Тематична виставка
"Безпека та захист інформаційного простору"

(надходження II півріччя 2017 р.)

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

Р 359378
33

Варналій, Захарій Степанович.
Ринок економічної інформації: проблеми формування та перспективи розвитку [Текст] : монографія / Варналій З. С., Клевчік Л. Л. - Чернівці : Технодрук, 2016. - 279 с. : граф., табл. - Бібліогр.: с. 253-271 та у виносках.

Зі змісту:

Розділ 4. **Інформаційна безпека в системі захисту економічної інформації**
4.1. Поняття та зміст інформаційної безпеки як чинника захисту економічної інформації
4.2. Методи забезпечення інформаційної безпеки держави
4.3. Державна політика у сфері забезпечення інформаційної безпеки України.

Гуцалюк М. В. Вдосконалення чинного законодавства з питань протидії кіберзлочинності та забезпечення кібербезпеки / М. В. Гуцалюк // Інформація і право. – 2017. – № 2. – С. 99-107.

Р/844

В статті досліджуються питання інформаційної безпеки та протидії кіберзлочинності. Пропонуються напрями вдосконалення чинного законодавства у даній галузі та запровадження безпечного сегменту *Інтернет – ID-web*.

Давидюк Н. В. Методика оценки требуемого уровня защищенности информационных ресурсов автоматизированных систем обработки информации и управления / Н. В. Давидюк // Научный вестник Новосибирского государственного технического университета. – 2016. – № 4. – С. 100-109.

Р/882

В статье представлена поэтапная методика получения количественной оценки требуемого уровня обеспечения безопасности информационных ресурсов, циркулирующих в автоматизированных системах обработки информации и управления, с привлечением экспертных групп. Предложенная автором процедура подразумевает подробный анализ и декомпозицию исследуемой информационной системы на звенья, обеспечивающие функции или участвующие в обработке, хранении, передаче информационных ресурсов системы. Кроме того, в рамках методики в процессе анализа обрабатываемой информации осуществляется учет ее ценности, а также свойств информационной безопасности.

Дегтярьова Л. М. Практичні прийоми та керівні принципи розробки комплексів інформаційної безпеки / Л. М. Дегтярьова // Системи управління, навігації та зв'язку. – 2017. – Вип. 2. – С. 94-97.

Р/2152

У статті розглянуті результати порівняльного аналізу розвитку ***концепції інформаційної безпеки автоматизованих систем,*** використання сучасних інтелектуальних технологій в сфері інформаційної безпеки.

Доронін І. М. Правове регулювання забезпечення кібербезпеки у реалізації окремих функцій держави / І. М. Доронін // Інформація і право. – 2017. – № 1. – С. 104-111.

Р/844

У статті на підставі аналізу документів стратегічного планування держави, актів законодавства та проектів законодавчих актів, досліджено питання реалізації окремих функцій держави у формі правового регулювання забезпечення кібербезпеки.

Б 18386
004

Захист інформації і безпека інформаційних систем [Текст] : матеріали VI міжнар. наук.-техн. конф., 1-2 червня 2017 р. / НАН України, М-во науки та вищої освіти Республіки Польща, Нац. ун-т "Львівська політехніка" [та ін.]. - Л. : Вид-во Львів. політехніки, 2017. - 178 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст укр. та англ.

Зі змісту:

Секція І. Управління інформаційною безпекою
Секція ІІ. Захист інформації в інформаційно-комунікаційних системах
Секція ІІІ. Криптографічні та стенографічні методи захисту інформації
Секція IV. Технічний захист інформації
Секція V. Захист інформації в кіберфізичних системах.

Б 18209
004

Information Technology and Security [Text] / National Technical University of Ukraine "Kyiv Politechnic Institute", State Institution "Institute of special Communication and information Protection". - K. : [State Institution "Institute of special Communication and information Protection of Nat. Technical Univ. of Ukraine "KPI"], 2012 - .
Vol. 4, Issue 1 (6), January-June 2016. - K., 2016. - 132 p. - Бібліогр. наприкінці ст. - Текст англ. та укр.

Зі змісту:

Кожедуб Ю. **Сучасні аспекти оновлення міжнародних стандартів серії ISO/IEC 27000.** – С. 20-26.

Корченко О. Г. Метод оцінювання ризиків інформаційної безпеки на основі відкритих баз даних уразливостей / О. Г. Корченко, С. В. Казмірчук // Безпека інформації. – 2016. – Т. 22, № 2. – С. 214-224. – Текст рос.

Р/1408

… пропонується метод оцінювання ризиків на основі відкритих баз даних уразливостей. Він дозволяє автоматизувати процес оцінювання ризиків без залучення експертів відповідної предметної області.

Котенко А. Класифікації загроз інформаційній безпеці для виділення меж відповідальності та правової компетентності служб/інституцій / А. Котенко // Освіта регіону. Політологія. Психологія. Комунікації. – 2016. – № 4. – С. 66-73.

Р/990

Стаття присвячена аналізу наукових поглядів та стану нормативно-правового регулювання класифікації загроз інформаційній безпеці для виділення меж відповідальності та правової компетентності служб/інституцій, завданням яких є протидія інформаційно-психологічним впливам.

Р 359106
35

Лісовський, Петро Миколайович.
Безпекознавство: особистість, держава, суспільство (системний аналіз) [Текст] : [навч. посіб.] / П. М**.** Лісовський, Ю. П. Лісовська. - К. : Кондор, 2017. - 368 с. - Бібліогр.: с. 348-367.

У навчальному посібнику викладено основи безпекознавства, що на сьогодні є основним пріоритетом і базою, яка постійно створює та примножує загальний потенціал людини, держави та суспільства. Це дозволить протистояти різного роду соціальним негараздам, катаклізмам, військовим конфліктам. При цьому акцентується увага на особистість, державу та суспільство, яким надається концептуальний аналіз.

Зі змісту:

Розділ 2. Методологічні аспекти безпекознавства в структурі духовного та інформаційного ресурсів
2.3. Концептуальний аналіз інформаційної безпеки. – С. 136-152.

Р 357299
327

Міжнародна інформація: терміни і коментарі [Текст] : навч. посіб. / Є. А. Макаренко, М. М. Рижков, О. П. Кучмій, О. М. Фролова ; Київський нац. ун-т імені Тараса Шевченка, Ін-т міжнар. відносин Київ. нац. ун-ту імені Тараса Шевченка. - [2-ге вид., допов. та переробл.]. - К. : Центр вільної преси, 2016. - 518 с. - (Серія: "Міжнародні інформаційні відносини"). - Бібліогр.: с. 504-512. - Перелік статей: с. 514-517.

Навчальний посібник присвячено теоретичним та прикладним питанням міжнародної інформації як складової сучасних міжнародних відносин. У посібнику подано тлумачення основних понять міжнародної інформації та розширений коментар до них, проаналізовано сучасні теорії та практику міжнародних інформаційних відносин, представлено тематичну антологію.

Зі змісту:

Розділ 4. **Міжнародна інформаційна безпека.** – С. 259-349.

С 21415
663

Національний університет харчових технологій.
Наукові праці Національного університету харчових технологій [Текст] = Scientific Works of National University of Food Technologies : [наук. вид.]. - К. : НУХТ. -
Т. 22, № 6. - К., 2016. - 253 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст укр., рос. та англ. мов.

Зі змісту:

Менеджмент і стратегічне управління
Білоконь Д. С., Федулова І. В. **Процес управління ризиками інформаційної безпеки.** – С. 84-91.
У статті досліджено основні процедури, принципи, функції і методичне забезпечення процесу аналізу й управління ризиками інформаційної безпеки підприємства. Розглянуто сутність методології OCTAVE, особливості впровадження механізму інформаційної безпеки, проаналізовано методику управління ризиками інформаційної безпеки OCTAVE.

Пилипчук В. Г. Інформаційна безпека та приватність у сфері захисту персональних даних / В. Г. Пилипчук, В. М. Брижко // Інформація і право. – 2016. – № 4. – С. 60-70.

Р/844

Стаття присвячена проблемі інформаційної безпеки приватності у сфері захисту персональних даних в умовах формування інформаційного суспільства. Здійснено теоретичне опрацювання пропозиції щодо запровадження в Україні інституту права приватної власності людини на свої персональні дані.

Р 357866
34

Політанський, В'ячеслав Станіславович.
Право на інформацію як фундаментальне право людини [Текст] : монографія / В. С. Політанський ; Національний юридичний ун-т імені Ярослава Мудрого. - Х. : Право, 2017. - 208 с. - Бібліогр.: с. 185-207 та у виносках.

