Тематична виставка
"Безпека та захист інформаційного простору "

(надходження II півр. 2018)

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

Аванесова І. Інформаційна безпека у системі захисту прав споживачів фінансових послуг / І. Аванесова // Вісник Київського національного торговельно-економічного університету. – 2018. – № 2. – С. 55-66.

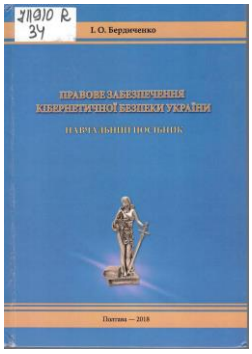
Р/1193

Розкрито основи теоретичного сприйняття інформаційної безпеки споживачів фінансових послуг як складової системи захисту їх прав та інтересів, яка ґрунтується на постулатах «об'єднана відповідальність» та «формалізація».

Аносов А. О. Інформаційно-орієнтована модель як реалізація методики виявлення впливу на достовірність інформації в інформаційному просторі / А. О. Аносов, З. М. Пузняк // Сучасний захист інформації. – 2017. – № 4. – С. 55-59.

Р/2300

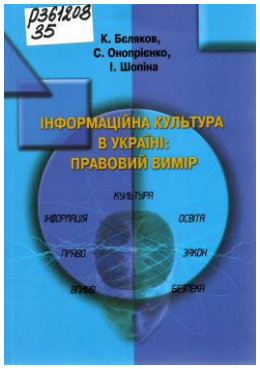
Розглянуто характеристики інформаційного простору, визначено критерії оцінки достовірності інформації в інформаційному просторі. Також запропонована і розглянута інформаційно-орієнтована модель як реалізація методики виявлення впливу на достовірність інформації.



711910 R
34

Бердиченко, Ірина Олегівна.
Правове забезпечення кібернетичної безпеки України [Текст] : навч. посібник / І. О. Бердиченко. - Полтава : [Вид-во ТОВ "Копі-центр"], 2018. - 128 с. : рис. - Бібліогр.: с. 120-126 (88 назв).

У представленому виданні зроблено спробу узагальнити нові теоретичні здобутки та існуючу практику протидії кібернетичній злочинності в Україні, що відображена лекційними темами з розробленого авторкою навчального спецкурсу «Правове забезпечення кібернетичної безпеки України» для студентів магістратури за спеціальністю «право». Навчальний посібник містить теоретико-прикладний навчальний матеріал, що стане в нагоді не лише здобувачам відповідного рівня освіти, а й практикуючим юристам, зокрема у сфері кібернетичної безпеки.



Р 361208
35

Бєляков, Костянтин Іванович.
Інформаційна культура в Україні: правовий вимір [Текст] : [монографія] / К. Бєляков, С. Онопрієнко, І. Шопіна ; [за заг. ред. К. І. Бєлякова] ; Науково-дослідний ін-т інформатики і права Нац. академії правових наук України. - К. : КВІЦ, 2018. - 170 с. - Бібліогр.: с. 148-169 та у виносках . - Дод. тит. арк англ.

У монографії висвітлюється феномен інформаційної культури на міждисциплінарному рівні з акцентом на інформаційно-правові дослідження. Аналізуються перспективи впровадження міжнародного досвіду організаційно-правового забезпечення та пропонуються шляхи підвищення ефективності формування інформаційної культури в контексті удосконалення чинного національного законодавства та діяльності органів виконавчої влади України. Інформаційна культура розглядається як засіб протидії негативним інформаційним впливам та елемент інформаційної безпеки людини, суспільства, держави.

Гребенніков А. Б. Аналіз використання моделей зрілості процесів в ході оцінювання рівня інформаційної безпеки / А. Б. Гребенніков, Ю. М. Щебланін // Сучасний захист інформації. – 2018. – № 1. – С. 33-37.

Р/2300

В роботі проаналізовано методику оцінки інформаційної безпеки підприємства на базі моделей зрілості процесів інформаційної безпеки та запропоновано рекомендації щодо їх впровадження.

Грищук Р. Методологія побудови системи забезпечення інформаційної безпеки банківської інформації в автоматизованих банківських системах / Р. Грищук, С. Євсеєв // Безпека інформації. – 2017. – Т. 23, № 3. – С. 204-214.

Р/1408

Методологія з єдиних системних позицій дозволяє здійснювати побудову системи забезпечення інформаційної безпеки банківської інформації. В основу методології покладено запропоновану концепцію побудови синергетичної моделі загроз інформаційній безпеці банківської інформації в автоматизованих банківських системах.

Б 18851
32

Державно-приватне партнерство в сфері кібербезпеки: **міжнародний досвід та можливості для України** [Текст] : аналітична доповідь / [авт. кол.: Дубов Д. В., Бойко В. О., Гнатюк С. Л. та ін. ; за заг. ред. Д. Дубова] ; Нац. ін-т стратегічних досліджень. - К. : [НІСД], 2018. - 82 с. - Бібліогр. у виносках. - Авт. зазнач. на звороті тит. арк.

Аналітична доповідь присвячена питанням формування ефективного державно-приватного партнерства з питань кібербезпеки. Проаналізовано теоретичні підходи до державно-приватного партнерства та їх особливості в питаннях кібербезпекової сфери. Досліджено світовий досвід (США, ЄС, Німеччини, Великої Британії, Польщі) із розбудови довіри між державним та приватним сектором з питань безпеки кіберпростору. ***Розглянуто нормативно-правові та організаційні основи державно-приватного партнерства в Україні,*** наведено ефективні приклади такого партнерства. Окреслено перспективні напрямки розвитку кібербезпекового державно-приватного партнерства в Україні та можливі шляхи їх імплементації.

Довгань О. Д. Система інформаційної безпеки України: онтологічні виміри / О. Д. Довгань, Т. Ю. Ткачук // Інформація і право. – 2018. – № 1. – С. 89-103.

Р/844

У статті досліджується зміст категорії «система інформаційної безпеки» та визначаються складові відповідної системи, а також обґрунтовується необхідність розмежування системи інформаційної безпеки та системи забезпечення інформаційної безпеки.

Р 360907
004

Дудикевич, Валерій Богданович.
Основи інформаційної безпеки [Текст] : навч. посіб. / В. Б. Дудикевич, В. О. Хорошко, Ю. Є. Яремчук ; Вінницький національний технічний університет. - Вінниця : ВНТУ, 2018. - 316 с. : рис., табл. - Бібліогр.: с. 301-303.

У посібнику наводяться суть, підходи забезпечення та основні особливості інформаційної безпеки. Розглядаються основні поняття та положення інформаційної безпеки, концепції та моделі інформаційної безпеки, найпоширеніші загрози та методологія формування множини загроз інформації, критерії оцінювання безпеки інформації, політика інформаційної безпеки, основні поняття та етапи керування ризиками інформації, керування доступом до інформації та безпекою інформаційних технологій, основні програмні та технічні заходи забезпечення інформаційної безпеки.

Р 360880
35

Забезпечення інформаційної безпеки держави [Текст] : навч. посіб. / [В. Б. Дудикевич, І. Р. Опірський, П. І. Гаранюк та ін.] ; Національний університет "Львівська політехніка". - Львів : Видавництво Львівської політехніки, 2017. – 204 с. : табл. - Бібліогр.: с. 200-201. - Авт. зазнач. на звороті тит. арк.

Наведено сучасні погляди на стан та забезпечення інформаційної безпеки особистості, суспільства та держави. Інформаційна безпека особистості – це насамперед захищеність психіки і свідомості людини від небезпечних інформаційних впливів: маніпулювання свідомістю, дезінформування, спонукання до самогубства, образ тощо. Інформаційна безпека держави (суспільства) характеризується мірою захищеності держави (суспільства) та стійкості основних сфер життєдіяльності (політики, економіки, науки, техносфери, сфери управління, військової сфери і т. ін.) відносно небезпечних інформаційних впливів, причому як з упровадження, так і добування інформації. Інформаційна безпека держави – це здатність нейтралізувати такі впливи.

Золотар О. О. Генеза суспільних відносин щодо інформаційної безпеки людини / О. О. Золотар // Інформація і право. – 2018. – № 1. – С. 139-148.

Р/844

Досліджуються історичні передумови становлення інституту інформаційної безпеки людини.

Ілляшенко О. О. Оцінювання інформаційної безпеки систем на програмовній логіці з використанням кейсів: таксономія, нотація, концепція / О. О. Ілляшенко // Наука і техніка Повітряних Сил Збройних Сил України. – 2018. – № 2. – С. 97-103.

Р/2266

Робота присвячена аспектам оцінювання безпеки інформаційно-керуючих систем, які використовують програмовну логіку як об’єкт реалізації основних функцій. Для виявлення всіх розбіжностей в процесах оцінювання та забезпечення безпеки розглянуто процесно-продуктну модель оцінювання безпеки. Наведено порівняння існуючих кейсів безпеки. Представлено результати розробки концепції оцінювання інформаційної безпеки систем на програмовній логіці з використання покращених кейсів запевнення інформаційної безпеки.

