Тематична виставка "Безпека та захист інформаційного простору"

(надходження І півр. 2019)

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

Р/625

Бюлетень законодавства і юридичної практики України. – 2018. – № 7 (ІТ-сфера в Україні: законодавство, судова практика, коментар).

Це видання містить чинні нормативно-правові акти органів державної влади України та судову практику, які пов'язані з використанням інформаційних технологій та забезпечення прав та інтересів їх учасників.

Крім цього, наведено коментарі до чинного законодавства з урахуванням міжнародної та вітчизняної практики забезпечення та захисту ІТ-бізнесу.

Аналіз доцільності реалізації заходів щодо забезпечення інформаційної безпеки / С. Б. Гордієнко, О. О.Манько, В. О. Манько, О. М. Скубак // Управління розвитком складних систем. – 2018. – Вип. 36. – С. 89-94.

Р/2319

Розглянуто деякі аспекти прийняття рішень щодо управління інформаційною безпекою. За основу аналізу і подальшого прийняття рішень розглянуто економічний аналіз, який передбачає вивчення всіх факторів, під впливом яких відбувається розвиток аналізованих систем, закономірностей їх поведінки, динаміки зміни. Складність завдань економічного аналізу практично у всіх сферах діяльності, як правило, обумовлюється тим, що багато ключових параметрів економічних моделей неможливо достовірно оцінити. Як основний критерій здебільшого використовують функцію віддачі від інвестицій (ROI). Незважаючи на складні розрахунки згідно цієї моделі, ***пропонована методологія*** дає змогу менеджерам та спеціалістам у сфері засобів захисту інформації отримувати достовірні результати і правильно оцінювати ефективність засобів захисту інформації, а також визначати напрям їхнього розвитку.

Гребенюк М. В. Досвід Ізраїлю у сфері забезпечення кібербезпеки / М. В. Гребенюк, Б. Д. Леонов // Інформація і право. – 2018. – № 2. – С. 45-50.

Р/844

У статті аналізується досвід держави Ізраїль у сфері забезпечення кібербезпеки. Висвітлюється система органів, які відповідають за кібербезпеку. Аналізуються законодавчі ініціативи держави Ізраїль у сфері забезпечення кібербезпеки.

Гуржій Т. Інформаційне право: виклики гібридної війни / Т. Гуржій // Зовнішня торгівля: економіка, фінанси, право. – 2018. – № 4. – С. 16-26.

Р/1792

Проаналізовано сучасний стан та перспективи розвитку національного інформаційного права. На прикладі сучасної України визначено коло інформаційних загроз гібридної війни, проаналізовано їх вплив на сферу національної безпеки, окреслено напрями нейтралізації, зокрема – засобами інформаційного права.

Гуцалюк М. В. Протидія використанню учасниками злочинних угруповань мережі «Даркнет» / М. В. Гуцалюк // Інформація і право. – 2018. – № 3. – С. 111-117.

Р/844

У статті досліджуються питання протидії кіберзлочинності, зокрема використання мережі «Даркнет». Пропонуються напрями вдосконалення чинного законодавства.

Довгань О. Д. Наукова рефлексія інформаційної безпеки України: від позитивізму до метафізики права / О. Д. Довгань, Т. Ю. Ткачук // Інформація і право. – 2018. – № 4. – С. 79-89.

Р/844

У статті досліджуються історичні засади становлення сучасного розуміння інформаційної безпеки. На основі використання філософських методів досліджено особливості змісту інформаційної безпеки, критично проаналізовано сутнісні її характеристики. Визначені основні пріоритети розвитку інформаційного суспільства на сучасному етапі.

Довгань О. Д. Правове забезпечення інформаційної безпеки держави як підгалузь інформаційного права: теоретичний дискурс / О. Д. Довгань // Інформація і право. – 2018. – № 2. – С. 73-85.

Р/844

У статті досліджується система правового забезпечення інформаційної безпеки держави та визначаються основні її складові. Науково обгрунтовується, що правове забезпечення інформаційної безпеки держави є підгалуззю інформаційного права.

Журиленко Б. Вероятностная надежность защиты информации в зависимости от направления взлома / Б. Журиленко, Н. Николаева // Захист інформації. – 2018. – Т. 20, № 3. – С. 174-179.

Р/1428

«Научная новизна заключается в разработке новой методологии в подходе к проектированию, анализу рабочего состояния работающей ТЗИ (технической защиты информации) с целью экономии финансовых затрат, вкладываемых в защиту».

Кальченко В. В. Огляд методів проведення тестування на проникнення для оцінки захищеності комп'ютерних систем / В. В. Кальченко // Системи управління, навігації та зв'язку. – 2018. – Вип. 4. – С. 109-114.

Р/2152

Проаналізовано міжнародні стандарти і керівництва з інформаційної безпеки, розглянуті методології тестування на проникнення, проаналізовано нормативні акти різних країн в яких закріплено вимоги з проведення даного виду тестування. Наведено перелік найбільш розповсюджених міжнародних методологій проведення пентестінгу, надано їх короткий опис. Проаналізовано методи проведення пентестінгу, визначені основні переваги і недоліки таких методів.

Кожедуб Ю. Організаційна парадигма забезпечення інформаційної безпеки / Ю. Кожедуб // Information Technology and Security. – January-June 2018. – Vol. 6, Iss.1(10). – P. 26-36.

Р/1212

Досліджуються теоретико-методологічні основи застосування організаційних теорій управління для забезпечення інформаційної безпеки. Розглянуто основні терміни щодо систем та їх класифікацій, процесу управління та його функції, теорії, процесу й організації. Узагальнено основні положення щодо теорії управління, теорії систем, теорії організацій, що дають можливість встановити основу наукового підходу для сталого функціонування організацій, зокрема і тих, що працюють в сфері захисту інформації. Проаналізовані класичні підходи до формування наукових основ теорії систем, теорії організацій та теорій управління для забезпечення інформаційної безпеки. Зосереджено увагу на поєднанні означених теорій. Завдяки цьому сформульовано вимоги і задокументовано правила щодо ефективного і результативного управління інформаційною безпекою організацій різних видів, різного статусу, будь-якої сфери діяльності.

Кожедуб Ю. Реалізація процесного підходу до керування ризиками інформаційної безпеки в документах NIST / Ю. Кожедуб // Information Technology and Security. – July-December 2017. – Vol. 5, Iss.2(9). – P. 76-89.

Р/1212

Досліджуються методологічні основи діяльності Національного інституту стандартів і технологій Сполучених Штатів Америки (National Institute of Standards and Technology, NIST). Зосереджується увага на процесному підході до створення рекомендацій, настанов, керівних вказівок, рамкових документів. У цій статті аналізуються методичні документи щодо інформаційної безпеки, кібербезпеки та комп'ютерної безпеки, що дозволяють допомогти вибрати набір заходів контролю безпеки.

Кожедуб Ю. Функціональна модель системи забезпечення інформаційної безпеки / Ю. Кожедуб // Information Technology and Security. – July-December 2018. – Vol. 6, Iss.2(11). – P. 29-42.

Р/1212

Предметом дослідження є моделювання системи забезпечення інформаційною безпекою для організацій. Виокремлено проблеми моделювання означених систем, що пов'язані з розкриттям як природи процесу забезпечення інформаційної безпеки, так і з напрямом розробки практичних методів безпеки інформації. При цьому ретельно вивчаються статистика порушень, причини, що їх обумовлюють, особи порушників, сутність прийомів, які використовуються порушниками, обставини, за яких було виявлене порушення (модель порушника інформаційної безпеки).

715318 R
34

Кушакова-Костицька, Наталія Вадимівна.
Право на інформацію в інформаційну епоху. Порівняльне дослідження [Текст] : монографія / Н. В. Кушакова-Костицька ; [наук. ред. М. В. Костицький]. - К. : Логос, 2018. - 272 с. - Бібліогр.: с. 251-271 (340 назв).

Книгу присвячено важливому питанню сьогодення – формуванню інформаційного суспільства, яке безпосередньо пов'язано із реалізацією та захистом права людини на інформацію, і насамперед – переосмисленню цих прав на світоглядному рівні. Автором проаналізовано сучасний стан суспільно-правових відносин в інформаційній сфері з урахуванням філософських, правових, психологічних, технологічних та інших аспектів проблеми, які виникають у зв'язку із загальносвітовими тенденціями глобалізації та віртуалізації повсякденного життя.