Робота присвячена дослідженню процесу еволюції права на інформацію від його зародження як засобу боротьби за політичну свободу до набуття ним оновленого змісту в умовах формування інформаційного суспільства, що дає підстави розглядати його в контексті третього покоління прав людини. Визначено основні особливості закріплення та реалізації права на інформацію в Україні відповідно до стандартів відкритості, доступності та свободи обміну інформацією, закріплених у міжнародно-правових документах з прав людини. Здійснено порівняльно-правовий аналіз особливостей становлення, розвитку та здійснення права на інформацію в країнах сталої демократії (на прикладі Франції, ФРН, США) та в країнах, які стали на шлях свого демократичного розвитку (на прикладі Польщі, Чехії, Словаччини).

Радзієвська О. Г. Правові засади та пріоритети розвитку протидії негативним інформаційним впливам на дітей / О. Г. Радзієвська // Інформація і право. – 2017. – № 2. – С. 88-98.

Р/844

Стаття присвячена аналізу сучасного стану і наукових поглядів на проблему ***правового регулювання протидії негативним інформаційним впливам на дітей та дослідженню пріоритетних напрямів розвитку системи правового регулювання*** щодо забезпечення їх інформаційної безпеки в Україні.

Р 357321
327

Регіональні стратегії США і Європи: зовнішньополітичний і безпековий вимір [Текст] : монографія / [Бєлоусова Н. Б., Головченко В. І., Доброжанська О. Л. та ін.] ; Київський нац. ун-т імені Тараса Шевченка, Ін-т міжнар. відносин Київ. нац. ун-ту імені Тараса Шевченка. - К. : [Центр вільної преси], 2016. - 528 с. : рис. - (Наукова серія "Трансатлантичні дослідження"). - Бібліогр. наприкінці підглав.

Монографія присвячена дослідженню зовнішньополітичних і безпекових аспектів регіональних стратегій США і Європи, аналізу багатостороннього співробітництва США і Європи з ключовими акторами міжнародної взаємодії, з'ясуванню особливостей зовнішньої безпекової політики у сучасній системі міжнародних відносин.

Зі змісту:

Глава 1.5. **Інформаційна безпека США у сучасних зарубіжних дослідженнях** (Кучмій О. П.). – С. 106-138.

Глава 3.5. **Регіональна політика Європейського Союзу: інформаційно-комунікаційний аспект** (Тихомирова Є. Б.). – С. 434-462.

Рижук О. Аналіз концепцій визначення «інформаційної безпеки» в умовах глобалізації / О. Рижук // Освіта регіону. Політологія. Психологія. Комунікації. – 2016. – № 4. – С. 74-77.

Р/990

В цій статті наведено широкий перелік визначень які даються вітчизняними і закордонними науковцями до поняття «інформаційна безпека». Враховуючи те, що питання інформаційної безпеки в умовах глобалізації мають гострий характер, необхідно визначити оптимальні шляхи усунення інформаційних загроз і небезпек та мінімізації впливу негативних наслідків у сфері інформаційної діяльності держави.

Романюков М. Г. Дослідження оптимального коефіцієнту витрат на технічний захист інформації об'єкту інформаційної діяльності / М. Г. Романюков // Інформатика та математичні методи в моделюванні. – 2017. – Т. 7, № 1-2. – С. 119-126.

Р/2357

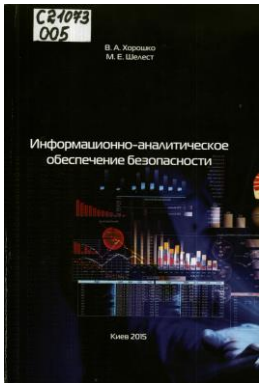
Концепцією технічного захисту інформації в Україні визначено злочинну діяльність, спрямовану на незаконне отримання інформації, закритої для доступу сторонніх осіб, з метою досягнення матеріальної вигоди або нанесення шкоди юридичним або фізичним особам. Виникає необхідність на прикладі побудови моделі порушника розрахувати оптимальний варіант витрат на організацію технічного захисту інформації віброакустичним каналом витоку та встановити величину витрат для надійного захисту інформації. Розглянути організаційно-технічні заходи та порядок їх проведення під час ***побудови системи технічного захисту інформації з обмеженим доступом з урахуванням державних нормативних документів.***

Сибикина И. В. Анализ рисков информационной безопасности с использованием системы нечеткого вывода / И. В. Сибикина // Научный вестник Новосибирского государственного технического университета. – 2016. – № 4. – С. 121-134.

Р/882

Обоснованы необходимость и возможность использования нечеткого моделирования при реализации политики безопасности предприятия или организации. Отмечена сложность задачи оценки рисков информационной безопасности в связи с отсутствием общепринятых подходов и методик для оценки рисков. ***Проанализированы достоинства и недостатки существующих методик анализа рисков информационной безопасности.*** Описаны процедуры сбора и обработки экспертной информации, необходимой для построения системы нечеткого вывода.

Предложена методика построения лингвистических шкал, в основу которой положен метод статистического эксперимента.



С 21073
005

Хорошко, Владимир Алексеевич.
Информационно-аналитическое обеспечение безопасности [Текст] : монография / В. А. Хорошко, М. Е. Шелест. - К. : [ВПВ "Задруга"], 2016. - 183 с. : рис. - Библиогр.: с. 178-182.

В монографии рассматривается широкий круг проблем по работе с различными по форме и содержанию источниками информации, обеспечению процесса подготовки и ведения информационно-аналитической работы. Подробно раскрываются основные понятия, выбор методов исследования, структура и содержание этапов информационной и аналитической деятельности, последовательность поиска, анализа и предоставления результатов работы.

Хорошко В. Концепція застосування інформаційних впливів та протидія інформаційній зброї / В. Хорошко, Ю. Хохлачова, М. Прокофьєв // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2016. – Вип. 1. – С. 9-23.

Р/2287

Проведено аналіз загальнотеоретичної суті інформаційних впливів і протидії інформаційній зброї. У ході проведеного дослідження було сформовано рекомендації щодо протистояння інформаційній війні.

Б 18259
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. 1 (59)**. - К., 2017. - 142 с. : табл. - Бібліогр. наприкінці ст. - Текст кн. укр., англ., рос.

Зі змісту:

Кульчицький О. С., Грицюк В. В., Зотова І. Г. **Визначення нормативно-правових аспектів захисту персональних даних в інформаційних системах Збройних Сил України.** – С. 73-77.

Кірпічніков Ю. А., Федорієнко В. А., Головченко О. В., Андрощук О. В. **Аналіз рамкових архітектур побудови інформаційних систем НАТО та визначення особливостей архітектури C4ISR.** – С. 78-84.

Б 18218
61

Якість і безпека: сучасні реалії [Текст] : матеріали Наук.-практ. конф., 02-03 березня 2017 р. / Вінницький нац. техн. ун-т, Вінницький нац. аграр. ун-т, Вінницький мед. коледж ім. акад. Данили Заболотного. - Вінниця : ВНТУ, 2017. - 92 с. - Бібліогр. наприкінці ст.
Текст кн. укр. , англ.

Зі змісту:

Ратушняк М. С. **Основні вимоги до стратегії забезпечення кібербезпеки України.** – С. 64-67.

Програмні системи захисту інформації

Б 18257
681

Автоматика, вимірювання та керування [Текст] : зб. наук. пр. / голова редакційно-видавничої ради Н. І. Чухрай. - Л. : Вид-во Львів. політехніки, 2016. - 184 с. : іл., табл. - (Вісник / Національний університет "Львівська політехніка" ; № 852). - Бібліогр. наприкінці ст. - Текст укр., англ.

Зі змісту:

Олійник Г. В., Литвинов В. А., Грибков С. В. **Обрання програмної платформи для побудови модуля безпеки web-орієнтованої системи підтримки прийняття рішень.** – С. 137-142.

Борншлегл С. Функциональная безопасность в стандарте CompactPCI 3U / С. Борншлегл // Мир Автоматизации. – 2016. – № 3. – С. 44-48.

Р/2214

В статье рассматривается новый подход к построению функционально безопасных систем на основе процессорной платы F75P компании MEN, выполненной на базе трех процессоров. Данная плата соответствует высшему уровню безопасности SIL 4, и поставляется с полным набором документации, необходимой для сертификации готовой системы.

Бучик С. С. Реалізація програмного забезпечення визначення функціональних профілів захищеності автоматизованої системи від несанкціонованого доступу / С. С. Бучик, О. К. Юдін, Р. В. Нетребко // Вісник Інженерної академії України. – 2017. – Вип. 1. – С. 54-59.