Климович О. К. Методичні основи оцінки контролю захищеності інформаційно-телекомунікаційної мережі спеціального призначення / О. К. Климович // Системи озброєння і військова техніка. – 2018. – № 1. – С. 143-147.

Р/1903

Дана робота присвячена розгляду методичних основ оцінки контролю захищеності інформаційно-телекомунікаційних мереж спеціального призначення за рахунок використання у якості базового методу аналізу ієрархій та апарату нейро-нечітких мереж для оцінки захищеності мереж даного класу. Наведена узагальнена характеристика основних груп методів оцінки контролю захищеності інформаційно-телекомунікаційних мереж даного класу.

Р 361281
004

Комплексні системи захисту інформації [Текст] : навч. посіб. / [Яремчук Ю. Є. Павловський П. В., Катаєв В. С., Сінюгін В. В.] ; Вінницький національний технічний університет. - Вінниця : ВНТУ, 2018. - 118 с. - Бібліогр.: с. 116-117. - Авт. зазнач. на звороті тит. арк.

В посібнику розглядаються питання, що належать до галузі інформаційної безпеки; висвітлені основи організації захисту інформації, методи оцінювання захищеності та основні положення побудови комплексних систем захисту інформації

Левченко О. В. Концептуальні основи формування системи забезпечення інформаційної безпеки / О. В. Левченко // Наука і техніка Повітряних Сил Збройних Сил України. – 2018. – № 1. – С. 7-12.

Р/2266

У статті обґрунтовано концептуальний підхід до формування системи забезпечення інформаційної безпеки як складової загальнодержавної системи забезпечення воєнної безпеки. Визначено мету, завдання і функції та розроблено принципи побудови даної системи. З позицій системного підходу запропоновано її базову структуру, що складається з функціональних підсистем. Окреслено призначення і завдання кожної підсистеми.

Марущак А. Вплив тіньових інформаційних технологій на інформаційну безпеку суб'єкта господарювання / А. Марущак, О. Скіцько // Безпека інформації. – 2018. – Т. 24, № 1. – С. 69-74.

Р/1408

В статті здійснено аналіз загрози, що набирає все більших масштабів в інформаційній сфері і пов'язана з використанням мобільних або носимих пристроїв (wearable device) на робочому місці. Розроблено визначення «тіньові інформаційні технології» та приведена структура можливих місць прояву відповідної загрози.

Марущак А. І. Інформаційно-правові аспекти протидії кіберзлочинності / А. І. Марущак // Інформація і право. – 2018. – № 1. – С. 127-132.

Р/844

У статті досліджуються питання інформаційно-правових аспектів протидії кіберзлочинності в Україні. Сформульовано пропозиції щодо удосконалення інформаційного та кримінального процесуального законодавства з метою підвищення ефективності розслідування кіберзлочинів правоохоронними органами України.

Марущак А. І. Проблеми розслідування кіберзлочинів в Україні / А. І. Марущак // Економіка. Фінанси. Право. – 2018. – № 1. – С. 23-27.

Р/687

У статті досліджуються проблеми правового регулювання і правозастосування, які не дозволяють ефективно розслідувати кіберзлочини в Україні. Зроблено висновок про необхідність подальшої імплементації положень Конвенції про кіберзлочинність, регламентації механізмів сприяння правоохоронним органам України операторів, провайдерів телекомунікаційних послуг, а також використання можливостей міжнародного співробітництва у розслідуванні кіберзлочинів.

Модель класифікатора об'єктів критичної інформаційної інфраструктури держави / О. Корченко, Ю. Дрейс, О. Романенко, В. Бичков // Захист інформації. – 2018. –Т. 20, № 1. – С. 5-11.

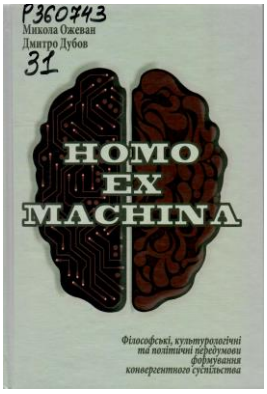
Р/1428

Відповідно до існуючого нормативно-правового забезпечення, пов'язаного з об'єктами критичної інфраструктури, прослідковується неповнота щодо можливості їх коректної класифікації, також не сформований перелік ІТС таких об'єктів, відсутні критерії щодо оцінювання негативних наслідків від кібератак. Вирішення зазначених питань дозволить сформувати такий класифікатор об'єктів критичної інформаційної інфраструктури, який дасть можливість створити умови для підвищення їх стійкості до кібератак. Відповідно до цього пропонується засіб класифікації об'єктів критичної інформаційної інфраструктури.

Носов В. Організаційно-практичні аспекти побудови комплексної системи захисту інформації для системи з інформацією, що публікується в глобальній мережі / В. Носов, І. Манжай // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2017. – Вип. 2. – С. 56-68.

Р/2287

Проаналізовано нормативно-правову базу в сфері побудови комплексної системи захисту інформації. Розглянуто коло суб'єктів, можливі варіанти та послідовність дій власника інформаційно-телекомунікаційної системи щодо розробки та впровадження комплексної системи захисту інформації. Визначено послуги, які надаються виконавцем при створенні та супроводженні комплексної системи захисту інформації. Окреслено окремі елементи контролю відповідної системи, а також проаналізовано орієнтовні час і витрати на її розробку.



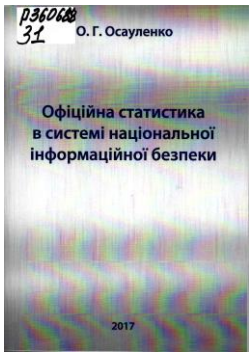
Р 360743
31

Ожеван, Микола Андрійович.
Homo ex Machina. Філософські, культурологічні та політичні передумови формування конвергентного суспільства [Текст] : монографія / Микола Ожеван, Дмитро Дубов ; Нац. ін-т стратегічних досліджень. - К. : [НІСД], 2017. - 272 с. - Бібліогр.: с. 252-271.

…Грунтовно висвітлено проблему перетворення глобального інформаційного суспільства на простір зіткнення та конкуренції держав, вплив сучасних технологій на концепцію державного суверенітету (в межах побудови «цифрового суверенітету»).

Зі змісту:

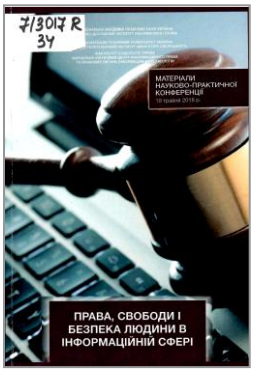
Частина ІІ. **Інформаційне суспільство: вчора, сьогодні, завтра**
Розділ 5. Глобальне інформаційне суспільство як сфера національно-державного домінування: геостратегія творення й подолання цифрових розривів
Розділ 6. Концепція суверенітету та інформаційне суспільство: проблеми реалізації.



Р 360688
31

Осауленко, Олександр Григорович.
Офіційна статистика в системі національної інформаційної безпеки [Текст] : монографія / О. Г. Осауленко. - [К.] : [ТОВ "Август Трейд"], 2017. - 368 с. - Бібліогр.: с. 348-367.

У монографії розглядаються науково-методологічні засади побудови офіційної статистики на міжнародному та національному рівнях з урахуванням її місця і ролі в глобальній системі інформаційної безпеки. Досліджуються проблеми інформаційної безпеки державної статистики як невід'ємної складової національної інформаційної безпеки в цілому. Пропонуються практичні рекомендації щодо нормативно-правових, методичних та організаційно-технічних аспектів безпеки статистичної інформації в контексті вимог інформаційної безпеки держави, суспільства й особи.



713017 R
34

Права, свободи і безпека людини в інформаційній сфері [Текст] : матеріали науково-практичної конференції, 10 травня 2018 р., Київ / Нац. акад. правових наук України, НДІ інформатики і права, Нац. техн. ун-т України "КПІ імені І. Сікорського", Факультет соціології і права, Навчально-науковий центр інформаційного права та правових питань інформаційних технологій. - К. : КПІ ім. Ігоря Сікорського, 2018. - 176 с. - Бібліогр. наприкінці ст. - Текст конф. укр., рос.

Матеріали конференції присвячені розгляду теоретико-правових та практичних питань забезпечення прав, свободи і безпеки людини в інформаційній сфері в сучасних умовах, а також шляхів їх вирішення.

У конференції беруть участь провідні експерти і вчені наукових установ і навчальних закладів, представники зацікавлених державних органів та громадських організацій.

Б 18732
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. 14. - Житомир, 2017. - 187 с. : іл., граф., табл. - Бібліогр. наприкінці ст. - Текст укр., рос., англ.

Зі змісту:

Нетребко Р. В. **Аналіз нормативно-правового забезпечення та методів визначення рівня захищеності інформаційно-телекомунікаційної системи від несанкціонованого доступу**. – С. 79-84.

Радутний О. Е. Штучний інтелект, інформаційна безпека та законотворчий процес (кримінально-правовий аспект) / О. Е. Радутний // Інформація і право. – 2018. – № 1. – С. 149-158.

