Тематична виставка
"Безпека та захист інформаційного простору"

(надходження І півр. 2018)

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

Б 18566
34

Актуальні проблеми правознавства [Текст] : зб. наук. пр. / Тернопільський нац. екон. ун-т, Юрид. ф-т. - Т. : ТНЕУ, 2017 - . -
Вип. 1. - Т., 2017. - 102 с. - Бібліогр. наприкінці ст.

Зі змісту:

Колесніков А., Зяйлик М. **Економіко-правові засади розвитку кіберзлочинності та методів боротьби з нею.** – С. 26-29.
Терехов В. **Удосконалення адміністративно-правового регулювання реалізації політики інформаційної безпеки в органах місцевого самоврядування.** – С. 43-47.

Б 18567
34

Актуальні проблеми правознавства [Текст] : зб. наук. пр. / Тернопільський нац. екон. ун-т, Юрид. ф-т. - Т. : ТНЕУ, 2017 - . -
Вип. 2. - Т., 2017. - 148 с. - Бібліогр. наприкінці ст.

Зі змісту:

Марків С. **Історико-правовий аспект кібертероризму.** – С. 103-106.

Акулов М. Г. Сучасний стан та перспективи розвитку інформаційної безпеки / М. Г. Акулов, О. О. Пінцевич // Регіональна бізнес-економіка та управління. – 2017. – № 4. – С. 99-105.

Р/1919

У статті розглянуто сутність інформаційної безпеки на державному рівні, визначено особливості державного регулювання інформаційної безпеки, досліджено необхідність міжнародного співробітництва в галузі забезпечення інформаційної безпеки.

Білак Ю. Ю. Інформаційна безпека як елемент підвищення ефективності інноваційного розвитку України / Ю. Ю. Білак, А. В. Легеза, І. М. Лях // Вісник Київського національного університету технологій та дизайну. Серія: Економічні науки. – 2017. – № 4. – С. 44-50.

Р/1733

У статті розкрито підходи до визначення стану інформаційної безпеки як ключового елементу підвищення ефективності інноваційного розвитку України. Визначено, що нівелювання системних загроз національній безпеці й захист національних інтересів забезпечуються ефективним механізмом управління інформаційною безпекою. Розкрито основні протиріччя, що існують у чинних алгоритмах оцінювання рівня інформаційної безпеки. Запропоновано основні підходи до процедури оцінювання та моделювання інформаційної безпеки як елементу підвищення ефективності інноваційного розвитку України.

Б 18640
621.39

Військовий інститут телекомунікацій та інформатизації.
Збірник наукових праць [Текст] = Collection of Scientific Papers / Міноборони України. - К. : [ВІТІ].
Вип. № 4. - К., 2017. - 146 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст укр., рос. та англ.

Зі змісту:

Положення Стратегії кібероборони України базуються на вимогах Закону України «Про оборону України», «Воєнної доктрини України», Стратегії національної безпеки України та Стратегії кібербезпеки України і розкривають основні принципи, за якими сили оборони використовують кіберпростір для протистояння викликам у сфері забезпечення кібероборони держави, водночас зміцнюючи взаємовигідне співробітництво з питань кібероборони у військовій, воєнно-економічній та військово-технічній сферах з усіма заінтересованими державами-партнерами.

Вороненко І. В. Концептуальні засади щодо регулювання кіберпростору. Міжнародний аспект / І. В. Вороненко, К. Л. Тужик // Економіка. Менеджмент. Бізнес. – 2017. – № 4. – С. 73-80.

Р/2331

В статті досліджено теоретичні аспекти формування кіберпростору, систематизовано основні положення міжнародних нормативно-правових норм, що регламентують функціонування та регулювання кіберпростору на міжнародному рівні. Здійснено аналіз рівня готовності щодо забезпечення результативного світового регулювання кіберпростором за допомогою глобального індексу кібербезпеки.

Гладун А. Я. Таксономія стандартів інформаційної безпеки / А. Я. Гладун, К. О. Хала // Наука, технології, інновації. – 2017. – № 2. – С. 53-64.

Р/863

У статті представлено таксономію (структурну класифікацію) стандартів інформаційної безпеки, що є певним системним аналізом стандартів як на думку їх розробників, так і проектувальників та розробників захищених систем.

Демченко П. С. Інформаційно-електронна безпека виборчого процесу: українські реалії та зарубіжний досвід (на прикладі останніх президентських виборів у США 2016 р. та Франції 2017 р.) / П. С. Демченко // Економіка. Фінанси. Право. – 2017. – № 8/1. – С. 32-37.

Р/687

У статті розглядаються основні положення щодо сутності інформаційно-електронної безпеки виборчого процесу, виявлення її особливостей необхідних для забезпечення безпеки проведення виборів в державі. Наводяться приклади Сполучених Штатів Америки та Франції як держав, які мають сталу концепцію інформаційно-електронної безпеки та досвід останніх президентських виборів. На основі цих теоретико-практичних особливостей пропонуються основи щодо встановлення інформаційно-електронної безпеки виробного процесу в правовій та технічній сферах в Україні.

Друк В. В. Практичні аспекти реалізації основних напрямів державної політики в інформаційній сфері / В. В. Друк // Інвестиції: практика та досвід. – 2017. – № 17. – С. 103-105.

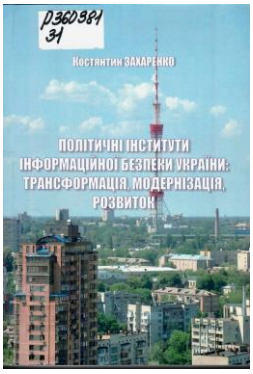
Р/2124

У статті проведено аналіз основних напрямів державної політики в інформаційній сфері в контексті сучасних загроз, задекларованих у Доктрині інформаційної безпеки України, та на цій основі виокремлено практичні аспекти їх реалізації.

Р 359634
351

Запобігання новим викликам та загрозам інформаційній безпеці України: правові аспекти [Текст] : матеріали наук.-практ. конф., 06 жовтня 2016 року / В. Ф. Морфлюк, І. С. Карпенко ; Науково-дослідний ін-т інформатики і права НАПрН України, Навч.-наук. центр інформаційного права та правових питань інформ. технологій ФСП Нац. техн. ун-ту України "Київський політехнічний інститут ім. Ігоря Сікорського", Кафедра правових наук та філософії Вінницького держ. пед. ун-ту імені Михайла Коцюбинського. - К. : [КПІ ім. Ігоря Сікорського, Політехніка], 2016. - 202 с. - Бібліогр. наприкінці ст. - Текст кн. укр., англ.

Подано основні результати досліджень за вказаною НДР та матеріали з актуальних проблем і шляхів правового запобігання новим викликам й загрозам у сфері інформаційної безпеки України.



Р 360381
31

Захаренко, Костянтин Володимирович.
Політичні інститути інформаційної безпеки України: трансформація, модернізація, розвиток [Текст] : монографія / Костянтин Захаренко ; Національний пед. ун-т імені М. П. Драгоманова. - К. : Вид-во НПУ імені М. П. Драгоманова, 2017. – 389 с. - Бібліогр.: с. 360-388 (314 назв) та у виносках.

Інформаційна революція спонукає бурхливий розвиток інформаційних потоків, електронних засобів комунікації, інформатики, створення глобальної інформаційної мережі. В останні роки в Україні, через розв'язану Росією гібридну війну, особливо актуальним стало поняття «інформаційної безпеки». Останнє потребує більш глибокого наукового визначення проблеми змісту та функціональних особливостей державної інформаційної політики, її ролі у створенні та реалізації безпечних інформаційних систем та технологій, гарантуванні свободи інформаційної діяльності та права доступу до інформації.

Р 360435
004

Информационные технологии и безопасность [Текст] : материалы XVII международной науч.-практ. конф. [ИТБ-2017] / НАН Украины, Ин-т проблем регистрации информации НАН Украины. - К. : [ООО "Инжиниринг"].
Вып. 17. - К., 2017. - 292 с. : ил., табл. - Библиогр. в конце ст. - Текст кн. укр., рос., англ.

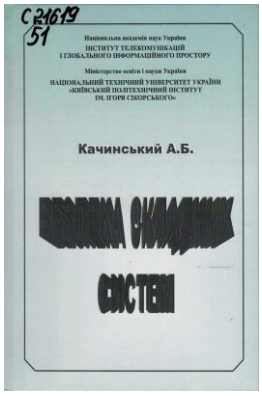
В сборнике представлены статьи, посвященные вопросам кибернетической безопасности критических инфраструктур, моделированию и противодействию информационным операциям, технологиям информационно-аналитических исследований на основе открытых источников информации, онтологическому подходу, семантическим сетям, сценарному анализу при обеспечении информационной поддержки принятия решений, компьютерному моделированию процессов и систем, актуальным проблемам технологического и правового обеспечения информационной и кибернетической безопасности.

Р 359177
622

Качество минерального сырья [Текст] : сборник научных трудов / [Вилкул Ю. Г., Азарян А. А., Колосов В. и др.] ; Акад. горных наук Украины, ГВУЗ "Криворожский нац. ун-т", Исполнительный комитет Криворожского городского совета [и др.]. - Кривой Рог : ФЛП Чернявский Д. А., 2017 - .
Т. 1. - Кривой Рог, 2017. - 700 с. : рис., табл. - Библиогр. в конце ст. - Текст кн. на рос., укр., англ. яз.

Из содержания:

Михайлів В. І. **Програма і методика випробувань інформаційних технологій для захисту даних в хмарних обчислювальних системах.** – С. 228-239.