Р/1139

В статті показано основні етапи реалізації програмного забезпечення визначення функціональних профілів захищеності автоматизованої системи від несанкціонованого доступу на основі раніше проведених авторами теоретичних досліджень. Вказано, на основі яких критеріїв оцінюється автоматизована система, що потрібно для визначення функціонального профілю захищеності. Здійснено проектування роботи програми за допомогою діаграм Data Flow Diagram. Побудовані більш детальні блок-схеми роботи програмного забезпечення та алгоритмів. Реалізовано прототип програмного забезпечення та приведено приклади роботи по кожному з основних блоків роботи,

Василенко В. В. Масштабованість SDN на основі реконфігурації моделі мережі з урахуванням безпеки і QOS обмежень / В. В. Василенко // Сучасний захист інформації. – 2016. – № 3. – С. 48-55.

Р/2300

Досліджено питання масштабованості при використанні графа атак на основі аналізу моделі безпеки в програмному і віртуалізованому мережному середовищі.

Главчев М. І. Формування програмного комплексу захисту комерційного програмного забезпечення персонального використання / М. І. Главчев, О. І. Баленко // Системи управління, навігації та зв'язку. – 2016. – Вип. 4. – С. 63-66.

Р/2152

Розглянуто формування програмного комплексу захисту комерційного програмного забезпечення на основі послідовності рівнів захисту, що включають формування ключової інформації, організацію прихованої мітки, захист від відлагодників, захист від дизасемблювання, online-підтримка контролю запуску.

Давидов В. В. Комплекс процедур ліцензійного ключа для захисту авторських прав інтелектуальної власності на програмне забезпечення / В. В. Давидов, Д. С. Гребенюк // Системи управління, навігації та зв'язку. – 2017. – Вип. 1. – С. 11-15. – Текст рос.

Р/2152

В статті описано процес розробки програмного комплексу генерації ліцензійного ключа захисту авторських прав інтелектуальної власності на програмне забезпечення, що враховує індивідуальні дані кінцевого користувача.

Р 358599
004

Дискретні та алгоритмічні структури в інструментарії програмної інженерії [Текст] : навч. посіб. / В. В. Скалозуб, В. М. Ільман, Ю. М. Івченко, В. О. Андрющенко ; Дніпропетровський нац. ун-т залізн. трансп. імені академіка В. Лазаряна. - Д. : [Дніпропетр. нац. ун-ту залізничного транспорту ім. акад. В. Лазаряна], 2016. - 255 с. : іл.: 42, табл.: 11. - Бібліогр. наприкінці розд. (110 назв.). - Авт. на тит. арк. не зазнач.

Викладено основні положення комп'ютерної математики, формальних конструктивних граматичних і алгоритмічних структур, методи оцінки характеристик алгоритмів, прикладні питання трансляторів, теорії графів, мереж Петрі, що призначені для розвитку навичок структуризації

предметних областей програмування, створення конструктивних об'єктів та їх застосування при моделюванні завдань програмної інженерії.

Зі змісту:

Розділ 6.11. **Архітектура забезпечення безпеки.** – С. 229-235.

6.11.1. Служби безпеки
6.11.2. Спеціальні механізми забезпечення безпеки
6.11.3. Загальні механізми забезпечення безпеки
6.11.4. Ілюстрація взаємозв'язку служб і механізмів забезпечення безпеки
6.11.5. Розміщення служб і механізмів безпеки.

Єремізін О. Перспективи використання нечіткого хешування в антивірусному захисті / О. Єремізін, І. Стьопочкіна // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2016. – Вип. 1. – С. 80-84.

Р/2287

«… актуальним питанням залишається ***вироблення рекомендацій щодо застосування функцій нечіткого хешування в антивірусному програмному забезпеченні,*** які сприятимуть більш ефективному використанню властивостей цих функцій».

Рабчун Д. І. Логіко-динамічна модель процесу управління ресурсами захисту в умовах інформаційного протистояння / Д. І. Рабчун // Сучасний захист інформації. – 2016. – № 3. – С. 62-66.

Р/2300

Питання управління ресурсами (ресурсна оптимізація) в комплексах ПЗЗІ при функціонуванні в умовах динамічного інформаційного протистояння є досить складними. У зв'язку з цим основною і найбільш важливою є проблема змістовного, коректного і разом з тим конструктивного опису комплексу ПЗЗІ (складної технічної системи) як об'єкта управління. Цей опис має бути приведений у категоріях і символах, які забезпечують ефективне застосування сучасних методів загальної теорії управління та теорії логіко-динамічних систем. У статті розглянута логіко-динамічна модель процесу управління ресурсами КПЗЗІ в умовах інформаційного протистояння як основа методу ресурсної оптимізації.

Савенко О. С. Програмне забезпечення інформаційної технології моделювання поширення вірусних кодів в гетерогенних мережах / О. С. Савенко // Вісник Хмельницького національного університету. Серія: Технічні науки. – 2017. – № 1. – С. 144-148.

Р/1055«Т»

Розроблено програмне забезпечення інформаційної технології моделювання поширення вірусних кодів в гетерогенних мережах для прогнозування часу і напрямку розповсюдження вірусних програм з врахуванням топології мережі та системного програмного забезпечення, встановленого на комп'ютерних системах. Застосування розробленого програмного забезпечення надає можливість передбачати ймовірність проникнення вірусів в комп'ютерні системи мережі із врахуванням рівня захищеності комп'ютерних систем та часу їх експлуатації.

Системи реєстрації особливостей введення паролів на основі штучної нейронної мережі / О. В. Наумцева, В. В. Ярмолюк, О. О. Яковенко, М. В. Калашніков // Вісник Інженерної академії України. – 2017. – Вип. 1. – С. 76-80.

Р/1139

Для класифікації особливостей введення пароля використовується штучна нейронна мережа. З метою поліпшення захисту персональних даних була створена програма яка розпізнає характер введення символів з клавіатури.

Чуприн В. Захист операційного середовища систем Інтернет голосування / В. Чуприн, В. Вишняков, М. Пригара // Захист інформації. – 2017. – Т. 19, № 1. – С. 56-66.

Р/1428

В даній роботі запропоновано метод створення захищеного операційного середовища для сервера системи Інтернет голосування. Метод базується на концепції ядра безпеки і реалізує профіль захищеності, згідно якому в оперативній пам'яті сервера створюється ділянка, в межах якої доступ до даних має виключно процес підрахунку голосів наперед вивіреною відкритою прикладною програмою.

Чуруброва С. М. Політика інформаційної безпеки в системах інформаційно-аналітичного забезпечення підтримки прийняття організаційних рішень / С. М. Чуруброва // Проблеми програмування. – 2016. – № 4. – С. 97-103.

Р/1373

У статті описано політику безпеки інформації у системах підтримки організаційних рішень. Визначені основні вимоги захисту інформаційних об'єктів, наведені особливості функціонування та інформаційні ресурси інтелектуальної інформаційної технології підтримки прийняття організаційних рішень. Розроблено загальні правила та вимоги розмежування та керування доступу на базі ABAC-моделі.

Б 18218
61

Якість і безпека: сучасні реалії [Текст] : матеріали Наук.-практ. конф., 02-03 березня 2017 р. / Вінницький нац. техн. ун-т, Вінницький нац. аграр. ун-т, Вінницький мед. коледж ім. акад. Данили Заболотного. - Вінниця : ВНТУ, 2017. - 92 с. - Бібліогр. наприкінці ст. - Текст кн. укр. , англ.

Зі змісту:

Чорний В. М., Томчук М. А. **Засоби захисту програмних продуктів.** – С. 84-86.

Телекомунікаційні мережі та інформаційно-комунікаційні технології

Б 18257
681

Автоматика, вимірювання та керування [Текст] : зб. наук. пр. / голова редакційно-видавничої ради Н. І. Чухрай. - Л. : Вид-во Львів. політехніки, 2016. - 184 с. : іл., табл. - (Вісник / Національний університет "Львівська політехніка" ; № 852). - Бібліогр. наприкінці ст. - Текст укр., англ.

Зі змісту:

Костяк М. Ю., Пархунь Л. Т. **Особливості проектування захищених інформаційних мереж спеціального призначення.** – С. 88-92.

Самойленко Д. М. **Створення безпечних шаруватих структур мовою PHP/ Secure layers construction on PHP.** – С. 93-98.

Аль-Судані Мустафа Кахтан Абдулмунем. Оцінювання безпеки інформаційно-керуючих систем розумних будинків з використанням дерев аналізу атак / Аль-Судані Мустафа Кахтан Абдулмунем, Аль-Хафаджі Ахмед Валід, В. С. Харченко // Радіоелектронні і комп'ютерні системи. – 2016. – № 3. – С. 30-40. – Текст англ.