Марущак А. І. Міжнародне співробітництво у боротьбі з транснаціональною кіберзлочинністю / А. І. Марущак // Інформація і право. – 2018. – № 3. – С. 104-110.

Р/844

У статті досліджуються питання міжнародного співробітництва у боротьбі з транснаціональною кіберзлочинністю. Сформульовано пропозиції щодо покращення співробітництва вітчизняних правоохоронних органів із зарубіжними партнерами з метою підвищення оперативності розслідування відповідних злочинів.

Марущак А. І. Тенденції розвитку медіа-сфери України у контексті інформаційної безпеки держави / А. І. Марущак // Інформація і право. – 2018. – № 2. – С. 96-102.

Р/844

У статті розкриваються тенденції розвитку медіа-сфери України у контексті інформаційної безпеки держави. Виокремлено тенденції, які не мають істотного негативного впливу на інформаційну безпеку України, які спрямовані на нейтралізацію загроз інформаційній безпеці держави, а також загрозливі для інформаційної безпеки держави тенденції.

Мохор В. Аналіз способів представлення оцінок ризиків інформаційної безпеки / В. Мохор, О. Бакалинський, В. Цуркан // Information Technology and Security. – January-June 2018. – Vol. 6, Iss.1(10). – P. 75-82.

Р/1212

Розглянуто способи представлення оцінок ризиків інформаційної безпеки. Серед них виокремлено дерево ризиків, троянду (зірку) та спіраль ризиків, карту ризиків і коридор прийнятності ризиків.

Мохор В. Представлення оцінок ризиків інформаційної безпеки картою ризиків / В. Мохор, О. Бакалинський, В. Цуркан // Information Technology and Security. – July-December 2018. – Vol. 6, Iss.2(11). – P. 94-104.

Р/1212

Розглянуто особливості представлення оцінок ризиків інформаційної безпеки картами ризику. На практиці така карта відображається координатною площиною. Її осями позначено параметри ризику інформаційної безпеки. Це ймовірність реалізації загрози та величина втрат. Завдяки цьому визначається прийнятність окремого або групи ризиків інформаційної безпеки. Вона встановлюється шляхом вибору шкали оцінювання.

713507 R
338

Правове регулювання економіки [Текст] : зб. наук. пр. / Держ. вищ. навч. закл. "Київський нац. екон. ун-т імені Вадима Гетьмана", Навч.-наук. ін-т "Юридичний ін-т". - К. : КНЕУ. -
№ 16. - К., 2017. - 276 с. : рис., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., англ.

Зі змісту:

Маркарян М. В. **Стан і перспективи адаптації законодавства України до вимог ЄС у сфері кіберзлочинності.** – С. 212-222.

Родін Є. С. Метод інформаційно-аналітичної підтримки управління ризиками безпеки ресурсів відомчих інформаційних систем / Є. С. Родін // Проблеми програмування. – 2018. – № 4. – С. 82-92.

Р/1373

Запропоновано формалізацію вразливостей та загроз за допомогою введення лінгвістичних змінних. Практично використано гібридні моделі та *soft computing* при побудові залежності рівня ризику виникнення помилок за двома факторами. Запропоновано два варіанти оцінювання впливу вразливостей на рівень ризику результуючого фактора. Запропоновано комбінацію використання статистичних даних та експертних оцінок для аналізу стану інформаційної безпеки організації. Запропоновано визначення сукупного ризику інформаційного ресурсу.

713743 В
34

Сучасні правові стандарти Європейського Союзу у сфері захисту персональних даних [Текст] : зб. документів / [неофіційний пер. з англ. І. Майстренко, за ред. В. Брижко, передмова В. Пилипчука] ; НДІ інформатики і права НАПрН України. - К. : [ТОВ "Вид. дім "АртЕк"], 2018. - 180 с. - Бібліогр. у виносках.

У запропонованому збірнику документів опублікованого вченими НДІІІ НАПрН України наукового видання «Сучасні правові стандарти Європейського Союзу у сфері захисту персональних даних» наведено документальні матеріали «Пакету захисту даних» Європейського Союзу, що набули чинності у травні 2018 року.
Видання розраховане на фахівців, експертів і вчених, представників державних і недержавних органів, закладів, установ, підприємств та організацій і має прикладне значення в контексті євроінтеграції України.

715068 R
004

Технології комплексного захисту інформації в кіберпросторі [Текст] : навч. посібник / Політанський Л. Ф., Політанський Р. Л., Толюпа С. В. [та ін.]; [за заг. ред. Л. Ф. Політанського] ; Чернівецький нац. ун-т імені Ю. Федьковича. - Чернівці :

Чернівецький нац. ун-т ім. Юрія Федьковича, 2018. - 204 с. : рис., табл. - Бібліогр.: с. 201-203 (32 назви). - Авт. на тит. арк. не зазнач.

У навчальному посібнику у доступній формі викладено методологічні основи комплексної інформаційної безпеки підприємств, установ та організацій. Матеріал підготовлено із застосуванням загально визначених логічних модулів, які забезпечують його ліпше сприйняття та засвоєння.

Для студентів, слухачів, аспірантів і викладачів навчальних закладів відповідного профілю.

Ткачук Н. А. Правове регулювання взаємодії Служби безпеки України з приватним сектором у сфері забезпечення кібербезпеки / Н. А. Ткачук // Інформація і право. – 2018. – № 4. – С. 104-111.

Р/844

У статті автор досліджує основні проблемні питання правового регулювання взаємодії СБ України з приватним сектором у сфері забезпечення кібербезпеки та пропонує шляхи їх вирішення.

Ткачук Т. Ю. Складові інформаційної безпеки держави: функціональний аналіз основних суб'єктів забезпечення / Т. Ю. Ткачук // Бизнес и безопасность. – 2018. – № 4. – С. 2-10.

Р/1070

Проблематика забезпечення інформаційної безпеки сьогодні привертає увагу науковців та практиків у різних сферах, втім питання визначення складових інформаційної безпеки та критеріїв, що використовуються з цією метою, досі залишається недостатньо розробленим. Не визначені складові інформаційної безпеки й на рівні законодавства. То ж актуальним є дослідження критеріїв виокремлення складових інформаційної безпеки та визначення щодо сутності останніх, що становить мету цієї статті.

715441 R
355

Турченко, Юлія Вікторівна.
Реалізація державної інформаційної політики України у сфері оборони [Текст] : [монографія] / Турченко Юлія Вікторівна ; Київський нац. ун-т імені Тараса Шевченка, Філософський ф-т, Військовий ін-т. - К. : Кондор, 2018. - 146 с. - Бібліогр.: с. 131-145.

Монографію присвячено висвітленню процесів інституціоналізації державної інформаційної політики України у сфері оборони. Особливу увагу надано визначенню суб'єктів її реалізації. Цінністю роботи виступає забезпечення інформаційної відкритості сфери оборони, за участю державних та недержавних суб'єктів її здійснення.

Уханова Н. С. Виклики і загрози правам та безпеці людини в інформаційній сфері / Н. С. Уханова // Інформація і право. – 2018. – № 4. – С. 33-45.

Р/844

У статті проаналізовано вплив загроз інформаційній безпеці. Охарактеризовано принципи забезпечення прав людини в умовах розвитку інформаційного суспільства. Досліджено світовий досвід дотримання прав людини у контексті розвитку інформаційних технологій.

713047 В
355

Центр воєнно-стратегічних досліджень Національного університету оборони України.
Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського [Текст] : [наук. вид.]. - К. : [ЦВСД НУОУ]. - **Вип. 2 (63)**. - К., 2018. - 148 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., англ., рос.

Зі змісту:

Сніцаренко П. М., Саричев Ю. О., Семененко В. М., Ткаченко В. А. **Удосконалення чинного інформаційного законодавства України як необхідна умова адекватності заходів щодо забезпечення інформаційної безпеки держави.** – С. 68-74.

714901 В
37

Центральноукраїнський державний педагогічний університет імені Володимира Винниченка.
Наукові записки [Текст] : [наук. вид.]. - Кропивницький : [ТОВ "Полімед-Сервіс"]. - (Серія: Право). -
Вип. 5. - Кропивницький, 2018. - 208 с. : табл. - Бібліогр. наприкінці ст. - Текст кн. укр., англ.

