Тематична виставка
"Безпека та захист інформаційного простору "

(надходження II півріччя 2021)

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

732553 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 (59). - Харків, 2021. - 232 с. : граф., табл. - Бібліогр. наприкінці ст. - Текст кн. укр. та англ.

Зі змісту:

Котух Є. В. **Національні стратегії кібербезпеки: порівняльний аналіз.** – С. 32-42.
Стаття присвячена аналізу стратегій кібербезпеки 14 країн світу, виокремлено цілі та зацікавлені сторони реалізації таких стратегій. Розглянуто вплив міжнародної спільноти на формування національних стратегій кібербезпеки, запропоновано низку пунктів, які має включати національна стратегія кібербезпеки будь-якої країни.

Бакалинський О. О. Аналіз вимог до кіберзахисту автоматизованих систем управління технологічними процесами як об'єктів критичної інформаційної інфраструктури / О. О. Бакалинський, Д. В. Пахольченко // Електронне моделювання. – 2021. – Т. 43, № 4. – С. 103-112.

Р/518

Проведено аналіз чинного законодавства та кращих світових практик з кіберзахисту автоматизованих систем управління технологічними процесами, де запропоновано вимоги до реалізації кіберзахисту об'єктів критичної інформаційної інфраструктури. Наведено проблемні питання стосовно кіберзахисту об'єктів критичної інформаційної інфраструктури.

Бойченко О. Метод розрахунку ймовірності реалізації загроз інформації з обмеженим доступом від внутрішнього порушника / О. Бойченко, Р. Зюбіна // Безпека інформаційних систем і технологій. – 2019. – № 1(1). – С. 19-26.

Р/1227

У статті проведено аналіз нормативно-правових документів, які регламентують питання захисту інформації в інформаційно-телекомунікаційній системі. За результатами проведеного аналізу сформовано мету наукового дослідження, яке полягає в удосконаленні методу розрахунку ймовірності реалізації загроз інформації з обмеженим доступом від внутрішнього порушника.

Бондаренко Р. В. Інформаційна безпека держави / Р. В. Бондаренко , В. М. Михальчук // Інвестиції: практика та досвід. – 2021. – № 5. – С. 95-101.

Р/2124

У статті систематизовано теоретико-методологічні погляди науковців до розуміння категорії "інформаційна безпека держави" як важливого показника в контексті забезпечення національної безпеки в умовах глобалізації. В статті сформульовано трактування поняття "інформаційна безпека" як стан захищеного інформаційного простору, що здатен забезпечити реалізацію загальнонаціональних інтересів, збереження стійкості держави до екзогенних і ендогенних чинників, що становлять загрозу та пов'язані із активним розвитком цифровізації.

Брижко В. М. Безпека персональних даних: правові стандарти Європейського Союзу та сучасні прикладні проблеми / В. М. Брижко, В. Г. Пилипчук // Інформація і право. – 2021. – № 1(36). – С. 17-28.

Р/844

Стаття є продовженням низки наукових праць щодо стану, тенденцій і подальшого забезпечення безпеки персональних даних в умовах цифрової трансформації та пов'язаних з нею проблем правового регулювання нових суспільних відносин у цій сфері. Розглядаються та оцінюються ключові аспекти документів ЄС, затверджених останніми роками, зокрема, Регламенту GDPR, Директиви NIS і проекту правового акту e-Privacy.

731453 R
34

Вплив пандемії коронавірусу COVID-19 на права, свободи і безпеку людини в інформаційній сфері [Текст] : матеріали другої наук.-практ. студ. конференції, 18 листопада 2020 р., м. Київ / [упоряд.: В. М. Фурашев, С. Ю. Петряєв, О. А. Самчинська] ; Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", ННЦ інформ. права та правових питань інформ. технологій, Каф. інформ. права та права інтелект. власності, НДІ інформатики і права НАПрН України. - Київ : КПІ ім. І. Сікорського , 2020. - 96 с. : граф., табл. - Бібліогр. в кінці ст.

Матеріали другої конференції присвячені розгляду питань впливу пандемії коронавірусу COVID-19 на права, свободи і безпеку людини в інформаційній сфері через вісім місяців спроб її подолання.

Участь у конференції взяли виключно студенти, переважно Київського політехнічного інституту імені Ігоря Сікорського різних спеціальностей та спеціалізації.

Зі змісту:

Ковтко Ю. А. **Влив карантинного та посткарантинного періодів на забезпечення конституційних прав і свобод людини в інформаційній сфері**. – С. 5-8.

Ланкін С. В. **Влив карантинного та посткарантинного періодів на роль та місце інформаційної безпеки в системі забезпечення конституційних прав і свобод людини в інформаційній сфері**. – С. 8-11.

Водько Ю. В. **Забезпечення конституційних прав і свобод людини в інформаційній сфері в умовах карантину**. – С. 12-15.

Долматов І. О. **Виклики інформаційній безпеці спричинені пандемією коронавірусу**. – С. 20-22.

Шпак І. В. **Кібербезпека під впливом пандемії та карантинного режиму**. – С. 22-24.

Пастущак Д. В. **Застосунок для комплексного пошуку злочинного контенту на веб-сайтах з використанням інструментів Big Data**. – С. 30-33.

Та ін.

Карєв І. Ю. Кіберсталкінг: відображення у національному законодавстві / І. Ю. Карєв, В. М. Фурашев // Інформація і право. – 2021. – № 1(36). – С. 29-34.

Р/844

Стаття присвячена кіберсталкінгу – виду специфічного кіберзлочину, при якому психологічний тиск на жертву відбувається за допомогою ІТ-технологій, та його відображення у національному законодавстві.

Кирилюк Р. Кібервійська як складова трансформації системи національної безпеки : Створення кібервійськ в Україні – визначення, проблеми, ризики, варіанти / Р. Кирилюк, Є. Шелест // Оборонний вісник. – 2021. – № 9. – С. 4-10.

Р/1134

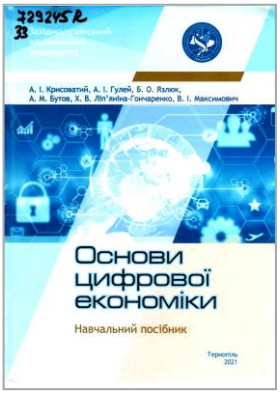
В контексті триваючої агресії Російської Федерації проти України та розвитку теорії та практики "гібридного протиборства" Україна зобов'язана знайти адекватні відповіді на виклики та загрози національній безпеці. Сучасне безпекове середовище та тенденції його змін на перспективу актуалізують діяльність щодо забезпечення кібербезпеки як однієї з основних складових в загальній системи

національної безпеки нашої держави. Зазначене охоплює одночасно два стратегічні напрями – розвиток спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному та перспективному безпековому середовищі на тлі одночасного реагування наявними ресурсами на поточні виклики та загрози, пов'язані з кіберпростором.

Кузнєцов О. М. Європейський досвід посилення спроможностей у сфері забезпечення кібербезпеки в сучасних умовах / О. М. Кузнєцов // Інформація і право. – 2021. – № 1(36). – С. 106-113.

Р/844

Здійснено огляд новел європейського законодавства у сфері забезпечення кібербезпеки. Узагальнено перспективи діджиталізації в ЄС. Розглянуто положення Стратегії кібербезпеки ЄС на 2021 – 2027 роки та Дорожньої карти "Цифровий компас". Деталізовано стратегічні цілі та напрями успішної цифрової трансформації Європи до 2030 року.



729245 R
33

Основи цифрової економіки [Текст] : навч. посібник / А. І. Крисоватий, А. І. Гулей, Б. О. Язлюк [та ін.] ; Західноукр. нац. ун-т. - Тернопіль : ЗУНУ, 2021. - 274 с. : рис., табл. - Бібліогр.: с. 265-268 (95 назв). - Предм. покажч.: с. 263-264.