С 21619
51

Качинський, Анатолій Броніславович.
Безпека складних систем [Текст] : монографія / А. Б. Качинський, ; за заг. ред. С. О. Довгого ; НАН України, Ін-т телекомунікацій і глобального інформаційного простору, Національний техн. ун-т України "Київський політехн. ін-т імені Ігоря Сікорського". - К. : [Юстон], 2017. - 498 с. : рис., табл. - Бібліогр. наприкінці розд.

У монографії розглядається загальна теорія безпеки як системне явище, що включає три її найважливіші складові: безпеку, загрози та ризик. Приділяється значна увага математичному моделюванню небезпечних процесів різного характеру, а також системному аналізу процесів управління її забезпечення. Наведені приклади розв'язання реальних задач теорії безпеки.

Кожедуб Ю. Аналіз документів з керування ризиком кібербезпеки / Ю. Кожедуб // Information Technology and Security. – January-June 2017. – Vol. 5, Iss.1 (8). – P. 82-95.

Р/1212

У статті подано аналіз новітніх документів щодо менеджменту ризиків в сфері забезпечення інформаційної безпеки та кібербезпеки. Дослідження сучасних стандартів показують, що їхню увагу зосереджено на ризиках, як це було започатковано в стандартах на системи менеджменту Міжнародної організації зі стандартизації.

Козка О. Використання програмного забезпечення. Як не порушувати авторські права / О. Козка // Справочник экономиста. – 2017. – № 10. – С. 68-74.

Р/1804

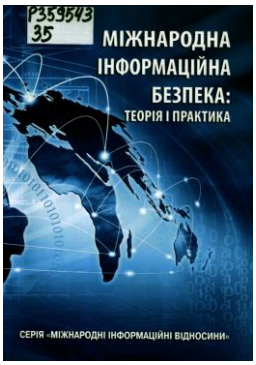
В своїй діяльності практично всі суб'єкти господарювання використовують комп'ютерні програми (КП) та бази даних (БД). Але ліцензійні продукти доволі дорого коштують. Тому багато хто встановлює так зване піратське програмне забезпечення. А це вже порушення авторських прав. Як чинне законодавство регулює авторське право на КП та БД і які санкції чекають на його порушників?

Б 18542
339

Львівський торговельно-економічний університет.
Вісник Львівського торговельно-економічного університету [Текст] : зб. наук. праць / [редкол.: Куцик П. О., Барна М. Ю., Семак Б. Б. та ін.]. - Л. : Вид-во Львів. торг.-екон. ун-ту. - (Економічні науки).
Вип. 52. - Л., 2017. - 188 с. : граф., табл. - Бібліогр. наприкінці ст. - Текст укр., англ.

Зі змісту:
Боднар І. Р. **Основні проблеми реалізації державної інформаційної політики.** – С. 21-26.

Р 359543
35



Міжнародна інформаційна безпека: теорія і практика [Текст] : підручник для студ. ВНЗ, які навч. за напрямом підготов. "Міжнародні відносини" та "Міжнародна інформація" / Є. Макаренко, М. Рижков, М. Ожеван [та ін.] ; Ін-т міжнародних відносин Київського нац. ун-ту ім. Тараса Шевченка. - К. : Центр вільної преси, 2016. - 418 с. - (Серія "Міжнародні інформаційні відносини"). - Бібліогр.: с. 394-416. - Парал. тит. арк. англ. Авт. на обкл. не зазнач.

Підручник присвячено теоретичним та прикладним дослідженням міжнародної інформаційної та кібербезпеки як складової міжнародної системи підтримання миру і стабільності. У підручнику подано тлумачення основних понять міжнародної інформаційної безпеки, охарактеризовано сучасні теорії інформаційної безпеки та інформаційного протиборства, розглянуто класифікацію інформаційних та кіберзагроз для системи міжнародної безпеки, проаналізовано стратегії і практику міжнародних організацій та національних держав у сфері інформаційної безпеки, представлено правові засади міжнародної інформаційної безпеки.

Р 360533
63

Національний лісотехнічний університет України.
Науковий вісник НЛТУ України [Текст] : збірник наук.-техн. праць. - Л. : [РВВ НЛТУ України]. - **Вип. 26.8**. - Л., 2016. - 400 с. : рис., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., рос., англ.

Зі змісту:

Грицюк Ю. І. **Кіберінтервенція та кібербезпека України: проблеми та перспективи їх подолання.** – С. 327-337.

«*Мета роботи* полягає в деталізації пріоритетних напрямків державної політики у сфері забезпечення кібербезпеки України в умовах проведення військових дій з Росією на Сході нашої країни та визначити шляхи вдосконалення концептуальних засад ведення державної політики у вказаній сфері».

Р 359561
34

Нашинець-Наумова, Анфіса Юріївна.
Інформаційна безпека: питання правового регулювання [Текст] : монографія / А. Ю. Нашинець-Наумова ; Київський ун-т імені Бориса Грінченка. - К. : [Гельветика], 2017. - 168 с. - Бібліогр.: с. 151-167.

У монографії розглядаються загальнонаукові категорії інформаційної безпеки в Україні та в світі. Авторка акцентує увагу на особливостях функціонування системи інформаційної безпеки. Окремо досліджуються питання захисту інсайдерської інформації суб'єктів господарювання.

Негрич О. М. Підвищення результативності надання адміністративних послуг в умовах забезпечення інформаційної безпеки / О. М. Негрич // Інвестиції: практика та досвід. – 2017. – № 22. – С. 87-90.

Р/2124

Розглянуто основні засади реалізації заходів переведення державних послуг у категорію публічних. Визначено обов'язки державних органів у сфері використання інформаційних технологій. Досліджено пріоритети реалізації державної політики в інформаційній сфері.

Р 359531
004

Перспективні напрями захисту інформації, всеукраїнська науково-практична конференція (3 ; 2017 ; Одеса).
Третя всеукраїнська науково-практична конференція "Перспективні напрями захисту інформації", 02-06 вересня 2017 року [Текст] : збірник тез / Одеська нац. акад. зв'язку імені О. С. Попова. - О. : ОНАЗ, 2017. - 104 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., рос.

У збірник включені тези доповідей за такими напрямками:
– організаційно-правові методи захисту інформації;
– системи ідентифікації і обробки персональних даних;
– системи квантової криптографії;

– технічні засоби виявлення каналів витоку інформації;
– засоби захисту інформації в інформаційних і телекомунікаційних системах;
– елементи і компоненти для систем захисту інформації;
– методи та засоби захисту господарських об'єктів.

Пилипчук В. Г. Реформування і розвиток системи захисту персональних даних в Україні / В. Г. Пилипчук, В. М. Брижко // Інформація і право. – 2017. – № 3. – С. 5-21.

Р/844

У статті висвітлено історико-правові аспекти та основні етапи формування національного законодавства з питань захисту персональних даних, процеси трансформації та нові правові стандарти ЄС у цій сфері, а також надано низку пропозицій щодо реформування і розвитку системи захисту персональних даних в контексті євроінтеграції України.

Пузняк З. М. Методика виявлення впливу на достовірність інформації в інформаційному просторі / З. М. Пузняк, Д. А. Шеремет // Сучасний захист інформації. – 2017. – № 3. – С. 50-55.

Р/2300

Розглянуто класифікацію інформаційних загроз, визначено критерії оцінки достовірності інформації в інформаційному просторі. Також запропонована методика виявлення впливу на достовірність інформації в інформаційному просторі на основі інформаційно-орієнтованої моделі.

Р 359585
34

Розвиток національної системи нормативно-правової інформації: комунікаційний та правовий аспекти (у контексті децентралізації влади в Україні) [Текст] : матеріали наук. практ. конф., 26 травня 2017 року / НДІ інформатики і права НАПрН України, Ф-т соціології і права Національного техн. ун-ту України "Київський політех. ін-т імені Ігоря Сікорського". - К. : КПІ ім. Ігоря Сікорського, [Політехніка], 2017. - 121 с. : рис. - Бібліогр. наприкінці ст. - Текст кн. укр., рос., англ.

Матеріали конференції присвячено проблемним питанням створення та розвитку національної системи нормативно-правової інформації з використанням сучасних засобів та прийомів інформаційно-комунікаційних технологій в умовах децентралізації влади в Україні. Особливу увагу приділено національній системі нормативно-правової інформації у процесах децентралізації влади, розбудові «електронного» парламенту та представницьких органів влади, а також процесам підвищення правової обізнаності суспільства.

Б 18537
339

Сервісна економіка в умовах глобальної конкуренції: правовий та інституційний виміри [Текст] = Service Economy in the Context of Global Competition: Legal and Institutional Dimensions : матеріали Міжнар. наук.-практ. конф., Київ, 15-16 листопада 2017 р. / [відп. ред. А. А. Мазаракі] ; Київський нац. торг.-екон. ун-т (м. Київ, Україна), Економічний ун-т (м. Варшава, Польща), Вільнюський ун-т (м. Вільнюс, Литва). - К. : [КНТЕУ], 2017. - 508 с. : граф., табл., рис. - Бібліогр. наприкінці ст. - Текст. укр., рос., англ.

Зі змісту:

Б 18310
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. 3 (149). - Х., 2017. - 184 с. : іл., табл. - Бібліогр. наприкінці ст. - Алф. покажч.: с. 183. - Текст укр., рос., англ.

Зі змісту:

Добринін І. С., Мальцева Н. О. **Вдосконалення методики факторного аналізу інформаційних ризиків**. – С. 146-150.
Запропонована методика оцінки ризиків базується на методиці факторного аналізу інформаційних ризиків з імплементацією до міжнародного стандарту ISO/IEC 27001:2013 та дозволяє отримувати кількісну оцінку інформаційних ризиків.

Ткачук Т. Ю. Забезпечення інформаційної безпеки у країнах позаблокового статусу / Т. Ю. Ткачук // Бизнес и безопасность. – 2017. – № 5. – С. 2-5.