Зі змісту:

Сікорський О. П., Гілецький М. В. **Сучасний стан та перспективи удосконалення адміністративно-правового механізму реалізації політики інформаційної безпеки України.** – С. 189-193.

Яцишин М. Ю. Використання сили у кіберпросторі в рамках міжнародного права / М. Ю. Яцишин // Інформація і право. – 2018. – № 4. – С. 22-32.

Р/844

У статті досліджується питання міжнародно-правової кваліфікації кібервоєн. Розглядається співвідношення понять «кібератака», «кібернапад», «кіберзлочин» та «кібервійна», на підставі чого автор пропонує власні дефініції. Детально аналізуються підстави застосування норм міжнародного гуманітарного права і міжнародного кримінального права до кібервоєн. Досліджуються проблеми поширення дії основних принципів міжнародного права у кіберпросторі.

Програмні системи захисту інформації

Гавриленко С. Ю. Система ідентифікації шкідливого програмного забезпечення на основі контекстно-вільних граматик / С. Ю. Гавриленко, В. В. Челак, В. А. Василев // Сучасні інформаційні системи = Advanced Information Systems. – 2018. – Т. 2, № 2. – С. 101-105.

Р/543

Метою є дослідження існуючих моделей виявлення вірусів на базі формальних мов та граматик та удосконалення моделі за рахунок використання LL(1)-граматики. *Завдання:* розробити математичну модель ідентифікації шкідливого програмного забезпечення на основі контекстно-вільних граматик; вибрати ефективний алгоритм її роботи, розробити програмну модель та виконати тестування.

Гізун А. Програмний комплекс виявлення та оцінювання кризових ситуацій в інформаційній сфері / А. Гізун // Безпека інформації. – 2018. – Т. 24, № 2. – С. 137-146.

Р/1408

В цій роботі пропонується до уваги опис-програмного забезпечення, яке реалізує розроблений обчислювальний комплекс виявлення та оцінювання кризових ситуацій в інформаційній сфері, робота якого ґрунтується на використанні нечітких слабоформалізованих моделей та методів з застосуванням експертних підходів.

714775 В
62

Дніпровський державний технічний університет.
Збірник наукових праць Дніпровського державного технічного університету [Текст] = Collection of scholarly papers of Dniprovsk State Technical University : зб. наук. пр. - Кам'янське : [ДДТУ], 2017 - . - (Technical Sciences) (Технічні науки). -
Вип. 1 (32). - Кам'янське, 2018. - 195 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., англ.

Зі змісту:

Демченко Ю. Ю., Бабенко М. В. **Використання колірної моделі RGB та методу LSB при стеганографічному захисті інформації у файлах формату OFFICE OPEN XML**. – С. 106-110.

Постановка задачі. Засобами мови програмування C# розробити програмне забезпечення, за допомогою якого можна буде приховати таємну інформацію таким чином, щоб про її існування не дізнався будь-хто інший.

Добринін І. С. Оптимізація вибору варіанту побудови системи захисту інформації від атак при антагоністичній грі / І. С. Добринін, М. П. Борова // Системи озброєння і військова техніка. – 2018. – № 2. – С. 89-93.

Р/1903

У статті запропоновано використання математичного апарату теорії ігор для обгрунтування прийняття рішення щодо вибору варіанту побудови системи інформаційного захисту корпоративної мережі.

Евдокимов В. Централизованный синтез реконфигурируемых аппаратных средств информационной безопасности на высокопроизводительных платформах / В. Евдокимов, А. Давыденко, С. Гильгурт // Захист інформації. – 2018. – Т. 20, № 4. – С. 247-258.

Р/1428

Основна функція сигнатурних мережевих систем виявлення вторгнень (ССОВ) – пошук в інтенсивному потоці даних ознак відомих атак з бази сигнатур, що містять останнім часом десятки тисяч записів. У зв'язку зі стагнацією частоти мікропроцесорів, а також постійним зростанням мережевого графіку й збільшення кількості та складності атак традиційним програмним рішенням все складніше відповідати посилюючим вимогам інформаційної безпеки. Тому все більшого поширення набувають апаратні рішення з використанням реконфігуровних пристроїв на базі ПЛІС типу FPGA, які поєднують в собі близьку до апаратної продуктивність із гнучкістю програмного забезпечення.

Зосімов В. В. Технологія автоматизованої адаптації веб-додатків на основі ідентифікації кіберсутностей / В. В. Зосімов, О. В. Христодоров, О. С. Булгакова // Управляющие системы и машины. – 2018. – № 3. – С. 51-59.

Р/487

Описано програмне забезпечення для автоматизованої адаптації користувацьких інтерфейсів. Подано стислий опис програмної розробки, спрямованої на автоматизовану адаптацію інтерфейсів під потреби користувачів. Програмний продукт забезпечує псевдоідентифікацію користувачів (вибудування бази анонімних користувачів та правил на основі їх перебування у веб-додатках).

Ільєнко А. В. Програмний модуль з використанням процедури формування та верифікації електронного цифрового підпису / А. В. Ільєнко, С. С. Ільєнко // Наукоємні технології. – 2018. – № 3. – С. 345-354.

Р/2289

Описано програмний модуль реалізації електронно-цифрового підпису за національним стандартом ДСТУ 4145-2002 з модифікацією на базі алгоритму ECNR, що заснована на проблемі дискретного логарифмування в групі точок еліптичної кривої та проведено оцінювання ефективності програмної реалізації з умови забезпечення конфіденційності та цілісності.

Казмірчук С. Аналіз систем виявлення вторгнень / С. Казмірчук, А. Корченко, Т. Паращук // Захист інформації. – 2018. – Т. 20, № 4. – С. 259-276.

Р/1428

… в роботі проведений узагальнений аналіз програмних засобів систем виявлення вторгнень за визначеною базовою множиною характеристик («Клас кібератак», «Адаптивність», «Методи виявлення», «Управління системою», «Масштабованість», «Рівень спостереження», «Реакція на кібератаку», «Захищеність» та «Підтримка операційної системи»). Це дасть певні можливості щодо вибору таких засобів та розробки для них найбільш ефективних механізмів безпеки при впливах кібератак.

Коваленко О. В. Методи якісного аналізу та кількісної оцінки ризиків розробки програмного забезпечення / О. В. Коваленко // Системи управління, навігації та зв'язку. – 2018. – Вип. 3. – С. 116-125.

Р/2152

В роботі визначено і вирішено одне з протиріч, що виникають при розробці ПЗ, яке полягає в нехтуванні фірмами-розробниками ПЗ факторів вразливості безпеки ПЗ. Розроблено метод кількісної оцінки ризиків розробки ПЗ.

Програмне забезпечення формування еталонів параметрів для систем виявлення кібератак / А. Корченко, О. Заріцький, Т. Паращук, В. Бичков // Захист інформації. – 2018. – Т. 20, № 3. – С. 133-148.

Р/1428

На основі відомої системи виявлення кібератак, яка базується на методології виявлення аномалій (породжених кібератаками) та множини відповідних методів і моделей запропоноване програмне забезпечення, яке, за рахунок базового алгоритму та низки розроблених процедур (конструювання координатної сітки; ініціації величин на основі набору баз даних та модулів; графічного формування параметрів; пошуку спільних точок відповідно базових правил та графічної інтерпретації результату) дозволяє автоматизувати процес формування еталонів параметрів для сучасних систем виявлення атак та відображати результати детектування аномального стану у заданий проміжок часу.

Факториальные числа в задачах защиты информации / А. Борисенко, А. Горячев, В. Сердюк, М. Ермаков // Безпека інформації. – 2018. – Т. 24, № 3. – С. 169-174.

Р/1408

У статті розглядається метод захисту даних на перестановках для одночасного захисту даних від несанкціонованого доступу і перешкод. Запропонований метод для своєї реалізації вимагає перетворення вихідного повідомлення в відповідну йому перестановку символів. В роботі для такого перетворення використовуються факторіальні числа. *Метою статті* є розробка перешкодостійкого методу ідеального шифрування з достатньою для практичних завдань швидкодією роботи.

Телекомунікаційні мережі та інформаційно-комунікаційні технології

714284 R
621.39

Восьма міжнародна науково-практична конференція "Інфокомунікації – сучасність та майбутнє", 14-16 листопада 2018 року [Текст] : зб. тез : [у 4 ч.] / Одес. нац. акад. зв'язку ім. О. С. Попова. - О. : ОНАЗ, 2018. -
Ч. 1. - О., 2018. - 175 с. : рис., табл. - Бібліогр. в кінці ст.

