Тематична виставка
"Безпека та захист інформаційного простору "

(надходження II півр. 2020)

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

725278 В
34

Актуальні проблеми правознавства [Текст] = Actual Problems of Law : зб. наук. пр. / Тернопільський нац. екон. ун-т, Юрид. ф-т. - Тернопіль : ТНЕУ, 2019 - .
Вип. 1(21). - Тернопіль, 2020. - 207 с. : рис., табл. - Бібліогр. наприкінці ст. - Текст кн. укр. та англ.

Зі змісту:

Панченко В. **Управління інформаційною безпекою держави та підприємств: правові та організаційні аспекти.** – С. 103-109.
Розглянуто складові державної інформаційної політики щодо забезпечення інформаційної безпеки країни і визначено основні напрямки діяльності органів державної влади у цій сфері. На основі аналізу стану нормативно-правового регулювання інформаційної безпеки України визначено основні здобутки та недоліки у нормативно-правовому полі держави щодо забезпечення інформаційної безпеки. Наведено визначення поняття інформаційної безпеки підприємства.
Сліпченко Т. **Кібербезпека як складова системи захисту національної безпеки: європейський досвід.** – С. 128-133.
Досліджено передумови й особливості формування законодавства України у сфері кібербезпеки, визначено проблеми та перспективи його подальшого розвитку з точки зору оцінювання наявних небезпек та загроз.

Багмет М. О. Досвід країн ЄС відносно розроблення та реалізації моделей державної інформаційної політики / М. О. Багмет, А. М. Гаркуша // Публічне управління та регіональний розвиток. – 2020. – № 8. – С. 515-539.

Р/662

Стаття присвячена висвітленню досвіду Німеччини, Франції, Італії, Іспанії, Польщі, Нідерландів та інших країн, які входять до складу ЄС по впровадженню в практику інформаційно-комп'ютерних технологій в ході сучасного всесвітнього глобалізаційного процесу. Окремо зазначається і роль Великобританії, яка хоча і заявила про вихід із складу ЄС, але має значний доробок в розроблення головних політико-правових аспектів в ході реалізації державної інформаційної політики та інформаційної стратегії...

Вилков А. С. Методики разработки правил безопасного подключения к Internet / А. С. Вилков, С. Л. Вилков, М. М. Тараскин // Вопросы защиты информации. – 2020. – № 2(129). – С. 63-76.

Р/0171

Рассмотрены вопросы функционирования глобальной сети Internet, проблемы защищенной передачи информации в глобальной сети Internet, а также процедуры разработки правил (методик) безопасного подключения к Internet.

Жилін А. Проблематика захисту інформаційних ресурсів при використанні хмарних технологій / А. Жилін, А. Дивіцький, А. Козачок // Information Technology and Security. – July-December 2019. – Vol. 7, Iss. 2(13). – P. 171-182.

Р/1212

"*Метою статті* є аналізування проблематики захисту інформаційних ресурсів при використанні хмарних технологій. Для досягнення сформованої мети проаналізовано технології хмарних обчислень та виконано порівняльний аналіз нормативно-правових документів щодо захисту інформації при використанні хмарних технологій".

723793 В
004

Информационные технологии и безопасность [Текст] : материалы XIX международной науч.-практ. конф. [ИТБ-2019] / НАН Украины, Ин-т проблем регистрации информации НАН Украины. - К. : [ООО "Инжиниринг"].
Вып. 19. - Киев, 2019. - 236 с. : ил., табл. - Библиогр. в конце ст. - Текст кн. укр., рос., англ.

В сборнике представлены статьи, посвященные вопросам безопасности живучести критических инфраструктур, моделирования и противодействия информационным операциям, информационных технологий в управлении, методов и способов информационной поддержки принятия решений, компьютерного моделирования систем организационного управления, информационно-аналитических исследований на основе открытых источников информации, сценарного анализа при обеспечении информационной поддержки принятия решений, актуальным проблемам обеспечения информационной и кибернетической безопасности.

Коломицев М. В. Порівняльний аналіз моделей оцінки зрілості інформаційної безпеки / М. В. Коломицев, С. О. Носок, Р. О. Тоцький // Захист інформації. – 2019. – Т. 21, № 4. – С. 224-232. – Текст рос.

Р/1428

Мета даної статті – описати і порівняти найбільш використовувані моделі зрілості інформаційної безпеки для аналізу їх відповідності цілям використання спільно з стандартом ISO 27001.

Метод інформаційно-часового супроводження глобальних, локальних соціально-політичних та інших процесів у сучасному безпековому середовищі / В. Ю. Богданович, А. М. Сиротенко, Г. В. Пєвцов [та ін.] // Наука та інновації. – 2020. – Т. 16, № 2. – С. 101-107.

Р/1928

Використання методу забезпечує співставлення фактів, подій, виявлених в ході моніторингу БС, з глобальними й локальними процесами, що дає змогу ідентифікувати геополітичні та інші інтереси, наміри інших держав, вчасно виявляти заходи щодо дезінформації, інформаційного прикриття, різних маніпуляцій і психологічного впливу та своєчасно приймати управлінські рішення в системі забезпечення національної безпеки.

724403 R
32

Методологічні аспекти інформатизації військової логістики [Текст] : колективна монографія / [авт. кол. : Поліщук В. Б., Нетесін І. Є., Закалад М. А. та ін.] ; [за ред. В. Б. Поліщука] ; Український наук. центр розвитку інформаційних технологій (УкрНЦ РІТ). - Київ : УкрНЦ РІТ, 2019. - 106 с. : рис., табл. - Бібліогр. наприкінці розділів. - Кол. авт. зазнач. на звороті тит. арк.

У монографії узагальнені матеріали науково-практичних семінарів, які проводились Українським науковим центром розвитку інформаційних технологій (УкрНЦ РІТ) Міністерства освіти і науки України та Центром воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського за участю наукових співробітників та спеціалістів Міністерства оборони України, інших установ і компаній, а також результати НДДКР з тематики інформатизації військової логістики, виконаних УкрНЦ РІТ.
Методологічні аспекти інформатизації військової логістики, розглянуті у широкому контексті – від концептуальних питань розроблення стратегії розвитку інформаційних технологій оборонного відомства до прикладів автоматизації логістичного забезпечення засобами ERP- та BI-систем.

Організаційно-правові механізми державного управління забезпеченням кібербезпеки та кіберзахисту України: сутність, стан та перспективи розвитку / А. І. Семенченко, В. Л. Плескач, О. А. Заярний, М. В. Плескач // Проблеми програмування. – 2020. – № 2–3. Спец. вип. – С. 278-286.

Р/1373

У дослідженні здійснено аналіз організаційно-правових механізмів державного управління забезпеченням кібернетичної безпеки та кібернетичного захисту України, надано визначення його сутності, місця в системі стратегічного планування та управління сектором безпеки та оборони, проведено оцінку окремих аспектів забезпечення кібернетичної безпеки в Україні. Крім того, у статті містяться рекомендації щодо вдосконалення системи забезпечення кібернетичної безпеки в Україні, зокрема надано пропозиції щодо усунення наявних колізій і прогалин в основних нормативно-правових актах, що регулюють сферу забезпечення національної, інформаційної та кібернетичної безпеки України, у тому числі шляхом гармонізації українського законодавства з міжнародними правовими актами у цій галузі.

725780 R
004

Пащенко, Руслан Едуардович.
Захист просторово-розподілених даних у комп'ютерних системах [Текст] : конспект лекцій / Р. Е. Пащенко ; Нац. аерокосм. ун-т ім М. Є Жуковського "Харків. авіац. ін-т". - Харків : ХАІ, 2020. - 104 с.

Розглянуто відомості щодо нормативно-правового забезпечення захисту інформації і рівнів забезпечення інформаційної безпеки. Наведено класифікацію шкідливих програм, дані щодо їх впровадження у комп'ютерні системи та їх шкідливу дію на просторово-розподілені дані. Розглянуто методи виявлення шкідливих програм. Викладено основні проблеми, пов'язані з безпекою в мережі інтернет, та основні компоненти і приклади брандмауерів. Подано дані щодо можливості тайної передачі інформації і методів криптографічного захисту просторово-розподілених даних у комп'ютерних системах, моделі цифрового підпису.

Петренко В. И. Анализ существующих методик оценки защищенности информационных систем / В. И. Петренко, А. В. Шерстобитов // Вопросы защиты информации. – 2020. – № 2(129). – С. 49-58.

Р/0171

Проведен сравнительный анализ методик оценки защищенности информационных систем. Рассмотрены слабые и сильные стороны наиболее известных подходов к ее оценке. Использование результатов данного исследования позволит в дальнейшем усовершенствовать наиболее оптимальный метод оценивания защищенности информационных систем.

Піддубна Л. В. Інформаційна безпека в системах електронного документообігу / Л. В. Піддубна, В. М. Павліченко // Науковий вісник Полтавського університету економіки і торгівлі. Серія: Економічні науки. – 2019. – № 4. – С. 59-66.

Р/1484

Мета статті полягає у виявленні загроз інформаційної безпеки систем електронного документообігу, які використовуються в державних та комерційних структурах, на великих та середніх підприємствах, в організаціях, установах, і шляхів їх подолання.

725110 В
34

Повітряне і космічне право. Юридичний вісник [Текст] : наук. пр. Нац. авіац. ун-ту / Нац. авіац. ун-т. - Київ : [НАУ]. -
№ 2(55). - Київ, 2020. - 232 с. : табл. - Бібліогр. наприкінці ст. - Текст укр., англ.

Зі змісту:

Тична Б. М. **Інформаційна безпека як основа інформаційної діяльності Збройних сил України.** – С. 108-113.

На основі аналізу законодавства та наукового обґрунтованих підходів до розуміння змісту інформаційної безпеки, існуючих (та можливих) інформаційних загроз у сфері оборони країни, узагальнено зміст інформаційної безпеки у діяльності Збройних сил України. На основі аналізу норм Конституції України сформульовані принципові засади, які детермінують інформаційну діяльність Збройних сил України щодо забезпечення інформаційної безпеки.

Юринець Ю. Л., Бєлкін Л. М., Бєлкін М. Л. **Проблеми легітимізації Інтернет-ресурсів як засобів масової інформації в контексті інформаційної безпеки держави.** – С. 114-122.