Р/1070

… обравши євроінтеграційний курс, Україна має орієнтуватися на стратегію розвитку провідних європейських країн в інформаційній сфері, критично оцінюючи та адаптуючи до власних реалій їх позитивний досвід у сфері забезпечення інформаційної безпеки. У цьому контексті, корисним та цікавим буде досвід таких країн, як Австрія, Швейцарія, Фінляндія та Ірландія, адже вони є успішним прикладом втілення у життя оптимальної моделі інформаційного суспільства, створення розвиненої інфраструктури інформаційних технологій та забезпечення високого рівню доступу населення до них.

Ткачук Т. Забезпечення інформаційної безпеки у країнах Центральної та Східної Європи: сучасний етап та уроки для України / Т. Ткачук // Бизнес и безопасность. – 2017. – № 4. – С. 21-29.

Р/1070

Аналізуючи підходи до забезпечення інформаційної безпеки, прийняті у країнах Європи, слід дійти висновку, що на сьогоднішній день не існує уніфікованої моделі побудови національної системи безпеки у цій сфері. Втім потреба реалізації ефективних заходів із протидії сучасним загрозам інформаційній безпеці, передусім – кіберзагрозам, зумовлює потребу вдосконалення форм і методів захисту інформації.

Ткачук Т. Політика інформаційної безпеки НАТО / Т. Ткачук // Бизнес и безопасность. – 2017. – № 4. – С. 14-20.

Р/1070

«… набуває все більшого значення координація діяльності органів виконавчої влади, ЗМІ тощо з питань співробітництва з НАТО в інформаційній сфері. Цей вектор розвитку зовнішньої політики України впливає й на правове регулювання системи безпеки інформації як складової частини євроатлантичного безпекового простору».

Р 359546
34

Університетські наукові записки [Текст] = University Scientific Notes : часопис Хмельницького ун-ту управління та права / Хмельницький ун-т упр. та права, Нац. акад. держ. упр. при Президентові України, Ін-т законодавства Верховної Ради України = Universitatis Scientiae Notoriare. - Хмельницький : Вид-во ХУУП. - (Право. Економіка. Управління.). -
№ 2 (62). - Хмельницький, 2017. - 276 с. : граф., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., рос., англ.

Зі змісту:

Савицький В. Т. **Інформаційна безпека в системі національної безпеки України.** – С. 195-207.
На основі аналізу чинного законодавства з'ясовується сутність національної та інформаційної безпеки, розглядаються загрози інформаційній та національній безпеці, основні напрями державної політики, спрямовані на протидію інформаційній експансії як складовій гібридної війни Російської Федерації проти України.

С 21620
34

Університетські наукові записки [Текст] = University Scientific Notes : часопис / Хмельниц. ун-т упр. та права. - Хмельницький : Вид-во ХУУП. - (Право. Економіка. Управління). -
Вип. 3 (63). - Хмельницький, 2017. - 414 с. - Бібліогр. наприкінці ст. - Текст укр., англ.

Зі змісту:

Харитонов Є. О., Харитонова О. І. **«Інтернет-відносини» та «інтернет-правовідносини»: до визначення поняття і сутності.** – С. 27-38.
Доводиться, що вони є частиною більш широкого поняття «ІТ-відносини», під якими розуміється вся сукупність суспільних відносин, що виникають у процесі створення і використання інформаційних технологій.

С 21621
34

Університетські наукові записки [Текст] = University Scientific Notes : часопис / Хмельниц. ун-т упр. та права. - Хмельницький : Вид-во ХУУП. - (Право. Економіка. Управління). -
Вип. 4 (64). - Хмельницький, 2017. - 370 с. - Бібліогр. наприкінці ст. - Текст укр., англ.

Зі змісту:

Савицький В. Т. **Доступ і обмеження доступу до інформації: забезпечена свобода і застережена небезпека.** – С. 116-135.
… ставиться мета ***дослідити нормативно-правове регулювання інформаційної сфери*** з точки зору співвідношення інтересів особи і держави у забезпеченні права доступу особи до інформації та обмеження такого доступу з міркувань забезпечення національної безпеки.

Б 18453
355

Центр воєнно-стратегічних досліджень Національного університету оборони України.
Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського [Текст] : [наук. вид.]. - К. : [ЦВСД НУОУ].
Вип. 2 (60). - К., 2017. - 146 с. : табл. - Бібліогр. наприкінці ст. - Текст кн. укр., англ., рос.

Зі змісту:

Воєнна безпека та воєнна політика держави
Ткаченко А. Л., Михайлов О. В., Педь М. О., Троцько Л. Г., Цимбал І. В. **Оцінка термінів впровадження телекомунікаційних стандартів НАТО в Збройних Силах України.** – С. 13-16.

Б 18568
34

Юридичні науки [Текст] : [зб. наук. пр.] / голова РВР Н. І. Чухрай. - Л. : Вид-во Львів. політехніки, 2017. - 580 с. - (Вісник / Національний університет "Львівська політехніка" ; № 861). - Бібліогр. наприкінці ст. - Текст кн. укр., рос. та англ.

Зі змісту:

Перун Т. **Загальна характеристика правовідносин у сфері забезпечення інформаційної безпеки в Україні.** – С. 328-332.

Б 18456
004

Information Technology and Security [Text] : [ukrainian research papers collection] / National Technical University of Ukraine "Igor Sikorsky Kyiv Politechnic Institute", Institute of special Communication and information Protection. - K. : [Institute of special Communication and information Protection of Nat. Technical Univ. of Ukraine "Igor Sikorsky KPI"], 2016 - . –
Vol. 4, Issue 2 (7), July-december 2016. - K., 2016. - 288 p. - Бібліогр. наприкінці ст. - Текст англ. та укр.

Зі змісту:

Кожедуб Ю., Лісніченко Т. **Збір, обробка, застосування та захист інформації в документах високої соціальної значимості.** – С. 199-206.

Програмні системи захисту інформації

Аносов А. О. Генерування унікального паролю зі змінним правилом ускладнення / А. О. Аносов, А. В. Платоненко // Сучасний захист інформації. – 2017. – № 3. – С. 81-85.

Р/2300

Розглянуто метод підвищення захисту бездротових мереж від перехоплення інформації та впливу на неї шляхом створення надійного паролю зі змінним правилом ускладнення. Даний метод дає змогу його використання для програмних та апаратних засобів захисту, а також можливість застосовувати його для підвищення захисту облікових записів користувачів та інших систем захисту, де необхідне використання надійного паролю.

Богдан І. Верифікація моделей об'єктно-орієнтованих програм: перевірка на несуперечливість та узгодженість / І. Богдан // Технічні науки та технології. – 2017. – № 2. – С. 110-115. – Текст рос.

Р/1125

У випадку з об'єктно-орієнтованим програмним забезпеченням верифікації підлягає як сама програма, так і її модель, що представлена множиною UML-діаграм. Існує досить багато різних методів верифікації UML-діаграм, однак жоден з них не перевіряє на несуперечливість та узгодженість діаграми, що входять до складу тієї ж самої моделі.

Бородюк А. Решения для IoT с защитой от хакеров / А. Бородюк // Мир Автоматизации. – 2017. – № 1. – С. 82-84.

Р/2214

«Очевидно, что Индустрия 4.0 (Industry 4.0) дала существенный толчок инновациям в производственном секторе. А это в свою очередь уже требует повышенных мер безопасности в сфере IoT (Интернета вещей), в то время как их только начинают разрабатывать и внедрять», – говорится в исследовании, проведенном немецким Федеральным министерством по экономическим вопросам и энергетике (BMWI) на тему «IT-безопасность для Индустрии 4.0».

Бородюк А. Тренды рынка IoT: безопасность в приоритете / А. Бородюк // Мир Автоматизации. – 2017. – № 3-4. – С. 48-50.

Р/2214

«Первым продуктом Kontron Security Solution является комбинированное аппаратное и программное решение Kontron Approtect. Оно включает в себя встроенный модуль безопасности и программное обеспечение, объединяя широкий набор функций безопасности».

Гавриленко С. Ю. Дослідження методів вторгнення в комп'ютерні системи, засноване на показнику Херста / С. Ю. Гавриленко, В. В. Челак, М. Білогорський // Сучасні інформаційні системи = Advanced Information Systems. – 2017. – Т.1, № 2. – С. 58-61. – Текст рос.

Р/543

Завдання: дослідження сучасних засобів антивірусного захисту комп'ютерних систем; дослідження показника Херста для оцінки стану комп'ютерної системи; розробка програмної моделі оцінки стану комп'ютерної системи, що базується на показнику Херста, аналіз отриманих експериментальних даних.

Гавриленко С. Ю. Розробка методу і програмної моделі статичного аналізатора шкідливих файлів / С. Ю. Гавриленко, Д. М. Саєнко // Сучасні інформаційні системи = Advanced Information Systems. – 2017. – Т.1, № 1. – С. 44-48. – Текст англ.

Р/543

Проаналізовано РЕ-структуру файлу, обрані секції для подальшого аналізу. Розроблена програмна модель статичного детектування файлів і виконано аналіз безпечних і шкідливих файлів. Обрані ознаки у вигляді рядків і API функцій, сформована бітова маска для подальшого аналізу файлів. Виконано сканування 3500 файлів шкідливого і безпечного програмного забезпечення, проведено їх аналіз.

Р 358932
004

Каплун, Валентина Аполінаріївна.
Захист програмного забезпечення [Текст] : лабор. практикум / В. А. Каплун, О. В. Дмитришин, Ю. В. Баришев ; Вінницький національний технічний університет. - Вінниця : ВНТУ, 2017. - 75 с. : табл., рис. - Бібліогр.: с. 74.