Зі змісту:

Секція – Сучасні системи мобільного зв'язку та широкосмугового радіо доступу. – С. 4-89.
Секція – Мультисервісні засоби телекомунікацій та телекомунікаційні мережі. – С. 90-134.
Секція – **Інформаційна безпека**. – С. 135-170.

Голубничий О. Аналіз конфіденційності передавання інформації у системах DSSS за умов обмеженості систем використовування сигнально-кодових конструкцій / О. Голубничий // Захист інформації. – 2018. – Т. 20, № 4. – С. 221-230.

Р/1428

Технічний захист інформації у телекомунікаційних системах може бути реалізований на фізичному рівні цих систем шляхом забезпечення енергетичної та структурної прихованості передавання інформації. До телекомунікаційних технологій, які є найбільш придатними для реалізації таких методів захисту інформації, належать технології широкосмугових систем зв'язку, зокрема технологія DSSS (Direct Sequence Spread Spectrum).

Зубок В. Використання технології DNSSEC для захисту доменних імен в українському сегменті мережі Інтернет / В. Зубок // Information Technology and Security. – July-December 2017. – Vol. 5, Iss.2(9). – P. 43-50.

Р/1212

Система доменних імен є невід'ємною частиною адресації в мережі Інтернет. Дефекти в реалізації протоколу DNS дозволяють використовувати його для зловмисних дій, під час яких може бути порушено цілісність і доступність даних при обміні даними між DNS-клієнтом та DNS-сервером. Технологія DNSSEC, що призначена для захисту цілісності при обміні даними DNS, запобігає отриманню фальшивих даних DNS-клієнтами.

Зубок В. Ю. Визначення напрямків протидії кібератакам на глобальну маршрутизацію в мережі Інтернет / В. Ю. Зубок // Електронне моделювання. – 2018. – Т. 40, № 5. – С. 67-75.

Р/518

Попри фундаментальність протокол глобальної маршрутизації BGP-4 не є безпечним, оскільки оснований на довірі між учасниками глобальної маршрутизації. Розглянуто напрямки протидії, які дозволяють досягти зменшення можливих збитків від атак на глобальну маршрутизацію на рівні великого оператора, галузі, регіону. Запропоновано два напрямки: запобігання перехопленню маршрутів до власних префіксів та виявлення маршрутів до перехоплених префіксів і блокування трафіку до цих префіксів.

Катков Ю. І. Аналіз причин критичних ситуацій в інформаційно-інтелектуальних системах / Ю. І. Катков // Зв'язок. – 2018. – № 3. – С. 12-19.

Р/776

Розглянуто логічний ряд понять, пов'язаних із категорією «небезпека», що дозволить ранжувати спектр можливих загроз безпеці функціонування складної організаційно-технічної системи (СОТС) у критичних ситуаціях і сприятиме розробці затребуваних адекватних технологій протидії впливам зовнішнього середовища на інформаційну систему із мінімізацією негативних наслідків і, зрештою, дасть змогу вдосконалювати існуючу систему забезпечення безпеки СОТС. З огляду на згаданий логічний ряд понять з'ясовано причини виникнення критичних ситуацій в інформаційно-інтелектуальних системах і запропоновано класифікацію факторів-стресорів, зумовлюваних виникненням критичних знань, котрі, у свою чергу, призводять до критичного стану СОТС.

Козленко О. Побудова нечіткої онтології для аналізу системи захисту інформації в ІТС / О. Козленко // Безпека інформації. – 2018. – Т. 24, № 3. – С. 156-162.

Р/1408

«*Задачею роботи* є побудова нечіткої онтології сценаріїв витоку інформації та культури інформаційної безпеки. *Метою роботи* є визначення типів зв'язків між елементами системи захисту інформації в ІТС для можливого подальшого використання для формальної оцінки захищеності системи».

Кучернюк П. В. Методи і технології захисту комп'ютерних мереж (мережний, транспортний та прикладний рівні) / П. В. Кучернюк // Мікросистеми, Електроніка та Акустика. – 2018. – Т. 23, № 1. – С. 52-56.

Р/1325

Реферат – Розглянуто найбільш поширені рішення, які підтримуються виробниками обладнання для комп'ютерних мереж (комутатори 2-го та 3-го рівнів, маршрутизатори), реалізовані у операційних системах та протоколах і можуть бути використані при розробці та реалізації комплексних систем захисту корпоративних мереж. Стаття є другою з циклу статей, присвячених аналізу методів і технологій захисту. Наведено типові загрози комп'ютерним мережам мережевого, транспортного та прикладного рівнів моделі OSI та проведено аналіз особливостей методів і технологій захисту.

Метод розробки архітектури глибокої нейронної мережі, призначеної для розпізнавання комп'ютерних вірусів / І. Терейковський, О. Заріцький, Л. Терейковська, В. Погорелов // Захист інформації. – 2018. – Т. 20, № 3. – С. 188-199.

Р/1428

Стаття присвячена вирішенню задачі вдосконалення систем розпізнавання комп'ютерних вірусів.

Особливості створення мережевої системи виявлення вторгнень у комп'ютерні системи / Є. В. Риндич, В. В. Коняшин, С. В. Зайцев, Я. Ю. Усов // Математичні машини і системи. – 2018. – № 3. – С. 89-96.

Р/1052

Досліджено існуючі мережеві системи виявлення вторгнень (Intrusion Detection System, IDS) на основі хоста (Host-based intrusion detection system, HIDS) та мережеві системи виявлення вторгнення (Network intrusion detection system, NIDS). Особливу увагу приділено системам з відкритим програмним кодом як таким, що надають можливість провести дослідження не лише роботи, а й архітектури програмного забезпечення та принципів їх реалізації. Досліджено такі системи, як Snort, Suricata, Bro IDS, Security Onion.

Пархоменко І. І. Аналіз стеганографічних методів захисту інформації / І. І. Пархоменко, А. С. Ткаченко, А. О. Заїка // Вісник Інженерної академії України. – 2018. – № 2. – С. 73-76.

Р/1139

З розвитком інформаційних технологій питання інформаційної безпеки стає все більш актуальним, що стимулює пошук нових методів захисту інформації. Нові комп'ютерні технології надали імпульсу розвитку і вдосконаленню різних напрямів в галузі захисту інформації. Наразі дуже великий інтерес науковців та дослідників викликали методи цифрової стеганографії.

Пелещишин А. М. Фактори соціальних середовищ Інтернету в системі національної безпеки / А. М. Пелещишин, В. А. Вус // Вісник Інженерної академії України. – 2018. – № 2. – С. 76-81.

Р/1139

У статті здійснено аналіз соціальних середовищ Інтернету в сучасних умовах. Визначено фактори соціальних середовищ Інтернету як середовища, у яких здійснюється як корисна так і шкідлива інформаційна діяльність. Подано типи соціальних середовищ з точки зору системної організації процесу комунікації. Здійснено аналіз форм публічної інформаційної діяльності в соціальних середовищах Інтернету.

Розробка системи управління кіберінцидентами в мережах LTE / Р. Одарченко, В. Гнатюк, Т. Федюра, А. Коберник // Безпека інформації. – 2018. – Т. 24, № 2. – С. 84-90.

Р/1408

… було проведено аналіз механізмів забезпечення інформаційної безпеки найпопулярнішого в світі типу мереж LTE. Проведені дослідження показали, що мережі LTE, незважаючи на ряд переваг, мають також недоліки. Щоб виявити та боротися з кіберінцидентами, було створено архітектуру системи управління кіберінцидентами в мережах LTE. В роботі також наведена класифікація кіберінцидентів, розглянута служба реагування та комп'ютерні інциденти (CERT) та параметри звернень до цієї служби.

715729 В
004

Системи обробки інформації [Текст] = Information Processing Systems : щоквартальне наукове видання / Міноборони, Харківський нац. ун-т Повітряних Сил імені Івана Кожедуба. - Х. : [Видавництво ХНУПС імені Івана Кожедуба]. -
Вип. 4 (15). - Х., 2018. - 166 с. : іл., табл. - Бібліогр. наприкінці ст. - Алф. покажч.: с. 166. - Текст укр., рос., англ. Дод. тит. арк. англ.

