знання, наукові розробки стали наріжним каменем, фундаментальною основою розбудови електронного суспільства в галузі культури, освіти, науки, медицини, економіки провідних країн світу.

Блокчейн інфраструктура для захисту кіберсистем / О. С. Адамов, В. І. Хаханов, С. В. Чумаченко, В. Г. Абдуллаєв // Радиоэлектроника и информатика. – 2018. – № 4. – С. 64-85.

Р/1138

Пропонується блокчейн інфраструктура і математичний апарат створення інфраструктури програмно-апаратних телекомунікаційних інформаційних кібернетичних систем (КС), орієнтована на захист від несанціонованого доступу до сервісів, визначений у специфікації системи, шляхом проникнення через легальні інтерфейси взаємодії компонентів, що мають уразливості.

717232 В
621.39

Військовий інститут телекомунікацій та інформатизації Національного технічного університету України "Київський політехнічний інститут".

Збірник наукових праць [Текст] = Collection of Scientsfsc Papers. - К. : [ВІТІ НТУУ "КПІ"].
Вип. № 4. - К., 2018. - 149 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст укр., рос. та англ.

Зі змісту:

Субач І. Ю., Здоренко Ю. М., Фесьоха В. В. **Методика виявлення кібератак типу JS(HTLM)/SCRINJEST на основі застосування математичного апарату теорії нечітких множин.** – С. 125-131.

Шевченко А. С., Самойлов І. В., Пономарьов О. А., Науменко О. Г. **Аналіз застосування штучних нейронних мереж у задачах виявлення кіберзагроз.** – С. 141-146.

Гавловський В. Д. Аналіз стану кіберзлочинності в Україні / В. Д. Гавловський // Інформація і право. – 2019. – № 1(28). – С. 108-117.

Р/844

В статті досліджуються питання, що виникають при формуванні статистичної звітності із протидії кіберзлочинності в Україні. Надано порівняльний аналіз стану кіберзлочинності за 2018 р.

Гавловський В. Д. Захист інформації шляхом посилення ефективності протидії кібератакам / В. Д. Гавловський // Інформація і право. – 2019. – № 3(30). – С. 105-110.

Р/844

У статті розглянуто окремі аспекти захисту інформації шляхом посилення ефективності протидії кібератакам. Проаналізовано стан виконання рішення РНБО України щодо розмежування послідовності розслідування кіберзлочинів.

Гахов С. О. Аналіз методів виявлення подій та інцидентів інформаційної та кібернетичної безпеки SIEM-системами / С. О. Гахов // Сучасний захист інформації. – 2018. – № 4. – С. 11-16.

Р/2300

У статті досліджуються методи автоматичного виявлення подій та інцидентів інформаційної та кібернетичної безпеки SIEM-системами. Розглянуто принципи кореляції вхідних даних та правил, які реалізуються в SIEM-системах. Встановлено перспективний напрямок подальшого розвитку теорії захищених інформаційних систем.

Гончаренко Г. Ю. О некоторых мероприятиях и средствах обеспечения безопасности домашнего сервера / Г. Ю. Гончаренко, Д. А. Ермолатий, К. В. Пителинский // Вопросы защиты информации. – 2019. – № 1. – С. 47-52.

Р/0171

Показано, что обеспечение безопасности сервера – одна из наиболее важных проблем защиты информации. Рассмотрены некоторые меры и средства достижения должного уровня безопасности информационных ресурсов, хранящихся на домашнем сервере.

Гурєєв В. О. Моделювання і візуалізація кібератак в енергетиці з використанням комп'ютерних розподілених тренажерних систем / В. О. Гурєєв, Є. М. Лисенко, О. В. Аветісян // Електронне моделювання. – 2019. – Т. 41, № 1 – С. 81-91. – Текст рос.

Р/518

Розглянуто питання синтезу і динамічних відеограм для паралельного відображення результатів моделювання режимів роботи великих електроенергетичних систем і потенціальних кібератак з використанням розподілених тренажерних систем підготовки оперативно-диспетчерського персоналу в енергетиці.