У навчальному посібнику розглянуто основні тренди та перспективи розвитку цифрової економіки в Україні та світі. ***Розглянуто базові поняття теорії інформаційної безпеки,*** фінансових технологій, роботи з Big Data та їх застосуванням, також розглянуто сфери застосування IOT, основи електронної торгівлі, цифрового маркетингу та управління електронним бізнесом.

Петров В. Кіберможливості та національні спроможності : Перше системне оцінювання кіберпотужностей 15 країн, яке проводилось за сімома категоріями / В. Петров // Оборонний вісник. – 2021. – № 9. – С. 12-16.

Р/1134

Кіберпростір – це область комп'ютерних мереж, в яких інформація зберігається, спільно використовується і передається в режимі онлайн. Кібернетичний потенціал передбачає використання кіберпростору для досягнення ефекту, який може носити оборонний характер (наприклад, захист і стійкість) або наступальний (наприклад, вплив, примус, відволікаючий маневр і руйнування).

Поддубний В. О. Менеджмент вразливостей як складова частина політики безпеки ІТС / В. О. Поддубний, О. В. Сєвєрінов, О. С. Пустомельник // Системи управління, навігації та зв'язку. – 2020. – № 4(62). – С. 55-58.

Р/2152

Мета роботи – розгляд сучасних стандартів, нормативних документів, що встановлюють та регулюють процеси управління вразливостями та ризиками, що пов'язані з вразливостями. В статті здійснюється розгляд процесу інтеграції менеджменту вразливостей в системі управління інформаційною безпекою та його форми.

Субіна Т. В. Інформаційна безпека як один з видів національної безпеки України / Т. В. Субіна // Ірпінський юридичний часопис. Серія: Право. – 2020. – Вип. 3. – С. 103-113.

Р/812

У статті проаналізовано генезис наукових думок про сутність та понятійний апарат "інформаційної безпеки" та надано власне визначення інформаційної безпеки, а саме це – система унормованих методів, заходів, засобів, способів дотримання належного рівня охорони і захисту інформації з метою реалізації конституційних прав, свобод і законних інтересів людини та громадянина, суспільства і держави.

Особлива увага зверталася на аналіз нормативно-правового забезпечення інформаційної безпеки, а саме було розкрито, що інформаційна безпека є однією з видів національної безпеки та важливою самостійною сферою забезпечення національної безпеки.

732278 В
623

Сучасна спеціальна техніка [Текст] : науково-практичний журнал / Державний н.-д. ін-т МВС України. - Київ : [Видавець ФОП Горбенко Ю. В.].
№ 4 (63). - Київ, 2020. - 160 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., англ.

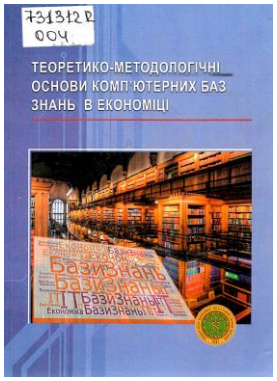
Зі змісту:

Кухаренко С. В. **Забезпечення кібербезпеки в Україні.** – С. 48-54.
Прийняття закону України "Про основні засади забезпечення кібербезпеки України" і посилення міжнародного співробітництва в сфері захисту кіберпростору стало актуальним як ніколи. У статті аналізуються забезпечення кібербезпеки в державі та сучасний стан національного законодавства в цій сфері.

729212 R
004

Тарасюк, Анатолій Васильович.
Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи [Текст] : монографія / Анатолій Тарасюк ; НДІ інформатики і права Нац. акад. правових наук України. - Київ ; Одеса : Фенікс, 2020.

У монографії йдеться про фундаментальні засоби, особливості та відмінності правового забезпечення кібернетичної безпеки України. За допомогою комплексного методологічного інструментарію та на основі соціонормативного та аксіологічного підходу здійснено порівняльний аналіз правових норм стосовно забезпечення кібербезпеки людини, суспільства, держави. На цій теоретичній та емпіричній основі розроблено концептуальні правові засади забезпечення кібербезпеки України та практичні рекомендації щодо удосконалення відповідних механізмів. Авторська концепція екстраполюється на процеси, пов'язані з російською анексією Криму та неоголошеною війною на сході нашої держави.



731312 R
004

Теоретико-методологічні основи комп'ютерних баз знань в економіці [Текст] : монографія / [Ріппа С. П., Антоненко В. М., Боднар О. С. та ін.]; за заг. ред. С. П. Ріппи ; Університет Державної фіскальної служби України. - Ірпінь : [УДФСУ], 2021. - 170 с. : рис., табл. - Бібліогр. наприкінці ст. - Авт. зазнач. на звороті тит. арк.

Основу монографії становлять результати досліджень провідних вчених України. У виданні представлено наукові роботи з проблематики комп'ютерного моделювання сучасних соціально-економічних процесів з використанням комп'ютерних баз знань в економіці, взаємовпливів синергетичних ефектів у міждисциплінарному інформаційному моделюванні баз знань. Розглянуто окремі моделі безпеки й оцінки складності розробки програмного забезпечення, важливі питання професійної компетентності майбутніх фахівців фіскальної служби України, Мінфіну та інших відомств, деякі специфічні інтерактивні технології навчання, використання хмарних обчислень в освіті, електронній комерції та популяризації понять інформаційної безпеки у контексті знання-орієнтованих технологій.

732555 В
35

Теорія та практика державного управління [Текст] = Theory and Practice of Public Administration : зб. наук. пр. / Нац. акад. держ. упр. при Президентові України, Харк. регіон. ін-т держ. упр. - Харків : [Магістр], 2009 - .
Вип. 2 (73). - Харків, 2021. - 200 с. : граф., табл. - Бібліогр. наприкінці ст. - Текст кн. укр. та англ.

Зі змісту:

Живило Є. О., Живило І. О. **Об'єднана підготовка персоналу складових Сил оборони сфери кібербезпеки в умовах тотальної оборони держави.** – С. 144-153.

Проаналізовано теоретичні аспекти формування та порядку набуття індивідуальних спроможностей фахівцями з кібербезпеки відповідно до розроблених стандартів підготовки, з метою досягнення сумісності в підготовці складових Сил оборони та держав – членів НАТО.

Акцентовано увагу на питаннях стандартизації підготовки зі спеціальності 125 "Кібербезпека" та на фахових компетенціях спеціалістів у сфері кібербезпеки для набуття ними об'єднаних спроможностей, які необхідні для швидкого та спільного реагування на загрози воєнній безпеці України, а також загрозам в інших сферах діяльності держави, які забезпечать формування та реалізацію державної політики у сфері цивільного захисту.

Котух Є. В. **Реалізація національних стратегій кібербезпеки: економіко-політичний аспект.** – С. 171-175.

Стаття присвячена розгляду проблем захисту інфраструктури та врегулювання ситуацій на національному рівні. Три кроки присвячено захисту саме критичної інфраструктури. Доведено, що публічно-приватне партнерство є обов'язковою умовою досягнення цих цілей захисту критичної інфраструктури.

Функціонування Експертної ради інформаційної та кібербезпеки як демократичний інноваційний інструмент державно-приватної взаємодії / Д. Дубов, Л. Олексюк, О. Потій, А. Семенченко // Науковий вісник: Державне управління. – 2021. – № 2(8). – С. 92-110.

Р/1443

Метою статті є узагальнення національного та міжнародного досвіду застосування інструментів державно-приватної взаємодії суб'єктів кібербезпеки та кіберзахисту, визначення ролі, концептуальних засад та моделі функціонування Експертної ради інформаційної та кібербезпеки як демократичного інноваційного інструменту державно-приватної взаємодії основних суб'єктів кібербезпеки та кіберзахисту, її місця в перспективній організаційно-технічній моделі кіберзахисту.