Зі змісту:

Касім Аббуд Маxді. **Аналіз трафіку анонімності протоколу на основі використання скритої марківської моделі довіри.** – С. 66-76. – Текст англ.

Сорокин А. Как оградить детей от Интернет / А. Сорокин // Бизнес и безопасность. – 2018. – № 6. – С. 34-35.

Р/1070

… мы настоятельно рекомендуем не ограничивать доступ ребенка к ПК, а лучше просто ограничить доступ к некоторым сайтам и сервисам. В нашем материале мы расскажем вам, как ограничить вашему ребенку действия в сети.

Соснін О. В. Безпекові проблеми інформаційно-комунікаційної діяльності / О. В. Соснін // Юридична Україна. – 2018. – № 9. – С. 17-27.

Р/1880

Актуальність досліджень проблем інформаційно-комунікаційної безпеки в сучасному світі, що глобалізується, визначається тим, що її стан, головним чином, обумовлює поширення все нових і нових за функціональними можливостями інформаційно-комунікаційних технологій. Все це постійно змушує переосмислювати роль та значення інформації та інформаційного ресурсу суспільства країни як соціально-публічного блага в координатах правового виміру феномена його розвитку.

716653 R
31

Соціальні технології: актуальні проблеми теорії та практики [Текст] : зб. наук. праць / Класичний приватний університет. - Запоріжжя : Класичний приватний ун-т.
Вип. 80. - Запоріжжя, 2018. - 116 с. : табл. - Бібліогр. наприкінці ст. - Текст кн. укр., рос. англ.

Зі змісту:
Зоська Я. В., Бесараб А. О. **Споживчі інтенції українців щодо контенту й послуг Інтернету.** – С. 61-71.
Проданюк Р. І. **Інформаційна безпека в контексті неофункціоналізму Н. Лумана.** – С. 91-100.

Субач І. Модель виявлення кібернетичних атак на інформаційно-телекомунікаційні системи на основі описання аномалій їх роботи зваженими нечіткими правилами / І. Субач, В. Фесьоха // Information Technology and Security. – July-December 2017. – Vol. 5, Iss.2(9). – P. 145-152.

Р/1212

У статті розглядається актуальна задача захисту інформаційно-телекомунікаційних систем та мереж від кібернетичних атак в умовах їхнього постійного розвитку та поліморфізму шкідливого програмного забезпечення. Проведено аналіз та зроблено висновок про доцільність застосування моделей ідентифікації аномалій, що одночасно оперують якісними і кількісними даними та ґрунтуються на математичному апараті теорії нечітких множин та нечіткого логічного виводу.

Чуприн В. Метод протидії атакам посередника у транспарентній системі Інтернет голосування / В. Чуприн, В. Вишняков, О. Комарницький // Захист інформації. – 2018. – Т. 20, № 3. – С. 180-187.

Р/1428

Атака посередника, яку називають MITM (Man In The Middle), є однією з найбільш небезпечних загроз для систем Інтернет голосування (ІГ). Розглянуто метод протидії атакам посередника для транспарентних систем ІГ, у яких все без винятку програмне забезпечення є відкритим для перевірок та існує можливість в режимі реального часу контролювати відсутність модифікації штатного програмного забезпечення, а також перевіряти точність і своєчасність виконання штатних дій персоналом з боку необмеженої кількості активістів.

Інформаційне протиборство у воєнних конфліктах. Інформаційно-психологічна безпека

Барабаш О. В. Виявлення загроз інформаційній безпеці держави у змісті текстового контенту соціальних Інтернет-сервісів / О. В. Барабаш, Р. В. Грищук, К. В. Молодецька-Гринчук // Наукоємні технології. – 2018. – № 2. – С. 232-239.

Р/2289

… в світлі останніх подій, соціальні Інтернет-сервіси (СІС) використовуються провідними державами світу як дієвий інструмент проведення інформаційних операцій. У роботі запропоновано концептуальний базис дослідження інформаційного впливу на акторів у змісті текстового контенту СІС.

Верголяс О. О. Інформаційно-правове забезпечення спеціальних інформаційних операцій / О. О. Верголяс // Інформація і право. – 2018. – № 4. – С. 126-133

Р/844

В цій статті проаналізовано роль та місце інформаційного етапу спеціальних інформаційних операцій (на прикладі операції «Гюльчатай» центру «Миротворець») у загальному алгоритмі проведення спеціальних інформаційних операцій, а також розглянуто актуальний стан та проблеми правової регламентації спеціальних інформаційних операцій на сучасному етапі.

Комплексна система протидії негативному інформаційно-психологічному впливу на особовий склад Збройних Сил України / П. М. Сніцаренко, Ю. О. Саричев, В. А. Ткаченко, Л. В. Хоменко // Наука і оборона. – 2018. – № 2. – С. 40-45.

Р/810

У статті викладено погляди на створення системи протидії негативному інформаційно-психологічному впливу на особовий склад військ (сил) на основі реалізації розробленої та верифікованої методики, що дає змогу проводити заходи випереджувального адекватного реагування.

Левченко О. В. Інформаційні загрози як різновид воєнних загроз державі / О. В. Левченко, Ю. І. Міхєєв // Наука і техніка Повітряних Сил Збройних Сил України. – 2018. – № 3. – С. 14-19.

Р/2266

У статті розглядається поняття та сутність інформаційних загроз безпеці держави. Проведено аналіз нормативно-правових актів, які визначають можливі інформаційні загрози для України. На основі аналізу перебігу процесів анексії Російською Федерацією Автономної Республіки Крим та сучасних збройних конфліктів визначено особливості прояву інформаційних загроз та їх розвиток у воєнній сфері.

«*Мета статті* – обґрунтування необхідності врахування під час забезпечення національної безпеки держави заходів захисту від зовнішніх ІЗ як різновиду воєнних загроз державі».

Методи виявлення прихованих сугестивних інформаційно-психологічних впливів в інформаційних ресурсах текстового змісту / В. В. Бараннік, Т. В. Белікова, О. П. Мусієнко, О. В. Довбенко // Наукоємні технології. – 2018. – № 3. – С. 331-337.

Р/2289

… інформаційно-психологічний вплив характеризується різною семантичною насиченістю. Тому особливу увагу при обробці інформаційних ресурсів необхідно приділити аналізу сугестивної насиченості, тобто найбільш значимої інформації з прихованим інформаційно-психологічним впливом. Обґрунтовується вибір технології обробки інформаційних ресурсів, при якій вдасться вилучити ключову інформацію. Запропоновано варіант спеціального програмного забезпечення з використанням наведених методів.

Мосов С. П. Протидія негативним інформаційним впливам на людину і суспільство в умовах гібридної війни / С. П. Мосов, Н. С. Уханова // Інформація і право. – 2018. – № 2. – С. 134-141.

Р/844

Стаття присвячена проблематиці негативного інформаційного впливу на українське суспільство в умовах гібридної війни, виявлення та блокування його джерел, а також протидії надходженню викривленої та маніпулятивної інформації, що спрямована на безпосередню дезорієнтацію самосвідомості українців.

Мохор В. Негативний інформаційно-психологічний вплив на індивідуальну свідомість за соціоінженерним підходом / В. Мохор, О. Цуркан // Information Technology and Security. – July-December 2017. – Vol. 5, Iss.2(9). – P. 13-19.

Р/1212

Проаналізовано напрями досліджень шляхів подолання цієї проблеми. Серед них виокремлено здійснення негативного інформаційно-психологічного впливу за соціоінженерним підходом. Методи соціальної

інженерії спрямовані на таку зміну психіки, при якій змінюється об'єктивна реальність, умови діяльності. Особливістю такого впливу є те, що людина може не помічати його і не сприймати його як загрозу. З огляду на це запропоновано шляхи забезпечення безпеки індивідуальної свідомісті від негативного інформаційно-психологічного впливу за соціоінженерним підходом.

Рекунков И. С. Правовые основы мониторинга средств массовой информации в интересах информационного противоборства (войны) / И. С. Рекунков, В. К. Новиков // Вопросы защиты информации. – 2018. – № 3. – С. 68-71.

Р/0171

Представлен один из подходов мониторинга средств массовой информации (СМИ) для выявления и определения опасной информации (сведений, сообщений), распространяемой сайтами сети Интернет – сетевых изданий (социальных сетей), региональных и общероссийских СМИ, способной оказывать негативное воздействие на морально-психологическое состояние граждан.