Р/844

В статті розглянуто недоліки сучасного стану законотворчої діяльності, що межують з проявами інформаційної агресії, та досліджено можливості використання штучного інтелекту під час підготовки законопроектів та експертизи чинних нормативних актів.

Рзаєв Г. І. Нормативно-законодавча підтримка інформаційної безпеки відповідно до потреб економічного аналізу / Г. І. Рзаєв, О. С. Джус // Вісник Хмельницького національного університету. Серія: Економічні науки. – 2018. – № 3, Т.1. – С. 259-264.

Р/1055«Е»

В статті досліджено сутність інформаційної безпеки у розрізі площин її вивчення. Окреслено основні його характеристики та обґрунтовано їх значення. Розглянуто нормативно-законодавчу підтримку інформаційної безпеки підприємства у розрізі Законів України та окреслено сферу їх регулювання.

Рощук М. Розвиток електронного урядування в Україні: правовий аспект забезпечення безпеки інформації / М. Рощук // Безпека інформації. – 2018. – Т. 24, № 1. – С. 17-22.

Р/1408

Проаналізовано національну нормативно-правову базу з питань електронного урядування, зокрема щодо забезпечення інформаційної безпеки держави. Розглянуті організаційно-правові механізми розвитку електронного формату діяльності державних органів, розроблені в рамках відповідних державних програм. Проаналізовано Концепцію розвитку електронного урядування в Україні до 2020 року.

711599 В
005

Системи підтримки прийняття рішень. Теорія і практика [Текст] : зб. доп. наук.-практ. конф. з міжнар. участю, 5 червня 2017, м. Київ, Україна / НАН України, Ін-т проблем математичних машин і систем. - К. : [Вид-во "Юстон"], 2017. - 140 с. : рис., табл. - Авт. покажч.: с. 139. - Бібліогр. наприкінці ст. - Текст укр., рос., англ.

Зі змісту:

Коваленко Т. О., Коваленко О. Є. **Модель знань для управління безпекою інформаційної системи.** – С. 113-116.

«Один із способів використання бази знань в галузі управління безпекою є «підхід заснований на онтології безпеки», який встановлює концептуальні відношення між суб'єктами, які представляють інформацію і мають системний погляд на проблему з метою ідентифікації, аналізу та визначення заходів протидії загрозам безпеки. Багато міжнародних та інших стандартів безпеки і захисту визначають правила для оцінки ризиків і підготовки профілів захисту та цілей безпеки».

Соколов К. О. Аналіз загальних підходів щодо побудови системи інформаційної безпеки / К. О. Соколов // Наука і техніка Збройних Сил України. – 2018. – № 1. – С. 13-17. – Текст англ.

Р/2266

В зазначеній статті було проведено аналіз підходів щодо побудови системи інформаційної безпеки провідних країн світу. Автором пропонується здійснювати синтез системи інформаційної безпеки шляхом формування властивостей системи, вимог до неї та виконуваних функцій; структурним синтезом її системи – формування елементів системи, а після чого здійснювати параметричний синтез системи з визначенням параметрів елементів структури.

Соснін О. В. Безпекові проблеми інформаційно-комунікаційної діяльності: теоретико-правові та праксеологічні аспекти / О. В. Соснін, В. В. Повидиш // Юридична Україна. – 2017. – № 7-8. – С. 60-66.

Р/1880

Виявлення проблем безпеки зростає у зв'язку із розвитком інформаційно-комунікаційних технологій і появою штучного інтелекту, що стає одним із ключових місць у системі забезпечення усіх без винятку життєво важливих інтересів країн. Все це змушує встановлювати більш досконалі норми права, які виникають при зборі, опрацюванні, накопиченні, зберіганні, вилученні, передачі, розподілі та споживанні інформації, особливо за допомогою комп'ютеризованих засобів зв'язку та інструментів штучного інтелекту.

Р 360621
004

Становлення і розвиток правових основ та системи захисту персональних даних в Україні [Текст] : монографія / Пилипчук В. Г., Брижко В. М., Баранов О. А., Мельник К. С. ; НДІ інформатики і права Нац. акад. правових наук України. - Ужгород : [ТОВ "Видавничий дім "Артек"], 2017. - 226 с. - Бібліогр.: с. 117-123.

У науковому виданні на основі історичного та системного аналізу розглядаються актуальні проблеми формування і розвитку правових основ та системи захисту персональних даних в контексті євроінтеграції України. Висвітлюється стан наукової розробки, історико-правові аспекти формування інституту захисту персональних даних, відповідний досвід країн-членів Ради Європи та Європейського Союзу, організаційно-правові проблеми захисту персональних даних в Україні. У додатках наводяться тексти проектів та чинних правових актів у цій сфері.

Б 18735
33

Стратегічні пріоритети [Текст] = Strategic priorities : науково-аналітичний щокварт. зб. / Національний ін-т стратегічних досліджень. - [К.] : [НІСД]. -
№ 4 (45). - [К.], 2017. - 236 с. : граф., рис., табл. - Бібліогр. наприкінці розд. - Текст кн. укр., рос., англ.

Зі змісту:

Жиляєв І. Б., Семенченко А. І. **Організаційно-правові механізми розвитку національної системи кібербезпеки України.** – С. 55-63.

Ткачук Н. А. Організаційно-правові засади формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави / Н. А. Ткачук // Інформація і право. – 2018. – № 1. – С. 133-138.

Р/844

У статті автор досліджує організаційно-правові засади, стан та проблемні питання формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави як важливого елемента системи заходів із забезпечення кіберзахисту та кібербезпеки України.

Ткачук Т. Ю. Забезпечення інформаційної безпеки: досвід окремих країн Східної Європи / Т. Ю. Ткачук // Інформація і право. – 2017. – № 4. – С. 62-72.

Р/844

Стаття присвячена дослідженню питань забезпечення інформаційної безпеки у країнах Східної Європи. В ході дослідження визначаються пріоритети та проблеми забезпечення інформаційної безпеки у вказаних країнах. Також оцінюється значущість досвіду країн Східної Європи у сфері забезпечення інформаційної безпеки для України.

711408 R
34

Фігель, Юлія Осипівна.
Інформаційне право [Текст] : навч. посіб. / Фігель Ю. О. ; Центральна спілка споживчих товариств України, Львівський торговельно-економічний ун-т. - Л. : Вид-во Львів. торг.-екон. ун-ту, 2017. - 262 с. : табл. - Бібліогр. наприкінці тем.

Навчальний посібник відповідає типовій навчальній програмі з навчальної дисципліни «Інформаційне право». Він підготовлений на основі сучасних досягнень науки права, з урахуванням вітчизняного та зарубіжного академічного досвіду, наукових потреб і сучасної практики. Зміст роботи розкриває методологічні та наукові підходи до вивчення й викладання курсу «Інформаційне право».
Для студентів спеціальності «Право», викладачів курсу, а також широкого загалу читачів, які цікавляться суспільними відносинами, що виникають з приводу обігу інформації.

Хлапонін Д. Господарсько-правове забезпечення кібербезпеки в Україні / Д. Хлапонін // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2017. – Вип. 2. – С. 108-115.

Р/2287

… потреба наукової розробки даного напряму обумовлена необхідністю теоретичного обґрунтування, вдосконалення господарсько-правового забезпечення кібербезпеки, напрацювання науково обґрунтованих пропозицій з цього питання та рекомендацій, спрямованих на подальше вдосконалення правозастосовної практики в цій сфері.

Хлапонін Д. Ю. Правові аспекти створення та впровадження систем захисту інформації в Україні / Д. Ю. Хлапонін, Т. В. Німченко // Вісник Інженерної академії України. – 2017. – № 4. – С. 188-191.

Р/1139

Проаналізовано сучасний стан нормативно-правової бази в галузі технічного захисту інформації, наведено деякі протиріччя, які існують в термінології та вимогах нормативно-правових актів з технічного захисту інформації.

Р 360829
004

Юдін, Олександр Костянтинович.
Державні інформаційні ресурси. Методологія побудови та захисту українського сегмента дерева ідентифікаторів [Текст] : [монографія] / О. К. Юдін, С. С. Бучик ; Національний авіаційний ун-т. - К. : [НАУ], 2018. - 319 с. : рис., табл. - Бібліогр.: с. 251-275.

Проведено аналіз існуючого забезпечення захисту державних інформаційних ресурсів (ДІР) в інформаційно-телекомунікаційних системах та українського сегмента дерева ідентифікаторів ДІР, концептуальний аналіз уразливостей ДІР. Визначено правові аспекти формування системи ДІР.

Наведено методологію побудови класифікатора загроз ДІР на основі впровадженого вперше методу «подвійної трійки захисту», яка дала змогу створити дієздатний класифікатор загроз ДІР; моделі та принципи інформаційної безпеки ДІР, основною з яких є загальна модель формування системи захисту ДІР, яка здійснює структурно-логічну схему реалізації системи захисту ДІР методом «подвійної трійки захисту»; методи та моделі реалізації системи управління інформаційної безпеки ДІР, основними з яких є метод визначення рівня ризику застосування контрзаходів щодо визначених ресурсів, метод кластеризації ризиків на основі транзитивного замикання бінарного відношення активів, метод визначення функціональних профілів захищеності вузлів дерева ідентифікаторів ДІР; структурно-логічну модель організації ієрархічної гілки кодів вузлів українського сегмента міжнародного дерева ідентифікаторів об'єктів; технологію побудови та захисту дерева ідентифікаторів ДІР на основі ризик-менеджменту.