Р/1769

Інформаційно-керуючі системи розумних будинків розглядаються як множина підсистем, включаючи підсистему BAS (building automation system). Безпека і готовність BAS впродовж життєвого циклу оцінюються з використанням аналізу дерев атак ATA (Attack Tree Analysis) та аналізу видів і критичності наслідків відмов FMECA (Failure Modes and Effects Criticality Analysis). FMECA застосовується на

початковій стадії аналізу для оцінювання критичності відмов, обумовлених дефектами програмних і апаратних засобів, комунікацій на різних рівнях BAS, а також атаками на вразливості. Модифікація FMECA – IMECA (Intrusion Modes and Effects Criticality Analysis) дозволяє аналізувати види і наслідки відмов внаслідок атак на вразливості. АТА аналіз використовується для дослідження втручань у BAS і визначення ймовірності відмов з їх урахуванням. Аналіз базується на комбінуванні результатів для різних компонент і рівнів системи.

Аносов А. О. Модель перехоплення захисту інформації в бездротових мережах / А. О. Аносов, А. В. Платоненко // Сучасний захист інформації. – 2017. – № 2. – С. 90-94.

Р/2300

Розглянуто вразливості бездротових мереж, шляхи перехоплення інформації та впливу на бездротову мережу, а також методи та засоби захисту, що можуть використовуватись для запобігання від несанкціонованого доступу, який несе за собою небезпеку для інформації, що зберігається та передається з використанням сучасних мобільних пристроїв.

Бараннік В. В. Метод формування кодограм в градієнтному просторі для підвищення доступності динамічних відеоінформаційних ресурсів / В. В. Бараннік, С. С. Шульгін // Безпека інформації. – 2016. – Т. 22, № 2. – С. 175-183. – Текст рос.

Р/1408

У статті викладається, що для підвищення безпеки та ефективності функціонування відомчих організацій, стратегічно важливих виробництв необхідно забезпечити своєчасність і достовірність отримання відеоінформації з віддалених об’єктів.

Бістабільна інтегрована кортежна модель характеристик ризику / О. Г. Корченко, С. В. Казмірчук, Ю. О. Дрейс, А. Ю. Гололобов // Захист інформації. – 2016. – Т. 18, № 4. – С. 314-323.

Р/1428

В роботі ***визначені множини базових характеристик ризику для галузі інформаційної безпеки.*** На підставі цього пропонується відображати задані ідентифікуючі і оціночні характеристики у вигляді бістабільної (біфіксованої) інтегрованої кортежної моделі.

Бовда Е. Аналіз існуючих та перспективних систем управління інформаційно-телекомунікаційними системами / Е. Бовда, В. Ляшенко, В. Терещенко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2016. – Вип. 2. – С. 9-20.

Р/2287

Розглянуто проблеми управління в складних системах управління інформаційно-телекомунікаційних систем та можливі шляхи підвищення якості управління такими системами з використанням апарату теорії мереж зв’язків.

Визначення оптимальних параметрів сигналів з підвищеною завадостійкістю для когнітивних радіомереж FH-OFDMA / В. Г. Сайко, О. В. Дікарєв, Д. О. Лисенко [та ін.] // Телекомунікаційні та інформаційні технології. – 2016. – № 3. – С. 22-30.

Р/1921

Розроблено вдосконалений метод, який забезпечує можливість суттєвого пониження ймовірності переривання зв’язку при передаванні особливо цінної інформації сигналами OFDMA в умовах гранично низьких відношень сигнал-шум та обмеженої кількості частотних каналів.

Використання технологій OSINT для отримання розвідувальної інформації / О. В. Минько, О. Ю. Іохов, В. Т. Оленченко, К. В. Власов // Системи управління, навігації та зв'язку. – 2016. – Вип. 4. – С. 81-84.

Р/2152

Розкрито сутність діяльності з отримання розвідувальної інформації з відкритих джерел – OSINT (Open Source INTelligence) та визначені перспективи використання сучасних розвідувальних технологій у Національній гвардії України.

С 21263
339

Глобалізаційні виклики розвитку національних економік [Текст] = Global Challenges of National Economies Development : матеріали Міжнар. наук.-практ. конф., Київ, 19 жовтня 2016 р. / Київський нац. торг.-екон. ун-т, Білорус. держ. екон. ун-т, Будапештський екон. ун-т [та ін.]. - К. : [КНТЕУ], 2016. - **Ч. 2** / [відп. ред. Мазаракі А. А.]. - К., 2016. - 1047 с. : граф., табл. - Бібліогр. наприкінці ст. - Обкл. англ. Текст укр., рос. мов.

Зі змісту:

Інформаційні технології та економіко-математичне моделювання в економіці

Краснощок В. М., Шестак Я. І. **Аналіз факторів успіху розвитку інформаційних технологій в Україні.** – С. 712-721.

Гончар С. Алгоритм визначення актуальних загроз безпеці інформації на об'єктах критичної інфраструктури / С. Гончар, О. Юдін, Г. Леоненко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2016. – Вип. 2. – С. 40-48.

Р/2287

Запропоновано алгоритм визначення актуальних загроз безпеці інформації на об'єктах критичної інфраструктури. Цей алгоритм можливо застосувати під час експлуатації автоматизованих систем управління об'єктів критичної інфраструктури, при здійсненні моніторингу та оцінки/переоцінки загроз безпеці інформації.

Гринкевич Г. О. Аспекти безпеки та конфігурація несправностей при розгортанні SDN мереж / Г. О. Гринкевич // Сучасний захист інформації. – 2016. – № 3. – С. 56-61.

Р/2300

У даній статті наведено проблеми та дано короткий огляд рішень, запропонованих для вирішення питань управління мережею, які необхідні для оперативного використання в SDN. Проведені дослідження, що дають повне уявлення про потенційні і відкриті питання, що стосуються OpenFlow на основі архітектури SDN. Проаналізовано ряд проблем, які необхідно вирішити, коли оператори розгортають SDN у своїх мережах.

Даниліна Г. В. Рівні взаємодії та конфліктного управління у захищених інформаційних системах із псевдосервісами / Г. В. Даниліна // Телекомунікаційні та інформаційні технології. – 2016. – № 3. – С. 48-54. – Текст рос.

Р/1921

Розроблено математичну модель і методику багаторівневого захисту мережі в умовах апріорної невизначеності стану мережі і загроз з боку активного (розумного) партнера. Модифікований метод конфліктного управління з прогнозуванням розвитку ситуації. Запропонований спосіб захисту мереж на основі рефлексивного управління.

Дахно Н. Б. Аналіз захищеності інформації в інформаційно-комунікаційних системах і мережах, що моделюються інтегро-диференційними рівняннями з малою нелінійністю на основі модифікованих градієнтних методів / Н. Б. Дахно, Т. В. Майсак, Г. В. Шевченко // Сучасний захист інформації. – 2017. – № 1. – С. 115-119.

Р/2300

На основі проведеного аналізу зроблено висновки про достатню ефективність і перспективність застосування модифікованих градієнтних методів до аналізу моделей захисту інформації в нелінійних випадках.

Р 359006
004

Дронюк, Іванна Мирославівна.
Технології захисту інформації на матеріальних носіях [Текст] : монографія / І. М. Дронюк ; Нац. ун-т "Львівська політехніка". - Л. : Вид-во Львів. політехніки, 2017. - 200 с. : рис., табл. - Бібліогр.: с. 174-188.

Монографія присвячена розвитку цифрових методів та засобів захисту інформації на матеріальних носіях. Розвинуто теоретичні основи інформаційних технологій захисту. Застосовано методи теорії диференціальних рівнянь для побудови математичних моделей. Розроблено Ateb-перетворення як узагальнення поняття тригонометричних перетворень. Реалізовано комп'ютерні застосування для задач захисту інформації на матеріальних носіях.

Замула О. А. Інформаційні технології синтезу похідних систем сигналів для додатків сучасних інформаційно-комунікаційних систем / О. А. Замула, В. Л. Морозов, Д. О. Семченко // Системи управління, навігації та зв'язку. – 2017. – Вип. 2. – С. 112-116. – Текст рос.

Р/2152

Обгрунтовується доцільність застосування КС в захищених ІКС, в тому числі, при формуванні похідних систем сигналів, з метою поліпшення показників завадозахищеності, завадостійкості, скритності функціонування та інформаційної безпеки інформації в захищених ІКС.

Зінченко А. О. Концепція інформаційно-сенсорної решітки на основі технології MIMO / А. О. Зінченко, В. І. Слюсар // Наука і оборона. – 2016. – № 4. – С. 47-51.