Лабораторний практикум містить практичні відомості щодо методів захисту програмного забезпечення від несанкціонованого копіювання і використання, від статичного та динамічного дослідження. Детально розглянуто основні засоби програмування для використання цих методів у реалізації задач побудови систем захисту програмного забезпечення.

Кассем Халіфе. Оцінка вразливості системного програмного забезпечення / Кассем Халіфе, Г. Я. Криховецький, Г. А. Кучук // Системи управління, навігації та зв'язку. – 2017. – Вип. 6. – С. 141-144.

Р/2152

У статті запропонована методика оцінки вразливості системного програмного забезпечення. Теоретична частина методики базується на методі динаміки середніх. Відмінною особливістю розробленої методики є врахування можливості масштабування процесу розробки програмного забезпечення шляхом впровадження фахівців з безпеки *(PersonNon, SecDev)* без суттєвої зміни ефективності розробки. На прикладі стратегії, прийнятої при імітаційному моделюванні, проведено дослідження і доведена доцільність використання додаткових фахівців з безпеки.

Коваленко А. В. Масштабирование имитационной модели технологии тестирования безопасности / А. В. Коваленко // Системи управління, навігації та зв'язку. – 2017. – Вип. 6. – С. 181-184.

Р/2152

В данной работе разработана и усовершенствована имитационная модель технологии тестирования безопасности на основе положений теории масштабирования имитационных моделей, отличающаяся от известных адаптацией выбора входных операторов управления и данных к повышению требований оперативности разработки и реализации модели, для оценки результатов математического моделирования технологий тестирования безопасности Web-приложений.

Коваленко О. В. Технологія тестування DOM XSS уразливості / О. В. Коваленко, К. Молодецька-Гринчук // Автоматизація технологічних і бізнес-процесів. – 2017. – Т. 9, № 2. – С. 36-42.

Р/2307

В роботі представлені результати дослідження та алгоритми тестування на вразливість до одних з найбільш поширених видів атак на Web-додатки – Міжсайтовий Скриптінг – XSS (Cross Site Scripting) – DOM XSS.

Козачок В. А. Технології протидії шкідливим програмам та завідома фальшивому програмному забезпеченню / В. А. Козачок, А. А. Рой, Л. В. Бурячок // Сучасний захист інформації. – 2017. – № 2. – С. 30-34.

Р/2300

Обгрунтована необхідність створення систем захисту від шкідливого програмного забезпечення в інформаційних системах. Розглянуті сучасні засоби захисту від шкідливих програм. Показана необхідність використання прогресивних та перспективних технологій інформаційної безпеки.

Лисенко С. М. Метод виявлення шкідливих програмних засобів на основі алгоритму найближчих сусідів / С. М. Лисенко, В. В. Гуменюк // Вісник Хмельницького національного університету. Серія: Технічні науки. – 2017. – № 6. – С. 96-101.

Р/1055«Т»

В роботі представлено метод виявлення шкідливого програмного забезпечення на основі алгоритму *k*-найближчих сусідів, який здійснює класифікацію програмного забезпечення на шкідливе і нормальне.

Р 359953
004

Литвин, Александр Иванович.
Информатика и программирование. Открытые системы [Текст] : монография / А. И. Литвин, М. А. Литвин. - Д. : Издатель Белая Е. А., 2017. - 422 с. : ил., табл.

Продемонстрированы реальные возможности отказа самого широкого круга пользователей от дорогостоящего и небезопасного программного обеспечения и перехода на программное обеспечение с открытым кодом. В качестве альтернативы для компьютерных систем, которые в подавляющей массе работают на платформе *Windows*, предложен переход на компьютерную платформу *Linux Ubuntu* с интегрированным офисным пакетом *LibreOffice* и многими десятками других программ и приложений.

Р 360280
51

Математичне та комп'ютерне моделювання [Текст] : збірник наук. праць / Ін-т кібернетики імені В. М. Глушкова НАН України, Кам'янець-Подільський нац. ун-т імені Івана Огієнка. - [Кам'янець-Подільський] : Кам'янець-Подільський нац. ун-т імені Івана Огієнка, 2008 - . - (Серія: Технічні науки). -
Вип. 15. - [Кам'янець-Подільський], 2017. - 272 с. : іл., табл. - Бібліогр. наприкінці ст. - Алф. покажч. авторів: с. 267-268. - Текст кн. укр., рос., англ. Дод. тит. арк. англ.

Зі змісту:

Маслова Н. О. **Застосування задачі розподілу ресурсів в системах захисту інформації**. – С. 120-125. Проаналізовано застосування задач розподілу ресурсів в системах захисту інформації та методів їх вирішення; описано програмне забезпечення, яке дозволяє проводити експериментальні дослідження з вибору ефективного за часом алгоритму.

Пархоменко І. І. Способи захисту каналів корпоративних мереж на базі апаратно-програмних засобів / І. І. Пархоменко, В. В. Галкін // Вісник Інженерної академії України. – 2017. – № 2. – С. 81-85.

Р/1139

В статті розглянуто процеси захисту інформації, передані в рамках розподіленої корпоративної мережі, що використовує мережі відкритого доступу, з використанням апаратно-програмних засобів і тим самим вирішуючи питання захисту інформації, що циркулює між довіреними мережами.

Родін Є. С. Задачі з керування ризиками інформаційної безпеки апарата прийняття рішень / Є. С. Родін // Проблеми програмування. – 2017. – № 4. – С. 89-97.

Р/1373

Запропоновано перелік завдань, вирішення яких веде до побудови моделі залежності рівня ризику інформаційної безпеки ресурсу від наявності зв'язків та ступеню впливу вразливостей, загроз і наслідків на даний інформаційний ресурс та організацію в цілому.

Семенов С. Г. Удосконалений спосіб масштабування гнучкої методології розробки програмного забезпечення / С. Г. Семенов, Кассем Халіфе, М. М. Захарченко // Сучасні інформаційні системи = Advanced Information Systems. – 2017. – Т.1, № 1. – С. 79-84. – Текст рос.

Р/543

Проведено аналіз існуючих гнучких методологій розробки програмного забезпечення, визначені перспективні напрямки і підходи даної індустрії, виявлені можливості масштабування гнучких методологій. Удосконалено схему життєвого циклу розробки програмного забезпечення, відмінною рисою якої є введення додаткових підрозділів і ролей, що мають на меті підвищення безпеки програмного забезпечення. Удосконалено структуру управління розробкою програмного забезпечення, що відрізняється від відомих урахуванням ризиків безпеки в процесі розробки.

Федухин А. В. К вопросу о связи надежности и достоверности функционирования компьютерных систем / А. В. Федухин, Н. В. Сеспедес Гарсия, Ар. А. Муха // Математичні машини і системи. – 2017. – № 2. – С. 145-155.

Р/1052

Розглянуто питання визначення аналітичної залежності достовірності функціонування комп'ютерних систем від типу структур та їх характеристик. Проведено розрахунки показників достовірності та ймовірності безвідмовної роботи, класифікація типів конфігурацій систем, розрахунок достовірності, ступінь компенсації наслідків відмови.

С 21563
62

"Харківський політехнічний інститут". Національний технічний університет.
Вісник Національного технічного університету "ХПІ" [Текст] : збірник наук. праць. - Х. : НТУ "ХПІ". - (Серія: Інформатика та моделювання). -
№ 21 (1243). - Х., 2017. - 178 с. : граф., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., рос., англ.

Зі змісту:

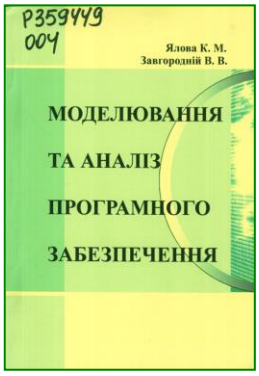
Проблемы защиты информации в современных системах

Грішин І. Ю., Тіміргалєєва Р. Р., Міронов М. В. **Аналіз ефективності моделей аутентифікації користувачів на основі клавіатурного почерку.** – С. 153-164. – Текст рос.
Завданням дослідження була перевірка працездатності програмного прототипу моделі, а також дослідження його функціональних можливостей. Здійснено оцінку правильності роботи програмного прототипу моделі на кожному з етапів. Для проведення експериментальних досліджень розроблений програмний комплекс, що дозволяє провести необхідний перелік експериментів, а також здійснити статистичну обробку результатів, оцінити значення помилок першого і другого роду при аутентифікації. Іл.: 5. Бібліогр.: 13 назв.

Швачич Г. Г. Деякі аспекти інформаційної безпеки функціонування багатопроцесорних обчислювальних систем / Г. Г. Швачич, О. В. Іващенко, В. В. Бусигін // Сучасні інформаційні системи = Advanced Information Systems. – 2017. – Т.1, № 2. – С. 62-69. – Текст рос.

Р/543

Відповідно до деяких аспектів побудови багатопроцесорних систем розглянуто та виявлено ключові елементи, які вимагають особливої уваги при розробці системи безпеки. У роботі показано, що для паралельної системи потрібно більше апаратних та програмних засобів і з кожним додатковим модулем обчислення система ускладнюється. А це, в свою чергу, ще більше ускладнює систему захисту в цілому. Для захисту даних в таких системах розглядається та аналізується ряд методів. Проте в перспективі запропонований підхід дозволяє забезпечити підвищену безпеку функціонування багатопроцесорних систем.



Р 359449
004

Ялова, Катерина Миколаївна.
Моделювання та аналіз програмного забезпечення [Текст] : навч. посіб. для студ. вищ. навч. закл. / К. М. Ялова, В. В. Завгородній ; Дніпровський держ. технічний ун-т. - Кам'янське : ДДТУ, 2017. - 378 с. - Бібліогр.: с. 373-375. - Предм. покажч.: с. 376-377.