Програмні системи захисту інформації

Б 18790
681

Автоматика, вимірювання та керування [Текст] : зб. наук. пр. / голова редакційно-видавничої ради Н. І. Чухрай. - Л. : Вид-во Львів. політехніки, 2017. - 116 с. : граф., рис., табл. - (Вісник / Національний університет "Львівська політехніка" ; № 880). - Бібліогр. наприкінці ст. - Текст укр., англ.

Зі змісту:

Дудикевич В. Б., Березюк Б. М., Піскозуб А. З. **Особливості будови та захисту корпоративних сховищ даних.** – С. 44-50.
Сформульовано базові задачі комплексного захисту корпоративного сховища даних та розглянуто програмно-апаратні засоби їх вирішення.

Струзік В. А., Харкянен О. В., Грибков С. В. **Аналіз засобів забезпечення додаткового захисту корпоративних баз даних.** – С. 60-67.
Проведено огляд та порівняння функціональності та принципів роботи програмних продуктів для підвищення ефективності захисту корпоративних баз та сховищ даних під час їх роботи та рефакторингу.

Вахонин С. DLP vs кейлоггеры = обеспечение безопасности vs нарушение прав граждан / С. Вахонин // Информационная безопасность / Information Security. – 2018. – № 1. – С. 38-39.

Р/365

В июле 2017 года Федеральный суд по трудовым спорам Германии опубликовал судебный вердикт[1], довольно интересный в плане легального практического использования специфических программных продуктов, реализующих функции отслеживания действий сотрудников через запись нажатий на клавиатуре (кейлоггер) и регулярного снятия снимков экрана.

Б 18661
004

Комп'ютерні науки та інформаційні технології [Текст] : [зб. наук. пр.] / гол. ред. Н. І. Чухрай. - Л. : Вид-во Львів. політехніки, 2017. - 324 с. : іл., табл. - (Вісник / Національний університет "Львівська політехніка" ; № 864). - Бібліогр. наприкінці ст. - Текст укр., англ.

Зі змісту:

Лисенко С. М. Метод виявлення троянських програм на основі апарату нечіткої кластеризації / С. М. Лисенко, Ю. О. Гайбура, В. С. Стецюк // Комп’ютерно-інтегровані технології: освіта, наука, виробництво. – 2018. – № 30-31. – С. 75-82.

Р/2346

Робота системи виявлення нових троянських програм здійснюється на основі обробки зібраних системних подій в комп’ютерній системі множини ознак, які вказують на присутність троянських програм в комп’ютерній системі.

Миронюк Т. В. Дослідження методів захисту он-лайн спілкування / Т. В. Миронюк, Л. Т. Дуда // Вісник Черкаського державного технологічного університету. Серія: Технічні науки. – 2017. – № 4. – С. 138-143.

Р/1308

В даній статті розглядаються основні методи захисту он-лайн спілкування на прикладі програм та програмних комплексів для обміну повідомленнями. Досліджуються основні технології захисту особистої інформації в мережі Інтернет. Особлива увага приділяється огляду спеціалізованих програмних продуктів для безпечного обміну повідомленнями інформацією, які присутні зараз на ринку. Описано створення експериментального он-лайн-чату на основі узагальнених потреб та побажань користувачів з урахуванням недоліків подібних програм по безпечності, комфорту користування та надійності. Виділено найбільш важливі проблеми, які потрібно було вирішити при реалізації програмного продукту.

Програмне забезпечення для шифрування та дешифрування інформації криптографічними методами засобами Visual Studio / С. В. Гринюк, М. М. Поліщук, О. І. Міскевич, Р. В. Харковець // Комп’ютерно-інтегровані технології: освіта, наука, виробництво. – 2018. – № 30-31. – С. 26-31.

Р/2346

Дається класифікація алгоритмів шифрування та дешифрування інформації. На основі розглянутих алгоритмів шифрування було створено програмне забезпечення для шифрування та дешифрування файлів, використовуючи засоби Visual Studio.

Савенко О. С. Критерії класифікації методів виявлення шкідливого програмного забезпечення / О. С. Савенко // Вісник Хмельницького національного університету. Серія: Технічні науки. – 2018. – № 1. – С. 23-27.

Р/1055«Т»

Виокремлено критерії класифікації, зокрема, характер отриманих даних, ознаки, що виступають об’єктом пошуку та дослідження, методи аналізу, алгоритми, прийняття рішення, очікуваний результат та оцінка класифікації.

Савенко О. С. Модель та архітектура розподіленої багаторівневої системи виявлення шкідливого програмного забезпечення в локальних комп'ютерних мережах / О. С. Савенко // Вісник Хмельницького національного університету. Серія: Технічні науки. – 2018. – № 2. – С. 153-163.

Р/1055«Т»

Розроблена система здійснюватиме перевірку наявного програмного забезпечення та запущених процесів в комп'ютерних системах локальної мережі на можливість віднесення до шкідливого програмного забезпечення.

Б 18760
004

Системи обробки інформації [Текст] = Information Processing Systems : щоквартальне наукове видання / Міноборони, Харківський нац. ун-т Повітряних Сил імені Івана Кожедуба. - Х. : [Видавництво ХНУПС імені Івана Кожедуба]. -
Вип. 5 (151). - Х., 2017. - 172 с. : іл., табл. - Бібліогр. наприкінці ст. - Алф. покажч.: с. 172.

Зі змісту:

Молодецька-Гринчук К. В. **Прототип програмного комплексу виявлення ознак загроз інформаційній безпеці держави у соціальних інтернет-сервісах та оцінювання їх рівня.** – С. 122-129.
Розроблений прототип програмного комплексу є складовою системи забезпечення інформаційної безпеки держави і автоматизує процеси раннього виявлення загроз у соціальних інтернет-сервісах.
Шаров С. В., Лубко Д. В. **Розробка та використання сніферу як засобу забезпечення безпеки TCP з'єднань.** – 138-144.
У статті повідомляється про розробку програмного засобу для перехоплення та аналізу вихідних TCP з'єднань (сніферу), описуються етапи його розробки та вимоги до використання, подається коротка інструкція користувача.

Шевченко В. Л. Вибір і обґрунтування інтегрального показника і критеріїв ефективності цільового застосування комплексів інформаційної безпеки програмного забезпечення / В. Л. Шевченко, Д. І. Рабчун // Системи озброєння і військова техніка. – 2018. – № 1. – С. 203-207. – Текст англ.

Р/1903

Для оцінювання якості функціонування складних технічних систем, таких як комплекси програмних засобів захисту інформації, в різних умовах протистояння і впливу зовнішнього середовища, і порівняння їх між собою, використовують показники і критерії якості та ефективності.
У роботі проведений аналіз показників та критеріїв для оцінки результатів функціонування реальних комплексів програмних засобів захисту інформації.

Шевченко В. Л. Постановка задачі ресурсної оптимізації комплексу програмних засобів захисту інформації в умовах динамічного інформаційного протистояння / В. Л. Шевченко, Д. І. Рабчун // Системи озброєння і військова техніка. – 2017. – № 3. – С. 89-94.

Р/1903

У статті запропонована формалізація та постановка задачі ресурсної оптимізації комплексів програмних засобів захисту інформації, що функціонують в умовах динамічного інформаційного функціонування з використанням теорії адаптивного управління та логіко-динамічних систем.

Телекомунікаційні мережі та інформаційно-комунікаційні технології

Аналіз систем та методів виявлення несанкціонованих вторгнень у комп'ютерні мережі / В. В. Литвинов, Н. Стоянов, І. С. Скітер [та ін.] // Математичні машини і системи. – 2018. – № 1. – С. 31-40.

Р/1052

Систематизовані, узагальнені і розвинені уявлення про методи і системи аналізу комп'ютерних мереж, які підлягають захисту. Приведений математичний апарат формування образу нормального функціонування систем, визначення узагальненої оцінки стану системи, яка підлягає захисту. Описані основні недоліки та напрями подальшого розвитку систем виявлення вторгнень.

Василенко В. В. Віртуалізація хмарних обчислень і питання безпеки в хмарній системі / В. В. Василенко // Зв'язок. – 2017. – № 5. – С. 33-38.

Р/776

Наведено опис сучасних технологій віртуалізації та проаналізовано механізми захисту, необхідні для досягнення надійної ізоляції віртуальних машин, їх опосередкованого спільного використання та налагодження безпечного зв'язку між ними, що має зрештою гарантувати захист приватного трафіку у віртуальних мережах.

Василенко В. С. Методики визначення вихідних даних для оцінки залишкових ризиків при забезпеченні конфіденційності інформаційних об'єктів / В. С. Василенко, О. Я. Матов // Реєстрація, зберігання і обробка даних. – 2017. –Т. 19, № 4. – С. 45-55.