Р/810

Уперше запропонована концепція інтеграції інформаційної та сенсорної підсистем мережецентричного ведення бойових дій у єдину інформаційно-сенсорну підсистему з перетворенням інформаційної компоненти на інформаційно-сенсорну решітку. Створення радарно-телекомунікаційної мережі інформаційно-сенсорної решітки має стати початком подальшої інтеграції інформаційної підсистеми із системою систем різнотипних сенсорів. Це дасть можливість охопити розгалуженим інформаційно-сенсорним контролем весь космічний, повітряний, наземний, надводний та підводний простір у відведеній операційній зоні.

Р 356079
004

Информационные технологии в управлении, образовании, науке и промышленности [Текст] : [монография] / [Бессонов А. А., Белецкий А. Я., Беседовский А. Н. и др. ; под ред. Пономаренко В. С.] ; МОН. - Х. : [Издатель Рожко С. Г.], 2016. - 566 с. : рис., граф. - Библиогр.: с. 551-564. - Авт. указ. на с. 566.

В монографии отражены результаты научных исследований в области разработки и практического применения современных информационных технологий.

Монография представляет интерес как для специалистов, сфера деятельности которых непосредственно связана с разработкой IT-технологий, ***способов обеспечения безопасности и передачи в коммуникационных системах,*** так и для более широкого круга специалистов.

Исследование баз данных уязвимостей информационной безопасности / А. Корченко, С. Казмирчук, А. Арджомандифард, Т. Панивко // Захист інформації. – 2016. – Т. 18, № 3. – С. 175-192.

Р/1428

Досліджено широкий спектр відповідних баз даних і визначені критерії, за якими можна здійснити їх порівняльний аналіз. Це дасть можливість підвищити ефективність вирішення завдань оцінювання стану безпеки ресурсів інформаційних систем.

Исследование средств оценивания рисков безопасности ресурсов информационных систем / Ф. Приставка, П. Павленко, С. Казмирчук, М. Коломиец // Захист інформації. – 2017. – Т. 19, № 1. – С. 47-56.

Р/1428

Проведено дослідження множини засобів оцінювання ризиків з метою визначення набору необхідних порівняльних характеристик. Щодо зазначених засобів з урахуванням відомої аналітико-синтетичної кортежної моделі характеристик ризику формується кортеж, який дає можливість щодо певних параметрів уніфікувати процес порівняльного аналізу таких засобів.

Р 358885
621.8

Інтегровані інтелектуальні робототехнічні комплекси (ІІРТК-2017) [Текст] : десята міжнар. наук.-практ. конф., 16-17 травня 2017 р., Київ, Україна : збірка тез / Національний авіац. ун-т, Нац. ун-т водного госп-ва та природокористування, Wroclaw Univercity of Science and Technology, Інженерна акад. України. - К. : [НАУ], 2017. - 314 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Дод. тит. арк. англ.

Містить результати наукових, експериментальних та теоретичних досліджень вчених та аспірантів.

Зі змісту:

Секція 6. **Захист інформації та телекомунікаційні системи.** – С. 224-289.

Р 358631
004

Інформаційні технології: проблеми та перспективи [Текст] : монографія / [Н. Г. Аксак, О. Г. Алексієв, В. О. Алексієв та ін.] ; за заг. ред. В. С. Пономаренка ; МОН України. - Х. : [Видавець Рожко С. Г.], 2017. - 447 с. : табл., рис. - Бібліогр.: с. 434-446. - Авт. зазнач. на с. 447.

Розглянуто й обґрунтовано результати наукових досліджень в галузі розробки і практичного застосування сучасних інформаційних технологій.

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

Б 18209
004

Information Technology and Security [Text] / National Technical University of Ukraine "Kyiv Politechnic Institute", State Institution "Institute of special Communication and information Protection". - K. : [State Institution "Institute of special Communication and information Protection of Nat. Technical Univ. of Ukraine "KPI"], 2012 - . -

Vol. 4, Issue 1 (6), January-June 2016. - K., 2016. - 132 p. - Бібліогр. наприкінці ст. - Текст англ. та укр.

Зі змісту:

Ланде Д. В. Аналіз інформаційних потоків у глобальних комп'ютерних мережах : за матеріалами наукової доповіді на засіданні Президії НАН України 25 січня 2017 р. / Д. В. Ланде // Вісник Національної академії наук України. – 2017. – № 3. – С. 45-53.

Р/250

Показано параметри сучасного інформаційного простору, існуючі теоретичні і технологічні рішення. Наведено опис методологічних та інструментальних засобів аналізу інформаційних потоків, розроблених в Інституті проблем реєстрації інформації НАН України.

Мазуренко А. Аудит настроек безопасности MS SQL SERVER / А. Мазуренко // Захист інформації. – 2017. – Т. 19, № 1. – С. 43-46.

Р/1428

З безлічі доступних параметрів, автор виділяє основні, згрупувавши їх у п'ять категорій, які повинні контролюватися адміністратором в обов'язковому порядку. Для контролю параметрів безпеки по кожній з цих категорій, автор пропонує набір процедур у вигляді SQL-запитів.

Манько О. Використання пасивних оптичних пристроїв для захисту інформації у волоконно-оптичних лініях зв'язку та мережах / О. Манько, О. Шматок, А. Петренко // Захист інформації. – 2017. – Т. 19, № 2. – С. 143-147.

Р/1428

... для створення оптичних ліній з підвищеним рівнем захисту інформації необхідні додаткові заходи. З цією метою в роботі запропоновано використання маскування оптичного лінійного коду за рахунок збільшення кількості одиничних символів шляхом використання таких пасивних елементів, як оптичні лінії затримки та оптичні розгалужувачі.

Мельник Р. П. Підвищення інформаційної безпеки телекомунікаційної системи ДСНС України шляхом моніторингу інцидентів та оцінки ризику реалізації загроз безпеки / Р. П. Мельник, О. Г. Мельник, Г. П. Чепурний // Наукові праці Чорноморського держаного університету імені Петра Могили комплексу «Києво-Могилянська академія». Серія: Комп'ютерні технології. – 2016. – Вип. 271. – С. 65-69.

Р/1886«КТ»

У статті проведено аналіз останніх досліджень у сфері захисту інформації в структурних підрозділах ДСНС України. Запропоновано впровадження в телекомунікаційну систему ДСНС України удосконаленої системи моніторингових спостережень за інцидентами з розрахунком можливості реалізації загроз безпеки інформації.

Методи забезпечення стійкості мережі майбутнього до дії зовнішніх дестабілізуючих факторів / С. І. Отрох, В. О. Ярош, В. О. Власенко, Ю. М. Зіненко // Телекомунікаційні та інформаційні технології. – 2017. – № 2. – С. 24-30.

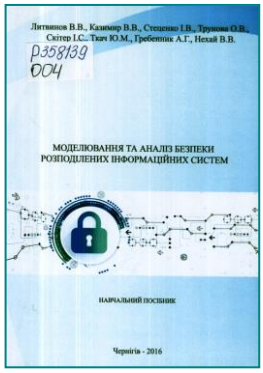
Р/1921

Наведено методи забезпечення стійкості елементів мережі майбутнього. Під стійкістю ми розуміємо здатність елементів мережі майбутнього виконувати свої функції та зберігати параметри у встановлених границях під час або після дії зовнішніх дестабілізуючих факторів. Сформульовано можливість знаходження сумарної стійкості мережі майбутнього.

Мєшечко С. С. Методи і способи захисту CMS Wordpress / С. С. Мєшечко, В. Я. Пєвнєв, В. А. Погорєлов // Системи управління, навігації та зв'язку. – 2017. – Вип. 1. – С. 23-25. – Текст рос.

Р/2152

Блоги, міні-сайти, а то й цілі портали – все це будується на основі такого зручного движка-конструктора як Wordpress. Авторами проведено аналіз методів і способів захисту CMS Wordpress. Описано детальні дії щодо підвищення стійкості системи до DDos-атакам так і основні помилки при адмініструванні сайту.



Р 358139
004

Моделювання та аналіз безпеки розподілених інформаційних систем [Текст] : навч. посіб. [для студ. спец. 121 "Інженерія програмного забезпечення"] / Литвинов В. В., Казимир В. В., Стеценко І. В. [та ін.] ; Чернігівський нац. технол. ун-т. - Чернігів : [Чернігівський нац. технол. ун-т], 2016. - 254 с. : іл. - Бібліогр. наприкінці розд. - Авт. на тит. арк. не зазнач.

У посібнику розглянуто питання структури розподілених інформаційних систем (РІС); основних понять кібербезпеки; інструментальних засобів організації та проведення атак; архітектури системи виявлення вторгнень; ознак, умов, методів виявлення атак; визначення джерел небезпечних вторгнень.