Навчальний посібник містить інформацію про сучасні способи моделювання програмного забезпечення із використанням патернів проектування на основі аналізу предметної області та з метою створення якісного програмного коду.

Телекомунікаційні мережі та інформаційно-комунікаційні технології

Аналіз ризиків інформаційно-телекомунікаційної мережі на основі когнітивних карт і причинно-наслідкової діаграми / В. В. Косенко, О. В. Малєєва, О. Ю. Персіянова, А. І. Роговий // Сучасні інформаційні системи = Advanced Information Systems. – 2017. – Т.1, № 1. – С. 49-56. – Текст англ.

Р/543

Проведена класифікація приватних ризиків ІТМ з причин та за факторами їх виникнення. Визначено негативні наслідки, що негативно впливають на основні характеристики функціонування ІТМ. В результаті сформована структурна системна модель ризиків ІТМ, в якій відображені взаємозв'язки між елементами основних аспектів ризику. Для кількісної оцінки впливу ризику на функціонування ІТМ запропонований метод, заснований на теорії причинного аналізу. Модель ризиків заснована на побудові та аналізі імовірнісних або нечітких когнітивних карт.

Грищук Р. В. Класифікація профілів інформаційної безпеки акторів у соціальних інтернет-сервісах (на прикладі мікроблогу Twitter) / Р. В. Грищук, В. М. Мамарєв, К. В. Молодецька-Гринчук // Інформаційні технології та комп'ютерна інженерія. – 2017. – № 2. – С. 12-19.

Р/1954

Важливим науковим завданням є своєчасне виявлення ознак інформаційних операцій у СІС. На попередніх етапах досліджень розроблено метод побудови профілів інформаційної безпеки акторів у СІС, який дозволяє оцінити рівень їх загрози як можливого учасника інформаційної операції. Перспективним напрямком досліджень є адаптація даного методу для конкретного СІС і його верифікація для подальшого використання у системі забезпечення інформаційної безпеки держави.

Дмитренко Ю. Угрозы облачной безопасности / Ю. Дмитренко // Бизнес и безопасность. – 2017. – № 5. – С. 36-39.

Р/1070

Работа в облаках обладает огромным потенциалом в бизнес-среде. Зачастую применение облачных вычислений – наилучший способ решения корпоративных задач, на которые не хватает мощности собственной ИТ-инфраструктуры. Помимо существенной экономической выгоды, важным аргументом использования этой технологии для многих компаний может стать возможность доступа к данным из любой точки планеты.

Дудатьєв А. В. Моделі інформаційної підтримки управління комплексною інформаційною безпекою / А. В. Дудатьєв, О. П. Войтович // Радіоелектроніка, інформатика, управління. – 2017. – № 1. – С. 107-114.

Р/0170

Наукова новизна проведеного дослідження полягає в тому, що вперше запропоновано модель оцінювання комплексної інформаційної безпеки багаторівневої соціотехнічної системи на рівнях управління «підприємство – регіон – держава».

Практична новизна полягає у розробці програмного забезпечення, яке реалізує процес аналізу та оцінювання рівня комплексної інформаційної захищеності багаторівневої соціотехнічної системи на рівнях управління «підприємство – регіон – держава», а також синтезу управлінських рішень на базі сформованих баз знань.

Р 358205
3

Запорізька державна інженерна академія.

Гуманітарний вісник Запорізької державної інженерної академії [Текст] = Humanities Bulletin of Zaporizhzhe State Engineering Academy : збірник наук. праць = Гуманитарный вестник Запорожской государственной инженерной академии. - Запоріжжя : ЗДІА. -

Вип. 68. - Запоріжжя, 2017. - 290 с. : іл. - Бібліогр. наприкінці ст. - Текст укр., рос., англ. Дод. тит. арк. рос., англ.

Зі змісту:

Соснін О. В. **Концептуальні засади інформаційної безпеки в Україні як умови інноваційного розвитку держави та сучасного тренду суспільства.** – С. 130-139.
Проаналізовано комплекс проблем інформаційної безпеки, які пов'язані з проникненням інформаційно-комунікаційних технологій (ІКТ) в усі сфери життєдіяльності людини.

Ігнатенко О. П. Теоретико-ігровий підхід до проблеми безпеки мереж / О. П. Ігнатенко // Проблеми програмування. – 2017. – № 3. – С. 149-160.

Р/1373

В даній роботі здійснено огляд основних напрямків застосування теоретико-ігрового підходу до розв'язання актуальних проблем безпеки. Описано сучасний стан області, виділені основні напрямки загроз та відповідні моделі і методи теорії ігор. Запропоновано класифікацію ігрових підходів у області кібербезпеки та проведено порівняння різних класифікацій. Окремо розглядаються атаки на відмову.

Р 359864
621.39

"Інфокомунікації - сучасність та майбутнє", міжнародна науково-практична конференція (7 ; 2017 ; Одеса).

Сьома міжнародна науково-практична конференція "Інфокомунікації - сучасність та майбутнє", 26- 27 жовтня 2017 року [Текст] : збірник тез / Одеська нац. акад. зв'язку імені О. С. Попова : [в 3-х ч.]. - О. : ОНАЗ, 2017. -

Ч. 1. - О., 2017. - 148 с. : іл., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., рос., англ.

У збірник включені тези доповідей за такими напрямками:

- сучасні системи мобільного зв'язку та широкосмугового радіодоступу;
- мультисервісні засоби телекомунікацій та телекомунікаційні мережі;
- ***інформаційна безпека.***

Р 359908
004

Інформаційні технології в освіті, науці і виробництві, Міжнар. наук.-практ. конф. (6 ; 2017 ; Луцьк).

Тези доповідей VI Міжнародної науково-практичної конференції "Інформаційні технології в освіті, науці і виробництві", (ІТОНВ-2017), 25-27 травня 2017 року [Текст] : [наук. вид.] / Ін-т модернізації змісту освіти МОНУ, Волинська облрада, Українська Федерація Інформатики [та ін.]. - Луцьк : ЛНТУ, 2017. - 236 с. : іл., табл. - Бібліогр. наприкінці ст. - Текст укр., рос., англ.

Зі змісту:

Мельник К. В., Лотоцький І. М., Мельник В. М., Багнюк Н. В. **Нейромережевий детектор відстеження вірусних атак.** – С. 205-208.

Панасюк Н. Л., Парфенюк Ю. О. **Захист даних в Wi-Fi мережах.** – С. 217-220.

Кец Д. Ідентифікація загроз несанкціонованого доступу до конфіденційних мережевих ресурсів / Д. Кец, Д. Присяжний, О. Салієва // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2017. – Вип. 1. – С. 59-70.

Р/2287

Розглянуто існуючі атаки на конфіденційні мережеві ресурси і способи їх виявлення, а також запропоновано метод і алгоритм ідентифікації загроз несанкціонованого доступу, що базується на аналізі фактичних даних об'єму мережевого трафіку. У роботі представлено тестування розробленого алгоритму, яке показало високу точність виявлення аномальної мережевої активності.

Князев Д. Інтернет-шахрайство: новітні реалії / Д. Князев, С. Князев // Бизнес и безопасность. – 2017. – № 5. – С. 32-35.

Р/1070

«Світова павутина» дозволяє майже безмежне спілкування, не звертаючи уваги на відстань та кордони, пропонує різноманітні віртуальні розваги, сприяє веденню бізнеса, здійсненню покупок за найбільш привабливими цінами та асортиментом, проведенню фінансових розрахунків тощо. Разом з тим, переваги on-line можливостей іноді можуть виявитись достатньо небезпечними для інтернет-користувачів, а новітні технології в руках шахраїв дієвим інструментом для протиправних дій.

Кучернюк П. В. Модель загроз безпеки в інформаційно-комунікаційних системах на основі регресійного аналізу / П. В. Кучернюк, А. О. Довгаль // Електроніка та зв'язок. – 2017. – Т. 22, № 2. – С. 79-84.

Р/1325

Засобами регресійного аналізу з використанням багаторівневої класифікації загроз, яка базується на моделі OSI, розроблена математична модель загроз безпеці інформаційно-комунікаційних систем. Бібл. 10, табл. 2.

Б 18495
004

Методи та засоби кодування, захисту й ущільнення інформації [Текст] = Методы и средства кодирования, защиты и сжатия информации : тези доп. шостої Міжнар. наук.-практ. конф., м. Вінниця, Україна, 24-25 жовтня 2017 року / Вінницький нац. техн. ун-т, Прикарпатський нац. ун-т імені Василя Стефаника, Ін-т кібернетики імені В. М. Глушкова НАН України [та ін.]. - Вінниця : [ВНТУ], 2017. - 170 с. : рис. - Бібліогр. наприкінці ст. - Текст кн. укр., рос., англ.

Збірник містить матеріали доповідей Шостої Міжнародної науково-практичної конференції з сучасних проблем кодування, захисту й ущільнення інформації за чотирма основними напрямками: методи та засоби завадостійкого кодування; методи та засоби захисту інформації від несанкціонованого доступу; методи та засоби ущільнення інформації; методи та засоби перетворення форм інформації.

Молодецька-Гринчук К. Метод оцінювання ознак загроз інформаційній безпеці держави у соціальних інтернет-сервісах / К. Молодецька-Гринчук // Автоматизація технологічних і бізнес-процесів. – 2017. – Т. 9, № 2. – С. 36-42.

Р/2307

Відсутність ефективних методик виявлення ознак загроз у соціальних інтернет-сервісах створює передумови для проведення інформаційних операцій в інтересах провідних держав світу чи зацікавлених осіб. Розроблено метод оцінювання ознак загроз, який ґрунтується на їх скалярній згортці по нелінійній схемі компромісів. Перевагами методу є застосування сучасних підходів до виявлення ознак інформаційних акцій у соціальних інтернет-сервісах, компроміс між частинними критеріями і оптимальність отриманого рішення за Парето. Виконано експериментальне дослідження запропонованого методу оцінювання ознак загроз на прикладі реальної інформаційної акції.