Цвілій О. О. Система сертифікації кібербезпеки інформаційних та комунікаційних технологій / О. О. Цвілій // Наукові праці ОНАЗ ім. О.С. Попова. – 2020. – № 2. – С. 121-134.

Р/1485

... в статті запропоновані основи Системи сертифікації кібербезпеки та Схеми сертифікації кібербезпеки продукції ІКТ і хмарних сервісів з акцентуванням на таких елементах, як оціночні стандарти; акредитація органів з сертифікації; взаємне визнання результатів сертифікації.

Програмні системи захисту інформації

Бичков О. Вимоги до механізмів захищеності ОС в рамках класу використання / О. Бичков, Я. Шестак // Безпека інформаційних систем і технологій. – 2020. – № 1(2). – С. 40-49.

Р/1227

При розробці програмного забезпечення слід спиратися на механізми безпеки, які передбачені операційною системою або інформаційною системою. Це потрібно для уніфікації та спрощення системи безпеки, полегшення її обслуговування, за рахунок зменшення кількості механізмів, які створені для розв'язання однієї і тієї ж задачі. Очевидно, що неправильний захист операційної системи може привести до провалу системи безпеки в цілому, бо робота спеціалізованого програмного забезпечення та робота з периферійними пристроями відбувається саме під контролем операційної системи.

Говорущенко Т. О. Концепція інформаційно-пошукової системи (на основі онтологій) для галузі якості програмного забезпечення / Т. О. Говорущенко, Ю. С. Мартинюк // Комп'ютерні системи та інформаційні технології = Computer Systems and Information Technologies. – 2020. – № 1. – С. 7-12.

Р/1110

У статті запропоновано концепцію інформаційно-пошукової системи (на основі онтологій) для галузі якості програмного забезпечення, зокрема, розроблено онтологію предметної галузі якості програмного забезпечення, яка відображає семантичні відношення між концептами предметної галузі та ляже в основу пошуку інформації про якість програмного забезпечення, зокрема, в основу тезаурусу майбутньої інформаційно-пошукової системи.

Жульковська І. І. Сучасні методи виявлення шкідливих програм / І. І. Жульковська, А. В. Плужник, О. А. Жульковський // Математичне моделювання. – 2021. – № 1(44). – С. 46-54.

Р/1286

В роботі виконано дослідження сигнатурного та евристичного методів виявлення шкідливого програмного забезпечення. Окремий аналіз присвячений застосуванню методів машинного навчання для класифікації шкідливих програм. Досліджено різні техніки машинного навчання для класифікації та виявлення зразків шкідливих програм та їх відповідних класів, їх фільтрації.

731174 В
004

Ільїн, Микола Іванович.
Зворотна розробка та аналіз шкідливого програмного забезпечення [Текст] : лабораторний практикум / М. І. Ільїн, Д. І. Якобчук ; Національний технічний університет України "Київський політехнічний інститут ім. Ігоря Сікорського". - Київ : КПІ ім. І. Сікорського , 2020. - 118 с. : іл. - Бібліогр.: с. 108-117.

Курс присвячено аналізу коду прикладного та системного програмного забезпечення, шкідливого програмного забезпечення з вихідними кодами та без них (reverse engineering; malware analysis, research and development). Метою є отримання навичок технічного аналізу інцидентів комп'ютерної безпеки із застосуванням шкідливого програмного забезпечення (incident response to malware attacks), аналізу шкідливого програмного забезпечення направлених атак (targeted malware analysis), дослідження засобів вторгнення, легального перехоплення та віддаленого керування для правоохоронних органів (intrusion software, lawful interception, computer surveillance tools R&D for LEA).

729241 R
004

Коваленко, Олександр Володимирович.
Моделі та методи розробки програмного забезпечення комп'ютерних систем для підвищення безпеки даних [Текст] : монографія / О. В. Коваленко ; Центральноукр. нац. техн. ун-т. - Кропивницький : КОД, 2019. - 256 с. : рис., табл., граф. - Бібліогр. наприкінці розд.

У монографії викладено теоретичні та практичні положення авторських досліджень моделей та методів розроблення безпечного програмного забезпечення комп'ютерних систем.

Можаєв М. О. Аналіз та порівняльні дослідження методів підвищення рівня безпеки програмного забезпечення / М. О. Можаєв, В. В. Давидов, Джан Ліцзян // Сучасні інформаційні системи. – 2020. – Т. 4, № 3. – С. 124-132. – Текст англ.

Р/543

У статті представлені результати аналізу основних методів виявлення вразливостей програмного забезпечення. Представлені результати досліджень ряду авторів, синтезуючих та регламентуючих знань про системи виявлення вразливостей програмного забезпечення. Розглянуті методи аналізу програмного забезпечення, що використовуються при проведенні сертифікаційних випробувань.

732559 В
629.7

Проблеми інформатизації та управління [Текст] : зб. наук. пр. / Нац. авіац. ун-т, Ф-т кібернетики, комп'ютерної та програмної інженерії. - Київ : [НАУ]. - **Вип. 66(2).** - Київ, 2021. - 72 с. : іл., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., рос., англ.

Збірник охоплює проблеми аналізу і синтезу комп'ютерно-телекомунікаційних систем та систем управління ними: створення ефективного інформаційно-вимірювального інструментарію визначення та оцінки параметрів об'єктів інформаційних технологій; математичне, лінгвістичне, апаратно-програмне забезпечення нових, включаючи кіберфізичні авіаційні, і вдосконалених існуючих розподілених комп'ютеризованих та комп'ютерних систем.

Зі змісту:

Гільгурт С. Я. **Порівняльний аналіз підходів до побудови компонентів реконфігурованих засобів технічного захисту інформації.** – С. 17-26.
"Найбільш ресурсномісткою задачею реального часу в апаратних засобах технічного захисту інформації є множинне розпізнавання фіксованих послідовностей символів (патернів) [3]. Від того, наскільки успішно вдасться вирішити цю задачу, залежить ефективність системи захисту в цілому".

Розроблення алгоритму прогнозування дефектів програмного забезпечення на основі карт Кохонена та ієрархічної кластеризації / В. Яковина, Н. Шаховська, Я. Матвійчук, Є. Засоба // Вісник Хмельницького національного університету. Серія: Технічні науки. – 2021. – № 1. – С. 78-82.

Р/1055«Т»

Метою статті є аналіз метрик програмного коду для виявлення залежностей між схильністю до дефектів програмного модуля та його метриками. У цьому дослідженні було використано JM1 загальнодоступний набір даних NASA з PROMISE Software Engin-Reering Repository.

Семенов С. Г. Дослідження моделі та вимог до безпеки програмного забезпечення / С. Г. Семенов, В. В. Давидов, Д. С. Гребенюк // Сучасні інформаційні системи. – 2021. – Т. 5, № 1. – С. 87-92. – Текст англ.

Р/543

У статті вирішуються наступні *завдання*: дослідження недоліків існуючої моделі забезпечення безпеки з метою виявлення основних її недоліків; дослідження характеристик якості програмного забезпечення, що впливають на її захищеність з метою виявлення можливості підвищення якості програмного забезпечення.

Семенов С. Г. Модифікація математичної моделі процесу тестування на проникнення в комп'ютерні системи / С. Г. Семенов, Цао Вейлін // Сучасні інформаційні системи. – 2020. – Т. 4, № 3. – С. 133-138. – Текст англ.

Р/543

Розроблено математичну модель процесу тестування на проникнення в комп'ютерні системи, що відрізняється від відомих урахуванням можливостей тестування безпеки спеціалізованих інформаційних платформ комп'ютерних систем, що дозволило оцінити ймовірність попадання часу виконання алгоритму тестування на проникнення в заданий інтервал. Запропонована математична модель процесу тестування на проникнення в комп'ютерні системи отримала подальший розвиток (модифікована).