Мужанова Т. М. Класифікації злочинів із використанням мобільного телефону / Т. М. Мужанова, Ю. М. Якименко // Сучасний захист інформації. – 2017. – № 1. – С. 28-33.

Р/2300

Проаналізовано передумови розширення масштабів злочинності у сфері мобільного зв'язку, розглянуто класифікації правопорушень із використанням мобільного телефону та охарактеризовано їх основні види. Представлено власну класифікацію.

Мясіщев О. А. Метод захищеності комп'ютерних мереж на етепах проектування і експлуатації / О. А. Мясіщев, О. О. Мартинюк, Н. М. Гневська // Вісник Хмельницького національного університету. Серія: Технічні науки. – 2017. – № 1. – С. 140-143.

Р/1055«Т»

Розглядається метод захищеності комп'ютерних мереж на основі побудови дерева атак на етапах проектування і експлуатації. Детально описано постановку завдання дослідження та методику аналізу захищеності комп'ютерних мереж.

Невойт Я. В. Аналіз загроз інформаційної безпеки в період 2015–2016 років / Я. В. Невойт // Сучасний захист інформації. – 2017. – № 2. – С. 79-84.

Р/2300

В статті проведено аналіз сучасних загроз інформаційної безпеки в період 2015–2016 років. Наведено статистику інцидентів інформаційної безпеки за сферами компаній та розглянуто основні атаки, що зазвичай використовуються зловмисниками. Сформовані тренди комп'ютерних атак, що спостерігали в останні роки. Сформовані ключові елементи інформаційної безпеки сучасного підприємства.

Оптимальність неусіченої послідовної процедури Вальда в задачах перевірки двох простих прогнозів несанкціонованого доступу в інформаційних мережах держави / В. Б. Дудикевич, І. Р. Опірський, П. І. Гаранюк, О. А. Ваврічен // Інформатика та математичні методи в моделюванні. – 2016. – Т. 6, № 3. – С. 215-226.

Р/2357

«Програми контролю і прогнозування мають в окремих випадках тисячі команд, а їх виконання зводиться до багаторазових звернень до пам'яті і підпрограмою контролю і прогнозу. Перечисленні особливості дають вирішальний вплив на питання раціонального розміщення вихідних даних, програм контролю та прогнозу в пам'яті ЕОМ і на організацію структури програм.

Таким чином, проблема визначення основних алгоритмів при перевірці прогнозів НСД і ІМД, а також розвитку теорії прогнозування НСД в ІМД на базі математичного апарату теорії ймовірностей є актуальним і потребує детального і подальшого наукового дослідження. В нашій роботі ми продовжуємо поглиблюватись у проблему прогнозування НСД в ІМД, використовуючи, конкретно в цій статті, сучасний математичний апарат теорії ймовірності, а саме використовуючи процедури Вальда».

Оцінка ефективності методів захисту даних в інформаційній управляючій системі критичного застосування / О. О. Можаєв, С. Г. Семенов, М. О. Можаєв [та ін.] // Энергосбережение. Энергетика. Энергоаудит. – 2016. – № 12. – С. 2-12.

Р/1974

У статті проведена оцінка ефективності методів і способів розподілу доступу та захисту даних, а також представлені методичні рекомендації щодо їх використання в комп'ютеризованих інформаційних управляючих системах (КІУС) критичного застосування. Розроблено імітаційну модель системи розподілу доступу та захисту інформації в КІУС критичного застосування.

Р 357960
004

Регульовані фільтри джерел живлення для захисту інформації в мікроконтролерах [Текст] : [монографія] / В. Я. Жуйков, Т. О. Терещенко, Ю. С. Ямненко, А. В. Мороз. - К. : Кафедра, 2016. - 182 с. : рис., табл. - Бібліогр.: с. 165-173.

Описано нові схеми та алгоритми регульованих фільтрів живлення мікроконтролерів із маскуванням інформаційних сигналів, в основу функціонування яких покладено вейвлет та спектральний аналіз у полярних координатах та досліджено їхню ефективність.

Сачанюк-Кавецька Н. В. Визначення чутливості ідентифікаційної функції до зміни вхідних характеристик обробки зображень для розпізнавання суб'єктів у системах захисту інформації / Н. В. Сачанюк-Кавецька // Реєстрація, зберігання і обробка даних. – 2017. – Т. 19, № 1. – С. 55-63.

Р/1346

Розглянуто особливості операції диференціювання логіко-часових функцій за змінною з метою визначення чутливості ідентифікаційної функції до зміни вхідних характеристик зображень, що використовуються для розпізнавання суб'єктів у системах захисту інформації, та основні властивості такої операції.

Система стратегічних комунікацій Міністерства оборони України та Збройних Сил України / А. М. Вербицька, В. А. Савченко, Т. М. Дзюба, В. О. Кацалап // Наука і оборона. – 2017. – № 1. – С. 9-12.

Р/810

Розглянуто варіант структури системи стратегічних комунікацій Міністерства оборони України та Збройних Сил України. Обгрунтовано основні складові системи стратегічних комунікацій Міністерства оборони України та Збройних Сил України.

Системи захисту персональних даних в сучасних інформаційно-телекомунікаційних системах / Г. М. Гулак, В. А. Козачок, П. М. Складанний [та ін.] // Сучасний захист інформації. – 2017. – № 2. – С. 65-71.

Р/2300

Обгрунтовано необхідність створення систем захисту персональних даних в інформаційних системах. Розглянуті сучасні засоби захисту персональних даних. Обгрунтована стратегія захисту персональних даних в сучасних інформаційно-телекомунікаційних системах. Показана необхідність використання прогресивних та перспективних технологій інформаційної безпеки.

Сотниченко В. М. Інформаційна безпека як базова складова економічної безпеки телекомунікаційного підприємства / В. М. Сотниченко // Економіка. Менеджмент. Бізнес. – 2017. – № 1. – С. 58-66.

Р/2331

Розглянуто основні аспекти залежності стану економічної безпеки підприємства від безпеки інформаційної, від ступеню надійності зберігання інформації та доступу до неї. Висвітлено окремі причини недостатньої захищеності інформації та шляхи покращення ситуації.

Спасітєлєва С. О. Комплексний захист гетерогенних корпоративних сховищ даних / С. О. Спасітєлєва, В. Л. Бурячок // Сучасний захист інформації. – 2017. – № 1. – С. 58-65.

Р/2300

Запропоновано підхід щодо комплексного захисту сучасних корпоративних баз та сховищ даних, які побудовані за принципом багатоаспектної персистентності з використанням різних технологій зберігання та аналізу даних. На підставі проведеного аналізу та засобів захисту даних для реляційних та NoSQL систем управління базами даних, визначені проблеми захисту даних для гетерогенного сховища даних та шляхи їх подолання.

Б 17950
623

Сучасна спеціальна техніка [Текст] : науково-практичний журнал / МВС України, Державний н.-д. ін-т. - [К.] : ДНДІ МВС України, [Видавець ФОП Озеров Г. В.]. -
№ 2(45). - К., 2016. - 115 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., рос., англ.

Зі змісту:

Лєнков С. В., Джулій В. М., Муляр І. В. **Динамічні показники оцінки рівня функціональної безпеки інформаційної системи.** – С. 59-67.
У статті розглядаються підходи до розрахунку основних динамічних показників захищеності інформації та аналіз щодобових розподілів ймовірностей не припинених нелегальних доступів у інформаційну систему.

Толюпа С. В. Захист об'єктів інформаційно-комунікаційної структури підприємства / С. В. Толюпа, В. Ю. Чигринюк // Вісник Інженерної академії України. – 2017. – Вип. 1. – С. 230-234.

Р/1139

В статті розглянуті види та джерела загроз інформаційній безпеці підприємства та підсистеми ефективного захисту об'єктів інформаційно-комунікаційної структури. Виток інформації спричиняють інсайдери, і левова частка конфіденційної інформації розповсюджується саме через публічні канали глобальних мереж. В даному випадку саме комплексний підхід може забезпечити досягнення максимальної ефективності захисту інформації, оскільки системність забезпечує необхідні складові захисту і встановлює між ними логічний і технологічний зв'язок, а комплексність, що вимагає повноти цих складових, всеосяжності захисту, забезпечує її надійність.

Черевко О. В. Сутність, роль та завдання інтерфейсної безпеки у процесі забезпечення інформаційної та економічної безпеки вищого навчального закладу / С. М. Черевко, Ю. М. Радзіховська // Економіка та держава. – 2016. – № 11. – С. 15-18.