Б 18406
621

Наукові нотатки [Текст] : міжвуз. зб. (за галузями знань "Технічні науки") / МОН, [Луцький нац. техн. ун-т]. - Луцьк : [РВВ ЛНТУ]. -
Вип. 58. - Луцьк, 2017. - 360 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст укр., рос. англ.

Зі змісту:

Крестьянполь Л. Ю. **Аналіз способів захисту інформації при несанкціонованому доступі з інтернету в локальну мережу.** – С. 193-197.

Р 359756
004

Наукоемкие технологии в инфокоммуникациях: обработка информации, кибербезопасность, информационная борьба [Текст] : монография / [В. В. Баранник, В. В. Твердохлеб, А. В. Хаханова и др.] ; под общ. ред. В. М. Безрука, В. В. Баранника ; Харьк. нац. ун-т радиоэлектроники. - Х. : Лидер, 2017. - 600 с. : рис. - Библиогр. в конце ст. - Авт. указ. в содержании.

Коллективная монография содержит материалы по актуальным направлениям наукоемких инфокоммуникационных технологий. Рассматриваются вопросы планирования и управления в инфокоммуникационных сетях, эффективного хранения, обработки, интеллектуализации инфокоммуникационного пространства, распознавания образов, распределенной обработки информации и облачных вычислений, многопрофильного кодирования, кибербезопасности и информационной борьбы с использованием инфокоммуникаций.

Б 18627
621.3

Перспективні напрямки сучасної електроніки, інформаційних і комп'ютерних систем [Текст] : тези доп. на II Всеукр. наук.-практ. конф. MEICS-2017, м. Дніпро, 22-24 листопада 2017 р. / Дніпровський нац. ун-т ім. Олеся Гончара. - [Кременчук] : [ПП Щербатих О. В.], 2017. - 320 с. : граф., рис. - Бібліогр. наприкінці ст. - Текст кн. укр., рос., англ. мов.

Зі змісту:

Шматько Ю. **Системи захисту інформації в інформаційний системі організації від несанкціонованого доступу.** – С. 171-172.
Захист інформації в комп'ютерній мережі ефективніше в тому випадку, коли проектування і реалізація системи захисту проходить три етапи: *аналіз ризику; реалізація політики безпеки; підтримка політики безпеки.*

Б 18479
34

Повітряне і космічне право. Юридичний вісник [Текст] : наук. пр. Нац. авіац. ун-ту / Нац. авіац. ун-т. - К. : [НАУ]. -
№ 3 (44). - К., 2017. - 184 с. : табл. - Бібліогр. наприкінці ст. - Текст укр., англ.

Зі змісту:

Сопілко І. М. **Становлення інформаційного суспільства та інформаційні загрози в мережі Інтернет.** – С. 61-69.

Виокремлено новий вид загроз, пов'язаних з Інтернетом, а саме ризики, що пов'язані із захистом об'єктів авторського права в мережі Інтернет, що потребують належного реагування держави, та проаналізовано напрямки вдосконалення захисту авторських прав у мережі Інтернет.

Проаналізовано інші види загроз, які актуалізувались у зв'язку із поширеністю мережевого суспільства та доступності до Інтернету.

Б 18431
621.3

Радіоелектроніка та телекомунікації [Текст] : зб. наук. пр. / голова ред.-вид. ради Н. І. Чухрай. - Л. : Вид-во Львів. політехніки, 2016. - 260 с. : іл., табл. - (Вісник / Національний університет "Львівська політехніка" ; № 849). - Бібліогр. наприкінці ст. - Текст кн. укр. та англ.

Зі змісту:

Толюпа С. В., Пархоменко І. І. **Захист інформації з інтелектуальною підтримкою організаційно-технічного й оперативного управління.** – С. 248-255. – Текст англ.

Для успішного використання сучасних інформаційних технологій необхідно ефективно управляти не тільки мережею, але і її системою захисту інформації (СЗІ), при цьому на рівні інформаційної системи автономно повинна працювати система, яка реалізує управління складом подій інформаційної безпеки, планування модульного складу СЗІ й аудиту.

Рылов А. Защита от взлома: как уберечь «умную сеть» от хакеров / А. Рылов // Энергия: экономика, техника, экология. – 2017. – № 1. – С. 53-55.

Р/294

Благодаря внедрению систем автоматизации удалось значительно улучшить управление электрическими сетями, их работа стала более надежной. Однако если такая система управляется удаленно, через интернет, то может появиться угроза взлома или вирусного заражения систем, управляющих работой сети.

Система оцінювання ризиків інформаційної безпеки – «РИЗИК-КАЛЬКУЛЯТОР» / О. Г. Корченко, Б. Б. Ахметов, С. В. Казмірчук, Є. А. Часновський // Безпека інформації. – 2017. – Т. 23, № 2. – С. 145-152. – Текст рос.

Р/1408

… запропоновано структурно-параметричну модель системи оцінювання ризиків – «РИЗИК-КАЛЬКУЛЯТОР», яка за рахунок базових структурних компонент (підсистем формування первинних і вторинних даних) дозволяє мінімізувати участь експерта і максимально автоматизувати процес формування необхідних для оцінювання параметрів. На її основі розроблені базовий алгоритм і програмний засіб, який, на відміну від відомих, використовує в якості вхідних даних оціночні параметри у вигляді метрик CVSS.

Б 18309
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 (148). - Х., 2017. - 256 с. : іл., табл. - Бібліогр. наприкінці ст. - Алф. покажч.: с. 256. - Текст укр., рос., англ.

Зі змісту:

Дудикевич В. Б., Микитин Г. В., Ребець А. І. **Комплексна система безпеки кіберфізичної системи «iPhone – Wi-Fi, Bluetooth – давачі».** – С. 84-87.

Мельник М. О., Константинова Н. С., Бескупський О. В. **Організація захисту інтернет-ресурсу від несанкціонованого доступу та програмний захист авторських прав.** – С. 122-125.

Мельник М. О., Нікітін Г. Д., Мезенцева К. О. **Аналіз побудови моделі політики інформаційної безпеки підприємства.** – С. 126-128.

Б 18519
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. 4 (150). - Х., 2017. - 262 с. : іл., табл. - Бібліогр. наприкінці ст. - Алф. покажч.: с. 260. - Текст укр., рос., англ.

Зі змісту:

Рудченко Д. В. **Виявлення спільнот та їх лідерів в соціальних мережах для забезпечення безпеки.** – С. 128-131.

Сігайов А. Ботнети: методи виявлення та протидії / А. Сігайов, А. Воловик // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2017. – Вип. 1. – С. 22-30.

Р/2287

Розглянуті історія ботнетів, їхня типова архітектура, тенденції розвитку. Надані рекомендації щодо їхнього виявлення та знешкодження.

Снігуров А. В. Підхід до прогнозування та оцінки ситуації при комплексній інформаційній атаці на організацію з використанням індикаторів ризиків інформаційної безпеки / А. В. Снігуров, В. Ю. Балашов, А. Ю. Нестеренко // Системи озброєння та військова техніка. – 2017. – № 2. – С. 184-188.

Р/1903

В статті представлений підхід до прогнозування та оцінки ситуації при комплексній інформаційній атаці на організацію. Для вирішення даного завдання пропонується використовувати теорію ризиків інформаційної безпеки та індикатори реалізації даних ризиків. Цей підхід пропонується для реалізації при створенні систем менеджменту інформаційної безпеки організацій (підприємств).

Субач І. Аналіз існуючих рішень запобігання вторгненням в інформаційно-телекомунікаційні мережі / І. Субач, В. Фесьоха, Н. Фесьоха // Information Technology and Security. – January-June 2017. – Vol. 5, Iss.1 (8). – P. 29-41.

Р/1212

Наведено порівняльний аналіз основних існуючих програмних рішень запобігання вторгненням в інформаційно-телекомунікаційні мережі, які відкриті на основі загальнодоступних ліцензій.

Толюпа С. В. Атаки аутентифікації та авторизації на WEB-ресурси / С. В. Толюпа, В. С. Білецький // Вісник Інженерної академії України. – 2017. – № 2. – С. 91-96.

Р/1139

В статті розглянуто уразливості аутентифікації та авторизації веб-додатків, які надають зловмисникам широкий простір для дій. Помилки проектування і адміністрування дозволяють зловмисникам отримувати важливу інформацію, а також порушувати функціонування веб-додатків, здійснювати атаки на користувачів, проникати у внутрішню мережу компанії і отримувати доступ до критично значущих ресурсів.

Б 18506
629.7

Харківський національний університет Повітряних Сил імені Івана Кожедуба.
Збірник наукових праць Харківського національного університету Повітряних Сил [Текст] = Scientific Works of Kharkiv National Air Force University Digest : щоквартальне наукове видання / Міноборони України. - Х. : [Видавництво ХНУПС імені Івана Кожедуба]. -
Вип. 4 (53) : Тематичний випуск присвячений 80-річчю факультету Автоматизованих систем управління та наземного забезпечення польотів авіації. - Х., 2017. - 182 с. : рис., табл. - Бібліогр. наприкінці ст. - Алф. покажч.: с. 181. - Текст кн. укр., рос., англ.

Зі змісту:

Інформаційна безпека

Васюта К. С., Захарченко І. В., Нікіфоров І. А. **Метод формування хаотичних сигнально-кодових конструкцій для передачі інформації в захищених інформаційних телекомунікаційних мережах.** – С. 46-53. – Текст англ.

Бараннік В. В., Рябуха Ю. М., Ларін В. В. **Обгрунтування необхідності підвищення захисту оперативної відеоінформації в бездротових інфокомунікаційних системах. –** С. 54-58. – Текст англ.