Констатовано, що європейська правова традиція не вважає регулювання обігу інформації в мережі Інтернет апріорі заходом, що порушує свободу слова. За умови належного правового регулювання (у відповідності із вимогами Конвенції про захист прав людини і основоположних свобод) таке регулювання, навпаки, підсилює гарантії діяльності журналістів і розширює коло інформації, до якої можна застосовувати презумпцію достовірності – при одночасному підвищенні відповідальності таких Інтернет-поширювачів за поширення неналежної інформації.

724402 R
32

Поліщук, Валерій Борисович
Інформаційні технології в управлінні оборонними ресурсами: методологічний контекст та приклади практичної реалізації [Текст] : монографія / Поліщук В. Б., Нетесін І. Є., Нестеренко О. В. ; Укр. нац. центр розвитку інформаційних технологій (УкрНЦ РІТ). - Київ : УкрНЦ РІТ.
Частина 1. - Київ : УкрНЦ РІТ, 2019. - 122 с. : табл., рис. - Бібліогр. наприкінці розділів.

У монографії викладені методичні підходи до формалізації процедур експертного оцінювання альтернативних варіантів оцінювання носіїв спроможностей в оборонному плануванні, які можуть бути реалізовані засобами інформаційних технологій та використовуватись як інструмент підтримки прийняття рішень. Розглянуто також аспекти побудови єдиного інформаційного простору сфери управління оборонними ресурсами та застосування індустріальних підходів до створення відповідного програмного забезпечення.

Структури архітектури систем управління інформаційною безпекою / В. В. Мохор, В. В. Цуркан, Я. Ю. Дорогий, Ю. М. Штифурак // Інформатика та математичні методи в моделюванні. – 2019. – № 4. – С. 209-221.

Р/2357

... проаналізовано окремі різновиди структур. Зокрема, огляд і порівняльний аналіз методологій розроблення архітектур організацій; рамкові архітектури побудови інформаційних систем НАТО; аспекти використання структур при розробленні критичної ІТ інфраструктури; підходи до описання архітектури систем і окремих компонентів. Завдяки цьому встановлено можливість застосування структур стосовно розроблення архітектури систем управління інформаційною безпекою.

Програмні системи захисту інформації

723768 В
004

Бабешко, Є. В.
Методи комплексування процедур оцінювання та забезпечення функціональної безпеки інформаційно-керуючих систем [Текст] / Є. В. Бабешко ; ред. В. С. Харченко ; Міністерство освіти і науки України . - Харків : Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ», 2019. - 185 с. - Бібліогр.: с. 160-173.

Монографія базується на результатах дисертаційного дослідження на здобуття наукового ступеня кандидата технічних наук (PhD) у галузі безпеки індустріальних інформаційно-керуючих систем (спеціальність 05.13.06 – інформаційні технології). Виконана в Національному аерокосмічному університеті ім. М.Є. Жуковського «Харківський авіаційний інститут», кафедра комп'ютерних систем, мереж і кібербезпеки. Присвячена розробленню методів комплексування процедур оцінювання та забезпечення функціональної безпеки інформаційно-керуючих систем і їх компонентів, що дозволяє шляхом сумісного використання процедур вплинути на якість проектних рішень із забезпечення надійності та безпеки ІКС. Результати впроваджені у проекті TEMPUS-SEREIN Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains (543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCP) при виконанні програми СТЗ.

Беляков И. Практические аспекты построения процесса безопасной разработки программного обеспечения / И. Беляков // Information Security/Информационная безопасность. – 2020. – № 1. – С. 42-43

Р/365

Наличие слабых мест в исходном коде программного обеспечения ухудшает его работу и провоцирует возникновение рисков, связанных с нарушением целостности и конфиденциальности информации. Чем грозит эксплуатация таких уязвимостей и можно ли сделать разработку приложения безопасной?

Буравцов А. Проблематика разработки программного обеспечения, функционирующего в рамках КИИ / А. Буравцов, А. Мелихов // Information Security/Информационная безопасность. – 2020. – № 1. – С. 36-38.

Р/365

В этой статье мы рассмотрим проблемы, связанные с разработкой программных продуктов офисного назначения для объектов КИИ, их соответствие требованиям регулятора, а также задачи переориентации технологии производства таких продуктов. за основу возьмем модель, в настоящий момент реализуемую в ООО "Новые Облачные Технологии".

726025 В
355

Військовий інститут Київського національного університету імені Тараса Шевченка.
Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка [Текст] : збірник наукових праць. - Київ : [ВІКНУ].
Вип. № 67. - Київ, 2020. - 160 с. : іл. - Бібліогр. наприкінці ст. - Текст кн. укр., рос., англ.

Зі змісту:

Джулій В. М., Бойчук В. О., Тітова В. Ю., Сєлюков О. В., Мірошніченко О. В. **Моделі і методи захисту від загрозливих програм інформаційних систем.** – С. 72-84.
У статті запропоновано підхід до розвитку методів захисту від загрозливих програм в сучасних інформаційних системах, що складається в розробці методів захисту, заснованих на реалізації контролю доступу до файлів по їх типам, які можуть бути ідентифіковані розширеннями файлів, що істотно перевершують відомі методи антивірусного захисту, як по ефективності захисту, так і в міру впливу на завантаження обчислювальних ресурсів інформаційної системи.

724464 В
621.39

Військовий інститут телекомунікацій та інформатизації.
Збірник наукових праць [Текст] = Collection of Scientific Papers / Міноборони України. - К. : [ВІТІ].
Вип. № 4. - К., 2019. - 148 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст укр., рос. та англ.

Зі змісту:

Леонтович С. П., Закалад М. А., Беляченко В. В. **Обґрунтування критеріїв оцінки претендентів з розробки програмного забезпечення для потреб Збройних Сил України.** – С.92-100.

724486 В
004

Інформаційні системи та мережі [Текст] : зб. наук. пр. / відп. ред. В. Пасічник ; Національний університет "Львівська політехніка". - Львів : Вид-во Львів. політехніки, 2019. - 110 с. : граф., рис., табл. - (Вісник / Національний університет "Львівська політехніка" ; вип. 6). - Бібліогр. наприкінці ст. - Текст кн. укр. та англ. мов.

Зі змісту:

Буров Є. В., Микіч Х. І., Верес О. М., Литвин В. В. **Система ідентифікації проблемних ситуацій тестування програмного забезпечення.** – С. 30-40.

724400 R
004

Качко, Олена Григорівна.
Навчальний посібник з дисципліни "Паралельне програмування". Використання SIMD-команд для паралельних обчислень [Текст] / О. Г. Качко, О. Ф. Осика ; Харківський нац. ун-т радіоелектроніки. - Харків : [ХНУРЕ], 2019. - 276 с. : табл. - Бібліогр.: с. 247-248 (21 назва).

Використання засобів паралельного програмування може суттєво збільшити продуктивність програм, тому ці засоби широко використовуються під час створення сучасного програмного забезпечення. Одним з напрямків паралельного програмування є застосування SIMD-команд, клас яких і функції постійно розширюються в сучасних процесорах. У навчальному посібнику розглянуто прийоми програмування за допомогою цього класу засобів, у тому числі, AVX, AVX512, виконується аналіз ефективності їх застосування, наведена велика кількість прикладів практичних задач та їх вирішення, насамперед, у галузі криптографії, де продуктивність має найважливіше значення.

724882 R
004

Ковтун, В'ячеслав Васильович.
Моделі атрибутів гарантоздатності інформаційної системи критичного застосування із автентифікацією суб'єкта за голосом [Текст] : монографія / В. В. Ковтун ; Вінницький національний технічний університет. - Вінниця : ВНТУ , 2020. - 412 с. : граф., рис. - Бібліогр.: с. 374-396.

В монографії розглянуто теоретичні основи оцінювання атрибутів гарантоздатності інформаційних систем критичного застосування із автентифікацією суб'єкта за голосом. Представлено моделі індивідуальності голосу у мовленнєвому сигналі із шумом для конфіденційної автентифікації суб'єкта. Формалізовано моделі конфіденційності, доступності, цілісності, безвідмовність, готовність, обслуговуваність, інтенсивність відмов і наробок на відмову такого класу інформаційних систем. Запропонований комплекс моделей дозволяє об'єктивно оцінити довільний екземпляр класу інформаційних систем критичного застосування у метриці атрибутів гарантоздатності, а також, підвищити його конфіденційність організацією доступу за схемою двохфакторної верифікації із автентифікацією суб'єкта-користувача за голосом як другого фактору.

Колесник Р. О. Розроблення програмного забезпечення для імітації військової гри за допомогою математичного аналізу / Р. О. Колесник, А. Б. Коба // Зв'язок. – 2020. – № 3(145). – С. 57-59.

Р/776

Проаналізовано можливість використання математичного аналізу для імітації військової гри. Описано програмне забезпечення імітаційного моделювання JCATS, за основу якого можна взяти імітаційні алгоритми та впровадити їх у військову гру.

725196 R
004

Математичне та імітаційне моделювання систем. МОДС 2020 [Текст] : п'ятнадцята міжнар. наук.-практ. конф., 29 червня - 01 липня 2020 р., м. Чернігів : тези доп. / НАН України, Акад. технологічних наук України, ДНДІ випробувань і сертифікації озброєння та військової техніки, Україна [та ін.]. - Чернігів : [ЧНТУ], 2020. - 370 с. : граф., рис., табл. - Бібліогр. наприкінці ст.

У збірник включені тези доповідей, які були представлені на конференції «**Математичне та імітаційне моделювання систем. МОДС 2020».** В доповідях розглянуті наукові та методичні питання з напрямку моделювання складних екологічних, технічних, фізичних, економічних, виробничих, організаційних та інформаційних систем з використання математичних та імітаційних методів.

Зі змісту:

Лисецкий Ю. М., Калбазов Д. И. **Инструментальные средства обеспечения информационной безопасности предприятия. –** С. 117-119.

Міщенко М. В., Гребенник А. Г., Трунова О. В. **Прогнозування рівня загроз з використання мереж Байєса.** – С. 120-122.

Тарасов О. Є., Гребенник А. Г., Трунова О. В. **Використання мультиагентних систем для захисту корпоративних мереж. –** С. 186-190.

724475 B
658

Менеджмент та підприємництво в Україні: етапи становлення і проблеми розвитку [Текст] = Management and Entrepreneurship in Ukraine: the stages of formation and problems of development : зб. наук. пр. Т. 1, № 2 / голов. ред. Ігор Олексів. - Львів : Вид-во Львів. політехніки, 2019. - 134 с. : рис., табл. - Бібліогр. наприкінці ст. - Текст укр. та англ.