731475 R
004

Формальні методи специфікації програм [Текст] : навч. посіб. / [А. Ю. Дорошенко, К. А. Жереб, Є. В. Іванов та ін.] ; Київський національний університет імені Тараса Шевченка. - Київ : ВПЦ "Київ. ун-т", 2018. - 367 с. : іл. - Бібліогр.: с. 310-332. - Авт. зазнач. на звороті тит. арк.

Викладено теоретичні основи формальної специфікації послідовних і паралельних програм із використанням алгебр алгоритмів і техніки переписувальних правил. У контексті розвитку ідей В. М. Глушкова з формалізації мов програмування розглянуто застосування методів формальної специфікації програм до задач проектування й генерації програм, а також для розв'язування прикладних задач. Досліджено формалізацію й верифікацію програм.

731627 B
004

Computer and information systems and technologies, International Scientific and Technical Conference (4 ; 2020 ; Kyarkiv).
Fourth International Scientific and Technical Conference "Computer and Information Systems and Technologies" [Text] : April 22-23, 2020 / Kharkiv national university of radioelectronics, ISMA University, National Aviation University [et al]. - Kharkiv : [Disa Plus LLC], 2020. - 90 p. : il. - Бібліогр. наприкінці ст. - Текст кн. англ.

Collection materials are published in the author's version without editing.

Телекомунікаційні мережі та інформаційно-комунікаційні технології

Бучик С. Реалізація групового визначення функціонального профілю захищеності та рівня гарантій інформаційно-телекомунікаційної системи від несанкціонованого доступу / С. Бучик, О. Юдін, Р. Нетребко // Безпека інформаційних систем і технологій. – 2019. – № 1(1). – С. 11-18.

Р/1227

У статті запропоновано, показано та проаналізовано основні етапи реалізації програмного забезпечення по груповій оцінці функціонального профілю та визначення або узгодження рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації інформаційно-телекомунікаційних систем від несанкціонованого доступу в Україні на основі раніше проведених авторами теоретичних досліджень.

730258 B
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. № 68. - Київ, 2020. - 132 с. : іл. - Алф. покажч.: с. 131.-Бібліогр. наприкінці ст. - Текст кн. укр., рос., англ.

Зі змісту:

Лєнков С. В., Джулій В. М., Сєлюков О. В., Орленко В. С., Атаманюк А. В. **Модель безпеки поширення забороненої інформації в інформаційно-телекомунікаційних мережах.** – С. 53-64.
Запропонована імітаційна модель ЗПЗІ в ІТКМ, яка враховує топологічні характеристики мережі, а також особливості інформаційної взаємодії абонентів як людино-машинних систем.

Толюпа С. В., Плющ О. Г., Пархоменко І. І. **Побудова систем виявлення вторгнень в інформаційно-телекомунікаційну мережу на основі методів інтелектуального розподілу даних.** – С. 80-89.
У статті запропонована комбінаторна побудова системи виявлення мережевих атак на основі вибраних методів інтелектуального аналізу даних та проведені експериментальні дослідження, що підтверджують ефективність створеної моделі виявлення для захисту розподіленої інформаційної мережі.

730287 В
621.39

Військовий інститут телекомунікацій та інформатизації.
Збірник наукових праць [Текст] = Collection of Scientific Papers / Міноборони України. - К. : [ВІТІ].
Вип. № 3. - Київ, 2020. - 146 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст укр., рос. та англ.

Зі змісту:

Куцаєв В. В., Штонда Р. М., Терещенко Т. П., Артемчук М. В., Нещерет І. Г. **Алгоритм блокування вірусу шифрувальника в інформаційно-телекомунікаційних системах.** – С. 43-55.
В статті запропоновано алгоритм дій адміністратора системи для протидії спробам несанкціонованого шифрування інформації в інформаційно-телекомунікаційній системі.
Фесьоха В. В., Фесьоха Н. О., Доброштан О. С. **Аналіз існуючих рішень автентифікації користувачів інформаційних систем та мереж спеціального призначення.** – С. 129-136.
У статті розглядається процедура визначення автентичності користувачів інформаційних систем та мереж (ІСМ) спеціального призначення на основі пред'явленого ними ідентифікатора у контексті процесу контролю доступу користувачів до ресурсів та/або сервісів.

Ефективність функціонування комп'ютерних мереж із SDN в умовах неповноти інформації про надійність / О. В. Зінченко, В. В. Вишнівський, Ю. В. Березовська, П. Седлачек // Сучасні інформаційні системи. – 2021. – Т. 5, № 2. – С. 103-107. – Текст англ.

Р/543

Для того, щоб забезпечити задані показники надійності комп'ютерної мережі пропонується використовувати їх гарантовані оцінки. Для підвищення рівня безпеки функціонування інформаційних систем та ввести в процес передачі пакетів поняття резерву часу необхідно відокремити функції передачі трафіку від функцій управління. В цьому і полягає основний принцип SDN.

Захист блоків інтелектуальної власності у спеціалізованих комп'ютерних засобах на базі ПЛІС / Я. М. Клятченко, О. С. Михайлюк, Л. М. Дудкова, О. В. Тарасенко-Клятченко // Інформаційні технології та комп'ютерна інженерія. – 2021. – № 1(50). – С. 15-21.

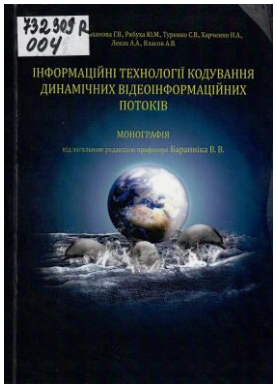
Р/1954

Широке використання ПЛІС для реалізації спеціалізованих комп'ютерних засобів спонукає до використання блоків інтелектуальної власності (intellectial property core, IP-core), оскільки для створення деяких екземплярів апаратних засобів необхідно реалізувати широкі функціональні можливості, що здійснюються завдяки IP. В роботі наводиться частина огляду ефективних реалізацій захисту IP, який є складною та важливою задачею. Описано різні підходи та методи організації такого захисту. Наводяться посилання на приклади використання додаткових структур – доповнюючих шифрування та аутентифікації, які унеможливлюють несанкціонований доступ.

Інформаційна технологія виявлення метаморфних вірусів на основі аналізу поведінки додатків у корпоративній мережі / А. О. Нічепорук, А. А. Нічепорук, І. А. Нега [та ін.] // Комп'ютерні системи та інформаційні технології = Computer Systems and Information Technologies. – 2020. – № 1. – С. 60-67.

Р/1110

Процес виявлення здійснюється на основі аналізу API викликів, що описують потенційно небезпечну поведінку програмного додатку. Після встановлення факту підозрілості поведінки додатку здійснюється порівняння дизасембльованого коду функціональних блоків підозрілого додатку з кодом функціональних блоків його зміненої версії. Для створення зміненої версії програмного додатку на хостах мережі встановлюються модифіковані емулятори. З метою підвищення загальної ефективності виявлення метаморфних вірусів, інформаційна технологія передбачає пошук відповідності між функціональними блоками метаморфного вірусу та його зміненої версії.



732309 R
004

Інформаційні технології кодування динамічних відеоінформаційних потоків [Текст] : монографія / [В В. Бараннік, Г. В. Хаханова, Ю. М. Рябуха та ін.] ; за заг. ред. В. В. Баранніка ; Харківський нац. ун-т радіоелектроніки. - Харків : [ФОП Бровін О. В], 2021. - 316 с. : граф., рис., табл. - Бібліогр.: с. 298-311. - Авт. на тит. арк. не зазнач.