Бараннік В. В., Тарнополов Р. В., Хаханова Г. В., Бараннік Д. В. **Метод підвищення оперативності та конфіденційності відеоданих в інфокомунікаційних технологіях.** – С. 59-61.

Чербан О. Атрибути влади засобів масової інформації в інформаційному суспільстві / О. Чербан // Освіта регіону: політологія, психологія, комунікації. – 2017. – № 1. – С. 78-82.

Р/990

Проаналізовано поняття інформаційного суспільства та виділено основні його ознаки. Дається визначення поняттю «інформаційний простір» та його складовій частині – засобам масової інформації. Подана етимологія слова «влада». На підставі проаналізованих понять визначено місце засобів масової інформації в кратологічному полі. Висвітлено місце засобів масової інформації в інформаційних війнах.

Шарадкін Д. Використання критерію виявлення змін поведінки об'єкта на основі аналізу коефіцієнта автокореляції в задачах забезпечення інформаційної безпеки / Д. Шарадкін // Information Technology and Security. – January-June 2017. – Vol. 5, Iss.1 (8). – P. 42-54.

Р/1212

Розглядаються методи виявлення факту зміни поведінки об'єктів, зокрема сучасних інформаційно-комп'ютерних мереж, на основі аналізу їх моделей функціонування у вигляді часових рядів.

Ярощук Д. О. Удосконалення методу обрахунку впливу загроз інформаційної безпеки на ефективність функціонування закритої телекомунікаційної мережі / Д. О. Ярощук, О. А. Мясищев // Вісник Хмельницького національного університету. Серія: Технічні науки. – 2017. – № 6. – С. 64-69.

Р/1055«Т»

Розглядається завдання забезпечення ефективного функціонування телекомунікаційних мереж (ТКМ). Розроблені методи оцінки захищеності об'єктів мережі від загроз інформаційної безпеки засновані на якісній експертній оцінці. Проведено удосконалення в переході до кількісної оцінки ефективності функціонування ТКМ на підставі критеріїв доступності інформації і послуг зв'язку.

Б 18456
004

Information Technology and Security [Text] : [ukrainian research papers collection] / National Technical University of Ukraine "Igor Sikorsky Kyiv Politechnic Institute", Institute of special Communication and information Protection. - K. : [Institute of special Communication and information Protection of Nat. Technical Univ. of Ukraine "Igor Sikorsky KPI"], 2016 - . -

Vol. 4, Issue 2 (7), July-december 2016. - K., 2016. - 288 p. - Бібліогр. наприкінці ст. - Текст англ. та укр.

Зі змісту:

Толюпа С., Успенський О. **Побудова систем захисту інформації на основі багаторівневої ієрархічної моделі.** – С. 172-181.

Павленко П., Віноградов М., Гнатюк С., Гізун А., Гнатюк В. **Метод формування правил екстраполяції інцидентів для мережево-центричного моніторингу інформаційно-телекомунікаційних систем.** – С. 189-199.

Інформаційне протиборство у воєнних конфліктах. Інформаційно-психологічна безпека

Гиріна Т. С. Комплексний розвиток аудіовізуального контенту в умовах забезпечення інформаційної безпеки держави / Т. С. Гиріна // Держава та регіони. Серія: Соціальні комунікації. – 2017. – № 4. – С. 87-91.

Р/1520

У статті подано результати емпіричного дослідження із визначення медіа смаків сучасних українців, визначення ставлення та рівня відповідності потребам аудиторії сучасного медіа-контенту в аспекті аудіовізуальних ЗМІ; проаналізовано зріз готовності українців віддавати перевагу національному контенту на противагу популярному закордонному.

Горовий В. М. Процес входження України і РФ в інформаційне суспільство як джерело міждержавних протиріч / В. М. Горовий // Вісник Національної академії наук України. – 2017. – № 8. – С. 65-71.

Р/250

У статті розглянуто прояв характерних особливостей інформаційного суспільства в еволюції Росії та України, проаналізовано відмінності в темпах розвитку демократизації обох країн, що стало однією з найважливіших причин їх нинішнього протистояння.

Киричок А. П. Історіографічний аналіз російсько-української інформаційної війни / А. П. Киричок // Держава та регіони. Серія: Соціальні комунікації. – 2017. – № 3. – С. 23-27.

Р/1520

У статті здійснено спробу окреслити основні етапи інформаційного протистояння двох сусідніх держав і визначити шляхи підвищення інформаційної обороноздатності України. Поетапно описано кожну стадію інформаційного протиборства та зроблено висновки щодо подальших дій України в цьому протистоянні.

Петрик В. Використання спеціального програмного забезпечення для аналізу інформаційної агресії Російської Федерації проти України / В. Петрик, А. Давидюк // Information Technology and Security. – January-June 2017. – Vol. 5, Iss.1 (8). – P. 21-28.

Р/1212

… аналізування інформаційної агресії Російської Федерації у глобальній мережі Internet за допомогою спеціального програмного засобу «Support Ukraine» *є метою даної роботи*. Для досягнення цієї мети проаналізовано існуючі засоби інтелектуальної обробки даних та інформаційного протистояння.

Рижук О. Інформаційна політика Росії щодо України як підготовка до відкритої агресії у гібридній війні / О. Рижук // Освіта регіону: політологія, психологія, комунікації. – 2017. – № 1. – С. 12-17.

Р/990

… у підходах російської інформаційної політики простежувалося бажання дискредитувати Україну усіма можливими засобами, а діяльність російських ЗМІ задовольняла ці бажання повною мірою. Згодом інформаційна експансія Російської Федерації переросла у збройний конфлікт, який у сучасному світі має назву «гібридної війни».

Сєров Ю. Відстеження появи небезпечного контенту онлайн спільнот як ключовий аспект інформаційно-психологічної безпеки онлайн-користувачів / Ю. Сєров // Безпека інформації. – 2017. – Т. 23, № 2. – С. 113-121.

Р/1408

У статті запропоноване вирішення актуальної задачі розроблення методів відстеження появи небезпечного контенту для користувачів онлайн спільнот з метою підвищення їхньої інформаційно-психологічної безпеки. Впровадження отриманих результатів в роботу онлайн спільноти дозволяють уникнути випадків притягнення до адміністративної та кримінальної відповідальності власників, адміністраторів, модераторів та пересічних користувачів онлайн спільнот. Запропоновані методи суттєво підвищать інформаційно-психологічну безпеку користувачам, адміністраторам та модераторам онлайн спільнот з жорсткою структурою, строгою ієрархією та своєрідною спеціалізацією.

Б 18519
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. 4 (150). - Х., 2017. - 262 с. : іл., табл. - Бібліогр. наприкінці ст. - Алф. покажч.: с. 260. - Текст укр., рос., англ.

Зі змісту:

Алімпієв А. М., Бараннік В. В., Белікова Т. В., Сідченко С. О. **Теоретичні основи створення технологій протидії прихованим інформаційним атакам в сучасній гібридній війні.** – С. 113-121.

Соціальна інженерія як загроза інформаційній безпеці / С. О. Мізюканова, М. І. Слабковська, О. В. Ізмайлова, Ю. І. Хлапонін // Бизнес и безопасность. – 2017. – № 3. – С. 2-4.

Р/1070

Головним аспектом у системі захисту інформації є людина. Через недбале відношення до довірених людині даних, ці дані можуть бути втрачені.

Одними із провідних загроз являються соціальна інженерія та ментальна інженерія. У них є спільна особливість, це – вплив на людину та її поведінку різними факторами для здобуття конфіденційної інформації.

Б 18529
339

Харківський національний університет імені В. Н. Каразіна.
Вісник Харківського національного університету імені В. Н. Каразіна [Текст] : [зб. наук. пр.]. - Х. : [Вид. ХНУ імені В. Н. Каразіна]. - (Серія "Міжнародні відносини. Економіка. Країнознавство. Туризм"). -
Вип. 6. - Х., 2017. - 222 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст укр., рос., англ.

Зі змісту:

Харченко І. М., Сапогов С. О., Шамраєва В. М., Новікова Л. В. **Основні засоби інформаційного протиборства та інформаційної війни як явища сучасного міжнародного політичного процесу.** – С. 77-81.

Б 18453
355

Центр воєнно-стратегічних досліджень Національного університету оборони України.
Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського [Текст] : [наук. вид.]. - К. : [ЦВСД НУОУ].
Вип. 2 (60). - К., 2017. - 146 с. : табл. - Бібліогр. наприкінці ст. - Текст кн. укр., англ., рос.

Зі змісту:

Рогов П. Д., Ткаченко В. А., Голубцов С. М. **Удосконалення морально-психологічного забезпечення як невід'ємна складова захисту військ (сил) та протидії негативному інформаційно-психологічному впливу.** – С. 58-65.

Кібербезпека – проблема XXI століття

Бєрковський В. В. Аналіз та класифікація методів виявлення вторгнень в інформаційну систему / В. В. Бєрковський, О. С. Безсонов // Системи управління, навігації та зв'язку. – 2017. – Вип. 3. – С. 57-62.

Р/2152

Виявлені недоліки пов'язані зі структурою СВВ та недоліки реалізації методів виявлення. Для підвищення ймовірності виявлення атак на ІС найперспективнішим буде використання комбінованого методу, а також створення уніфікованої СВВ для захисту як комп'ютерів так і мобільних пристроїв. Визначені подальші напрямки вдосконалення, пов'язані з усуненням недоліків сучасних СВВ.

Р 360374
33

Валіулліна, З. В.
Економіка та інформаційна безпека зарубіжних країн [Текст] : навч. посіб. / З. В. Валіулліна ; Національний ун-т водного господарства та природокористування. - Рівне : [Волинські обереги], 2017. - 276 с. : граф., рис., табл. - Бібліогр.: с. 268-275 (109 назв).