713747 В
623

Сучасна спеціальна техніка [Текст] : науково-практичний журнал / Державний н.-д. ін-т МВС України. - К. : [ФОП Тарнавська Л. І.]. -
№ 1 (52). - К., 2018. - 156 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., англ.

Зі змісту:

Грищук Р. В., Лагодний О. В. **Формалізована постановка наукового завдання для підвищення ефективності виявлення загроз за даними з мережі Інтернет.** – С. 23-29.
У статті розкрито особливості ведення інформаційного протиборства в умовах гібридної війни з використанням мережі Інтернет, яка використовується як засіб для розповсюдження загроз психологічного впливу визначеній цільовій аудиторії.

Хорошко В. О., Хохлачова Ю. Є. **Інформаційна війна. Протидія інформаційним впливам.** – С. 74-81.
У ході проведеного дослідження було сформульовано рекомендації щодо протистояння інформаційній війні. Здійснено аналіз факторів інформаційних впливів та протидії інформаційній зброї, у результаті якого зазначено ряд можливих дій для протидії російській інформаційній ескалації в Україні.

Теоретичне обгрунтування методу кількісного оцінювання маніпулятивного впливу мас медіа на суспільну думку / С. Гнатюк, О. Заріцький, Н. Сейлова, Ю. Поліщук // Безпека інформації. – 2018. – Т. 24, № 2. – С. 130-136.

Р/1408

У статті розроблено метод оцінювання маніпулятивного впливу, який за рахунок оцінювання фінансових витрат, визначення цілей, завдань і стратегій маніпулювання, вибору засобів мас медіа та класифікованих методів маніпулювання, на основі сформованих баз даних причин, цілей критеріїв, фокус-груп та мас медіа, дозволяє обчислювати кількісні параметри, що характеризують величину маніпулятивного впливу мас медіа на суспільну думку.

Ткач В. Ф. Інформаційний тероризм / В. Ф. Ткач // Оборонний вісник. – 2019. – № 3. – С. 4-9.

Р/1134

Головною особливістю використання інформаційно-психологічного фактору у сучасних війнах є використання новітніх досягнень в області комп'ютерних та інформаційних технологій, засобів масової комунікації, насамперед Інтернету, а також розвиток демократії у багатьох країнах світу.

Улічев О. С. Дослідження моделей розповсюдження інформації та інформаційних впливів в соціальних мережах / О. С. Улічев // Системи управління, навігації та зв'язку. – 2018. – Вип. 4. – С. 147-151.

Р/2152

Метою є дослідження існуючих моделей розповсюдження інформації та інформаційних впливів у віртуальних соціальних мережах, порівняння окремих моделей, виявлення характеристик та специфічних ознак,що не враховуються в існуючих моделях.

Улічев О. С. Програмне моделювання поширення інформаційно-психологічних впливів у віртуальних соціальних мережах / О. С. Улічев, Є. В. Мелешко // Сучасні інформаційні системи = Advanced Information Systems. – 2018. – Т. 2, № 2. – С. 35-39.

Р/543

Завдання: розробити програмну модель для визначення того, як впливає структура соціальної мережі та властивості і ролі її користувачів на швидкість поширення інформаційно-психологічних впливів, а також визначити ефективність різних стратегій поширення інформаційно-психологічних впливів.

716560 В
355

Центр воєнно-стратегічних досліджень Національного університету оборони України.
Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського [Текст] : [наук. вид.] / [гол. ред. Загорка Олексій Миколайович]. - К. : [ЦВСД НУОУ]. -
Вип. 3 (64). - К., 2018. - 146 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., англ., рос.

Зі змісту:
Богданович В. Ю., Ворович Б. О., Марко Є. І. **Інформаційна безпека як основа воєнної безпеки держави та суспільства.** – С. 44-47.

714901 В
37

Центральноукраїнський державний педагогічний університет імені Володимира Винниченка.
Наукові записки [Текст] : [наук. вид.]. - Кропивницький : [ТОВ "Полімед-Сервіс"]. - (Серія: Право). -
Вип. 5. - Кропивницький, 2018. - 208 с. : табл. - Бібліогр. наприкінці ст. - Текст кн. укр., англ.

Зі змісту:
Сікорський О. П., Якобчук М. Ю. **Інформаційно-психологічні війни: форми та методи**. – С. 193-198.

Кібербезпека – проблема XXI століття

Архипова М. ИТ&ИБ: кто сверху? / М. Архипова // Информационная безопасность = Information Security. – 2018. – № 4. – С. 17-19.

Р/365

Сразу оговорюсь: речь в данной статье пойдет не о безопасности в целом, а об ИТ-направлении отрасли (оно же компьютерная безопасность или, в более широком плане, *кибербезопасность*).

Борисов И. Обзор уровня зрелости процессов ИБ: о трендах и методологиях / И. Борисов // Информационная безопасность = Information Security. – 2018. – № 6. – С. 34-35.

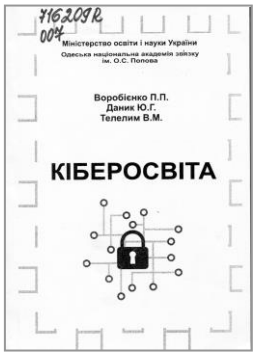
Р/365

В контексте кибербезопасности модели зрелости могут помочь разграничить организации, в которых информационная безопасность полноценно встроена в бизнес-деятельность, и те, в которых она выполняет в основном вспомогательную комплаенс-функцию.

Ванерке Р. EDR – обнаружение и реагирование // Информационная безопасность = Information Security. – 2018. – № 4. – С. 28-29.

Р/365

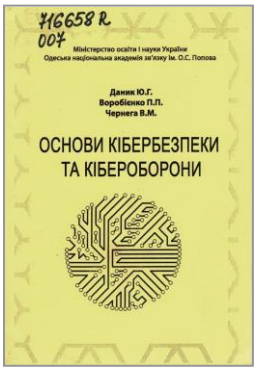
В настоящей статье будет рассмотрен один из относительно новых типов средств защиты информации – EDR (Endpoint Detection and Response), который предназначен для более эффективной защиты от целенаправленных атак и для реагирования на выявляемые инциденты информационной безопасности.



716209 R
007

Воробієнко, Петро Петрович.
Кіберосвіта [Текст] : монографія / П. П. Воробієнко, Ю. Г. Даник, В. М. Телелим ; Одес. нац. акад. зв'язку ім. О. С. Попова. - О. : ОНАЗ ім. О. С. Попова, 2018. - 208 с. : табл. - Бібліогр. в кінці розд.

У монографії розкрито сутність, зміст і взаємозв'язок кібернетичної та інформаційної безпеки, проведено аналіз формування та розвитку кіберосвіти в Україні та у світі. Обгрунтовано, що за сучасних умов знання з кібербезпеки у тих, хто навчається повинні формуватися в рамках базових курсів усіх без винятку навчальних закладів, запропоновано шляхи формування компетенцій з основ кібербезпеки у закладах вищої освіти. Для систематизації та удосконалення підготовки у сфері кібербезпеки авторами розроблено варіант реалізації організації системи освіти з питань кібербезпеки. Він охоплює всі рівні освіти від дошкільної та середньої до вищої та післядипломної. При цьому передбачається поетапне та безперервне формування необхідних у сучасному інформаційному суспільстві знань і компетенцій з питань кібербезпеки. Особливу увагу приділено питанню формування зазначених знань і компетенцій у військових закладах вищої освіти Сектору національної безпеки і оборони України. Запропонована і практично апробована цілісна, послідовна, взаємопов'язана та безперервна система підготовки з питань кібербезпеки та кібероборони на тактичному, оперативному і стратегічному рівнях підготовки та зміст навчання для її реалізації.



716658 R
007

Даник, Юрій Григорович.
Основи кібербезпеки та кібероборони [Текст] : підручник / Ю. Г. Даник, П. П. Воробієнко, В. М. Чернега ; Одеська національна академія зв'язку імені О. С. Попова. - О. : ОНАЗ ім. О. С. Попова, 2018. - 228 с. : граф., рис., табл. - Бібліогр. в кінці розд.