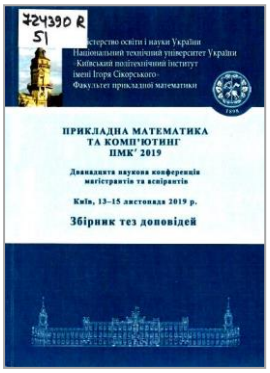
Зі змісту:

Кузьмін О. Є., Станасюк Н. С., Берднік Д. А. **Приклади результатів від дії негативних сценаріїв використання програмного забезпечення.** – С. 18-32.

Муха Ар. А. Количественная оценка уровня гарантоспособности компьютерных систем / Ар. А. Муха // Математичні машини і системи. – 2019. – № 4. – С. 146-153.

P/1052

Запропоновано метод, який дозволяє, отримавши чисельне значення рівня гарантоздатності досліджуваної системи, проводити її аналіз, а також виносити рішення про перевагу того чи іншого варіанта реалізації гарантоздатності системи. З цією метою сформульовано атрибутивну модель гарантоздатності комп'ютерних систем (АМГ), що базується на основних властивостях (атрибутах) гарантоздатних комп'ютерних систем (ГКС) і метриках цих властивостей.



724390 R
51

Прикладна математика та комп'ютинг. ПМК 2019 [Текст] : Дванадцята наукова конф. магістрантів та аспірантів, Київ, 13-15 листопада 2019 р. : зб. тез доп. / Нац. техн. ун-т України "Київський політехн. ін-т ім. Ігоря Сікорського", Ф-т прикладної математики. - Київ : Просвіта, 2019. - 500 с. : іл., табл. - Бібліогр. наприкінці ст.

У збірнику опубліковано тези доповідей на конференції з таких напрямів: прикладна математика та прикладні рішення; прикладна математика в ІТ-технологіях; системна інженерія проектів інформатизації організаційних систем; моделювання складних систем; апаратно-програмні засоби комп'ютеризованих і комп'ютерних систем та мереж; компоненти та пристрої обчислювальної техніки і систем керування; комп'ютеризовані технологічні процеси та інформаційно-вимірювальні системи; паралельні та розподілені обчислювальні системи і мережі; технічна діагностика, тестування, надійність і

відмовостійкість у комп'ютерних технологіях; кодування та ущільнення даних; захист інформації в інформаційно-комунікаційних системах; фізико-технологічні, алгоритмічні, логічні та мовно-програмні основи проектування технічних та програмних засобів; бази даних та знань, інтелектуальний аналіз та обробка інформації; інформаційні сховища та інформаційні колектори; системний аналіз та системне програмування, технології проектування програмного забезпечення комп'ютеризованих систем; компоненти штучного інтелекту в технічних системах; мультимедійні комп'ютерні засоби; веб-технології, комп'ютерна графіка.

Розрахунок надійності програмних засобів захисту інформаційних ресурсів критичної інфраструктури / А. Б. Петренко, В. А. Телюшенко, Р. В. Зюбіна, Ю. П. Бойко // Вісник Інженерної академії України. – 2019. – № 4. – С. 92-95.

Р/1139

Відмова в роботі визначеного програмного забезпечення призводить до нанесення значних економічних втрат. Оцінювання надійності програмного захисту включає в себе вимірювання таких характеристик як завершеність і стійкість до дефектів.

Саматов К. Применение методов анализа исходного кода при оценке защищенности информационных систем / К. Саматов // Information Security/Информационная безопасность. – 2020. – № 1. – С. 39-41.

Р/365

Разработчики программных продуктов уделяют много внимания функциональности и скорости доставки приложений, как правило, в ущерб безопасности, что подтверждается различными исследованиями. При этом достаточно эксплуатации даже одной уязвимости (например, выполнение произвольного кода), чтобы привести к полному нарушению работоспособности информационной системы и ее компрометации. О том, как этого избежать, пойдет речь в данной статье.

Сеспедес Гарсия Н. В. Уязвимости компьютерных систем – угроза информационной безопасности общества / Н. В. Сеспедес Гарсия, П. Д. Сеспедес Гарсия // Математичні машини і системи. – 2019. – № 4. – С. 3-8.

Р/1052

У статті наводиться опис певних компонентів комп'ютерного обладнання, завдяки яким можна дистанційно отримати несанкціонований доступ до комп'ютерів. До таких компонентів належать Intel Management Engine (Intel ME) і Intel AMT. Також у статті наводиться опис китайських мікрочіпів, які були вбудовані в обладнання Supermicro.

Синенко М. Математична модель методів активного захисту інформації / М. Синенко, Ю. Ткач // Технічні науки та технології. – 2020. – № 2(20). – С. 109-115.

Р/1125

Постановка проблеми. Перспективним напрямом у сфері захисту інформації є розробка активних методів забезпечення захисту, серед яких можна виділити, наприклад, упереджуючий удар, контратаку, дезінформування. Побудова математичних моделей таких методів є важливим етапом на шляху вироблення концепції активного захисту.

725111 В
004

Системи обробки інформації [Текст] = Information Processing Systems : щоквартальне наукове видання / Міноборони, Харківський нац. ун-т Повітряних Сил імені Івана Кожедуба. - Харків : Видавництво ХНУПС імені Івана Кожедуба. -
Вип. 1 (160). - Харків, 2020. - 152 с. : іл., табл. - Бібліогр. наприкінці ст. - Алф. покажч.: с.151. - Текст укр., рос., англ. Дод. тит. арк. англ.

Зі змісту:

Гапон А. О., Федорченко В. М., Поляков А. О. **Підходи до побудови моделі загроз для аналізу безпеки відкритого програмного кода.** – С. 128-135.

Гарантування безпеки програмного продукту з відкритим вихідним кодом є актуальною проблемою, бо навіть у проектах з закритим вихідним кодом можуть бути присутні open source бібліотеки, що робить можливим появу вразливості у них.

725138 В
623

Сучасна спеціальна техніка [Текст] : науково-практичний журнал / Державний н.-д. ін-т МВС України. - Київ : [Видавець ФОП Горбенко Ю. В.].

№ 4 (59). - Київ, 2019. - 156 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., англ.

Зі змісту:

Дудикевич В. Б., Микитин Г. В. **Багаторівнева безпека інформаційних систем.** – С. 14-23.

У статті розроблено багаторівневу модель інформаційної безпеки (ІБ) інформаційних систем (ІС) на основі концепції "об'єкт – загроза – захист". Зовнішній рівень моделі представлено комплексом систем безпеки: керування доступом, радіочастотної ідентифікації, відеоспостереження, біометрії.

Ткаченко В. Как взломать изолированный компьютер / В. Ткаченко // Сети и бизнес : телекоммуникации и сети – технологии и рынок. – 2020. – № 4(113). – С. 72-77.

Р/1698

Пока что эти атаки – в основном страшилки, но за последние годы были обнаружены образцы вредоносного ПО, способного проникать за "воздушный зазор".

Телекомунікаційні мережі та інформаційно-комунікаційні технології

724464 В
621.39

Військовий інститут телекомунікацій та інформатизації.

Збірник наукових праць [Текст] = Collection of Scientific Papers / Міноборони України. - К. : [ВІТІ].

Вип. № 4. - К., 2019. - 148 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст укр., рос. та англ.

Зі змісту:

Кононова І. В. **Метод побудови двосторонніх оцінок показників надійності обладнання телекомунікаційних систем в умовах апріорної невизначеності вихідних даних.** – С. 74-83.

724441 R
37

Воробієнко, Петро Петрович

Електронне навчання (управлінські, педагогічні, правові, технічні, організаційні та економічні аспекти) [Текст] : монографія / Воробієнко П. П., Каптур В. А. ; Нац. акад. пед. наук України, Одеська нац. акад. зв'язку імені О. С. Попова. - Одеса : ОНАЗ ім. О. С. Попова.

Частина 1. - Одеса : ОНАЗ ім. О. С. Попова, 2020. - 84 с. : табл., рис. - Бібліогр. наприкінці розділів.

Викладені матеріали досліджень авторів про роль інформаційно-комунікаційних технологій (ІКТ) в освіті. ***Основна увага приділена захисту дітей в Інтернеті. Розглянуто дві проблеми: організаційно-педагогічні***

та технічні аспекти захисту дітей в Інтернеті і техніко-економічні аспекти впровадження ІКТ у загальноосвітніх начальних закладах.

В рамках першої проблеми проаналізовано вітчизняний досвід реалізації проектів і програм з захисту дітей в Інтернеті та сучасний стан і перспективи розвитку методів фільтрації контенту в телекомунікаційних мережах. Запропонована модель отримання контенту крізь інформаційне середовище та узагальнена модель фільтрації нецільового контенту в мережі Інтернет. Розглянуті комплексні системи фільтрації контенту в мережі Інтернет. Визначені ключові аспекти розбудови та застосування систем фільтрації контенту (СФК) у сучасних телекомунікаційних мережах. В рамках другої проблеми розроблені та досліджені архітектурні моделі систем доставки навчального контенту до учнів загальноосвітніх навчальних закладів та студентів ВНЗ, а також принципів створення інфокомунікаційних послуг для використання в навчально-виховному процесі. Визначені найбільш ефективні способи підключення загальноосвітніх навчальних закладів України до сучасних телекомунікаційних мереж. Розвинені методи тарифоутворення на надання додаткових освітніх послуг із використанням ІКТ в навчальних закладах України.

Гребенник А. Виявлення та прогнозування рівня загроз для корпоративної комп'ютерної мережі / А. Гребеннік, О. Трунова, В. Казимир, М. Міщенко // Технічні науки та технології. – 2020. – № 2(20). – С. 175-185.

Р/1125

Постановка завдання. Враховуючи потребу в практичному застосуванні аномальних методів виявлення загроз інформації, було прийнято рішення про програмну реалізацію модулів інформаційної системи, які б виконували комплекс завдань збору, аналізу, моделювання розвитку подій у мережі, та були адаптовані до її типу та потреб.

724392 R
004

Груздо, Ірина Володимирівна.
Програмування в Internet [Текст] : [навч. посібник] / І. В. Груздо, З. В. Дудар, О. С. Назаров ; Харківський нац. ун-т радіоелектроніки. - Харків : [ХНУРЕ], 2020. - 133 с. - Бібліогр.: с. 119 (2 назви).