Р/1829

У контексті забезпечення інформаційної безпеки, інтерфейсною безпекою можна вважати стан захищеності інформаційних ресурсів ВНЗ від втрати ними цілісності, пошкодження, спотворення, викрадення або несанкціонованого використання контрагентами з метою забезпечення власної вигоди та/або на шкоду ВНЗ. Визначено завдання інтерфейсної безпеки у системі економічної безпеки ВНЗ.

Чуприн В. Метод протидії незаконному впливу на виборців у системі Інтернет голосування / В. Чуприн, В. Вишняков, М. Пригара // Безпека інформації. – 2017. – Т. 23, № 1. – С. 7-14.

Р/1408

Розглянуто систему Інтернет голосування з повністю відкритим для ознайомлення і випробування програмним забезпеченням, у якій для голосування можна користуватись яким завгодно пристроєм доступу до Інтернету. Для даної системи пропонується метод голосування, який забезпечує виборцям можливість вільного волевиявлення за умов наявності таких факторів незаконного впливу, як підкуп, залякування або силовий тиск.

Шишкова Н. Л. Засоби підвищення керованості безпекою облікової інформації / Н. Л. Шишкова // Економічний вісник Національного гірничого університету. – 2016. – № 3. – С. 119-127.

Р/1790

У статті розглядаються шляхи підвищення ефективності управління безпекою облікової інформації, за умови створення механізму попередження, профілактики, протидії загрозам якості та захисту облікової інформації. Запропоновано трирівневу систему управління безпекою облікової інформації з врахуванням аспектів її захисту.

Шульга В. П. Метод оцінки пошкоджень сервісів безпеки телекомунікаційної системи авіатранспортного комплексу / В. П. Шульга // Системи управління, навігації та зв'язку. – 2016. – Вип. 4. – С. 71-72.

Р/2152

У статті розглянуто метод оцінки пошкодження сервісів безпеки інформаційної системи для аналізу ризиків інформаційної безпеки на базі структури авіатранспортного комплексу з урахуванням специфіки інформаційної системи.

Інформаційне протиборство у воєнних конфліктах. Інформаційно-психологічна безпека

Антонюк В. В. Взаємодія державних та недержавних суб'єктів забезпечення інформаційної безпеки в процесі протидії збройній агресії РФ проти України / В. В. Антонюк // Вісник Київського національного університету імені Тараса Шевченка. Серія: Державне управління. – 2016. – № 3. – С. 5-8.

Р/1276

У статті досліджено сучасний стан взаємодії державних та недержавних суб'єктів забезпечення інформаційної безпеки в сучасних умовах збройного конфлікту між РФ та Україною. Недержавна система інформаційної безпеки охарактеризована як інституційний механізм її забезпечення. Проаналізовано різні форми і методи громадської активності як механізм протидії російським інформаційним впливам. Окреслено основні проблеми, що виникають у процесі даної взаємодії.

Вронська Т. В. Давньоіндійський трактат «Артхашастра» в контексті забезпечення інформаційної безпеки та протидії негативним інформаційно-психологічним впливам / Т. В. Вронська, М. В. Беланюк // Інформація і право. – 2017. – № 1. – С. 82-91.

Р/844

У статті крізь призму забезпечення інформаційної безпеки та протидії сучасним інформаційним операціям проаналізовано давньоіндійський трактат «Артхашастра», який і нині має важливе прикладне значення, оскільки у ньому висвітлені глибинні рушійні сили застосування деструктивного інформаційного впливу на різні групи громадян та широкий арсенал його методів.

Дзьобань О. П. Інформаційна безпека в контексті інформаційної культури / О. П. Дзьобань, Є. М. Мануйлов // Інформація і право. – 2017. – № 1. – С. 74-81.

Р/844

Показано, що ключовим фактором ризику для інформаційної підсистеми соціуму виступають масштабні соціокомунікативні та соціокультурні трансформації, що несуть у собі низку негативних соціальних наслідків.

Князєв Д. Інформаційна війна: причини виникнення та сучасні тенденції / Д. Князєв, С. Князєв // Бизнес и безопасность. – 2017. – № 2. – С. 20-24.

Р/1070

«… на боєздатність супротивника можна вплинути, знищивши його інфраструктуру, живу силу і техніку, а можна – порушивши його процеси обміну інформацією або запровадивши в інформаційні системи противника свою інформацію».

Лужецький В. Концептуальна модель системи інформаційного впливу / В. Лужецький, А. Дудатьєв // Безпека інформації. – 2017. – Т. 23, № 1. – С. 45-49.

Р/1408

Для реалізації інформаційного впливу, а також для захисту від нього у статті запропоновано концептуальну модель системи інформаційного впливу, яка формалузіє суб'єктно-об'єктну взаємодію у ході інформаційного протиборства і враховує необхідні для цього ресурси та процеси.

Любовець Г. Аналітико-прогностичні аспекти підходів до вивчення публічних негативів у комплексній структурі інформаційного простору країни / Г. Любовець, В. Король // Вісник Київського національного університету імені Тараса Шевченка. Серія: Військово-спеціальні науки. – 2017. – № 1. – С. 46-50.

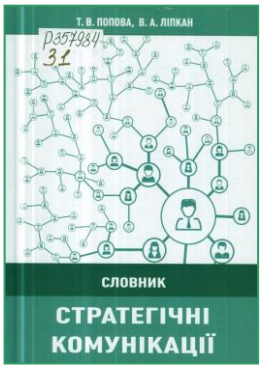
Р/1276

У статті розглядаються нові підходи до особливих реалій функціонування інформаційного простору, що виникли за умов динамічних креативно-технологічних комунікаційно-контентних агресій путінської Росії проти України та інших держав світу.

Мелешко Є. В. Дослідження методів визначення центральності акторів у соціальних мережах для задач інформаційної безпеки / Є. В. Мелешко, В. С. Гермак, С. М. Охотний // Системи управління, навігації та зв'язку. – 2016. – Вип. 4. – С. 67-70.

Р/2152

Розглянуто вплив величини центральності актора на ступінь його влади у соціальній мережі та здатність контролювати інформаційні потоки, а також здійснювати інформаційні впливи або захищатися від них.



Р 357984
31

Попова, Тетяна Валеріївна.
Стратегічні комунікації [Текст] : словник / Т. В. Попова, В. А. Ліпкан ; [за заг. ред. В. А. Ліпкана] ; М-во інформаційної політики України, Глобальна організація союзницького лідерства, Міноборони. - К. : ФОП О. С. Ліпкан, 2016. - 416 с. : табл. - Бібліогр.: с. 406-415.

Словник є першим в Україні виданням, в якому розглядається з позицій системного підходу та сучасних інформаціологічних та комунікативних стратегій феномен стратегічних комунікацій. У ньому зібрані основні поняття і терміни, якими послуговуються у сфері стратегічних комунікацій, а також користуються при реалізації кожного їх компонента.

Основна термінологія довідника успішно апробована при реалізації інформаційної політики. Однією з родзинок видання є формування авторських неологізмів, термінологічного поля стратегічних комунікацій, а також формування категорійно-понятійних рядів, що описують системні явища.

Трансформація парадигм захисту інформації, інформаційної та соціально-психологічної безпеки (Частина 2) / С. О. Гнатюк, В. О. Гнатюк, В. Г. Кононович, І. В. Кононович // Інформатика та математичні методи в моделюванні. – 2016. – Т. 6, № 4. – С. 322-332. – Текст англ.

Р/2357

У цій частині роботи представлені результати ретроспективного аналізу етапів трансформації парадигми сфери інформаційної безпеки: соціально-центрична парадигма інформаційної безпеки особи, суспільства, держави та, в цілому, національної безпеки; резюме щодо трансформації сфери інформаційної та кібернетичної безпеки; розподіл відносної значимості заходів захисту інформаційних ресурсів; парадигма мережної безпеки критичної інформаційної інфраструктури; система (технологія) визначення ідентичності та управління визначенням ідентичності; створення «довіреного» телекомунікаційного простору.

Отримана в частинах 1 та 2 систематизація та результати вирішення задач дозволяють підвищити ефективність роботи систем забезпечення інформаційної, кібернетичної та соціально-психологічної безпеки й формалізувати напрямки подальших досліджень щодо розробки ефективних систем безпеки.

Кібербезпека – проблема XXI століття

Борсуковський Ю. В. Базові напрями забезпечення кібербезпеки державного та приватного секторів / Ю. В. Борсуковський, В. Л. Бурячок, В. Ю. Борсуковська // Сучасний захист інформації. – 2017. – № 2. – С. 85-89.

Р/2300

В даній статті проведено аналіз актуальних кіберзагроз і напрямків їх використання. Сформульовано базові вимоги і рекомендації щодо забезпечення інформаційної та кібернетичної безпеки відповідно до діючих глобальних загроз в інформаційному просторі.