У монографії розглядаються актуальні питання щодо підвищення якості відеоінформаційного сервісу з використанням телекомунікаційних систем. Розроблено метод керування бітовою швидкістю відеотрафіку на кінцевих вузлах телекомунікаційної системи. Створено метод кодування та реконструкції передбачених кадрів на основі блочних кодів. Запропонована стратегія керування бітовою швидкістю відеопотоку, що дозволяє знайти оптимальні параметри стиснення методом лагранжевих релаксацій. Розроблено метод вибору типу обробки блоків передбачених кадрів, який базується на використанні в якості вирішуючого правила оцінки кількості структурної надмірності. Розроблено метод кодування передбачених кадрів на основі попереднього трансформування. Він проводиться з попередньою ідентифікацією типу обробки блоків і подальшим формуванням блочних кодових конструкцій. Це дозволяє додатково зменшити бітову швидкість без втрат якості та надати можливість контролю бітової швидкості стисненого відеопотоку по відношенню до заданих вимог, тобто у порівнянні зі стандартом MPEG забезпечується виграш по ступеню зниження бітової швидкості при заданому параметрі PSNR та зменшення часу при обробці відеопотоку. Розроблено базовий метод керування бітовою швидкістю відеопотоку на основі використання методу Лагранжевих релаксацій. Він працює на основі таких механізмів як: вибір формату кольорової субдискретизації, вибір типу обробки для кожного блоку в кадрі з урахуванням його інформативності та можливості контролю і зміни фактору якості при квантуванні. На основі чого розроблено стратегію керування бітовою швидкістю відеопотоку при обробці Р-кадрів, яка дозволяє виконувати корекцію інтенсивності відеопотоку у відповідності до поточних параметрів ТКС та КС. Таким чином, є можливість підвищити ефективність процесу керування бітовою швидкістю на етапі кодування відеопотоку, що дає змогу зменшити коефіцієнт використання вузла комутації при максимальній інтенсивності відеотрафіку та зменшити ймовірність втрати пакетів.

Касовська І. В. Програмні комплекси мережевого моніторингу для підвищення ефективності захисту мереж / І. В. Касовська, О. Д. Шаповаленко, І. М. Луценко // Сучасний захист інформації. – 2021. – № 1(45). – С. 47-52.

Р/2300

В роботі приведено основні методи та протоколи мережевого моніторингу. Проведений загальний огляд властивостей програмних комплексів мережевого моніторингу. Досліджені наявні у відкритому доступу програмні комплекси моніторингу мережевої безпеки та обґрунтовано вибір інструменту для подальшого дослідження. Розроблені рекомендації щодо заходів забезпечення мережевої безпеки.

Козел В. Класифікація та рекомендації захисту від MITM атак / В. Козел // Проблеми інформаційних технологій. – 2019. – № 1(25). – С. 58-65.

Р/2277

"*Метою даної статті* є розробка та дослідження сучасних комп'ютерних атак. Розробка класифікації загроз та розробка рекомендацій щодо захисту комп'ютерних мереж".

730351 R
004

Компьютерная конкурентная разведка [Текст] : [монография] / А. Г. Додонов, Д. В. Ландэ, В. В. Прищепа, В. Г. Путятин ; НАН Украины, Институт проблем регистрации информации. - Киев : [ТОВ "Інжиніринг"], 2021. - 354 с. - Бібліогр.: с. 341-348.

Книга посвящена рассмотрению вопросов компьютерной конкурентной разведки, разведки в открытых ресурсах сети Интернет. Компьютерная конкурентная разведка охватывает автоматизированные процедуры сбора и аналитической обработки информации, которые проводятся с целью поддержки принятия управленческих решений, повышения конкурентоспособности исключительно из открытых источников в компьютерных сетях веб-сайтов, блогосферы, социальных сетей, мессенджеров, баз данных. В книге рассматриваются различные вопросы информационно-аналитической деятельности в сетевой среде. В качестве теоретических основ компьютерной конкурентной разведки рассматриваются элементы теории информации, анализа социальных сетей, информационного и математического моделирования.

Метод забезпечення живучості високомобільної комп'ютерної мережі / В. М. Ткачов, А. А. Коваленко, Г. А. Кучук, Я. С. Ні // Сучасні інформаційні системи. – 2021. – Т. 5, № 2. – С. 159-165.

Р/543

В статті розглянуто особливості функціонування рухомих комп'ютерних мереж на базі малогабаритних літальних апаратів (високомобільні комп'ютерні мережі). Показано, що такі мережі, на відміну від стаціонарних або маломобільних, відрізняються низьким рівнем живучості при локальних пошкодженнях їх вузлів. *Метою статті* є розробка методу забезпечення живучості високомобільних комп'ютерних мереж в умовах деструктивного зовнішнього впливу, що призводить до локальної руйнації вузлів мережі або зв'язків між ними, з використанням методики оцінки живучості на всіх етапах функціонування мережі.

Метод розрахунку захисту інформації від взаємовпливу користувачів в соціальних мережах / В. А. Савченко, В. М. Ахрамович, Т. М. Дзюба [та ін.] // Сучасний захист інформації. – 2021. – № 1(45). – С. 6-13.

Р/2300

"Розроблено метод розрахунку захисту інформації від взаємовпливу користувачів в соціальних мережах, який враховує додаткові параметри та ґрунтується на припущеннях, що величина впливу залежить від центральності користувачів в соціальній мережі".

Моделювання механізму валідації вразливостей при активному аналізі захищеності корпоративних мереж за допомогою поліномів Бернштейна / Р. В. Киричок, Г. В. Шуклін, О. В. Барабаш, Г. І. Гайдур // Сучасні інформаційні системи. – 2020. – Т. 4, № 3. – С. 118-123.

Р/543

Предметом вивчення у статті є модель процесу активного аналізу захищеності інформаційних систем та мереж, зокрема одного з її ключових компонентів, а саме механізму валідації вразливостей.

Опірський І. Р. Виявлення кібератак в інформаційних мережах / І. Р. Опірський, Ю. М. Ткач, В. О. Хорошко // Інформатика та математичні методи в моделюванні. – 2020. – Т. 10, № 3-4. – С. 177-189.

Р/2357

Метою статті є виявлення кібернетичних атак в інформаційно-телекомунікаційних мережах. Зокрема, розглянуто задачу виявлення кібернетичної атаки на фоні білого гаусівського шуму за умови неперервного часу спостереження. Наведено теоретичне обґрунтування усередненого об'єкту прогнозування.

Підвищення функціональності і стабільності завадостійких безпроводових інформаційно-комунікаційних систем / В. М. Джулій, Ю. П. Кльоц, В. С. Орленко [та ін.] // Вісник Хмельницького національного університету. Серія: Технічні науки. – 2021. – № 1. – С. 12-16.

Р/1055«Т»

Завадостійкі безпроводові канали передачі інформації застосовують нові технології, які дозволяють у режимі реального часу гарантувати підвищення доступності комунікаційних послуг для якісної та вірогідної передачі інформації в умовах впливу різнотипних завад. Такі канали забезпечують необхідні значення показників вірогідної передачі різнотипної завадостійкої інформації, що здійснюється за рахунок використання необхідного типу кодування.

Приходько Т. Аналіз досліджень з розгортанням DNSSEC в Інтернеті / Т. Приходько, В. Козловський, І. Яковів // Захист інформації. – 2021. – Т. 23, № 2. – С. 123-130.

Р/1428

Система доменних імен є невід'ємною частиною адресації в мережі Інтернет. В статті досліджуються сучасний стан використання технології розширення безпеки системи доменних імен DNSSEC та розглядаються питання попиту на вивчення показників з розгортання протоколу DNSSEC і проблеми, що наразі існують з отриманням максимально повного уявлення про масштаби розгортання даного протоколу в Інтернеті.

730605 В
004

Реєстрація, зберігання і обробка даних [Текст] : щорічна підсумкова наук. конф., 28-29 вересня 2020 року / НАН України, Ін-т проблем реєстрації інформації ; [за ред. В. В. Петрова]. - Київ : [ІПРІ НАН України], 2020. - 134 с. : іл., табл. - Бібліогр. наприкінці ст. - Авт. зазнач. у змісті.