Р/1346

Для аналізу захищеності інформації автоматизованих систем запропоновано застосування кількісних характеристик у вигляді величин залишкового ризику чи ймовірностей подолання порушником засобів захисту тих чи інших властивостей захищеності. Для оцінки захищеності конфіденційності інформації телекомунікаційних мереж з використанням відповідних систем захисту інформації запропоновано математичні моделі для визначення ймовірностей подолання порушником складових системи захисту конфіденційності.

Грищук Р. Методологія побудови системи забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах / Р. Грищук, К. Молодецька-Гринчук // Захист інформації. – 2017. –Т. 19, № 4. – С. 254-262.

Р/1428

Запропонована методологія зводиться до трьох етапів – моніторинг текстового контенту в соціальних інтернет-сервісах (СІС), виявлення і оцінювання ознак загроз, прийняття рішення щодо заходів з протидії виявленим загрозам інформаційній безпеці держави (ІБД) у СІС.

Грищук Р. В. Постановка проблеми забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах / Р. В. Грищук, К. Молодецька-Гринчук // Сучасний захист інформації. – 2018. – № 1. – С. 43-53.

Р/2300

В статті виконано формалізацію проблеми забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах і визначено перспективні напрямки досліджень. Отримані результати можуть використовуватися для розв'язку частинних задач у рамках вирішення проблеми забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах.

Забезпечення функціональної стійкості інформаційних мереж на основі розробки методу протидії DDoS-атакам / О. В. Барабаш, Н. В. Лукова-Чуйко, А. П. Мусієнко, В. В. Собчук // Сучасні інформаційні системи. – 2018. – Т. 2, № 1. – С. 56-63.

Р/543

Метою є розробка методу протидії DDoS-атакам, що дозволяє ефективно захищати інформаційну мережу, як від атак на всьому часовому інтервалі, так і від повільних атак. *Завдання:* розробити алгоритми виявлення та блокування DDoS-атак, що описують послідовність дій при застосуванні методу протидії; провести оцінку ефективності запропонованого методу протидії DDoS-атакам.

Р 361077
004

Інформаційні технології: сучасний стан та перспективи [Текст] : монографія / [Альошин Г. В., Безсонов О. О., Білецький А. Я. та ін.] ; за заг. ред. В. С. Пономаренка. - Х. : ТОВ "Діса Плюс", 2018. - 462 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Авт. зазнач. на звороті тит. арк.

В монографії розглянуті сучасний стан та перспективи розвитку інформаційних технологій. Монографія представляє інтерес як для фахівців, сфера діяльності яких безпосередньо пов'язана з розробкою ІТ-технологій, способів забезпечення безпеки і передачі в комунікаційних системах, так і для більш широкого кола фахівців.

Б 18863
004

Інформаційні технології та комп'ютерне моделювання [Текст] = Information technologies and computer modelling : матеріали Міжнар. наук.-практ. конф., 15-20 травня 2017 року, Івано-Франківськ / Прикарпатський нац. ун-т імені В. Стефаника, Вінницький нац. техн. ун-т, Центр математичного моделювання ІППММ [та ін.]. - Івано-Франківськ : Видавець Супрун В. П., 2017. - 464 с. : рис., табл., граф. - Бібліогр. наприкінці ст. - Текст кн. укр., англ.

Зі змісту:

Секція 5. **Захист інформації в інформаційно-телекомунікаційних системах**. – С. 191-259.

Кіреєнко О. Модель порушника в інформаційно-комунікаційних системах / О. Кіреєнко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2017. – Вип. 2. – С. 69-77.

Р/2287

Представлено опис порушника в інформаційно-комунікаційних системах, підходи до розробки моделей та їх перевірки. Розглянуто просту модель, мультифакторну модель та мультифакторну модель із сценаріями.

Культенко О. В. Діахронічна еволюція інформаційно-комунікаційних технологій із 1774 по 2014 рр. та її вплив на рівень економічного розвитку України / О. В. Культенко // Науковий вісник Полтавського університету економіки і торгівлі. Серія: Економічні науки. – 2017. – № 3. – С. 37-44.

Р/1484

Методика дослідження. Вирішення поставлених у статті завдань здійснено за допомогою таких методів дослідження: аналізу та синтезу, систематизації, узагальнення та порівняння, діалектичного методу. *Результати.* У публікації розглянуто проблемні питання «цифрової нерівності держав». Проаналізовано теоретичний базис гуманітарних передумов виникнення і розвитку телекомунікації. Здійснено абстрагування фактів в історії телекомунікації за їх кількісними показниками за період 1774–2014 рр.

Кучернюк П. В. Методи і технології захисту комп'ютерних мереж (фізичний та канальний рівні) / П. В. Кучернюк // Мікросистеми, Електроніка та Акустика. – 2017. – Т. 22, № 6. – С. 64-68.

Р/1325

Наведено типові загрози комп'ютерним мережам фізичного та канального рівнів моделі OSI та проведено аналіз особливостей методів і технологій захисту.

Молодецька-Гринчук К. В. Адаптація методів теорії динамічного хаосу для забезпечення інформаційної безпеки у соціальних інтернет-сервісах / К. В. Молодецька-Гринчук // Вісник Житомирського національного агроекологічного університету. – 2017. – № 2, т. 1. – С. 180-187.

Р/1223

Взаємодія користувачів віртуальних спільнот, яких називають акторами, характеризується нелінійністю з можливим переходом до хаотичної динаміки. У статті обґрунтовано перспективність адаптації теорії динамічного хаосу для подальшого використання при побудові системи забезпечення інформаційної безпеки держави у соціальних інтернет-сервісах.

Р 360689
355

Національна академія Державної прикордонної служби України імені Богдана Хмельницького.
Збірник наукових праць Національної академії Державної прикордонної служби України [Текст] : [наук. вид.]. - Хмельницький : Вид-во НАДПСУ. - (Серія: Військові та технічні науки).
№ 2 (72). - Хмельницький, 2017. - 344 с. : рис., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., рос., англ.

Зі змісту:
Євсеєв С., Федорченко В., Андрощук О. **Побудова систем безпеки інформаційно-телекомунікаційних систем на основі комплексного криптографічного підходу.** – С. 258-268.

Пелещишин А. Спеціальна безпекова модель користувача соціальних середовищ Інтернету / А. Пелещишин, В. Вус, О. Тимовчак-Максимець // Безпека інформації. – 2018. – Т. 24, № 1. – С. 62-68.

Р/1408

У роботі запропоновано спеціальну безпекову модель користувача соціальних середовищ Інтернету та описано об’єкти інформаційної діяльності.

Саматов К. Penetration Test: что и зачем? / К. Саматов // Информационная безопасность/InformationSecurity. – 2018. – № 2. – С. 12-13.

Р/365

Penetration Test – метод оценки безопасности компьютерных систем или сетей передачи данных посредством моделирования атаки нарушителя, как правило, являющийся частью аудита информационной безопасности организации. В чем заключается указанный метод оценки безопасности, является ли он обязательным, как организовать его с получением максимального эффекта, читайте в данной статье.

Сачанюк-Кавецька Н. В. Кодування як засіб захисту інформації у системах контролю доступу з використанням логіко-часових функцій у формі поліномів і біометричних даних суб’єктів / Н. В. Сачанюк-Кавецька // Реєстрація, зберігання і обробка даних. – 2018. – Т. 20, № 2. – С. 60-67.

Р/1346

Розглянуто можливість циклічного кодування та правила побудови ключів асиметричного криптоалгоритму на базі ідентифікаційних логіко-часових функцій, що містять усі важливі характеристики переданих повідомлень. Для доступного формального опису такого кодування та правил побудови ключів використано подання логіко-часових функцій у формі поліномів.

Б 18760
004

Системи обробки інформації [Текст] = Information Processing Systems : щоквартальне наукове видання / Міноборони, Харківський нац. ун-т Повітряних Сил імені Івана Кожедуба. - Х. : [Видавництво ХНУПС імені Івана Кожедуба]. -
Вип. 5 (151). - Х., 2017. - 172 с. : іл., табл. - Бібліогр. наприкінці ст. - Алф. покажч.: с. 172.

Зі змісту:

У статті розглядаються два різних методи вирішення децентралізованого частково спостерігаємого процесу прийняття рішень Маркова (decentralized partially observable Markov decision process, DEC-POMDP). Запропонована цілком розподілена схема гібридної безпеки з використанням технології IDS та Honeypot.

Толюпа С. В. Аналіз вразливостей локальних бездротових мереж та способи їх захисту від можливих атак / С. В. Толюпа, І. І. Пархоменко, А. Д. Коноваленко // Вісник Інженерної академії України. – 2017. – № 3. – С. 114-117.

Р/1139

На сьогоднішній день бездротові технології отримали масовий розвиток і міцно увійшли в повсякденне життя. В статті розглянуто основні вразливості локальних бездротових мереж, механізми та способи захисту від несанкціонованого доступу, проаналізовано основні загрози інформації та механізми виявлення можливих атак.