Розглянуто актуальні перспективні підходи, методи та практичні елементи роботи з мовою програмування Python, наведено опис та приклади роботи з основними конструкціями мови, а також з ітераторами і генераторами, декораторами. Особливу увагу приділено регулярним виразам та використанню запитів до зовнішнього API і роботі з отриманими даними.

Розкрито основні переваги використання безкоштовного і вільного фреймворку для веб-застосувань у мові Python – Django, а саме: представлення і шаблони; форми і загальні представлення; тестування; статистичні файли. Досить повно розглянуто представлення і шаблони в Django, які направлені на обробку запитів і дозволяють виконувати автоматичну генерацію сторінок, що в свою чергу дає змогу за менший час розробити більш якісний додаток мовою Python. Форми і загальні представлення, що дозволяють виконувати стандартні операції Веб-застосувань, а також створити ПЗ з невеликою кількістю рядків коду на Python.

Подано інформацію щодо написання моделей в Django, які в свою чергу дають змогу при зміні вимог або сутностей в ПЗ швидше вносити зміни в структурований код програми. Розглянуто написання Views в Django, що дозволяє не розробляти часто вживаний функціонал ПЗ, а використати готові конструкції, що описані прямо в коді фреймворка.

Дослідження інформативних параметрів диграфів клавіатурного почерку для задач ідентифікації користувачів комп'ютерних мереж / Д. Ю. Горелов, О. О. Іванова, О. В. Кокорін [та ін.] // Радіотехніка. – 2020. – Вип. 201. – С. 194-200. – Текст рос.

Р/908

В першій частині проаналізовано інформативні ознаки клавіатурного почерку. В другій частині за допомогою бази даних "Keystroke Dynamics Benchmark Data Set" та програмного забезпечення Orange проведено дослідження щодо пошуку найінформативніших ознак монографів та диграфів клавіатури.

Застосування фрактальних функцій для шифрування даних в системах захисту інформації / О. В. Свинчук, О. В. Барабаш, Ю. І. Олімпієва, О. Ю. Ільїн // Телекомунікаційні та інформаційні технології. – 2020. – № 1(66). – С. 15-24.

Р/1921

Захист інформації є важливою проблемою сьогодення. Конфіденційні дані потребують захисту від сторонніх користувачів.

Для високого рівня безпеки сьогодні вже запропоновано багато різних методів шифрування тексту та зображень, але їх весь час потрібно постійно змінювати та вдосконалювати.

Фрактали, які мають цікаву хаотичну будову, можуть бути використані при побудові нових методів захисту документів. У теорії шифрування фрактальні функції використовуються як надійні датчики псевдовипадкових послідовностей, які перетворюють вхідні набори символів у числову послідовність.

Проаналізовано залежність між передачею інформації через канали зв'язку і початковими числовими наборами функції та її вплив на підвищення захисту інформації.

Зубок В. Ю. Нові метрики для ризикорієнтованого підходу до протидії атакам на глобальну маршрутизацію в Інтернеті / В. Ю. Зубок // Електронне моделювання. – 2020. – Т. 42, № 5. – С. 111-119.

Р/518

Вразливості системи глобальної маршрутизації зумовлюють великі ризики інформаційної безпеки, які потребують аналізу топології Інтернет, суб'єктів, об'єктів та процесів глобальної маршрутизації. Запропоновано нові метрики для оцінки ризику перехоплення маршрутів, базовані на топологічних характеристиках мережі.

Зубок В. Ю. Формальний опис об'єктів і процесів глобальної маршрутизації у мережі Інтернет для оцінки впливу кібератак на маршрутизацію / В. Ю. Зубок // Реєстрація, зберігання і обробка даних. – 2019. – Т. 21, № 4. – С. 67-75.

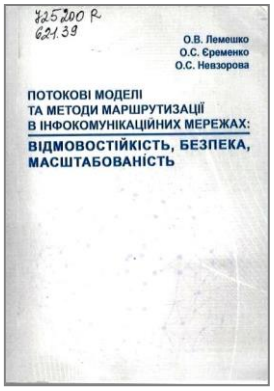
Р/1346

Одним із найважливіших етапів на шляху моделювання впливу атак на маршрутизацію є побудова формальної моделі глобальної інтернет-маршрутизації. Запропоновано формальний опис об'єктів глобальної маршрутизації і відносин між ними, а також процесу вибору маршруту.

724516 R
65

Колтун, Юрій Миколайович.
Інфокомунікаційні мережі та технології [Текст] : навч. посібник для студентів усіх форм навчання спец. 172 "Телекомунікації та радіотехніка" / Ю. М. Колтун, Ю. В. Скорик ; Харківський нац. ун-т радіоелектроніки. - Харків : [ХНУРЕ], 2020. - 200 с. : рис., табл., граф. - Бібліогр.: с. 197-199 (41 назва).

Посібник складається з шести розділів, у яких розкриваються наступні теми: концептуальні і архітектурні принципи побудови мереж наступного покоління, протоколи та технології транспортної платформи NCN, конвергентні сервісні платформи NCN, базові моделі систем керування сучасних мереж зв'язку, технології інжинірингу трафіку, забезпечення якості обслуговування в інфокомунікаціях. Ці теми за своїм змістом повністю відповідають сучасним дисциплінам підготовки магістрів за спеціальністю 172 – Телекомунікації та радіотехніка кафедри «Інформаційно-мережна інженерія» за освітньо-професійними та науковими програмами «Інформаційні мережі зв'язку», «Інформаційно-мережна інженерія», «Мобільний зв'язок».



725200 R
621.39

Лемешко, Олександр Віталійович.
Потокові моделі та методи маршрутизації в інфокомунікаційних мережах: відмовостійкість, безпека, масштабованість [Текст] : монографія / О. В. Лемешко, О. С. Єременко, О. С. Невзорова. - Харків : [ХНУРЕ], 2020. - 308 с. : граф., рис., табл. - Бібліогр. в кінці розд.

Монографія присвячена питанням, пов'язаним із синтезом математичних моделей і методів маршрутизації, які б слугували подальшою теоретичною основою перспективних протоколів маршрутизації та технологічних засобів управління трафіком для підвищення якості обслуговування, відмовостійкості та масштабованості інфокомунікаційних мереж, а також рівня їх мережевої безпеки.

724637 В
61

Львівський державний університет безпеки життєдіяльності.
Вісник Львівського державного університету безпеки життєдіяльності [Текст] : зб. наук. праць / Державна служба України з надзвичайних ситуацій. - [Львів] : [ЛДУ БЖД]. -
№ 20. - [Львів], 2019. - 134 с. : іл. - Бібліогр. наприкінці ст. - Текст кн. укр., англ., пол.

Зі змісту:

Балацька В. С., Шабатура М. М. **Дослідження комп'ютерної мережі сканером вразливості Nessus.** – С. 6-11.
... стан захищеності мережі потребує значної уваги щодо забезпечення рівня захисту мережі з метою підтримування конфіденційності та цілісності даних. Для пошуку слабких місць використовують сканери вразливості, які корисні для виявлення вад безпеки у кожній окремій системі, а також у всій мережі загалом. *Методи дослідження* – сканування мережі сканером вразливості Nessus Professional.

724859 R
004

Моделювання та інформаційні технології [Текст] : зб. наук. пр. / НАН України, Ін-т проблем моделювання в енергетиці імені Г. Є. Пухова. - Київ : [ПП "Системи,технології, інформаційні послуги"].
Вип. 88. - Київ, 2019. - 248 с. : рис., табл. - Бібліогр. наприкінці ст. - Текст укр., рос., англ.

Зі змісту:

Савельєв Д. В. **Захист веб-додатків – комплексна задача від проектування до експлуатації.** – С. 104-109.
У даній статті розглядаються етапи життєвого циклу розробки веб-додатків та веб-сервісів, наведені рекомендації при проектуванні та розробці з точки зору захищеності продукту, що допоможуть уникнути помилки як потенційні вразливості інформаційної безпеки.
Кобевко А. Т., Тимченко О. В. **Нечітке дерево рішень для мережевого захисту від DoS-атак.** – С. 203-208.
Мета статті. Побудувати нечітке дерево рішень для моніторингу мережевого потоку у випаду атак Smurf, Mail-Bomb та Ping-of-Dearth.

Навчальний стенд для вивчення дисциплін із забезпечення мережевого захисту інформації / Є. Риндич, Т. Петренко, Л. Черниш [та ін.] // Технічні науки та технології. – 2020. – № 2(20). – С. 229-236.
P/1125

Виклад основного матеріалу. У статті наведено аналіз, вимоги та півнатурна модель стенду комп'ютерної мережі для вивчення дисциплін з забезпечення мережевого захисту інформації.

Пахомова В. М. Дослідження двох підходів до виявлення мережних атак із використанням нейромережної технології / В. М. Пахомова, М. С. Коннов // Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту імені академіка В. Лазаряна. – 2020. – № 3(87). – С. 81-93.

Р/1815

Мета. У статті передбачено дослідити ефективність двох підходів до виявлення атак на комп'ютерну мережу з використанням нейромережної технології на основі нормалізованих даних відкритої бази NSL–KDD.

Методика. Як архітектурні рішення системи виявлення мережних атак запропоновано розглянути такі підходи: на основі однієї нейронної мережі, що визначає клас атаки (перший підхід), та ансамблю із п'яти нейронних мереж (другий підхід), який на першому етапі визначає категорію атаки (DoS, Probe, U2R, R2L), а на другому етапі – клас атаки, що належить до певної категорії.

Пуха М. С. Компонентна модель захисту передачі даних у системі електронного урядування / М. С. Пуха, В. А. Савченко, С. В. Панадій // Сучасний захист інформації. – 2020. – № 1. – С. 11-17.

Р/2300

Основний підхід авторів базується на збалансованому включенні різних технологій з огляду на забезпечення цілісності, конфіденційності та доступності інформації для користувачів, забезпечення контрольованості та швидкодії роботи систем на основі довіри між користувачами та службами Е-уряду. Пропонуються основні компоненти технічного та організаційного спрямування, а також підходи щодо їх поєднання.

Р/908

Радіотехніка : всеукр. міжвід. науч.-техн. зб. / Харьк. нац. ун-т радіоелектроніки. – 2020. – Вип. 200: **Інформаційна безпека**. – 229 с.

Розділи збірника:

- Перспективні методи та системи криптографічного захисту інформації
- Методи та механізми криптографічного захисту інформації в системі блокчейн
- Методи та засоби захисту в комунікаційних системах.