Зі змісту:

Германюк А. П. **Загрози безпеці функціонування територіально-розподіленої інформаційної комп'ютерної системи в єдиному інформаційному просторі.** – С. 57-58.
Мета роботи. Дослідити загрози безпеці функціонування територіально-розподіленої інформаційної комп'ютерної системи в єдиному інформаційному просторі.

Розроблення пристрою для захисту від несанкціонованого доступу на основі трифакторної ідентифікації та аутентифікації користувачів / А. О. Азарова, Н. О. Біліченко, В. С. Катаєв, П. В. Павловський // Реєстрація, зберігання і обробка даних. – 2021. – Т. 23, № 2. – С. 72-80.

Р/1346

Запропоновано пристрій для забезпечення захисту від несанкціонованого доступу до інформації на основі використання трифакторної ідентифікації та автентифікації користувачів з можливістю розмежування доступу до інформаційного середовища. Пристрій дозволяє: завчасно виявляти спроби несанкціонованого доступу, надавати доступ до інформаційних ресурсів санкціонованим користувачам, навіть у випадку відмови пристрою та під час виникнення аварійних ситуацій.

732278 В
623

Сучасна спеціальна техніка [Текст] : науково-практичний журнал / Державний н.-д. ін-т МВС України. - Київ : [Видавець ФОП Горбенко Ю. В.].
№ 4 (63). - Київ, 2020. - 160 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., англ.

Зі змісту:

Тишик І. Я., Фік Е. І. **Виявлення мережевих атак на основі віртуальної машини RedHunt.** – С. 55-64.
З метою порівняння ефективності пропонованої віртуальної машини в роботі здійснено огляд поширених систем виявлення атак й охарактеризовано їх переваги та недоліки. Було проведено моделювання процесу виявлення мережевих атак на основі системи RedHunt, у результаті якого надано практичні рекомендації щодо вибору утиліт та взаємопов'язаних груп утиліт для підвищення ефективності цього процесу.

Удосконалений метод автоматичного активного аналізу захищеності корпоративної мережі / Р. Киричок, О. Зінченко, І. Срібна [та ін.] // Захист інформації. – 2021. – Т. 23, № 2. – С. 83-89.

Р/1428

В основу даного методу покладено синтез математичної моделі аналізу кількісних характеристик процесу валідації вразливостей, методики аналізу якості роботи механізму валідації виявлених вразливостей корпоративної мережі та методу побудови нечіткої бази знань для прийняття рішень при валідації вразливостей програмних та апаратних платформ. Зокрема математична модель аналізу ґрунтується на поліномах Бернштейна та дозволяє описати динаміку процесу валідації вразливостей.

729368 В
629.7

Харківський національний університет Повітряних Сил імені Івана Кожедуба.
Збірник наукових праць Харківського національного університету Повітряних Сил [Текст] = Scientific Works of Kharkiv National Air Force University Digest : щоквартальне наукове видання / Міноборони України. - Харків : Видавництво ХНУПС імені Івана Кожедуба.
Вип. 1 (67). - Харків, 2021. - 156 с. : рис., табл. - Дод. тит. арк. англ. - Бібліогр. наприкінці ст. - Алф. покажч.: с. 155. - Текст кн. укр., рос., англ.

Зі змісту:

Проведено аналіз застосування біотехнологій ідентифікації доступу з застосуванням стеганографічного методу захисту інформації. Метод підвищення інформаційної безпеки інформаційно-телекомунікаційної системи, в основі якого запропоновано використання процедури розпізнавання особи за райдужною оболонкою та реакцією очного яблука на подразники.

Шагін В. Ю. Централізована розподілена система виявлення атак у корпоративних комп'ютерних мережах на основі мультифрактального аналізу / В. Ю. Шагін, А. А. Нічепорук, А. С. Каштальян // Вимірювальна та обчислювальна техніка в технологічних процесах. – 2021. – № 1. – С. 50-55.

Р/1051

У роботі запропоновано архітектуру та компоненти розподіленої системи виявлення мережевих атак, в якій поєднано вимоги централізованості, розподіленості, самоорганізованості та на її основі здійснено розробку централізованої розподіленої системи визначення мережевих атак в корпоративних комп'ютерних мережах на основі мультифрактального аналізу. Проведені експериментальні дослідження з реалізованою централізованою розподіленою системою визначення мережевих атак в комп'ютерних мережах підтвердили ефективність функціонування в комп'ютерній мережі.

Інформаційне протиборство у воєнних конфліктах. Інформаційно-психологічна безпека

Брадов В. В. Формування мережевого інструментарію інформаційної війни (на прикладі агресії Росії проти України) / В. В. Брадов // Держава та регіони. Серія: Соціальні комунікації. – 2021. – № 2(46). – С. 96-103.

Р/1520

Мета дослідження – визначення особливостей формування в медіапросторі Донбасу інтернет-ресурсів з антиукраїнським пропагандистським контентом і використання їх як інструментарію інформаційної агресії з боку РФ на сході України. *Методологія дослідження.* Використано методи: моніторингу, групування розрізнених даних, узагальнення – для визначення сукупності та особливостей формування інтернет-ресурсів у медіапросторі тимчасово окупованої частини Донбасу; контент-аналіз – для визначення характеристик їх вмісту; експертний – для визначення їх авдиторної спрямованості.

Модель управління протидією інформаційним атакам у кіберпросторі / А. А. Шиян, Л. О. Нікіфорова, І. О. Дьогтєва, Я. Ю. Яремчук // Реєстрація, зберігання і обробка даних. – 2021. – Т. 23, № 2. – С. 62-71.

Р/1346

Представлено модель управління протидією інформаційним атакам у кіберпросторі сучасного інформаційного суспільства. Вона ґрунтується на виокремлених інструментах щодо протидії негативним інформаційно-психологічним процесам як у соціальних групах, так і у суспільстві в цілому. Досліджено динаміку кількості суб'єктів, які підпадають під вплив інформаційних атак, із використанням відповідного математичного апарату, основою якого є нелінійні диференційні рівняння. Вони описують як зміну кількості у часі суб'єктів, так і відповідні задачі, поставлені перед службою кібербезпеки для запобігання негативним наслідкам потенційних чи реалізованих інформаційних атак.

732418 В
15

Панченко, Олег А.
Информационно-психологическая безопасность в эпоху турбулентности [Текст] : [монография] / Олег Панченко. - Киев : КВИЦ, 2020. - 471 с. : рис., табл. - Бібліогр. в кінці гл.

Монографія відображає сучасні тенденції прогресування інформаційно-психологічної безпеки в умовах турбулентності, що виявляється у всіх сферах суспільного і особистісного розвитку. Розроблено ряд нових базових понять, представлено авторські моделі забезпечення інформаційної безпеки в умовах інформаційної турбулентності. Розглянуто інформаційні аспекти здоров'я, роль інформації у виникненні стресу; інформаційний фактор розладів психіки людини; інформаційне насильство. Викладено нові принципові підходи до абілітації та реабілітації в умовах інформаційно-психологічного впливу, сучасні шляхи підвищення якості життя людини.

Самчинська О. А. Інформаційне насильство, інформаційна маніпуляція та пропаганда: поняття, ознаки та співвідношення / О. А. Самчинська, В. М. Фурашев // Інформація і право. – 2021. – № 1(36). – С. 55-65.

Р/844

У статті досліджено поняття "інформаційно-психологічний вплив", "інформаційне насильство", "інформаційні маніпуляції" та "пропаганда", їх основні ознаки та співвідношення.

732554 В
35

Теорія та практика державного управління [Текст] = Theory and Practice of Public Administration : зб. наук. пр. / Нац. акад. держ. упр. при Президентові України, Харк. регіон. ін-т держ. упр. - Харків : [Магістр], 2009 - .
Вип. 1 (72). - Харків, 2021. - 204 с. : граф., табл. - Бібліогр. наприкінці ст. - Текст кн. укр. та англ.