Гуцалюк М. В. Сучасні тенденції організованої кіберзлочинності / М. В. Гуцалюк // Інформація і право. – 2019. – № 1(28). – С. 118-128.

Р/844

В статті досліджуються сучасні тенденції кіберзлочинності, зокрема організовані її форми. Пропонуються заходи щодо посилення протидії кіберзлочинності.

Если мы не будем охотиться за угрозами, они будут охотиться за нами // Сети и бизнес. – 2019. – № 3. – С. 68-69.

Р/1698

Про упереджувальний підхід (Threat Hunting) до виявлення загроз безпеці: досвід і стратегія компанії "Світ ІТ".

719605 В
004

Журавська, Ірина Миколаївна.
Гетерогенні комп'ютерні мережі критичного застосування на основі роїв та зграй БПЛА [Текст] : монографія / Ірина Журавська ; Чорноморський державний університет імені Петра Могили. - Миколаїв : ЧНУ, 2019. - 192 с. : граф., рис., табл. - Бібліогр.: с. 170-190. - Алф. покажч.: с. 191.

Монографія написана в актуальній галузі, що швидко розвивається та пов'язана зі створенням і функціонуванням гетерогенних комп'ютерних мереж, побудованих на основі зграй і суб-роїв безпілотних літальних апаратів (БПЛА). Розглянуто питання використання моніторингових і технологічних мереж критичного застосування, обумовленого виходом з ладу або втратою управління окремими БПЛА. Також здійснено розвиток, створення нових і тестування алгоритмів, здатних зменшити обсяг обчислювальної потужності, засобів зв'язку і втручання людини, необхідних для виконання безпілотними літальними апаратами мікрозавдань, таких як запобігання зіткнень у критичних ситуаціях, у т.ч. у навколишньому середовищі, перевантаженому перешкодами. Основу монографії становить матеріал, підготовленої до захисту докторської дисертації. У монографії проаналізовано загальні питання підвищення ефективності функціонування та подовження часу життя різноманітних об'єктів зазначених комп'ютерних мереж, вузлів БПЛА з різними конструкціями та схемотехнічними рішеннями. Детально розглянуто особливості забезпечення стабільності зв'язку, поліпшення захищеності даних, що передаються між компонентами кіберфізичної системи (CPS) бездротовими каналами зв'язку та рівномірного навантаження компонентів обчислювальної плати на БПЛА у керованому або автономному режимах функціонування. Проведено аналіз систем та способів енергоживлення БПЛА і сформульовано перспективи вдосконалення таких систем.

Зідан А. М. Аналіз недоліків систем автоматизованого захисту інформації підприємства відносно інсайдерських атак та методи вдосконалення захисту / А. М. Зідан, А. М. Котенко // Сучасний захист інформації. – 2019. – № 1(37). – С. 48-52.

Р/2300

В статті розглянуто та проведений аналіз методів автоматизованого захисту інформації підприємства. Визначені недоліки систем автоматизованого захисту та запропоновані методи вдосконалення захисту.

Зубок В. Ю. Оцінювання ризику кібератак на глобальну маршрутизацію / В. Ю. Зубок // Електронне моделювання. – 2019. – Т. 41, № 2. – С. 97-109.

Р/518

Запропоновано нові теоретичні підходи щодо виявлення та оцінки ризику захоплення маршрутів. На основі єдиного методичного підходу [1] проведено систематизацію та класифікацію загроз, спричинених атаками на глобальну маршрутизацію. Запропоновано класичний підхід STRIDE до класифікації загроз безпеці маршрутизації та модель DREAD для оцінки кожної загрози за класифікацією STRIDE.

Зубок В. Ю. Поєднання традиційних методів і метричного підходу до оцінки ризиків від кібератак на глобальну маршрутизацію / В. Ю. Зубок // Реєстрація, зберігання і обробка даних. – 2019. – Т. 21, № 2. – С. 41-48.