В підручнику викладено сутність і зміст кібербезпеки. Розглянуто роль і місце кібербезпеки у системі національної безпеки держави. Надано аналіз побудови системи кібербезпеки. Розглянуто широке коло питань зі складових кібербезпеки, їх аналізу і дій для її всебічного забезпечення. Приділено значну увагу технологіям дій у кіберпросторі.

Підручник підготовлений за матеріалами наукових розробок авторів, вітчизняних та іноземних видань та призначений для підготовки студентів, може бути корисний для науково-педагогічних працівників, докторантів, ад'юнктів та широкого кола військових і цивільних фахівців, що працюють у галузі кібербезпеки.

Дмитренко Ю. Кибербезопасность / Ю. Дмитренко // Бизнес и безопасность. – 2019. – № 1. – С. 16-21.

Р/1070

«Кибербезопасность – это часть информационной безопасности любой организации. Но эффективность ее зависит не только от используемого ПО и оборудования. Как бы ни старались айтишники, какие бы жесткие меры они не предпринимали, какие бы изощренные средства защиты не устанавливали, в любой, самой надежной защите всегда остается слабое звено – пользователи».

Довгань О. Д. Глобальна культура кібербезпеки в системі запобігання кіберзлочинності в Україні / О. Д. Довгань, А. В. Тарасюк // Інформація і право. – 2018. – № 3. – С. 94-103.

Р/844

В статті досліджується питання дефініції поняття «глобальна культура кібербезпеки», розглядаються принципи та підходи формування глобальної культури кібербезпеки на національному рівні. Основна увага приділяється складовим феномена культури кібербезпеки, її ролі та місцю в системі запобігання кіберзлочинності.

Довгань О. Д. Корпоративна культура кібербезпеки суб'єктів наукової та науково-технічної діяльності // Інформація і право. – 2018. – № 2. – С. 51-61.

Р/844

У статті запропоновано авторське бачення поняття корпоративної культури кібербезпеки суб'єктів наукової та науково-технічної діяльності, її складових, принципів та методів формування. Основна увага приділяється питанням забезпечення кібербезпеки у контексті захисту авторських і суміжних прав, честі, гідності, ділової репутації фізичних і юридичних осіб.

Жилін А. Функціональна модель ситуаційного центру кіберзахисту / А. Жилін, М. Худинцев, М. Літвінов // Information Technology and Security. – July-December 2018. – Vol. 6, Iss.2(11). – P. 51-67.

Р/1212

… в статті проводились дослідження моделей аналізу кібератак з позиції дослідника (Діамантова модель та Q Модель), реалізації кібератак з позиції атакуючого (Модель Cyber Kill-Chain) та моделей, що враховують більш широкий спектр аналітичних підходів (Адаптивна модель безпеки). Грунтуючись на потребах в даних для аналізу кібератак, враховуючи етапи проведення кібератак та беручи за основу архітектуру Адаптивної системи безпеки визначено функції забезпечення кіберзахисту до, під час та після проведення кібератак. Результати аналізу вибраних моделей дозволили також запропонувати Організаційну модель ситуаційного центру кіберзахисту, визначити його складові та сформулювати основні функції.

715769 R
004

Забезпечення кібербезпеки: правові та технічні аспекти, наук.-практ. семінар (2018 ; Харків).

Збірник тез наукових доповідей науково-практичного семінару "Забезпечення кібербезпеки: правові та технічні аспекти", 8 листопада 2018 року [Текст] / Нац. аерокосм. ун-т імені М. Є. Жуковського "Харк. авіац. ін-т", Каф. права та каф. комп'ютерних систем, мереж та кібербезпеки [та ін.]. - Х. : [ФОП Лисенко І. Б.], 2018. - 115 с. - Бібліогр. у виносках . – Текст кн. укр., англ. та рос.

Публікації охоплюють питання забезпечення кібербезпеки в Україні, висвітлені науковцями, викладачами, а також працівниками правоохоронних органів.

Зі змісту:

Сесія 1. Технічні аспекти забезпечення кібербезпеки
Сесія 2. Особливості правового забезпечення кібербезпеки
Сесія 3. Комп'ютерна криміналістика
Трибуна молодого вченого.

715761 R
004

Засоби та системи технічного захисту інформації [Текст] : навч. посібник для студ. спец. 125 "Кібербезпека" спец. "Системи технічного захисту інформації" / [І. Є. Антіпов, А. М. Олейніков, Ю. В. Ликов та ін.] ; Харківський нац. ун-т радіоелектроніки. - Х. : [ХНУРЕ], 2019. - 216 с. : рис., табл. - Бібліогр.: с. 202-212 (171 назва).

У навчальному посібнику поєднуються дослідження з використанням

стандартних контрольно-вимірювальних приладів, спеціальних засобів ТЗІ і оригінальних програмних продуктів власної розробки, які дозволяють скоротити матеріальні витрати під час вивчення і практичних досліджень технічних каналів витоку інформації.

Зубок В. Ю. Визначення напрямків протидії кібератакам на глобальну маршрутизацію в мережі Інтернет / В. Ю. Зубок // Електронне моделювання. – 2018. – Т. 40, № 5. – С. 67-75.

Р/518

Попри фундаментальність протокол глобальної маршрутизації BGP-4 не є безпечним, оскільки оснований на довірі між учасниками глобальної маршрутизації. Розглянуто напрямки протидії, які дозволяють досягти зменшення можливих збитків від атак на глобальну маршрутизацію на рівні великого оператора, галузі, регіону. Запропоновано два напрямки…

Иванов М. Кибератаки – глобальная угроза для бизнеса / М. Иванов // Бизнес и безопасность. – 2018. – № 4. – С. 14-20.

Р/1070

Из заголовков статьи:

Что такое кибербезопасность?
Во сколько обходится устранение последствий?
Кибер-угрозы *Табл.1. Источники кибер-угроз. Табл. 2. Виды кибер-угроз*
Вирусы – вымогатели
Уязвимости облачных сервисов и систем с Big Data
Спам, фишинг и социальный инжиниринг
Искусственный интеллект в помощь
Новые стандарты идентификации
Возвращение к модели «нулевого доверия»
Социальная инженерия и другие мошенничества
Как белые хакеры прикидываются злоумышленниками *и др.*

715575 R
004

Информационные технологии и безопасность [Текст] : материалы XVIII международной науч.-практ. конф. [ИТБ-2017] / НАН Украины, Ин-т проблем регистрации информации НАН Украины. - К. : [ООО "Инжиниринг"].
Вып. 18. - К., 2018. - 359 с. : ил., табл. - Библиогр. в конце ст. - Текст кн. укр., рос., англ.

В сборнике представлены статьи, посвященные вопросам кибернетической безопасности критических инфраструктур, 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.

714897 В
004

Інформаційні системи та мережі [Текст] : зб. наук. пр. / голова ред.-вид. ради Н. І. Чухрай ; Національний університет "Львівська політехніка". - Л. : Вид-во Львів. політехніки, 2018. - 144 с. : граф., рис., табл. - (Вісник / Національний університет "Львівська політехніка" ; № 887). - Бібліогр. наприкінці ст. - Текст кн. укр. та англ. мов.

Зі змісту:

Дудикевич В. Б., Микитин Г. В., Ребець А. І. **Квінтесенція інформаційної безпеки кіберфізичної системи.** – С. 58-68.

Кондакова С. В. Кібербезпека в Великобританії. Перші враження / С. В. Кондакова, Ю. І. Хлапонін // Бизнес и безопасность. – 2019. – № 1. – С. 22-23.

Р/1070

Очима доцента кафедри кібербезпеки Київського національного університету будівництва та архітектури, яка проходить стажування в Йоркському університеті (University of York), Велика Британія.

Починаємо серію публікацій про стан кібербезпеки в провідних країнах світу.

Конредди Рамануджа. Интеграция аппаратной защиты элементов безопасности IoT / Рамануджа Конредди // CHIP-NEWS Украина. Инженерная микроэлектроника. – 2019. – № 2. – С. 28-30.

Р/900

В статье рассматриваются главные проблемы безопасности узлов Интернета вещей IoT и перечисляются основные виды хакерских атак. В качестве защиты от них предлагается микроконтроллер SAM L11, имеющий встроенные узлы безопасности. Показаны элементы структуры безопасности, реализованные в SAM L11.