Салієва О. В. Визначення допустимої інтенсивності зниження рівня захищеності об'єкта критичної інфраструктури ранжуванням загроз / О. В. Салієва, Ю. Є. Яремчук // Реєстрація, зберігання і обробка даних. – 2020. – Т. 22, № 2. – С. 63-76.

Р/1346

Здійснено ранжування загроз об'єкта критичної інфраструктури на основі транзитивного замикання нечіткого відношення схожості. Ступені впливу загроз на забезпечення доступності, цілісності, конфіденційності та достовірності інформації розраховані шляхом порівняння з найменшим впливом за шкалою Сааті.

На основі визначених рангів здійснено розбиття множини загроз на класи еквівалентні за вагомістю, відповідно до яких побудовано дерево декомпозиції. Визначено λ-характеристики загроз відносно допустимої інтенсивності зниження рівня захищеності об'єкта критичної інфраструктури.

Салієва О. В. Розробка когнітивної моделі для аналізу впливу загроз на рівень захищеності комп'ютерної мережі / О. В. Салієва, Ю. Є. Яремчук // Реєстрація, зберігання і обробка даних. – 2019. – Т. 21, № 4. – С. 28-39.

Р/1346

Розроблено когнітивну модель, яка відображає рівень захищеності комп'ютерної мережі при впливі на неї потенційних загроз. Сформовано матрицю взаємовпливів концептів нечіткої когнітивної карти та розраховано основні системні показники, такі як: консонанс, дисонанс і вплив концептів на систему.

725107 В
621.39

"Український науково-дослідний інститут зв'язку", державне підприємство.
Наукові записки Українського науково-дослідного інституту зв'язку [Текст] : науковий журнал / Державний університет телекомунікацій. - Київ : Держ. ун-т телекомунікацій .
№ 1(57). - Київ, 2020. - 46 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., рос., англ.

Зі змісту:

Черноштан А. М., Власов О. М. **Методика забезпечення захисту корпоративної мережі зв'язку при віддаленому управлінні.** – С. 10-14.
Показано принципи підвищення безпеки корпоративних мереж з урахуванням розробленої методики. Виконано огляд сучасних технологій захисту корпоративних мереж та методів впливу зловмисників на них.

Фролов В. В. Аналіз підходів до забезпечення безпеки хмарних сервісів / В. В. Фролов // Радіоелектронні і комп'ютерні системи. – 2020. – № 1. – С. 70-82. – Текст рос.

Р/1769

Стаття присвячена аналізу сучасних підходів, що забезпечують безпеку хмарних сервісів. Оскільки хмарні обчислення є однією з найбільш швидко зростаючих областей серед інформаційних технологій, вкрай важливо гарантувати безпеку і надійність процесів, які відбуваються у хмарах і убезпечити взаємодію між клієнтом і постачальником хмарних сервісів. *Об'єктом дослідження і аналізу* даної роботи є хмарні сервіси, які надаються різними провайдерами хмарних сервісів. *Метою дослідження* даної роботи є порівняння існуючих підходів, що забезпечують інформаційну безпеку хмарних сервісів, а також пропозиція нового підходу, заснованого на принципі диверсності.

724764 В
004

Internet-Education-Science, International Scientific-Practical Conference (2020 ; Vinnytsia).
Proceedings of the XII International Scientific-Practical Conference "Internet-Education-Science". IES-2020, 26-29 May, 2020, Vinnytsia, Ukraine [Текст] : [збірник праць] / Vinnytsia National Technical University, Baku State University, Georgian Technical University [et al.]. - Vinnytsia : VNTU, 2020. - 280 с. - Текст укр., рос., англ.

Доповіді у збірнику згруповані по секціях, відповідно до основних напрямків конференції:
A. Інтелектуальні інформаційні технології
B. Комп'ютерні мережеві технології
C. Комп'ютерна інженерія
D. Математичне моделювання
E. Комп'терні технології та Інтернет в інформаційному суспільстві
F. Інформаційні технології та Інтернет у навчальному процесі та наукових дослідженнях.

Інформаційне протиборство у воєнних конфліктах. Інформаційно-психологічна безпека

726018 В
35

Актуальні проблеми державного управління [Текст] = Pressing problems of public administration : зб. наук. пр. / Нац. акад. держ. упр. при Президентові України, Харківський регіон. ін-т держ. упр. - Харків : [Магістр], 2008 - .
Вип. 1 (57). - Харків, 2020. - 328 с. : граф., табл. - Бібліогр. наприкінці ст. - Текст кн. укр. та англ.

Зі змісту:

Панченко О. А., Антонов В. Г. **Концептуалізація поняття "інформаційне насильство" в контексті національної безпеки.** – С. 65-73.

Розглянуто поняття інформаційного насильства, його місце і роль у системі соціального насильства та заходи щодо забезпечення національної безпеки в цьому контексті. Запропоновано модель, що відображає аксіологічний підхід до забезпечення національної безпеки при об'єктивізації небезпеки у вигляді насильства, яка враховує наступні конструкти: превенція; збереження, захищеність, нарощування національних цінностей; усунення збитку, завданого насильством; пост-превенційні організаційно-правові заходи для мінімізації можливого збитку, завданого насильством.

Інформаційно-психологічне протиборство в Україні / М. М. Браіловський, І. С. Іванченко, І. Р. Опірський, В. О. Хорошко // Безпека інформації. – 2019. – Т. 25, № 3. – С. 144-149.

Р/1408

Описано 4 підходи до визначення інформаційної війни, які вміщують політико-правові, соціально-економічні, психологічні дії, що передбачають захоплення інформаційного простору ворога, знищення його комунікацій, позбавлення засобів передачі повідомлень тощо, а також концептуальні питання та основи теорії мережево-центричної системи управління й організації бойових дій та кібердій або кібернетичної війни. Досліджено впровадження стратегії кібернетичного підходу до організації дій під час проведення військових операцій для отримання максимального ефекту від впливу на три сфери – моральну, ментальну, фізичну. Також було досліджено вплив на найбільш уразливі об'єкти із використанням системного кібернетичного підходу.

723826 R
31

Парфенюк, Ігор Миколайович.
Інформаційно-психологічні війни [Текст] : навч. посібник / Ігор Парфенюк ; МОНмолодьспорт, Київський нац. ун-т культури і мистецтв, НДІ. - Київ : [КНУКіМ], 2020. - 188 с. - Бібліогр. наприкінці тем.

Інформаційно-психологічні війни на сьогодні ведуться різними суб'єктами впливу, незалежно від сфери і масштабів. У посібнику увага концентрується на сутності інформаційної війни, а саме її інформаційно-психологічному різновиді, а також основних інструментах інформаційно-психологічного впливу на прикладі в переважній більшості міждержавних комунікацій.

Назва посібника " Інформаційно-психологічні війни" зумовлена розглядом інформаційних війн в рамках впливу на індивідуальну та суспільну свідомість, з навмисним уникненням розгляду аспектів інформаційно-технічних війн. Саме тому посібник призначений для студентів і фахівців гуманітарного профілю (соціальні комунікації, журналістика, політологія, історія, філософія тощо).

Стародуб С. А. Комунікаційний процес як елемент інформаційної війни та впливу на маси / С. А. Стародуб // Держава та регіони. Серія: Соціальні комунікації. – 2019. – № 2. – С. 17-20.

Р/1520

Кожний комунікаційний елемент відіграє свою роль у впливі на маси. До таких комунікаційних елементів на сучасному етапі можна зарахувати соціальні медіа, є чинником, який впливає на доленосне прийняття рішення щодо існування певних політико-державницьких складових, елементів управління та виведення інформаційно-комунікаційних процесів на новий суспільний етап.

725137 В
623

Сучасна спеціальна техніка [Текст] : науково-практичний журнал / Державний н.-д. ін-т МВС України. - Київ : [Видавець ФОП Горбенко Ю. В.].

№ 3 (58). - Київ, 2019. - 136 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., англ.

Зі змісту:

Хорошко В. О., Іванченко І. С. **Інформаційне протиборство в геополітичному просторі.** – С. 26-36.

Установлено умови та зміст геополітичної конкуренції в інформаційному суспільстві і сформульовані загрози інформаційно-психологічного протиборства в геополітичному просторі.

Тарасенко Я. В. Забезпечення надійності функціонування комп'ютерних лінгвістичних стегосистем в умовах протидії інформаційній пропаганді / Я. В. Тарасенко // Безпека інформації. – 2019. – Т. 25, № 3. – С. 174-181.

Р/1408

В статті проводиться огляд існуючих методів підвищення надійності функціонування комп'ютерних лінгвістичних стегосистем. оскільки, в ході дослідження виявлено, що перспективним напрямком, особливо в умовах протидії інформаційній пропаганді є квантова стеганографія, тому розглядаються саме ці підходи для вирішення поставленої задачі.

724797 В
001

Knowledge,**Education**, **Law**, **Management** [Текст] : nauka, Oswiata, Prawo, Zarzadzanie / Instytut Spraw Administracji Publicznei. - Lublin : [Instytut Spraw Administracji Publicznei w Lublinie], 2019 - . - Загол. обкл. : KELM.
№ 2(26) czerwiec. - Lublin, 2019. - 302 с. - Бібліогр. в кінці ст. - Текст кн. укр., англ., пол. мов.

Зі змісту:

Балинська О., Благута Р., Живко З. **Інформація як засіб ведення сучасних гібридних воєн**. – С. 3-22. – Текст англ., укр.
Негативний інформаційний вплив, зорієнтований на підрив бойового духу армії та патріотичних настроїв населення, може завдати набагато більше шкоди державі, ніж чисельно і технічно сильніша армія супротивника.
Основним ілюстративним матеріалом у статті є гібридна війна Росії проти України.

Кібербезпека – проблема XXI століття

Барченко Н. Л. Методи теорії прийняття рішень в кібербезпеці / Н. Л. Барченко, В. К. Ободяк, В. Р. Татарінов // Вісник Інженерної академії України. – 2019. – № 4. – С. 116-118.

Р/1139

Розглянуто можливість застосування методів теорії прийняття рішень, а саме, методу аналізу ієрархії для вирішення завдання вибору програмного забезпечення для управління інформаційною безпекою.