Зі змісту:

Гайович Г. В., Твердохліб О. С. **Історіографічна та джерелознавча проблематика інформаційних війн у контексті загроз і викликів для державотворчих процесів сучасної України.** – С. 31-39.
Зроблено аналітичний огляд українських реалій щодо інформаційних війн у контексті загроз і викликів для сучасної України. Відмічено можливість використання інформації як зброї з метою впливу на свідомість і розум пересічних громадян. Зроблено припущення, що інформаційні операції/війни для України є не так науковою проблемою, як реальністю, у якій живе сучасне суспільство.

Кібербезпека – проблема XXI століття

Аналіз атак, що використовуються кіберзлочинцями під час пандемії covid 19 / В. Сусукайло, І. Опірський, А. Піскозуб [та ін.] // Захист інформації. – 2020. – Т. 22, № 4. – С. 220-226.

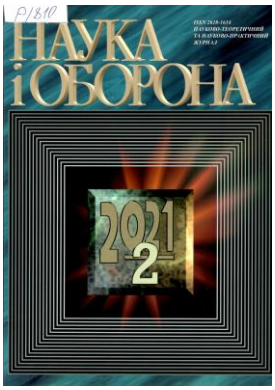
Р/1428

По мірі того як все більше висококваліфікованих фахівців з кібербезпеки долучається до блакитної команди, щодня запускається все більше шкідливих аплікацій, приблизно 230000 нових зразків шкідливих програм на день, згідно з інформацією дослідників з PandaLabs. Пандемію можна розглядати як подію, яка може призвести до виконання планів безперервності бізнесу або реалізації заходів з аварійного відновлення. Протягом цього часу слід аналізувати зростаючу кількість загроз кібербезпеки та визначати застосовні заходи безпеки.
У цій статті розкрито основні питання щодо моніторингу інфраструктури, а також забезпечення високого рівня управління вразливостями та реагування на інциденти. Наведено заходи управління, які необхідно використовувати у SOC центрах, а також представлено поглиблений аналіз векторів атак та заходів безпеки, які можна застосувати для їх запобігання.

Архипов А. Адаптивный подход к построению и обеспечению функционирования систем защиты информации / А. Архипов // Захист інформації. – 2021. – Т. 23, № 2. – С. 66-83.

Р/1428

Пропонується застосування підходу, суть якого полягає у використанні при створенні та управлінні СЗІ відомостей про особливості і характер поведінки обох сторін-учасників конфлікту. Узагальнення та "пакування" зазначених відомостей реалізується в формі математичних моделей – рефлексивних ризиків, структура і набір яких визначаються виділеними типовими сценаріями розвитку ситуації "атака / захист".



Білюга А. Д. Кіберзброя: сучасні загрози національній безпеці та шляхи протидії / А. Д. Білюга // Наука і оборона. – 2021. – № 2. – С. 42-49.

Р/810

Потужним засобом проведення незаконних дій та боротьби в кіберпросторі стала кіберзброя. Провідні країни світу розглядають кіберзброю як фактор, потенційно здатний впливати на перебіг воєнних дій і завдавати збитки економіці, порушувати управлінські функції конкретних держав тощо. Ураховуючи різноманітність дефініцій кіберзброї, автором запропоноване власне визначення цього виду зброї, проведений історіографічний опис кіберзброї, розглянутий досвід застосування кіберзброї в різних сферах людської діяльності. Надані пропозиції щодо подальшого поглиблення відносин України з НАТО в боротьбі з кіберзброєю.

Білявська Ю. Кібербезпека та захист інформації під час пандемії COVID-19 / Ю. Білявська, Н. Микитенко, Я. Шестак // Товари і ринки. – 2021. – № 1(37). – С. 34-46.

Р/2044

Зроблено огляд світових тенденцій кіберзлочинності, а також її географії та світових брендів, що зазнали найбільших збитків від неї. Досліджено структуру злочинів у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж і мереж електрозв'язку. Сформовано "портрет" сучасного кіберзлочинця. Узагальнено категорії жертв та типи кібератак в Україні, що спричинені пандемією COVID-19.

Василішин С. Удосконалення важелів управління діджиталізаційними ризиками економічної безпеки та формування кібербезпеки облікової системи / С. Василішин // Вісник економіки. – 2021. – № 1(99). – С. 97-110.

Р/1236

Проаналізовано структуру та типи основних правопорушень у галузі кібербезпеки українських підприємств. На основі результатів всеукраїнського експертного опитування-анкетування бухгалтерів визначено вагомість окремих груп та структуру диджиталізаційних ризиків обліково-аналітичного забезпечення. Розкриті технічний, програмний, інформаційний, кадровий та організаційний компоненти інформаційної безпеки підприємств. Розроблена адаптивна система забезпечення кібербезпеки підприємства на основі виокремлення експертної групи з інформаційної безпеки, яка є складовою служби економічної безпеки і виконує функції моніторингу кіберзагроз, координації тактичних дій та формування стратегій кіберзахисту підприємств або залучення послуг IT-компаній інтеграторів.

732289 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. № 70. - Київ, 2021. - 124 с. : іл. - Алф. покажч.: с. 117.-Бібліогр. наприкінці ст. - Текст кн. укр., рос., англ.

Зі змісту:

Лєнков С. В., Комарова Л. О., Дорошенко Т. В., Солодєєва Л. В. **Аналіз проблем лінгвістичного забезпечення кіберфізичних систем нанотехнологій.** – С. 69-76.

Статтю присвячено аналізу перспектив взаємодії нанотехнологій й прикладної лінгвістики у сфері функціонування інформації в автоматизованих наносистемах різних типів, зокрема використанню лексичних одиниць семантичного поля – "нанотехнології", обстеженню стану лексикографічних і термінографічних джерел професійної мови в області нанотехнологій і наноіндустрії в загальній системі інформаційної безпеки держави.

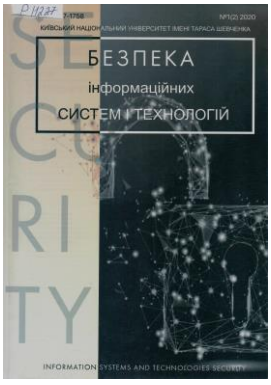
Городянська Л. В., Цюкало Л. В. **Інформаційна безпека суб'єктів малого підприємництва в умовах цифровізації.** – С. 105-114.

Уточнено тлумачення дефініцій "інформаційна безпека" та "економічна безпека". Визначено види інформації суб'єктів малого підприємництва, які підлягають захисту, та складові економічної безпеки. Сформовано пропозиції щодо створення комплексної програми безпеки.

730922 R
004

Волошин, Вячеслав Степанович.
Кибернетическая безопасность. Социальные и прикладные вопросы [Текст] : [науч. изд.] / Вячеслав Волошин. - [Киев] : Освита Украины, 2020. - 294 с. : граф., табл. - Бібліогр.: с. 274-293.

Настоящая книга является одним из немногих источников, в котором изложено несколько новое видение актуальной области знаний, которая носит название кибернетическая безопасность. Автор, специалист по безопасности технических систем, на основании многочисленных собственных исследований и исследований других авторов сделал попытку некоторого переосмысления этой важной современной области знаний, приблизив ее к пользователю, к человеку, как потребителю огромного многообразия информационной продукции, что является естественным для любых человеко-машинных систем, которые составляют естественную природу любого инженерного прогресса, в том числе, в современных *IT*. Не умаляя огромных достижений в областях защиты программного компьютерного продукта, безопасности современных баз данных, защиты персональных данных в современном интернет-пространстве, сделана попытка расширить область притязаний этой науки за счет исследования других аспектов безопасности человека, как участника глобального информационного пространства, что может обогатить эту науку новыми системными результатами.