Значну увагу приділено взаємодії національних економік у глобальному економічному просторі та розглянуто основні регіонально-інтеграційні угруповання країн світу. Детально проаналізовано моделі і тенденції економічного розвитку головних високорозвинутих країн світу, країн Центральної та Східної Європи, а також ряду країн з транзитивною економікою.

Висвітлено ***актуальні аспекти інформаційної безпеки в країнах світу, включаючи захист від кібератак на сучасному етапі розвитку суспільства,*** економічний стан інформаційної безпеки у світі, управління інформаційною безпекою корпоративної економіки та ін.

Веревкин Л. П. Киберпреступность в финансовой сфере / Л. П. Веревкин, А. А. Веревкин // Энергия: экономика, техника, экология. – 2017. – № 1. – С. 56-62.

Р/294

«Наиболее распространенными способами мошенничества в последние годы стали финансовые и информационные хищения при помощи мобильных технологий. По данным исследования Group IB, 40% зараженных телефонов имеют привязку к банковскому счету».

Б 18489
621.39

Військовий інститут телекомунікацій та інформатизації.
Збірник наукових праць [Текст] = Collection of Scientific Papers / Міноборони України. - К. : [ВІТІ].
Вип. № 3. - К., 2017. - 174 с. - Бібліогр. наприкінці ст. - Текст укр., рос. та англ.

Зі змісту:

Шевченко А. С., Самойлов І. В., Толстих В. А., Артюх С. Г. **Метод оцінювання ризику інформаційної безпеки внаслідок обмеження пропускної спроможності міжмережевими екранами наступного покоління при використанні додаткових активних систем захисту інформації.** – С. 165-170.

Горюшкіна А. Е. Аналіз сучасного стану інтелектуальної системи «Internet of Things» та тенденції її розвитку / А. Е. Горюшкіна, Р. В. Корольов // Сучасні інформаційні системи = Advanced Information Systems. – 2017. – Т.1, № 1. – С. 34-37. – Текст англ.

Р/543

Проведено аналіз сучасного стану інтелектуальної системи IoT, проаналізовано всі рівні функціонування та класифікацію атак хакерів за факторами їх виникнення. Визначено негативні наслідки, що негативно впливають на основні характеристики функціонування IoT. В результаті сформована структурна схема атак на всіх рівнях IoT.

Динамічні властивості процесів забезпечення кібербезпеки на прикладі аудиту кібербезпеки / О. Ю. Козлова, В. Г. Кононович, І. В. Кононович [та ін.] // Інформатика та математичні методи в моделюванні. – 2017. – Т. 7, № 3. – С. 205-212.

Р/2357

У роботі розглянуто процес розвитку від інформаційної безпеки до кібернетичної безпеки об'єктів інфраструктури, і зокрема процесів аудиту кіберзахищеності.

Р 359908
004

Інформаційні технології в освіті, науці і виробництві, Міжнар. наук.-практ. конф. (6 ; 2017 ; Луцьк).
Тези доповідей VI Міжнародної науково-практичної конференції "Інформаційні технології в освіті, науці і виробництві", (ІТОНВ-2017), 25-27 травня 2017 року [Текст] : [наук. вид.] / Ін-т модернізації змісту освіти МОНУ, Волинська облрада, Українська Федерація Інформатики [та ін.]. - Луцьк : ЛНТУ, 2017. - 236 с. : іл., табл. - Бібліогр. наприкінці ст. - Текст укр., рос., англ.

Зі змісту:

Кабак В. В., Костючко С. М. **Кібербезпека як фактор забезпечення національної системи захисту кіберпростору.** – С. 212-215.

Кібер атака на Українські енергомережі / P. Bock, J.-P. Hauet, R. Françoise, R. Foley // Промислова електроенергетика та електротехніка. – 2017. – № 3. – С. 28-34.

Р/1056

«Три енергетичні компанії західної України зазнали кібер атаку 23 грудня 2015. Оскільки з технічної точки зору є багато інформації, це надає можливість перевірити на живому прикладі підходи ISA/IEC 62443-3-3 Безпека промислової автоматики та систем керування. Частина 3-3: Вимоги до системи безпеки та рівні безпеки. Для цієї мети були використані декілька джерел, що, в цілому, забезпечує надзвичайно детальну інформацію».

Комплексний підхід до побудови системи кіберзахисту критичної інформаційної інфраструктури держави / І. П. Сініцин, П. П. Ігнатенко, О. О. Слабостицька, О. В. Артеменко // Проблеми програмування. – 2017. – № 3. – С. 128-148.

Р/1373

Надано комплексний підхід до вирішення проблем забезпечення кіберзахисту об'єктів критичної інформаційної інфраструктури держави з урахуванням кращих світових і вітчизняних практик та апробованих програмно-апаратних і програмних засобів кібернетичного захисту.

Критическая безопасность инфраструктуры. Обнаружение кибервторжений в автоматических распределительных энергосистемах с помощью микросинхрофазометра / Mahdi Jamei, Emma Stewart, Sean Peisert [и др.] // Промислова електроенергетика та електротехніка. – 2017. – № 4-6. – С. 34-41.

Р/1056

Разделы статьи:

1. Необходимость разработки безопасности в современных системах менеджмента распредэнергосистем
2. Современные методы безопасности
3. Данные о микросинхрофазометре (МСФ)
4. Всеохватывающая система оповещения атаки (СОА): как использовать ее ресурсы?

Лисенко С. М. Метод виявлення кібер-загроз на основі еволюційних алгоритмів / С. М. Лисенко, Д. І. Стопчак, В. В. Самотес // Вісник Хмельницького національного університету. Серія: Технічні науки. – 2017. – № 6. – С. 81-88.

Р/1055«Т»

Метод дозволяє забезпечити реагування на нові загрози, забезпечуючи захист комп'ютерних систем від як відомих, так і невідомих кібер-загроз.

Погосов О. Ю. Моделі прикладної інформатики врахування кінетики кібернетичних загроз в системі фізичного захисту АЕС / О. Ю. Погосов, О. В. Дерев'янко // Радіоелектроніка, інформатика, управління. – 2017. – № 2. – С. 53-60. – Текст рос.

Р/0170

Розглянуто актуальні підходи до превентивних оцінок і математичного моделювання процесів кібернетичних атак і надходження зовнішніх техногенних інформаційних загроз, які можуть бути спрямовані на систему фізичного захисту енергоблоків сучасних атомних електричних станцій.

Резанов Б. М. Фактори аутентифікації системи контролю та управління доступом / Б. М. Резанов, С. С. Бульба, Д. В. Шокотько // Системи управління, навігації та зв'язку. – 2017. – Вип. 3. – С. 63-65.

Р/2152

У статті розглянуті базові фактори процесу аутентифікації у системі контролю та управління доступом. Проведено порівняння факторів за позитивними та негативними показниками, що дає змогу чіткіше представити ризики які притаманні процесу аутентифікації у сучасних системах захисту різних форм власності.

Стрельницький О. О. Методи захисту інформації систем спостереження повітряного простору від несанкціонованого використання інформаційних ресурсів / О. О. Стрельницький // Системи управління, навігації та зв'язку. – 2017. – Вип. 5. – С. 105-107.

Р/2152

У статті наведені методи, які засновані на спадкоємному переході до синхронних мереж систем спостереження та дозволяють зняти проблему захисту інформації систем ідентифікації за ознакою «свій-чужий», як одного з головних інформаційних ресурсів системи контролю повітряного простору.

Стрельницький О. О. Протиріччя та проблема захисту інформації в мережі систем спостереження повітряного простору / О. О. Стрельницький // Системи управління, навігації та зв'язку. – 2017. – Вип. 3. – С. 66-68.

Р/2152

Показана неможливість здійснення захисту інформації ідентифікаційних систем спостереження на відомих принципах без суттєвого зниження інформаційних здібностей цих систем, що породжує проблему.

Б 18603
355

Центр воєнно-стратегічних досліджень Національного університету оборони України.
Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського [Текст] : [наук. вид.]. - К. : [ЦВСД НУОУ]. - **Вип. 3 (61).** - К., 2017. - 136 с. : табл. - Бібліогр. наприкінці ст. - Текст кн. укр., англ., рос.

Зі змісту:

Кива В. Ю., Дрозд Ю. С. **Аналіз існуючих методів кібернетичної розвідки і неформаційно-телекомунікаційних мереж.** – С. 62-66.

Юрчак О. В. Наймасштабніша кібер-атака на Україну. Які уроки та дії? / О. В. Юрчак // Промислова електроенергетика та електротехніка. – 2017. – № 3. – С. 24-27.

Р/1056

«Червень 2017 увійде в історію, як поворотний момент в історії кібер-безпеки країни. Принаймі, хочеться дуже вірити в це. Дві події, що відбулись в цьому місяці мали остаточно розбудити як державний та військовий істеблішмент, так і експертні спільноти. Огляд Асоціації Підприємств Промислової Автоматизації України (АППАУ) проливає більше деталей на аспекти реакції останніх».

Б 18456
004

Information Technology and Security [Text] : [ukrainian research papers collection] / National Technical University of Ukraine "Igor Sikorsky Kyiv Politechnic Institute", Institute of special Communication and information Protection. - K. : [Institute of special Communication and information Protection of Nat. Technical Univ. of Ukraine "Igor Sikorsky KPI"], 2016 - . -
Vol. 4, Issue 2 (7), July-december 2016. - K., 2016. - 288 p. - Бібліогр. наприкінці ст. - Текст англ. та укр.

Зі змісту:

Гончар С., Леоненко Г. **Аналіз факторів впливу на стан кібербезпеки інформаційної системи об'єкту критичної інфраструктури.** – С. 262-268.