Інформаційне протиборство у воєнних конфліктах. Інформаційно-психологічна безпека

Алещенко В. Інформаційно-психологічний вплив у ході збройної боротьби / В. Алещенко // Вісник Київського національного університету імені Тараса Шевченка. Серія: Військово-спеціальні науки. – 2018. – № 1(38). – С. 6-10.

Р/1134

Висвітлено сутність поняття та загальні підходи здійснення інформаційно-психологічного впливу в ході збройної боротьби. Розглянуто інформаційно-психологічну компоненту у військовій справі, що домінує в таких країнах, як США, ФРН, Великобританія, Франція, Китай, РФ; основні завдання, які покладаються на спеціальні інформаційні війська (сили). Запропоновано деякі пріоритетні напрями, шляхи і способи протидії інформаційно-психологічному впливу в ході збройної боротьби.

Антонов А. М. Пропаганда як опіум для народу / А. М. Антонов // Оборонний вісник. – 2018. – № 8. – С. 14-17.

Р/1134

Головним принципом діяльності пропагандистських структур Росії, який досягає бажаних ефектів забезпечення контролю інформаційних потоків і впливу на певні цільові аудиторії та російське суспільство в цілому, є принцип «виняткової монополії на інформацію».

Бомба А. Я. Про узагальнення однієї моделі інформаційної боротьби / А. Я. Бомба, А. А. Федонюк // Комп'ютерно-інтегровані технології: освіта, наука, виробництво. – 2018. – № 30-31. – С. 165-170.

Р/2346

Аналізується математична модель інформаційного впливу на соціум двох взаємовиключаючих ідеологій з введенням поняття запізнення в часі стосовно початку дії інформаційного потоку.

Р 360695
32

Інститут політичних і етнонаціональних досліджень імені І. Ф. Кураса НАН України.
Наукові записки Інституту політичних і етнонаціональних досліджень імені І. Ф. Кураса НАН України [Текст] : [наук. вид.]. - [К.] : ІПіЕНД імені І. Ф. Кураса НАН України. -
Вип. 3 (89) травень-червень. - [К.], 2017. - 284 с. : рис., табл. - Заголовок обкл. : Наукові записки. - Бібліогр. наприкінці ст. та у виносках. - Текст кн. укр., англ.

Зі змісту:

Кочубей Л. **Особливості сучасних інформаційно-комунікативних технологій в Україні.** – С. 44-70.
Метою статті є: проаналізувати сучасні ІКТ, їх різновиди, дієвість, переваги, цільову аудиторію в інформаційному просторі України та на прикладі ІКТ РФ проти України, визначити засоби протидії та запобігання руйнівним інформаційним впливам у вітчизняному інформаційному просторі. Таким чином, у цій статті здійснено спробу розглянути ІКТ переважно не з точки зору їх створення, а їх використання, як технології проектування та створення інформаційного продукту.

Курченко О. А. Розробка моделі паніки інформаційної безпеки підприємства / О. А. Курченко, Ю. О. Ковтун // Сучасний захист інформації. – 2017. – № 4. – С. 30-36.

Р/2300

В статті проаналізовано вплив соціального фактору, а саме паніки, на інформаційну безпеку підприємства. Визначені основні допустимі критерії для аналізу колективу. Створено модель паніки інформаційної безпеки підприємства на основі аналізу персоналу. Обгрунтовано рекомендації щодо мінімізації впливу соціального фактору на інформаційну безпеку підприємства.

Марушак А. І. Питання ефективності діяльності державних органів у сфері захисту інформаційного простору України / А. І. Марушак // Інформація і право. – 2017. – № 4. – С. 86-92.

Р/844

«Одну з найбільших загроз національній безпеці нашої держави на сьогодні становить інформаційна агресія Російської Федерації, основою якої є продукування і поширення неправдивої інформації з метою маніпулювання суспільною свідомістю».

Методичний підхід до виявлення та оцінювання негативного інформаційно-психологічного впливу на особовий склад військ (сил) / П. М. Сніцаренко, Ю. О. Саричев, Ю. І. Міхєєв, М. В. Праута // Наука і оборона. – 2017. – № 3/4. – С. 18-25.

Р/810

У статті викладено методичний підхід до виявлення та кількісного оцінювання негативного інформаційно-психологічного впливу на особовий склад військ (сил) як невід'ємної складової системи протидії такому впливу, яка має функціонувати за кібернетичним принципом.

Уханова Н. С. Захист інформаційного простору від терористичних посягань та негативних інформаційно-психологічних впливів / Н. С. Уханова // Інформація і право. – 2017. – № 4. – С. 99-105.

Р/844

В статті розглядаються інформаційно-психологічні та суспільно-правові аспекти використання сучасного інформаційного простору та інформаційно-комунікаційних технологій на шкоду людині, суспільству і державі. Розкрито питання терористичних викликів і загроз з використанням інформаційного простору. Проаналізовано інформаційно-психологічні механізми здійснення інформаційних операцій, маніпулювання, ідеологічного впливу і вербування прибічників терористичних та інших злочинних організацій з використанням інформаційно-комунікаційних технологій.

Р 360683
070

Феномен пропаганди та антипропаганди у сучасному світі: історико-політологічний дискурс [Текст] : монографія / [Мініч А. П., Люта С. С., Мальована Ю. Г. та ін. ; за наук. ред. Г. М. Васильчука, О. М. Маклюк, М. М. Бессонової] ; Запорізьке обласне т-во дослідників історії і культури Центральної та Східної Європи, Запорізький нац. техн. ун-т, Історичний ф-т, Каф. всесвітньої історії та міжнародних відносин. - Запоріжжя : Інтер-М, 2018. - 406 с. : іл. - Бібліогр. наприкінці підрозд. - Авт. зазнач. на с. 369-384. Парал. тит. арк. англ.

У монографії подано наукове осмислення широкого кола проблем, пов'язаних із вивченням різних форм пропаганди в історичному контексті від початку XX століття до сучасності; проаналізована специфіка пропаганди та антипропаганди у сучасному світовому медіапросторі та особливості її сприйняття різними категоріями населення.

Кібербезпека – проблема XXI століття

Б 18790
681

Автоматика, вимірювання та керування [Текст] : зб. наук. пр. / голова редакційно-видавничої ради Н. І. Чухрай. - Л. : Вид-во Львів. політехніки, 2017. - 116 с. : граф., рис., табл. - (Вісник / Національний університет "Львівська політехніка" ; № 880). - Бібліогр. наприкінці ст. - Текст укр., англ.

Зі змісту:

Дудикевич В. Б., Березюк Б. М. **Особливості інцидентів у сучасному кібернетичному просторі та їх вплив на безпеку суспільства.** – С. 73-78.
Розглянуто вплив інформаційно-комунікаційних технологій на формування сучасного кіберпростору. Наведено класифікацію кібернетичних втручань за їх видами та проаналізовано найпоширеніші інциденти та методи кіберрозвідки.

Аналіз вразливостей корпоративних інформаційних систем / Д. Мехед, Ю. Ткач, В. Базилевич [та ін.] // Захист інформації. – 2018. –Т. 20, № 1. – С. 61-66.

Р/1428

Оскільки конфіденційна інформація підприємства (електронні пошти, паролі до облікових записів, реквізити доступу до серверів, хеш-дані облікових записів користувачів та інша інформація, якої немає у відкритому доступі) є метою для багатьох кіберзлочинців, дані технології часто підлягають атакам різного роду. Проводячи аналіз ми спирались на дослідження зарубіжних вчених та практикуючих компаній, що займаються вивченням загроз та розробкою систем їх запобігання.

Борсуковський Ю. В. Визначення сучасних вимог щодо політики використання засобів криптографічного захисту інформації на підприємстві / Ю. В. Борсуковський, В. Ю. Борсуковська // Сучасний захист інформації. – 2018. – № 1. – С. 74-81.

Р/2300

В даній статті проведено детальний аналіз вимог до формування політики інформаційної безпеки щодо використання засобів криптографічного захисту інформації з метою реалізації організаційних та технічних заходів по запобіганню витокам конфіденційної інформації на підприємстві. Сформульовані базові вимоги та рекомендації щодо структури та змісту політики інформаційної безпеки для створення, впровадження та експлуатації превентивних процедур управління захистом інформації із обмеженим доступом. Враховано практичний досвід розробки, впровадження та управління сучасними політиками інформаційної безпеки щодо використання засобів криптографічного захисту конфіденційної інформації на підприємствах різної форми власності.

Борсуковський Ю. В. Прикладні аспекти захисту інформації в сучасних умовах / Ю. В. Борсуковський, В. Ю. Борсуковська // Сучасний захист інформації. – 2018. – № 2. – С. 6-11.

Р/2300

В даній статті проведено детальний аналіз актуального ландшафту кіберзагроз та напрямки забезпечення інформаційної безпеки зі сторони світової спільноти. Наведені категорії CIS Control, щодо напрямків пріоритетного забезпечення інформаційної безпеки бізнесу.

Борсуковський Ю. В. Рекомендації по категоріюванню інформації з обмеженим доступом / Ю. В. Борсуковський, В. Ю. Борсуковська // Сучасний захист інформації. – 2017. – № 4. – С. 9-17.