Р/1346

Запропоновано класифікацію загроз, ідентифікацію та оцінку ризиків перехоплення маршруту за допомогою комбінованого підходу до відомих моделей STRIDE та DREAD. Зроблено формальний опис двовимірної моделі оцінки ризику.

Інформаційна безпека: ключові загрози та засоби запобігання // І. Є. Андрущак, В. А. Кошелюк, А. А. Ящук [та ін.] // Комп'ютерно-інтегровані технології: освіта, наука, виробництво. – 2019. – № 35. – С. 5-9. – Текст англ.

Р/2346

В статті приведено обґрунтування проведення інформаційного аналізу тенденцій розвитку кібератак. Виділені фактори, що, найімовірніше, найбільше позначаються на коливаннях інтенсивності атак. Проведений аналіз факторів впливу на кількість кібератак на інформаційну безпеку web-ресурсів за останні кілька років.

717358 В
004

Інформаційні системи та мережі [Текст] : [зб. наук. пр.] / відп. ред. Н. І. Чухрай. - Л. : Вид-во Львів. політехніки, 2018. - 168 с. : іл., табл. - (Вісник / "Львівська політехніка", Національний університет; № 901). - Бібліогр. наприкінці ст. - Текст кн. укр. та англ.

Зі змісту:

Дудикевич В. Б., Микитин Г. В., Ребець А. І. **До проблеми управління комплексною системою безпеки кіберфізичних систем.** – С. 10-21.
Проаналізовано моделі управління інформаційною безпекою (ІБ) кіберфізичних систем (КФС) згідно з ISO/IEC TR 13335 та ISO/IEC 27001, що є підґрунтям розвитку методології управління комплексною системою безпеки (КСБ) в рамках моделі управління "плануй – виконуй – перевіряй – дій".

Кібераудит: примха чи необхідність? / колектив експертів консалтингової компанії "СІДКОН" // Бизнес и безопасность. – 2019. – № 4. – С. 7-9. – https://sidcon.com.ua/

Р/1070

У сучасному глобалізованому світі інформаційні технології стають невід'ємною частиною будь-якої бізнес діяльності. Бажаючи залишитися конкурентними, компанії активно використовують нові можливості, які надає кіберпростір. Разом з цим, вони стають більш уразливими до ризиків, адже кіберпростір стає також привабливим і для злочинців.

Кіберзагрози в електроенергетичних системах України / Ю. Г. Куцан, В. О. Гурєєв, Є. М. Лисенко, О. В. Аветісян // Електронне моделювання. – 2019. – Т. 41, № 2 – С. 63-80.

Р/518

Дано аналіз функціональної структури електроенергетичних систем (ЕЕС) і енергетичних об'єднань з метою виявлення найвірогідніших місць несанкціонованого впливу кібергзагроз на роботу об'єктів критичної інфраструктури.

Корченко О. Г. Стаціонарні системи виявлення і попередження кібератак в інтересах кіберзахисту та кіберконтррозвідки (на прикладі США) / О. Г. Корченко, І. Логінов, С. Скворцов // Безпека інформації. – 2019. – Т. 25, № 1. – С. 5-12.

Р/1408

... у статті викладено результати вивчення зарубіжного досвіду побудови систем виявлення і попередження кібератак в інтересах кіберзахисту і кіберконтррозвідки, визначено їх сутнісні характеристики, які доцільно врахувати у практичній діяльності з розбудови національної системи забезпечення кібербезпеки.

Криклій О. А. Внутрішній аудит як превентивна складова в системі кібербезпеки банку / О. А. Криклій, Л. Д. Павленко // Облік і фінанси. – 2019. – № 2. – С. 124-133.

Р/1875

Мета статті полягає у розробці теоретико-методичних основ системи внутрішнього аудиту кібербезпеки банку, з деталізацією її складових та науковому обґрунтуванні принципів функціонування, на основі чого можна було б вирішувати завдання забезпечення ефективного контролю кібербезпеки.