726024 В
355

Військовий інститут Київського національного університету імені Тараса Шевченка.
Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка [Текст] : збірник наукових праць. - Київ : [ВІКНУ].
Вип. № 66. - Київ, 2020. - 138 с. : іл. - Бібліогр. наприкінці ст. - Текст кн. укр., рос., англ.

Зі змісту:

Барабаш О. В., Галахов Є. М. **Дослідження функції інтенсивності кібератак за допомогою степеневого *p*-перетворення аналітичної функції.** – С. 54-65.
Представлено відомі методології аналізу інтенсивності кібератак на підприємство. Представлено математичне моделювання часових рядів інтенсивності кібератак на підприємство для надання комплексних рішень і прогнозів посилення стійкості підприємства проти поточних цільових кіберзагроз.
Даник Ю. Г., Вдовенко С. Г. **Проблеми та перспективи забезпечення кібероборони держави.** – С. 75-89.
У статті здійснено аналіз загальних принципів побудови систем кібербезпеки і кібероборони провідних країн світу в контексті можливості та доцільності впровадження їх досвіду в Україні; аналіз передумов, існуючого стану та проблемних питань формування систем кібербезпеки та кібероборони в Україні.

725101 В
621.39

Військовий інститут телекомунікацій та інформатизації.
Збірник наукових праць [Текст] = Collection of Scientific Papers / Міноборони України. - К. : [ВІТІ].
Вип. № 1. - Київ, 2020. - 122 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст укр., рос. та англ.

Зі змісту:

Паламарчук С. А., Шемендюк О. В., Ляшенко Г. Т., Ткач В. О. **Забезпечення захисту кіберпростору в провідних країнах світу.** – С. 58-64.
В статті проаналізовано стан забезпечення захисту кіберпростору (Франція, Японія, Південна Корея та Велика Британія, США, РФ); заходи для забезпечення захисту кіберпростору (організаційні, технічні); підходи щодо створення Кібернетичних військ.

726001 В
621.39

Військовий інститут телекомунікацій та інформатизації.
Збірник наукових праць [Текст] = Collection of Scientific Papers / Міноборони України. - К. : [ВІТІ].
Вип. № 2. - Київ, 2020. - 132 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст укр., рос. та англ.

Зі змісту:

Мартинюк В. В., Паламарчук Н. А., Паламарчук С. А., Сівоха О. М. **Задачі вдосконалення інформаційної та кібернетичної безпеки об'єктів критичної інфраструктури.** – С. 54-63.
У статті розглянуто становлення сфери забезпечення кібербезпеки в Україні та її імплементація зі сферами захисту інформації та інформаційної безпеки.
Чевардін В. Є., Мазулевський О. Є. **Аналіз структур кіберкомандувань розвинутих країн.** – С. 121-128.
У статті проведено аналіз структур військових органів управління систем захисту кіберпростору – "кіберкомандування" таких країн, як Сполучені Штати Америки, Федеративної Республіки Німеччини, Французької Республіки, Об'єднаного Королівства, Російської Федерації.

Горлинський В. Кібербезпека як складова інформаційної безпеки України / В. Горлинський, Б. Горлинський // Information Technology and Security. – July-December 2019. – Vol. 7, Iss. 2(13). – P. 136-148.

Р/1212

Сформульовано визначення інформаційної безпеки в широкому сенсі поняття, як сфери національної безпеки. Запропоновано підхід, згідно з яким, важливо, по-перше, відокремлювати змістовну сторону понять інформаційної та кібербезпеки як у широкому, так і вузькому сенсі слова, по-друге, згідно із сферою охоплення інформаційного і кіберпросторів, розрізняти їх функціональний зміст у державному, національному і глобальному вимірах.

Грищук О. М. Верифікація узагальненої диференційно-ігрової моделі шаблону потенційно небезпечної кібератаки / О. М. Грищук, Р. В. Грищук, В. В. Охрімчук // Телекомунікаційні та інформаційні технології. – 2020. – № 1(66). – С. 53-67.

Р/1921

В статті запропоновано один з підходів до верифікації узагальненої диференційно-ігрової моделі шаблону потенційно небезпечної кібератаки. У результаті всебічного дослідження: обґрунтовано її адекватність; збіжність з відомими результатами; встановлено переваги, порівняно із найближчими аналогами, які використовуються в системах інформаційної безпеки інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави.

Даник Ю. Г. Від кібербезпеки до кібероборони / Ю. Г. Даник, С. Г. Вдовенко // Оборонний вісник. – 2020. – № 11. – С. 10-15.

Р/1134

Сучасні високі технології змінюють процеси організації бойових дій та операцій і методи управління ними, і тому вимагають розробки та впровадження нових концепцій та стратегій оборони.

Даник Ю. Підхід до автоматизованого виявлення деструктивних кібервпливів / Ю. Даник, К. Соколов, О. Гудима // Information Technology and Security. – July-December 2019. – Vol. 7, Iss. 2(13). – P. 149-160.

Р/1212

В 2019 році підтверджено світову тенденцію щодо зростання кількості користувачів сервісів соціальних інформаційних мереж. Тому на теперішній час зростає важливість забезпечення виконання завдань інформаційної та кібернетичної безпеки в електронних засобах масової інформації та аналізування кіберпростору.

Демулен Н. Комплексный подход к безопасности IoT сетей / Н. Демулен // CHIP NEWS Украина. Инженерная микроэлектроника. – 2020. – № 2. – С. 19-20.

Р/900

В статье кратко описаны проблемы создания безопасного защищенного соединениия в сети IoT. Приведены некоторые методы решения проблемы. Представлен упрощенный механизм создания безопасного облачного соединения, разработанный Google Cloud совместно с компанией Microchip.

Душкевич В. ИБ с ограниченным бюджетом: как защититься от атак при помощи штатных средств ОС / В. Душкевич // Information Security/Информационная безопасность. – 2020. – № 1. – С. 20-21.

Р/365

Почти во всех ОС имеются инструменты, которые можно использовать для защиты от киберугроз. Решить проблему можно за счет грамотного построения ИТ-инфраструктуры предприятия, что позволит снизить последствия от действий злоумышленников. Так как же организациям, которые располагают лишь ограниченным бюджетом, справиться с информационными угрозами?

Иванов П. А. Разработка подхода к мониторингу безопасности IoT-устройств на базе MQTT-брокера / П. А. Иванов, И. В. Капгер // Вопросы защиты информации. – 2020. – № 1(128). – С. 30-32.

Р/0171

Для рассмотрения данной темы изучена зарубежная практика в области Интернета вещей. Предложен способ мониторинга с использованием шаблона передачи данных "издатель–подписчик", получением и обработкой данных мониторинга во времени, близком к реальному, и безагентной реализацией подключения устройств. Рассмотрены варианты реализации способа и преимущества использования IoT-ориентированного протокола передачи данных.

723769 В
004

Ілляшенко, О. О.
Методи і засоби забезпечення виконання вимог до кібербезпеки систем на програмовній логіці [Текст] : монографія / О. О. Ілляшенко ; ред. В. С. Харченко ; Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ». - Харків : Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ», 2019. - 195 с.

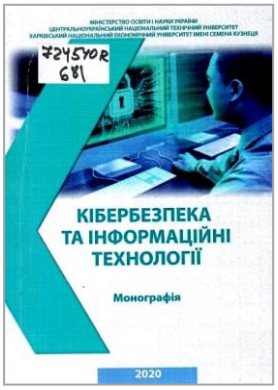
Монографія базується на результатах дисертаційного дослідження на здобуття наукового ступеня кандидата технічних наук (PhD) у галузі кібербезпеки індустріальних систем на програмовній логіці (спеціальність 05.13.05 - Комп'ютерні системи та компоненти). Виконана в Національному аерокосмічному університеті ім. М. Є. Жуковського «Харківський авіаційний інститут», кафедра комп'ютерних систем, мереж і кібербезпеки. Монографія присвячена розробленню методів та засобів забезпечення виконання вимог до кібербезпеки систем на програмовній логіці. Запропоновані методи та засоби дозволяють підвищити достовірність оцінювання та забезпечення виконання вимог до кібербезпеки систем на програмовній логіці. Результати впроваджені у міжнародних проектах за програмами Tempus: «Модернізація навчальних курсів з інформаційної безпеки та сталості для промисловості «SEREIN»,

«Національна мережа центрів інноваційної університетсько-індустріальної кооперації з інженерії безпеки «SAFEGUARD» та FP7 - «Інтеграція Національного аерокосмічного університету «XAI» в Європейський Науковий Простір «KhAI-ERA». Для студентів, аспірантів та викладачів університетів, інженерів та дослідників у сфері кібербезпеки індустріальних систем на програмовній логіці. Бібл. - 214 найменувань, рисунків - 37, таблиць - 9. Монографія рекомендована до видання Вченою радою Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут» (протокол № 4 від 20 листопада 2019 року).

Качинський А. Б. Інформаційний і кібернетичний простори як джерело сучасних загроз / А. Б. Качинський, І. В. Стьопочкіна // Математичне моделювання в економіці. – 2019. – № 3. – С. 5-17.

Р/1577

Виділено найбільш небезпечні тенденції розвитку сучасних загроз, проаналізовано історію вживання термінів "інформаційний простір", "кібернетичний простір" науковим суспільством на основі онлайнових баз публікацій із використанням математичного апарату, зокрема вперше обчислено статистичні характеристики, які дозволяють зробити висновки про взаємозалежність категорій при існуванні водночас суттєвих відмінностей.



724540 R
681

Кібербезпека та інформаційні технології [Текст] : монографія / [авт. кол. : Абдалла А., Альошин Г. В., Вдовиченко І. Н. та ін.] ; Центральноукр. нац. техн. ун-т, Харківський нац. екон. ун-т імені С. Кузнеця. - [Харків] : [ТОВ "ДІСА ПЛЮС"], 2020. - 380 с. : рис., табл., граф. - Бібліогр. наприкінці ст. - Текст кн. укр., англ., рос.

В монографії розглянуті сучасний стан та перспективи розвитку механізмів складових безпеки: кібербезпеки, інформаційної безпеки, безпеки інформації та інформаційних технологій. Монографія представляє інтерес як для фахівців, сфера діяльності яких безпосередньо пов'язана з розробкою механізмів складових безпеки та ІТ-технологій, способів забезпечення послуг безпеки та передачі даних в комунікаційних системах, так і для спеціалістів з безпеки інформації.

Клиен А. Обнаружение кибервторжений на цифровой подстанции / А. Клиен // Промислова електроенергетика та електротехніка. – 2020. – № 1. – С. 42-47.