Брежнєв Є. В. Розробка методу оцінки забезпечення кібербезпеки транспортних засобів / Є. В. Брежнєв, В. В. Бородавка, Р. В. Салахов // Радіоелектронні і комп'ютерні системи. – 2017. – № 1. – С. 28-35.

Р/1769

Пропонується метод оцінювання ризиків кібербезпеки транспортних засобів (ТЗ), який засновано на використанні багаторівневого нечіткого виведення (Multi Fuzzy Inference System – MFIS). Метод засновано на моделі загроз і ризиків, що враховує взаємовплив між ризиками активів і контрзаходами, а також між вузлами ТС і ризик-факторами.

Визначення ефективних видів нейромережевих моделей розпізнавання кібератак на мережеві ресурси / О. Корченко, І. Терейковський, Л. Терейковська [та ін.] // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2016. – Вип. 2. – С. 56-63. – Текст рос.

Р/2287

Разработаны правила, применение которых позволяет определить как множество эффективных видов, так и наиболее эффективный вид нейросетевой модели распознавания кибератак на сетевые ресурсы информационных систем.

Віноградов М. Метод оцінювання ефективності обробки кіберінцидентів центрами CSIRT / М. Віноградов, Є. Іванченко, В. Гнатюк // Безпека інформації. – 2017. – Т. 23, № 1. – С. 56-62.

Р/1408

Обробка та управління кіберінцидентами – важливі завдання, розв'язанням яких займаються спеціалізовані центри типу CSIRT. Проте на сьогодні відсутні механізми оцінювання їх роботи. У роботі проаналізовано сучасні методи оцінювання роботи персоналу, проведено їх багатокритеріальний аналіз. Опираючись на результати аналізу, розроблено метод оцінювання ефективності обробки кіберінцидентів центрами CSIRT.

Домарєв В. В. Універсальна логіко-лінгвістична матрична модель системи забезпечення кібернетичної безпеки / В. В. Домарєв // Бизнес и безопасность. – 2017. – № 3. – С. 20-25.

Р/1070

«Пропонується визначити логіко-лінгвістичну матричну модель безпеки – як формалізовану сукупність взаємопов'язаних між собою процесів функціонування системи безпеки. Йдеться про логіко-лінгвістичну матричну модель будь-якої системи безпеки».

Кононович В. Математичні моделі процесів забезпечення соціально-психологічної кібербезпеки / В. Кононович, І. Кононович, М. Романюков // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2016. – Вип. 2. – С. 49-55.

Р/2287

Показані можливості використання математичних методів моделювання процесів забезпечення соціально-психологічного захисту та кібернетичної безпеки. Запропоновано і продемонстровано застосування агентного моделювання для представлення динаміки виявлення й нейтралізації небезпечних співробітників, здатних спричинити витік інформації з обмеженим доступом.

Р 359254
004

Математичне та імітаційне моделювання систем. МОДС 2017 [Текст] : дванадцята міжнар. наук.-практ. конф., 26-29 червня 2017 р. : тези доп. / НАН України, Акад. технологічних наук України, Інженерна акад. України [та ін.]. - [Чернігів] : [ЧНТУ], 2017. - 444 с. : іл., табл. - Бібліогр. наприкінці ст. - Текст укр., англ.

Зі змісту:

Нехай В. В., Литвинов В. В. **Кібер-ситуаційна обізнаність рівень перший: суб'єктно-об'єктна модель колективного доступу до інформаційних ресурсів.** – С. 95-99.

Новаков Є. О. Використання навчаємих HIPS-антивірусів для протидії кіберзлочинності / Є. О. Новаков, М. В. Цуранов // Системи управління, навігації та зв'язку. – 2017. – Вип. 1. – С. 26-28. – Текст рос.

Р/2152

У статті приведений аналіз методів побудови антивірусних систем. Вказані переваги та недоліки основних методів захисту. Описані види HIPS-антивірусів. Розроблений алгоритм навчання HIPS-антивірусу, усуваючий недоліки класичних та експертних реалізацій антивірусу. Описана програмна модель пропонованого антивірусного продукту.

Пархоменко І. І. Способи та методи захисту інформаційних ресурсів мобільних пристроїв від кібератак / І. І. Пархоменко, Д. М. Баран // Вісник Інженерної академії України. – 2017. – Вип. 1. – С. 86-89.

Р/1139

У статті розглянуті основні способи та механізми захисту інформаційних ресурсів, проведений аналіз їх особливостей. Наведено базові заходи захисту мобільних пристроїв від втрати інформації. Описано основні принципи впровадження їх у реальне корпоративне середовище.

Пєвнєв В. Я. Збільшення швидкості передачі як засіб протидії кібератакам / В. Я. Пєвнєв, М. В. Цуранов // Системи управління, навігації та зв'язку. – 2017. – Вип. 2. – С. 98-101.

Р/2152

Представлений аналіз сучасних підходів до визначення якості каналу передачі інформації.

Присяжнюк М. М. Особливості забезпечення кібербезпеки / М. М. Присяжнюк, Є. І. Цифра // Реєстрація, зберігання і обробка даних. – 2017. – Т. 19, № 2. – С. 61-68.

Р/1346

Проведено аналіз історичних передумов виникнення поняття «кіберпростір», розкрито особливості кіберзагроз, здійснено порівняльний аналіз стратегій кібербезпеки провідних країн світу, наведено комплекс проблем вітчизняної кібербезпекової сфери, обґрунтовано необхідність створення загальнодержавної системи забезпечення кібербезпеки та показано першочергові пріоритети та завдання щодо протидії загрозам у кіберпростірі України.

Самойленко Д. Часова складність різних реалізацій диспетчера доступу мережевого ресурсу / Д. Самойленко // Захист інформації. – 2017. – Т. 19, № 2. – С. 132-136.

Р/1428

Для створення комплексної системи захисту інформаційного ресурсу, у відповідності до нормативних вимог, необхідно реалізовувати концепцію диспетчера доступу як єдиної точки проходження усіх запитів. Існує декілька різних підходів реалізації диспетчера доступу, що відрізняються показниками безпеки щодо надійності. Реалізовано чотири варіанти диспетчера доступу засобами сервера Apache та мови програмування PHP; здійснено експериментальне визначення їх часової складності за допомогою апарата регресійного аналізу.

Стрєлкіна А. А. Забезпечення кібербезпеки медичних систем: виклики і рішення в контексті Інтернету речей / А. А. Стрєлкіна, Д. Д. Узун // Радіоелектронні і комп'ютерні системи. – 2017. – № 1. – С. 44-50.

Р/1769

Авторами виявлено основні вразливості, загрози та ризики мережевих медичних пристроїв. В роботі в загальних рисах описуються основні регламентуючі документи в області забезпечення кібербезпеки, а саме, правила конфіденційності і безпеки HIPAA, вимоги кібербезпеки FDA до і після виходу медичного пристрою на ринок.

Б 18334
623

Сучасна спеціальна техніка [Текст] : науково-практичний журнал / МВС України, Державний н.-д. ін-т. - [К.] : ДНДІ МВС України, [Видавець ФОП Озеров Г. В.]. -
№ 4(47). - К., 2016. - 131 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., рос., англ.

Зі змісту:

Хорошко В. О., Грищук Р. В. **Кібернетична зброя: класифікація, базові принципи побудови, методи та засоби застосування й захисту від неї.** – С. 30-36.

Шевченко А. С. **Комплексний підхід до побудови системи кібернетичного захисту Збройних Сил України.** – С. 47-54.

Харченко В. Мультирівнева модель даних для ідентифікації забезпеченості вимог відповідно нормативно-правовому забезпеченню кібербезпеки цивільної авіації / В. Харченко, О. Корченко, С. Гнатюк // Захист інформації. – 2017. – Т. 19, № 1. – С. 95-104.

Р/1428

У цій роботі запропоновано мультирівневу модель даних, яка за рахунок використання базової моделі формування вимог до забезпечення кібербезпеки цивільної авіації, конкатенації бінарних послідовностей та бінарно-шістнадцяткового кодового представлення характеристик безпеки, множини моделей безпеки та підмножин характеристик безпеки, дозволяє формалізувати процес ідентифікації забезпеченості вимог та визначення режимів безпеки критичних авіаційних інформаційних систем.

Б 18259
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. 1 (59). - К., 2017. - 142 с. : табл. - Бібліогр. наприкінці ст. - Текст кн. укр., англ., рос.

Зі змісту:

Рогов П. Д., Воровичб Б. О., Ткаченко В. А. **Шляхи забезпечення кібернетичної безпеки об'єктів критичної інформаційної інфраструктури держави у воєнній сфері.** – С. 64-72.