719204 R
004

Ланде, Д. В.
Основи теорії і практики інтелектуального аналізу даних у сфері кібербезпеки [Текст] : навч. посіб. / Д. В. Ланде, І. Ю. Субач, Ю. Є. Бояринова ; Ін-т спец. зв'язку та захисту інформації НТУ України "КПІ ім. І. Сікорського" . - Київ : ІСЗЗІ КПІ ім. І. Сікорського, 2018. - 298 с. : граф., рис., табл. - Бібліогр. в кінці розд. - Предм. покажч.: с. 297.

У навчальному посібнику розглядаються базові питання теорії і практики інтелектуального аналізу даних: алгоритми, моделі, задачі класифікації, кластерного аналізу, пошуку, глибинного аналізу даних (Data Mining), теорії складних мереж (Complex Networks), а також приводяться відомості, необхідні для математичного і комп'ютерного моделювання та аналізу складних систем і мереж в сфері кібербезпеки.

Видання призначено для студентів, курсантів і аспірантів закладів вищої освіти, які навчаються за спеціальністю 122 Комп'ютерні науки, а також дослідників і наукових співробітників, що працюють у сфері кібербезпеки.

Лисенко С. М. Метод та програмні засоби виявлення кібератаки типу R.U.D.Y. на основі використання алгоритму визначення самоподібності трафіку / С. М. Лисенко, В. А. Ткачук // Вісник Хмельницького національного університету. Серія: Технічні науки. – 2019. – № 3. – С. 180-187.

Р/1055«Т»

В роботі представлено метод виявлення DoS-атаки типу R.U.D.Y. на основі використання алгоритму визначення самоподібності мережевого трафіку. Використання запропонованого методу дозволяє здійснювати виявлення DoS-атаки на прикладному рівні моделі OSI. Запропонований метод може бути основою для побудови програмного забезпечення систем виявлення кібератак.

Мілов О. В. Адаптивні системи підтримки прийняття рішень в кібербезпеці / О. В. Мілов // Сучасні інформаційні системи = Advanced Information Systems. – 2019. – Т. 3, № 1. – С. 131-135. – Текст англ.

Р/543

Мета – розробка базових принципів і моделей, що лежать в основі функціонування адаптивних систем підтримки прийняття рішень в області кібербезпеки.

Модель оцінки впливу загроз на стан захищеності систем електронних комунікацій / А. С. Сторчак, П. Г. Сидоркін, А. В. Микитюк, С. В. Сальник // Системи озброєння і військова техніка. – 2019. – № 2(58). – С. 46-54.

Р/1903

"Метою статті є побудова моделі оцінки впливу загроз на стан захищеності систем електронних комунікацій для її подальшого застосування при розробці методів оцінки стану захищеності інформаційних ресурсів на основі даних про кібератаки в Національній системі кібербезпеки".

Модель фінансування засобів кібербезпеки SMART CITY з процедурою отримання додаткових даних стороною захисту / В. Лахно, В. Малюков, Д. Касаткін [та ін.] // Безпека інформації. – 2019. – Т. 25, № 1. – С. 38-44.

Р/1408

У статті викладена модель вибору стратегій фінансування засобів кібербезпеки Smart City при неповній інформації про фінансові ресурси атакуючої сторони.

Мохор В. В. Методи оцінки сумарного ризику кібербезпеки об'єктів критичної інфраструктури / В. В. Мохор, С. Ф. Гончар, О. М. Дибач // Ядерна та радіаційна безпека. – 2019. – № 2. – С. 4-8.

Р/1232

У роботі наведені результати аналізу вітчизняної та зарубіжної літератури за темою методів оцінки ризиків кібербезпеки, у тому числі об'єктів критичної інфраструктури. У роботі запропоновано графічний та аналітичний методи оцінки сумарного ризику кібербезпеки інформаційних систем, у тому числі об'єктів критичної інфраструктури. Зазначені методи оцінки сумарного ризику базуються на визначенні максимальних значень наслідків для кожного ризику.