Р/1056

Многоуровневая защита необходима для обеспечения кибербезопасности подстанций. Криптография позволяет проверить подлинность устройств, но не все атаки могут быть предотвращены этими мерами. Брандмауэры и "воздушные зазоры" возможно обойти через существующие туннели удаленного доступа или через обслуживающие компьютеры, напрямую связанные с IED или станционной шиной. Поэтому необходимо принять меры в целях выявления угроз на подстанции для обеспечения быстрого реагирования и минимизации последствий. В этой статье будут описаны требования безопасности подстанций МЭК 61850 и различные подходы для обнаружения угроз в этих сетях. Также будет описан подход, разработанный для подстанции МЭК 61850 и технологической шины.

Коваленко О. В. Розбудова системи кібербезпеки Іспанії: уроки для України / О. В. Коваленко // Інвестиції: практика та досвід. – 2020. – № 17-18. – С. 149-153.

Р/2124

Метою статті є узагальнення та систематизація досвіду Республіки Іспанії у сфері забезпечення кібербезпеки та оцінка можливості його використання у вітчизняній державно-управлінській практиці.

Комаров М. Ю. Вимоги до таксономії кіберзагроз об'єктів критичної інфраструктури та аналіз існуючих підходів / М. Ю. Комаров // Електронне моделювання. – 2020. – Т. 42, № 3. – С. 111-124.

Р/518

Наведено вимоги до таксономії кіберзагроз. Проведено аналіз існуючих робіт за даною тематикою. Досліджено та наведено опис можливих підходів до розробки таксономії кіберзагроз. Надано визначення ключових понять. Проведено класифікацію технік вторгнень та типів атак на інформаційні системи. Наведено графічні подання вторгнення та інциденту.

726003 В
628

Комунальне господарство міст [Текст] = Коммунальное хозяйство городов : наук.-техн. зб. / Харк. нац. ун-т міського госп-ва імені О. М. Бекетова = Municipal economy of cities. - Харків : ХНУМГ. - (Серія: Технічні науки та архітектура). -
Вип. 3(156). - Харків, 2020. - 226 с. : граф., рис., табл. - Алф. покажч.: с. 226. - Бібліогр. наприкінці ст. - Текст кн. укр., англ.

Зі змісту:

Василенко М. Д., Козін О. Б., Козіна М. О., Рачук В. О. **Кібер-ризики в муніципальному господарстві в період пандемії: збитки та боротьба за кібербезпеку**. – С. 80-87.
Представлені результати вивчення нових кібер-ризиків муніципального господарства, що виникли у період пандемії, формулюється власний погляд щодо їх класифікації та методів протидії з боку муніципальних організацій та підприємств.

Кононович В. Г. Критерії ідентифікації плагіату в науковій літературі з кібербезпеки / В. Г. Кононович, М. Г. Романюк // Безпека інформації. – 2019. – Т. 25, № 3. – С. 167-173.

Р/1408

На відміну від захисту товарних знаків, поки не вироблено правил, процедур та методик виявлення плагіату у науковій та освітній сфері. Виходячи з цього, на базі історичного аналізу трансформації основних підходів до захисту авторських прав і виявлення плагіату, запропоновано й обґрунтовано адаптивний підхід до побудови системи критеріїв ідентифікації плагіату, заснований не на формальному збігу текстів, а на збігу семантики.

Лагута В. В. Підвищення якості кібернетичної безпеки в інформаційно-телекомунікаційній системі підприємства / В. В. Лагута // Сучасний захист інформації. – 2020. – № 1. – С. 37-41.

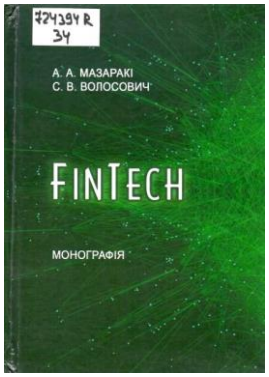
Р/2300

Проаналізовано принцип організації системи безпеки з використанням моделі OSI та рекомендації стандарту кібербезпеки ISO 27000. Показано переваги побудови системи безпеки з використанням доменного підходу. Розроблені рекомендації для побудови захищеної комп'ютерної мережі.

Лисенко С. М. Моделі кібератак мережного та хостового типу / С. М. Лисенко // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2019. – № 2. – С. 65-72.

Р/1051

В роботі представлено моделі кібератак мережного та хостового типу, які на відміну від відомих, враховують не тільки особливості їх поведінки, але й архітектурні особливості, що дозволить створити базу поведінок атак мережного та хостового типу для їх використання в процесі виявлення атак.



724394 R
34

Мазаракі, Анатолій Антонович.
FinTech [Текст] : монографія / А. А. Мазаракі, С. В. Волосович ; Київський нац. торговельно-економічний ун-т. - Київ : [Київ. нац. торг.-екон. ун-т], 2019. - 308 с. : рис., табл. - Бібліогр.: с. 217-260 (362 назви).

У монографії розкрито зміст фінансових технологій, їх значення для суспільних трансформацій. *Визначено роль фінансових технологій у забезпеченні зростання фінансової інклюзивності, а також детермінанти виникнення та реалізації кіберризиків.*

Досліджено природу криптовалюти та сформульовано пропозиції щодо державного регулювання криптовалютних операцій. Здійснено аналіз застосування інструментів фінансових технологій на ринках платіжних, страхових, інвестиційних, банківських послуг та у сфері державних фінансів.

Метод резервування та відновлення втрачених даних в глобальних мережах / К. В. Коляда, А. П. Марковський, А. П. Саверченко, А. И. Торашанко // Телекомунікаційні та інформаційні технології. – 2020. – № 1(66). – С. 4-14.

Р/1921

Запропоновано метод формування резервних пакетів при передачі даних в глобальних мережах, а також технологія їх використання для відновлення втрачених чи пошкоджених пакетів. Розглянутий метод гарантованого відновлення не більше трьох втрачених чи пошкоджених пакетів.

Наведено математичне і технічне обгрунтування запропонованого метода. Кожен з надлишкових резервних пакетів пропонується формувати у вигляді логічної суми певних підмножин інформаційних пакетів.

Для прискорення відновлення втрачених пакетів метод передбачає використання спеціальних таблиць передобчислень. Детально викладена технологія формування таких таблиць, які містять специфікації відновлення втрачених пакетів для різних варіантів втрат пакетів (інформаційних чи резервних). Кожен втрачений пакет відновлюється у вигляді логічної суми визначених специфікацією множин невтрачених інформаційних чи резервних пакетів. Розроблений спосіб формування специфікацій забезпечує низьку обчислювальну складність процесу відновлення пакетів.

Митрушкин Е. И. Безопасность распределенной автоматизированной системы / Е. И. Митрушкин, В. Р. Шавыкин // Вопросы защиты информации. – 2020. – № 1(128). – С. 42-48.

Р/0171

Предложена организация безопасности распределенной автоматизированной системы и ее составных частей.

Міщенко А. В. Нечітка модель оцінки ризиків інформаційної безпеки та підтримки рівня захищеності ERP-систем / А. В. Міщенко, О. В. Курило, О. А. Золотухіна // Телекомунікаційні та інформаційні технології. – 2020. – № 1(66). – С. 142-151.

Р/1921

Робота присвячена питанню використання нечіткої моделі для оцінки ризиків інформаційної безпеки та підтримки рівня захищеності ERP-систем.

Розглянуто вимоги до інформаційної безпеки ERP-систем та проаналізовано проблеми їх безпеки та вразливості.

Визначено основні фактори, що впливають на оцінку ризиків. Зважаючи на якісний, неточний та значною мірою не визначений, або неповний характер інформації про більшість факторів, запропоновано використання лінгвістичного підходу для їх опису. Такий підхід забезпечує можливість отримання кількісного опису елементів моделі за умов наявності лише нечіткої інформації про значення факторів ризику інформаційної безпеки і дозволяє спростити подальший процес ранжування факторів ризиків та чисельного розрахунку значень їх наслідків.

Модель трансформації національної системи кібербезпеки в умовах дії гібридних загроз / Р. М. Боярчук, В. А. Савченко, О. Й. Мацько, І. В. Новікова // Сучасний захист інформації. – 2020. – № 1. – С. 6-10.

Р/2300

У статті розглядається підхід щодо формування робочого плану трансформації національної системи кібербезпеки України. Основна ідея наведеної методології базується на використанні комбінованої моделі оцінки ризику та досвіду попередніх трансформацій з урахуванням існуючих процесів управління в окремих організаціях.

724695 R
004

Моделювання та інформаційні технології [Текст] : зб. наук. пр. / НАН України, Ін-т проблем моделювання в енергетиці імені Г. Є. Пухова. - Київ : [ПП "Системи, технології, інформаційні послуги"].
Вип. 89. - Київ, 2019. - 239 с. : рис., табл. - Бібліогр. наприкінці ст. - Текст укр., рос., англ.

Зі змісту:

Савельєв Д. В. **Методи оцінки ризиків кібербезпеки об'єктів критичної інформаційної інфраструктури.** – С. 136-149.
У даній статті розглядаються поняття ризику кібербезпеки, основні етапи оцінки ризику та методи, що можуть бути використані при оцінці ризиків кібербезпеки об'єктів критичної інформаційної інфраструктури.

Нестеренко А. В. Графовая модель кибербезопасности информационных ресурсов / А. В. Нестеренко, И. Е. Нетесин // Проблемы управления и информатика. – 2020. – № 4. – С. 91-108.

Р/677

Цель данной статьи – изучение и исследование существующих подходов в процессе решения экспертами практических задач по обеспечению кибербезопасности, а также описание модели безопасности систем ведения информационных ресурсов на основе онтологий и графового представления.

Оцінка стану кібербезпеки критичної інформаційної інфраструктури в ході виявлення та відслідковування кризових індикаторів / І. В. Ткаченко, В. А. Козачок, С. О. Гахов, В. Є. Дмітрієв // Сучасний захист інформації. – 2020. – № 1. – С. 54-57.

Р/2300

В статті розглянуто питання щодо стану кібербезпеки об'єктів критичної інформаційної інфраструктури з урахуванням індикаторів кіберзагроз будь якого масштабу та пошук кореляції між: даними аудиту стану захищеності об'єктів критичної інфраструктури, даних щодо оцінки ризиків та моделей кіберзагроз, данні про індикатори, що передують відомим кіберзагрозам.