Р/2300

В даній статті проведено детальний аналіз вимог щодо категоріювання інформації з обмеженим доступом для корпоративних користувачів. Сформульовані базові вимоги та рекомендації щодо структури та змісту політики категоріювання інформації з обмеженим доступом з врахуванням досвіду впровадження систем запобігання витокам інформації.

Бортник К. Я. Технології аналізу наслідків кібератак / К. Я. Бортник, Г. Ю. Ломінська // Комп'ютерно-інтегровані технології: освіта, наука, виробництво. – 2018. – № 30-31. – С. 10-13.

Р/2346

У статті розкриваються особливості та характеристики кібербезпеки і розглядаються способи, якими фахівці з кібербезпеки аналізують наслідки кібератак. Пояснюються різні категорії вразливостей програмного та апаратного забезпечення та систем безпеки.

Бурячок В. Рекомендації щодо розробки та реалізації моделі професійних компетентностей у сфері підготовки фахівців для національної системи кібербезпеки / В. Бурячок, В. Богуш // Захист інформації. – 2018. – Т. 20, № 2. – С. 72-78.

Р/1428

На основі результатів аналізу законодавства України щодо кібербезпеки та типового навчального плану НАТО з кібербезпеки запропоновано певну модель щодо підготовки фахівців для національної системи кібербезпеки. В статті запропоновано декілька основних класів моделі професійних компетентностей у сфері підготовки фахівців для національної системи кібербезпеки.

Волосович С. Детермінанти виникнення та реалізації кіберризиків / С. Волосович, Л. Клапків // Зовнішня торгівля: економіка, фінанси, право. – 2018. – № 3. – С. 101-115.

Р/1792

Виокремлено причинно-наслідковий, секторальний та інструментальний підходи до визначення дефініції кіберризиків. Запропоновано розглядати кіберризики у широкому та вузькому розумінні. Систематизовано кримінальні та некримінальні джерела кіберризиків. Проаналізовано явища кібератака та кіберінцидент як основні інструменти реалізації кіберризику. Виявлено кіберзагрзи для зовнішньої торгівлі. Досліджено основні кіберінциденти глобального масштабу.

Гахов С. О. Застосування положень імунології в теорії захищених інформаційних систем // Сучасний захист інформації. – 2018. – № 2. – С. 59-64.

Р/2300

Розглянуто принципи функціонування імунної системи живих організмів як основних тверджень теорії захищених інформаційних систем. Встановлено перспективний напрямок розвитку теорії захищених інформаційних систем.

Грипинська Н. В. Забезпечення кібербезпеки під час впровадження інтернету речей / Н. В. Грипинська, Н. І. Праворська // Вісник Хмельницького національного університету. Серія: Технічні науки. – 2018. – № 3. – С. 270-274.

Р/1055«Т»

Інтернет речей – це об'єднання великої кількості пристроїв з різним за обсягом програмним забезпеченням автономних пристроїв. В сучасному інформаційному середовищі визначають п'ять типових видів зловмисників, що можуть взаємодіяти з IoT. В статті наведено основні засади забезпечення безпеки IoT, що мають бути забезпечені в ході проектування та експлуатації систем IoT.

Ілляшенко О. О. Геп-аналіз кібербезпеки за допомогою кейсів запевнення: техніка та приклад використання / О. О. Ілляшенко, В. С. Харченко, А. Кор // Сучасні інформаційні системи. – 2018. – Т. 2, № 1. – С. 64-68. – Текст англ.

Р/543

Метою є розробка техніки аналізу розривів процесу аналізу кібербезпеки. *Завдання:* розробити метод аналізу розривів у процесі оцінювання нефункціональних вимог до функціональної та кібербезпеки ІКС, заснований на класифікації вимог з урахуванням можливості їх декомпозиції.

Киричок Р. В. Тест на проникнення як імітаційний підхід до аналізу захищеності корпоративних інформаційних систем / Р. В. Киричок // Сучасний захист інформації. – 2018. – № 2. – С. 53-58.

Р/2300

У даній статті проаналізовано основні методи та етапи проведення кібернападу з метою кращого розуміння зловмисників та розглянуто анатомію тесту на проникнення. А також запропоновано використання пентесту як імітаційного підходу до проведення комплексного аналізу та отримання об'єктивної оцінки рівня захищеності.

Кропачев А. Моделирование процессов распределения полномочий и обеспечения киберзащиты центров обработки данных / А. Кропачев, Д. Зуев // Захист інформації. – 2018. –Т. 20, № 1. – С. 49-54. – Текст англ.

Р/1428

Проанализировано распределение полномочий для центра обработки данных и разработка мер по обеспечению его кибербезопасности.

Ландшафт угроз для систем промышленной автоматизации. Второе полугодие 2017 года // Информационная безопасность/InformationSecurity. – 2018. – № 2. – С. 38-45.

Р/365

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky Lab ICS CERT) публикует результаты исследований ландшафта угроз для систем промышленной автоматизации, полученные в течение второго полугодия 2017 года. Основная цель публикаций – информационная поддержка глобальных и локальных команд реагирования на инциденты, специалистов по информационной безопасности предприятий и исследователей в области защищенности промышленных объектов.

Лисецкий Ю. М. Новые угрозы информационной безопасности или оружие массового заражения / Ю. М. Лисецкий, С. И. Бобров // Математичні машини і системи. – 2018. – № 1. – С. 41-50.

Р/1052

Розглянуто проблему використання Internet of Things як способу масового зараження вірусами інформаційних систем. Описано один із найбільш небезпечних засобів впливу, спрямований на відмову в обслуговуванні інформаційних систем як основний інструмент реалізації кібератак.

Ліпінський В. В. Вплив кібернетичних атак на інформаційну систему / В. В. Ліпінський, А. А. Кулько, Є. О. Толюпа // Сучасний захист інформації. – 2017. – № 4. – С. 60-65.

Р/2300

У статті розглянуто засоби виявлення кібернетичних атак, що забезпечують одержання даних з мережі про зловмисну активність в зрозумілу інформацію, яка може бути використана для усунення підтверджених порушень безпеки. Деталізовано можливості використання апаратних засобів віддзеркалення загроз, які дозволяють адміністраторам централізовано знаходити, визначати пріоритетність і відображення загрози за допомогою вже упроваджених в інфраструктуру мережевих пристроїв і пристроїв захисту.

Магаршак Ю. Б. Интернет противопоказан живой природе / Ю. Б. Магаршак // Энергия: экономика, техника, экология. – 2017. – № 11. – С. 69-71.

Р/294

«Перспектива того, что цивилизация интернета будет разрушена хакерами, абсолютно реальна. Компьютерная война, первые протуберанцы которой взбудоражили все медиа, уже началась. Хакеры способны уничтожить техногенную человеческую цивилизацию, если своевременно не предпринять защитных мер. Главная из них – изменения глобального направления развития техногенной цивилизации».

Модель оцінювання наслідків витоку державної таємниці від кібератак на критичну інформаційну інфраструктуру держави / О. Корченко, Ю. Дрейс, М. Рощук, О. Романенко // Безпека інформації. – 2018. – Т. 24, № 1. – С. 29-35.

Р/1408

… розроблено модель оцінювання негативних наслідків витоку ДТ від кібератак на критичну інформаційну інфраструктуру держави, яка за рахунок визначених множин потенційних порушень, типових загроз, ступенів секретності, зводу відомостей, що становлять державну таємницю, показників економічної шкоди, тяжких наслідків та інших (що входять до відповідного кортежу), і дає можливість створити метод оцінювання негативних наслідків витоку ДТ, як в межах окремих областей, так і для держави в цілому.

Р 360871
004

Моделювання та інформаційні технології [Текст] : зб. наук. пр. / НАН України, Ін-т проблем моделювання в енергетиці імені Г. Є. Пухова. - [Л.] : [ПП "Системи, технології, інформаційні послуги"]. - **Вип. 80**. - К., 2017. - 200 с. : рис., табл. - Бібліогр. наприкінці ст. - Текст укр., рос.

Зі змісту:

Гончар С. Ф. **Особливості забезпечення кібербезпеки об'єктів критичної інфраструктури.** – С. 27-32.

Р 360872
004

Моделювання та інформаційні технології [Текст] : зб. наук. пр. / НАН України, Ін-т проблем моделювання в енергетиці імені Г. Є. Пухова. - [Л.] : [ПП "Системи, технології, інформаційні послуги"]. - **Вип. 81**. - К., 2017. - 182 с. : рис., табл. - Бібліогр. наприкінці ст. - Текст укр., рос.

Зі змісту:

Комаров М. Ю., Гончар С. Ф. **Методика побудови системи управління інформаційною безпекою на об'єктах критичної інфраструктури.** – С. 12-19.

Смольянинов П. А., Кравцов Г. А. **Базовая модель информационных процессов управления индустриальных систем и их безопасность.** – С. 39-46.

Пєвнєв В. Я. Безпека баз даних: загрози та превентивні заходи / В. Я. Пєвнєв, С. Д. Капчинський // Сучасні інформаційні системи. – 2018. – Т. 2, № 1. – С. 69-72. – Текст англ.