Романюков М. Г. Метод розрахунку оптимальності витрат на інформаційну та кібербезпеку / М. Г. Романюков // Радіоелектроніка, інформатика, управління. – 2019. – № 2. – С. 167-176.

Р/0170

Мета роботи. Отримати метод по розрахунку оптимального коефіцієнту витрат на інформаційну та кібербезпеку об'єктів інформаційної діяльності, де циркулює інформація з обмеженим доступом.

Скворцов В. Э. Практика обеспечения функциональной безопасности системы защиты информации промышленного объекта / В. Э. Скворцов, В. И. Василец // Вопросы защиты информации. – 2019. – № 2. – С. 45-48.

Р/0171

Рассмотрены контуры системного подхода к обоснованию и оценке функциональной безопасности системы защиты информации промышленного объекта.

717222 В
33

Стратегічні пріоритети [Текст] = Strategic priorities : науково-аналітичний щокварт. зб. / Національний ін-т стратегічних досліджень. - [К.] : [НІСД].
№ 3-4 (48). - [К.], 2018. - 160 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., рос., англ.

Зі змісту:

Семенченко А. І., Мялковський Д. В., Станіславський Т. В. **Концептуальні засади огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури.** – С. 36-45.

Огляд стану кіберзахисту є однією із складових частин Комплексного огляду сектору безпеки та оборони. Він, серед інших видів огляду, вперше визначений в Законі України «Про національну безпеку України».

Ткаченко В. Когда заговорило кибероружие / В. Ткаченко // Сети и бизнес : Телекоммуникации и сети – технологии и рынок. – 2019. – № 4(107). – С. 60-63.

Р/1698

Стали известны детали атаки вируса Stuxnet – вероятно, первого в истории компьютерного взлома в политических целях. В последние годы зоной кибервойн стала Украина.

Ткаченко В. SOC, или Наука управления безопасностью / В. Ткаченко // Сети и бизнес : Телекоммуникации и сети – технологии и рынок. – 2019. – № 4(107). – С. 50-56.

Р/1698

Задача SOC – отследить и пресечь любой инцидент или атаку, лучше всего еще до ее начала. В будущем это будет происходить автоматически, но пока основная проблема – кадры.

Усов Я. Проблеми захищеності інформаційного середовища / Я. Усов // Технічні науки та технології. – 2019. – № 1. – С. 145-151.

Р/1125

У статті висвітлено проблеми захищеності інформаційного середовища, запропоновано аналіз низки звітів провідних організацій у сфері захисту інформації щодо загроз кібербезпеці за останній рік, сформульовано означення захищеного інформаційного середовища (ІС) та виділено його складові.

Шуклін Г. В. Теоретичні засади державного регулювання кібербезпеки на фондовому ринку: механізми, методи, інструменти / Г. В. Шуклін, О. В. Барабаш // Сучасний захист інформації. – 2018. – № 3. – С. 16-22.

Р/2300

Досліджено поняття "державного регулювання кібербезпеки", наведено власне визначення державного регулювання кібербезпеки, яке необхідно розглядати як систему, яка здійснює цілеспрямований вплив органів державної влади на рівень розвитку інформаційно-телекомунікаційних систем, з'ясовано зміст поняття "державне регулювання кібербезпеки фондового ринку", визначено механізм, методи та інструменти. Запропоновано математичну модель прогнозування кібернетичних атак.

Юрчук Л. П. Кібербезпека в країнах Азії / Л. П. Юрчук, Ю. І. Хлапонін // Бизнес и безопасность. – 2019. – № 3. – С. 29-31.

Р/1070

Кожна країна вирішує питання захисту з урахуванням національних особливостей. Країни Східної Азії мають високий темп розвитку інформаційних технологій, тому дослідження стану кібербезпеки цих країн розширює можливості поліпшення стану кібербезпеки в Україні.

Заголовки статті:

Стан кібербезпеки в Японії
Стан кібербезпеки в Китаї
Стан кібербезпеки в Південній Кореї.