724619 В
339

Підприємництво і торгівля [Текст] : збірник наукових праць / [редкол.: Куцик П. О., Апопій В. В., Семак Б. Б. та ін. ; Львівський торговельно-економічний ун-т]. - Львів : Вид-во Львівського торг.-екон. ун-ту. -
Вип. 25. - Львів, 2019. - 130 с. : рис., табл. - Бібліогр. наприкінці ст. - Текст укр., англ.

Зі змісту:

Дячков Д. В. **Формування моделі політики інформаційної безпеки на основі концепцій "глибинного захисту".** – С. 116-121.
Метою статті є аналіз існуючих моделей формування політики інформаційної безпеки та розробка моделі політики інформаційної безпеки на основі поєднання концепції "глибинного захисту" та "mind map".

Резильєнтність комп'ютерних систем в умовах кіберзагроз: таксономія та онтологія / С. М. Лисенко, В. С. Харченко, К. Ю. Бобровнікова, Р. В. Щука // Радіоелектронні і комп'ютерні системи. – 2020. – № 1. – С. 17-28.

Р/1769

... розроблено узагальнену таксономічну схему резильєнтності, пов'язану з інформаційною безпекою. В роботі подано операційний цикл резильєнтної КС як множину інформаційно-технічних станів, які проходить система (підготовка, захист системи, виявлення загроз, поглинання загроз, відповідь на загрозу, відновлення системи після здійснення кібератаки, адаптація). Розроблено схему онтології резильєнтності з точки зору інформаційної безпеки комп'ютерних систем в умовах кіберзагроз.

Ризики інсайдерських загроз в системах захисту інформації підприємств / В. В. Корчинський, Аль-Файюми Халед, Ю. В. Копитін, М. В. Копитіна // Наукові праці ОНАЗ ім. О.С. Попова. – 2019. – № 2. – С. 112-116.

Р/1485

За даними різних досліджень загрози інформаційній безпеці з боку інсайдерів становлять до 80%, тобто можуть породжуватися всередині самої організації. *Метою дослідження* є аналіз та мінімізація ризиків інсайдерських загроз в системах захисту інформації підприємства. У статті розглянуто ризики інсайдерсьвих загроз та наведена класифікація дій працівників підприємства, що приводить до інсайдерства.

Салієва О. Визначення рівня захищеності системи захисту інформації на основі когнітивного моделювання / О. Салієва, Ю. Яремчук // Безпека інформації. – 2020. – Т. 26, № 1. – С. 42-49.

Р/1408

У даній статті було розглянуто підходи до вирішення проблеми оцінювання рівня захищеності системи захисту інформації в умовах реалізації загроз. Запропоновано когнітивну модель на основі нечіткої когнітивної карти, яка дозволяє визначити рівень захищеності системи захисту інформації.

Салієва О. Ранжування загроз для визначення витрат на забезпечення захищеності системи захисту інформації на основі теорії нечітких відношень / О. Салієва, Ю. Яремчук // Захист інформації. – 2020. – Т. 22, № 1. – С. 51-59.

Р/1428

Для побудови та ефективного функціонування системи захисту інформації необхідним є проведення аналізу можливих загроз щодо рівня їхнього впливу на досліджувану систему та визначення допустимих витрат на забезпечення її захищеності. У переважній більшості дане питання вирішується за допомогою методів статистичного аналізу, які потребують розгляду значного обсягу інформації, складних розрахунків та займають тривалий час для опрацювання. Тому у роботі пропонується ранжування загроз системі захисту інформації з використанням теорії нечітких відношень.

725771 R
37

Самойленко, Олексій Олександрович.
Підготовка бакалаврів з кібербезпеки в умовах освітньо-цифрового середовища [Текст] : монографія / Самойленко О. О. - Київ : [МАУП], 2020. - 436 с. - Бібліогр.: с. 361-404.

У монографії розглядаються теоретичні, методичні та організаційно-технічні основи підготовки бакалаврів з кібербезпеки в умовах освітньо-цифрового середовища. Уточнено понятійний апарат проблеми дослідження та розкрито особливості освітньо-наукової підготовки бакалаврів з кібербезпеки в умовах розбудови інформаційного суспільства, окреслено методологічні підходи до розвитку професійної компетентності бакалаврів з кібербезпеки в умовах освітньо-цифрового середовища. Визначено особливості, становлення і розвиток та засоби реалізації масових відкритих дистанційних курсів у закладах вищої освіти. Розроблено експериментальну модель підготовки бакалаврів з кібербезпеки в умовах освітньо-цифрового середовища, критерії, показники та рівні готовності бакалаврів з кібербезпеки до професійної діяльності в умовах зазначеного середовища, а також педагогічні умови формування готовності бакалаврів з кібербезпеки до професійної діяльності. Запропонована технологія підготовки бакалаврів з кібербезпеки в умовах освітньо-цифрового середовища.

Селіверстова Л. С. Підходи до розвитку кіберстрахування як сегменту глобального страхового ринку / Л. С. Селіверстова, Д. А. Трухан // Економіка та держава. – 2020. – № 1. – С. 23-26.

Р/1829

В Україні кіберстрахування перебуває на початковому етапі становлення та потребує розробки підходів до подальшого розвитку, враховуючи накопичений позитивний досвід зарубіжних країн у цьому напрямі. З

розвитком кіберзагроз та кібератак страхування стає вагомим інструментом ризик-менеджменту для підприємств як державної, так і недержавної форми власності. Це перспективний напрям розвитку страхового бізнесу, оскільки створення страхових програм захисту, крім безпосереднього відшкодування збитків, значною мірою охороняє від таких ризиків та не дозволяє припинити або знищити бізнес.

724788 В
004

Системи обробки інформації [Текст] = Information Processing Systems: щоквартальне наукове видання / Міноборони, Харківський нац. ун-т Повітряних Сил імені Івана Кожедуба. - Харків : Видавництво ХНУПС імені Івана Кожедуба. -
Вип. 2 (161). - Харків, 2020. - 122 с. : іл., табл. - Бібліогр. наприкінці ст. - Алф. покажч.: с. 122. - Текст укр., рос., англ. Дод. тит. арк. англ.

Зі змісту:

Дудикевич В. Б., Микитин Г. В., Галунець М. О. **Системна модель інформаційної безпеки "розумного міста".** – С. 93-98.
У контексті розгортання Концепції 4.0 в Україні запропоновано системну модель інформаційної безпеки "розумного міста" на рівні: його сегментів; складових – "розумних об'єктів" та багаторівневих кіберфізичних систем (КФС) "фізичний простір (ФП) – комунікаційне середовище (КС) – кібернетичний простір (КП)"; загроз рівням КФС, компонентам рівня та процесам, що відповідають рівню: відбиранню інформації, передаванню/прийманню, обробленню, управлінню; технологій забезпечення безпеки структури та функціоналу сегменту "розумного міста" за профілями – конфіденційність, цілісність, доступність.

Соколов К. О. Підхід до розробки елементів структури системи виявлення деструктивного впливу у кіберпросторі / К. О. Соколов, О. П. Гудима // Наукоємні технології. – 2019. – № 4(44). – С. 426-432.

Р/2289

... метою статті є висвітлення підходу щодо побудови елементів структури системи виявлення деструктивного впливу (деструктивних кібердій) у кіберпросторі в межах створення в Міністерстві оборони України та Збройних Силах України відповідної Системи (організаційної структури) та буде зосереджена увага на її елементі, що здійснює заходи з виявлення та оцінювання деструктивного впливу.

Субач І. Архітектура та функціональна модель перспективної проактивної інтелектуальної SIEM-системи для кіберзахисту об'єктів критичної інфраструктури / І. Субач, А. Микитюк, В. Кубрак // Information Technology and Security. – July-December 2019. – Vol. 7, Iss. 2(13). – P. 208-215.

Р/1212

Запропонована нова архітектура перспективної проактивної інтелектуальної SIEM-системи, яка, додатково до традиційних рівнів – збору, управління та аналізу даних, включає четвертий рівень – рівень прийняття та реалізації рішень. Реалізація на практиці моделі дозволяє мінімізувати участь людини під час вирішення задачі реагування на кіберінциденти, тим самим підвищуючи оперативність та обґрунтованість рішень, які вона приймає.

Ткаченко В. Войны в "песочнице" / В. Ткаченко // Сети и бизнес. – 2020. – № 1. – С. 60-65.

Р/1698

Среди многочисленных технологий киберзащиты особое место занимают методы карантина и обмана. Их цель – заставить условный "коронавирус" проявить себя раньше времени.

Ткаченко В. Коронавірус атакує комп'ютери / В. Ткаченко // Сети и бизнес. – 2020. – № 2. – С. 66-69.

Р/1698

Пандемія – ідеальний час, щоб наловити рибки у каламутній воді. Різноманітні кібератаки, від фішингу до складних операцій, за якими стоять державні органи, створюють ще більший хаос – наче мало самого вірусу.

Ткаченко В. Повітряний патруль: вимірювання і захист бездротового середовища / В. Ткаченко // Сети и бизнес. – 2020. – № 3. – С. 57-60. – Текст рос.

Р/1698

Точки доступа не только раздают Wi-Fi, но и следят, чтобы вы не подцепили какую-нибудь "киберзаразу".

Ткаченко В. Полювання на здобичників / В. Ткаченко // Сети и бизнес. – 2020. – № 3. – С. 66-69.

Р/1698

Threat Hunting – це активний пошук кіберзлочинців у мережі. Якщо вчасно натрапити на їхній слід, можна добряче зекономити на усуненні наслідків.

Хугланд Бенсон. Лучшие практики кибербезопасности для промышленных контроллеров / Бенсон Хугланд // CHIP–NEWS Украина. Инженерная микроэлектроника. – 2020. – № 7. – С. 38-43.

Р/900

Защита систем промышленной автоматизации становится проще и эффективнее, если контроллеры содержат встроенные функции кибербезопасности.

Яковів І. Базова модель інформаційних процесів та поведінки системи кіберзахисту / І. Яковів // Information Technology and Security. – July-December 2019. – Vol. 7, Iss. 2(13). – P. 183-196.

Р/1212

З метою збільшення результативності процесу розробки засобів автоматизації для сучасних систем кіберзахисту на основі атрибутивно-трансфертного підходу до сутності інформації та базової моделі інформаційних процесів управління кіберсистемою розроблено нову модель такої системи.