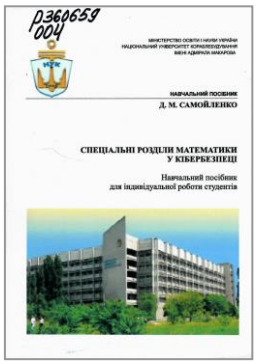
Р/543

Завдання: провести поглиблений аналіз різноманітних загроз і вразливостей та вибрати найбільш розповсюджені та найпроблематичніші з них, проаналізувати та запропонувати оптимальніші з превентивних заходів або рішень для кожної з переглянутих загроз.

Савченко В. А. Сдерживание в киберпространстве / В. А. Савченко // Сучасний захист інформації. – 2018. – № 2. – С. 72-76.

Р/2300

В докладе рассмотрены вопросы сдерживания в киберпространстве, как одного из ключевых элементов информационной безопасности государства. Проанализированы сходство и различия сдерживания в ядерной сфере и киберпространстве. Сделаны выводы относительно возможности реализации идеи сдерживания в сфере информационных технологий.



Р 360659
004

Самойленко, Денис Миколайович.
Спеціальні розділи математики у кібербезпеці [Текст] : навч. посіб. для індивід. роботи студентів / Д. М. Самойленко ; Національний ун-т кораблебудування імені адмірала Макарова. - Миколаїв : НУК, 2017. - 102 с. : граф., табл. - Бібліогр.: с. 86-87.

Розглянуто основи вибраних розділів математики, що не входять до базового курсу вищої математики та є необхідними для професійної підготовки фахівця з кібербезпеки. У першому розділі наведено основи теорії складності алгоритмів, їх класифікацію та асимптотичні оцінки. У другому розділі розглянуто базисні поняття та співвідношення теорії чисел. У третьому – числові методи оптимізації та пошуку. Наведено приклади програмної реалізації окремих обчислювальних алгоритмів.
Призначено для студентів ВНЗ, що навчаються за напрямом підготовки «Кібербезпека».

Сердюк В. Анализируй это… / В. Сердюк, Р. Ванерке // Информационная безопасность/InformationSecurity. – 2018. – № 2. – С. 18-19.

Р/365

… именно мониторинг поведения легитимных пользователей в информационной системе позволяет выявить возможные несанкционированные действия. Так, например, можно сделать вывод о том, что в случае сильного изменения поведения пользователя его учетные данные могут быть скомпрометированы и от его имени работает кто-то посторонний. Именно возможности профилирования и анализа активности пользователей и объектов ИТ-инфраструктуры реализованы в относительно новом сегменте рынка систем защиты, который получил название «средства поведенческого анализа пользователей и сущностей» – UEBA (User and Entity Behavioral Analytics).

Б 18823
004

Системи обробки інформації [Текст] = Information Processing Systems : щоквартальне наукове видання / Міноборони, Харківський нац. ун-т Повітряних Сил імені Івана Кожедуба. - Х. : [Видавництво ХНУПС імені Івана Кожедуба]. -
Вип. 1 (152). - Х., 2018. - 166 с. : іл., табл. - Бібліогр. наприкінці ст. - Алф. покажч.: с. 165. - Текст укр., рос., англ. Дод. тит. арк. англ.

Зі змісту:
Шевченко В. Л., Ткаченко М. В., Шевченко А. В. **Ідентифікація загроз «нульового дня» в кібербезпеці за допомогою таксонометричного методу.** – С. 136-141. – Текст англ.

711482 В
004

Системи обробки інформації [Текст] = Information Processing Systems : щоквартальне наукове видання / Міноборони, Харківський нац. ун-т Повітряних Сил імені Івана Кожедуба. - Х. : [Видавництво ХНУПС імені Івана Кожедуба]. -
Вип. 2 (153). - Х., 2018. - 172 с. : іл., табл. - Бібліогр. наприкінці ст. - Алф. покажч.: с. 172. - Текст укр., рос., англ. Дод. тит. арк. англ.

Зі змісту:
Борсуковський Ю. В., Борсуковська В. Ю., Бурячок В. Л., Складанний П. М. **Прикладні аспекти розробки політики категорування інформації з обмеженим доступом.** – С. 117-126.

Р 361105
004

Системні технології [Текст] = System Technologies : регіональний міжвузівський збірник наукових праць / МОН = Системные технологии. - Д. : [НМетАУ, ІВК "Системні технології"]. -
Вип. 5 (112). - Д., 2017. - 223 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., рос., англ.

Зі змісту:
Погорелов Е. В. **Дослідження нейромережевих засобів розпізнавання кібератак на мережеві ресурси інформаційних систем.** – С. 61-69.

Стасюк О. І. Математичні диференційні моделі і методи оцінки кібербезпеки інтелектуальних комп'ютерних мереж керування технологічними процесами електропостачання залізниць / О. І. Стасюк, Р. В. Грищук, Л. Л. Гончарова // Кибернетика и системный анализ. – 2018. – Т. 54, № 4. – С. 173-181.

Р/450

На основі теорії диференційних перетворень Пухова запропоновано ряд диференційних математичних моделей оцінки рівня кібербезпеки комп'ютерної мережі керування електропостачанням. Для диференційних зображень запропоновано критерій кібербезпеки і розроблено принцип мінімаксу для найгіршого варіанту поєднання інтенсивності кібератак і потоку захисних дій.

711879 В
623

Сучасна спеціальна техніка [Текст] : науково-практичний журнал / Державний н.-д. ін-т МВС України. - К. : [ФОП Тарнавська Л. І.]. -
№ 4 (51). - К., 2017. - 116 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., англ.

Зі змісту:
Козюра В. Д., Хорошко В. О. **Система кібернетичної безпеки в Україні.** – С. 34-41.
У статті розглянуті загрози кібербезпеці та національній безпеці України.

Терейковський І. А. Система виявлення кібератак / І. А. Терейковський, А. О. Корченко // Безпека інформації. – 2017. – Т. 23, № 3. – С. 176-180. – Текст рос.

Р/1408

… на базі відомої методології побудови систем виявлення аномалій, породжених кібератаками розроблена система виявлення атак. Вона, за рахунок баз даних кібератак, правил і еталонів, а також модулів формування поточних значень, α-рівневої номіналізації, ідентифікуючих термів, рівня аномальності і візуалізації, дозволяє будувати засоби, що розширяють функціональні можливості сучасних систем виявлення вторгнень.

Ткаченко В. Найти и уничтожить: SIEM – охотник за киберугрозами / В. Ткаченко // Сети и бизнес. – 2018. – № 2. – С. 68-31.

Р/1698

Кибератак становится все больше, но с ними борются новые средства аналитики на основе искусственного интеллекта и машинного обучения.

Федотова-Півень І. Шляхи задоволення потреб сучасної кібербезпеки в рамках протидії методам комп'ютерної лінгвістичної стенографії / І. Федотова-Півень, Я. Тарасенко // Безпека інформації. – 2017. – Т. 23, № 3. – С. 190-196.

Р/1408

В статті проводиться огляд поширених методів текстової стенографії, а саме методів довільного інтервалу, синтаксичних і семантичних методів, досліджуються існуючі шляхи протидії їм, а також засоби автоматизованого лінгвістичного аналізу тексту (морфологічного, синтаксичного, дискурсного) для автоматизації текстового стегоаналізу.

С 21740
62

"Харківський політехнічний інститут". Національний технічний університет.
Вісник Національного технічного університету "ХПІ" [Текст] : збірник наук. праць. - Х. : НТУ "ХПІ". - (Серія: Інформатика та моделювання). -
№ 50 (1271). - Х., 2017. - 161 с. : граф., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., рос., англ.

Зі змісту:
Проблемы защиты информации в современных системах
Гриб О. Г., Швець С. В., Бортніков О. В. **Синтез елементів енергосистеми за критерієм надійності в умовах кібербезпеки.** – С. 97-110. – Текст рос. – Бібліогр.: 10 назв.

711728 В
62

"Харківський політехнічний інститут". Національний технічний університет.
Вісник Національного технічного університету "Харківський політехнічний інститут" [Текст] : зб. наук. пр. - Х. : [НТУ "ХПІ"]. - (Серія: Нові рішення в сучасних технологіях). -
№ 16 (1292). - Х., 2018. - 200 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., англ., рос. Дод. тит. арк. англ.

Зі змісту:
Грудзинський Ю. Є., Харченко Д. Ю. **Деякі питання запобігання інцидентам при зовнішніх кібератаках на автоматизовану систему керування котлоагрегатом системи опалення.** – С. 112-116.

Эмм Д. Главные риски в онлайн-голосовании: мнение охотника за киберугрозами / Д. Эмм // Информационная безопасность / Information Security. – 2018. – № 1. – С. 30-31.

Р/365

Неэффективная процедура идентификации голосующего может крайне негативно сказаться на надежности всей системы электронного голосования. На примере банковских операций и онлайн-платежей мы знаем, что взлом системы идентификации может обернуться мошенничеством и воровством данных.