Кыдыралина Л. Предпосылки для формирования безопасной информационно-образовательной среды современного университета / Л. Кыдыралина // Захист інформації. – 2018. – Т. 20, № 4. – С. 205-214.

Р/1428

В роботі проведено огляд та аналіз попередніх досліджень у сфері забезпечення захисту інформаційно-освітнього середовища університетів (ІОСУ). Показано, що пріоритетність розвитку цифрових систем освіти в багатьох промислово розвинених державах світу вимагає відповідної техніко-методологічної підтримки фахівців не тільки в галузі педагогічної діяльності, а й інформаційних технологій з урахуванням проблематики кібербезпеки захисту інформації.

Лукацкий А. Как новые технологии влияют на стратегию ИБ? / А. Лукацкий // Информационная безопасность = Information Security. – 2018. – № 6. – С. 38-41.

Р/365

Во время обсуждения в Фейсбуке темы этой статьи возникла небольшая дискуссия, которая поделила всех участников на два лагеря. Одни говорили, что новые технологии никак не могут повлиять на стратегию ИБ, другие, наоборот, считали, что это вполне возможно. В этой статье я попробую примирить два лагеря и попробовать рассмотреть, как влияют новые технологии на кибербезопасность.

713218 В
004

Моделювання-2018, конф. (2018 ; Київ).
Збірка праць конференції "Моделювання-2018", 12-14 вересня 2018, Київ [Текст] = Simulation-2018 : [наук. вид.] / Ін-т проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України, Донец. нац. техн. ун-т, Ін-т проблем реєстрації інформації НАН України [та ін.]. - К. : [ВД "Академперіодика" НАН України], 2018. - 278 с. : рис., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., рос., англ. мов.

Зі змісту:

Мохор В. В., Зубок В. Ю. **Оцінка ризиків кібернетичних атак на глобальну маршрутизацію в мережі Інтернет.** – С. 147-153.

713005 R
004

Моделювання та інформаційні технології [Текст] : зб. наук. пр. / НАН України, Ін-т проблем моделювання в енергетиці імені Г. Є. Пухова. - К. : [ПП "Системи, технології, інформаційні послуги"]. - **Вип. 83**. - К., 2018. - 217 с. : рис., табл. - Бібліогр. наприкінці ст. - Текст укр., рос., англ.

Зі змісту:

Давиденко А. М., Суліма О. А. **Структурні підходи до методів оцінки рівня безпеки інформаційних систем.** – С. 11-21.

Савельєв Д. В. **Модель загрози кібербезпеки об'єктів критичної інформаційної інфраструктури у сфері ядерної енергетики.** – С. 42-48.

Пархоменко І. І. Способи захисту інформації у об'єктах Інтернету речей від загроз інформаційної безпеки / І. І. Пархоменко, А. С. Сторіжко, М. С. Іващенко // Вісник Інженерної академії України. – 2018. – № 2. – С. 69-73.

Р/1139

Інтернет речей – це вже об'єктивна реальність. Процес розвитку концепції неможливо зупинити, незважаючи на серйозні проблеми інформаційної безпеки. Збитки від реалізованих загроз виходять за межі кібернетичного простору впливаючи на людські життя. Хакери наразі продемонстрували ряд зламів побутової техніки, автомобілів і навіть кардіостимуляторів, підключених до Інтернету. Саме тому Інтернет речей вимагає посиленої уваги з боку безпеки.

Писаренко И. Современные способы управления доступом как часть задачи управления безопасностью / И. Писаренко // Информационная безопасность = Information Security. – 2018. – № 6. – С. 26-27.

Р/365

Управление доступом к информационным системам и ресурсам было и остается одной из важнейших задач обеспечения информационной безопасности для любой организации: правильно выстроенная система управления доступом позволяет существенно снизить риски получения пользователями «излишних» доступа и прав, связанных с этими рисками несанкционированных действий, утечек информации, внедрения вредоносных программ и других негативных действий.

Сачук Ю. Є. Професійна підготовка фахівців із кібербезпеки та захисту інформації: тезаурус та онтологія / Ю. Є. Сачук // Проблеми інженерно-педагогічної освіти. – 2018. – № 59. – С. 35-40.

Р/1605

… тезаурус поряд із онтологією є сучасною формою представлення знань, придатною для їх автоматизованої обробки, що корелює з набуттям та управлінням знань у процесі професійної підготовки фахівців із кібербезпеки та захисту інформації.

Семенченко А. І. Науково-методологічні підходи до проведення огляду кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури / А.І. Семенченко, Д. В. Мялковський, Т. В. Станіславський // Інвестиції: практика та досвід. – 2018. – № 18. – С. 87-94.

Р/2124

У статті розглянуто науково-методологічні підходи до організації та проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, актуальність дослідження яких обумовлена як вимогами чинного законодавства, так і тенденціями розвитку сфери національної безпеки і оборони, невідповідністю державної політики та державного управління вимогам надійного та оперативного реагування на кіберзагрози та кіберінценденти.

Тецький А. Г. Застосування дерев атак для оцінювання імовірності успішної атаки Web-додатка / А. Г. Тецький // Радіоелектронні і комп'ютерні системи. – 2018. – № 3. – С. 74-79. – Текст рос.

Р/1769

У даній статті розглянуті часті причини атак Web-додатків, створених за допомогою систем управління контентом. У зв'язку з високою активністю зловмисників необхідне створення методів оцінювання безпеки Web-додатків і методів протидії атакам.

713047 В
355

Центр воєнно-стратегічних досліджень Національного університету оборони України.
Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського [Текст] : [наук. вид.]. - К. : [ЦВСД НУОУ]. -
Вип. 2 (63). - К., 2018. - 148 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., англ., рос.

Зі змісту:
Телелим В. М., Даник Ю. Г., Зінченко А. О. **Модель оцінювання вразливостей систем із критичною кібернетичною інфраструктурою.** – С. 63-67.

716560 В
355

Центр воєнно-стратегічних досліджень Національного університету оборони України.
Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського [Текст] : [наук. вид.] / [гол. ред. Загорка Олексій Миколайович]. - К. : [ЦВСД НУОУ]. -
Вип. 3 (64). - К., 2018. - 146 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., англ., рос.

Зі змісту:
Алексєєв М. М. **Протидія кібернетичним загрозам у Польщі: досвід для України.** – С. 49-53.

Шуклін Г. В. Метод побудови стабілізаційної функції керування кібербезпекою на основі математичної моделі коливань під дією сил із запізненням / Г. В. Шуклін, О. В. Барабаш // Телекомунікаційні та інформаційні технології. – 2018. – № 2. – С. 110-116.

Р/1921

Досліджуються системи керування кібербезпекою, які містять запізнення – окремий вид адаптивних систем. Проаналізовано причини, які сприяють наявності запізнення в системах захисту інформації при кібернетичних атаках. Запропоновано математичну модель кількісної оцінки ефективності системи захисту інформації, на прикладі коливань, які виникають під дією сили з запізненням. На прикладі атак на брандмауер показана методика керування кібербезпекою.

Шуклін Г. В. Формування національної моделі державного регулювання кібербезпеки фондового ринку та новітні форми прогнозування в системі державного регулювання кібербезпеки / Г. В. Шуклін, О. В. Барабаш // Зв'язок. – 2018. – № 3. – С. 25-30.

Р/776

Запропоновано оригінальний концептуальний підхід до побудови національної моделі державного регулювання кібербезпеки фондового ринку, який за своєю функцією входить у загальнодержавну систему економіки. Подано принципово нову форму прогнозування кібернетичних атак на електронні торговельні системи фондового ринку за допомогою інструментів форсайту. Розкрито можливості форсайт-досліджень у державному регулюванні кібербезпеки фондового ринку. Для визначення пріоритетів регулювання запропоновано використання відповідних дорожніх карт.

Яковів І. Інформаційно-телекомунікаційна система, концептуальна модель кіберпростору і кібербезпека / І. Яковів // Information Technology and Security. – July-December 2017. – Vol. 5, Iss.2(9). – P. 134-144.

Р/1212

Семантичні невизначеності між базовими поняттями у галузі кібербезпеки значно звужують діапазон і знижують результативність наукових досліджень щодо методів аналізу і прогнозування, наприклад, APT кібератак або розробки комплексів захисту на основі формальних моделей доказу їх ефективності. Напрям можливого подолання проблеми – розробка концептуальної моделі кіберпростору і кібербезпеки.