Гнатієнко Г. Визначення пріоритетності заходів кібербезпеки при неповних експертних ранжуваннях / Г. Гнатієнко, Н. Тмєнова // Безпека інформаційних систем і технологій. – 2020. – № 1(2). – С. 9-15.

Р/1227

В роботі пропонується гнучкий математичний апарат для моделювання задач інформаційної безпеки та адекватного застосування аналізу думок колективу експертів на практиці. Описано підхід до знаходження результуючого ранжування пріоритетності заходів як розв'язку задачі багатокритеріальної оптимізації, де послідовність виконання заходів може передбачити взаємодію виконавців і вимагати регламентування послідовності дій усіх елементів та підсистем організаційної системи. Такий підхід дозволяє об'єднати різні за складом та пріоритетністю заходи інформаційної безпеки, запропоновані експертами різних підрозділів; знаходити компромісне рішення для різнорідної групи експертів; не порушувати задані переваги жодного експерта при обчисленні компромісного ранжування заходів кібербезпеки.

Грібоєдов С. М. Удосконалення державного планування у сфері забезпечення кібербезпеки в умовах гібридних загроз / С. М. Грібоєдов // Інформація і право. – 2021. – № 1(36). – С. 114-122.

Р/844

Розглянуто засади державного стратегічного планування у сфері забезпечення кібербезпеки. Визначено шляхи удосконалення державного управління у сфері кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів. Проаналізовано та узагальнено недоліки Стратегії кібербезпеки України 2016 року. Розглянуто проєкт Стратегії кібезбезпеки України на 2021 – 2025 роки та запропоновано напрями її удосконалення.

Гурєєв В. О. Топологічний метод оцінки чутливості до виявлення кібернетичних загроз в енергосистемах ОЕС України / В. О. Гурєєв, Є. М. Лисенко // Електронне моделювання. – 2021. – Т. 43, № 2. – С. 68-78.

Р/518

Розглянуто теоретичні питання побудови топологічного методу чутливості до виявлення кібернетичних загроз в електричних мережах енергосистем за допомогою моделювання режимів роботи окремих (виділених) підсистем.

Гуцалюк М. В. Новітні тенденції кіберзлочинності / М. В. Гуцалюк // Інформація і право. – 2021. – № 1(36). – С. 79-89.

Р/844

У статті досліджуються сучасні тенденції кіберзлочинності, у тому числі її організовані форми, надаються пропозиції щодо посилення протидії цьому явищу.

Дегтярьова Л. М. Контроль технічного стану складових елементів систем захисту інформації / Л. М. Дегтярьова, Ю. В. Вакуленко, О. Б. Одарущенко // Вісник Східноукраїнського національного університету імені Володимира Даля. – 2021. – № 4(268). – С. 49-52.

Р/1357

Система контролю повинна обробляти інформацію про ступінь працездатності контрольованої системи на підставі вимірювання змінних процесів. Ця система може мати два види контролю: динамічний та статистичний, кожен з яких має власні дії, що визначаються двома факторами: часом контролю і достовірністю контролю.

Емулятор загроз для верифікації систем виявлення кібератак / А. Корченко, Ю. Дрейс, Ю. Нагорний, В. Бичков // Захист інформації. – 2021. – Т. 23, № 2. – С. 101-116.

Р/1428

... *метою роботи* є розробка емулятора для проведення експериментального дослідження для підтвердження достовірності отриманих теоретичних положень, практичних результатів та адекватності роботи програмного модуля розробленої системи виявлення кібератак, що дозволить удосконалити функціональні властивості сучасних систем виявлення вторгнень для режиму реального часу.

Єріна А. М. Статистичні індикатори розвитку кібербезпеки в контексті цифрової трансформації економіки й суспільства / А. М. Єріна, І. А. Гончар, С. В. Заєць // Science and Innovation = Наука та інновації. – 2021. – V. 17, № 3(99). – P. 3-13. – Текст англ.

Р/1928

Мета. Узагальнення міжнародного досвіду оцінювання стану кібербезпеки, позиціонування країн за рівнем її розвитку у глобальному просторі, визначення сильних і слабких ланок в управлінні кібербезпекою та забезпечення дієвого захисту кіберпростору на національному рівні. *Матеріали й методи.* Використано компонентні індекси міжнародних рейтингів, які характеризують потенціал цифрової економіки (ICT IDI, NRI, EGDI) та участь країн у сфері кібербезпеки (GCI і NCSI).

Заікін С. С. Модель передбачення інса йдерської загрози в організації / С. С. Заікін, О. В. Кітура // Сучасний захист інформації. – 2021. – № 1(45). – С. 30-34.

Р/2300

У статті розглянуто поняття "інсайдерська загроза" та "інсайдер". Визначено загальні методи використання кіберзлочинцями інсайдерських загроз для компрометації мережевого середовища організації для отримання доступу до цінних активів. Досліджено різновиди інсайдерських загроз та їх критичність для організацій щодо боротьби з цими загрозами для зменшення ризику".

730261 В
004

Інформаційні системи та технології ІСТ-2020 [Текст] = "Information systems and technologies" IST-2020 : матеріали 9-ї Міжнародної наук.-техн. конф., присвяч. 90-річчю Харківського нац. ун-ту радіоелектроніки, 17-20 листопада 2020 р., Харків, Україна / [наук. ред.: А. Д. Тевяшев, Л. Б. Петришин, В. Г. Кобзев] ; НАН України, Люблінський від. Польської АН, Представництво "Пол. АН" у Києві, Харків. нац. ун-т радіоелектроніки [та ін.]. - Харків : [ХНУРЕ, Друкарня Мадрид], 2020. - 314 с. : граф., рис., табл. - Бібліогр. в кінці ст. - Паралел. назва англ.

Зі змісту:

Секція 8. **Захист інформації. Інформаційна безпека.** – С. 225-282.

Дехтяренко М. **Метод порогового розподілу секретної інформації.** – С. 247-249.

Левченко М., Турти М. **Інформаційна модель системи технічного захисту інформації на основі технології Honeypot.** – С. 258-261.

Баронова О., Турти М., Ганчо С. **Визначення рівня впливу кіберзагроз на розвиток морської галузі.** – С. 275-278.

Та інші.

Карпович І. Технології моделювання і оцінки ризиків інформаційної безпеки / І. Карпович, О. Гладка, Ю. Бухало // Технічні науки і технології. – 2021. – № 1(23). – С. 62-68.

Р/1125

Виконано моделювання, аналіз і оцінювання ризиків інформаційної безпеки на основі прикладних аспектів теорії графів в поєднанні з експертними методами оцінювання. Сформульовано рекомендації щодо підвищення ефективності системи захисту інформації. Запропонована модель може бути застосована на етапі аудиту безпеки організації для виявлення слабких місць системи захисту, а також для удосконалення діючої системи кіберзахисту.

Качинський А. Б. Операційна аналітика як інструмент моніторингу даних та управління подіями систем забезпечення кібербезпеки / А. Б. Качинський, М. С. Стремецька // Доповіді Національної академії наук України. Серія: Математика. Природознавство. Математичні науки. – 2021. – № 1. – С. 9-16.

Р/202

В статті запропонована оригінальна структурно-функціональна схема управління даними для SIEM-систем, що враховує прямі та зворотні зв'язки фізичного, математичного й аналітичного рівнів, заснована на теорії страт М. Месаровича.

731187 В
621.39

Київський політехнічний інститут, Національний технічний університет України.
Вісник Національного технічного університету України "Київський політехнічний інститут" [Текст] : [наук. вид.] / гол. ред. Шарпан О. Б. - Київ : ["Політехніка" КПІ ім. Ігоря Сікорського]. - (**Радіотехніка. Радіоапаратобудування**).
Вип. 83. - Київ, 2020. - 76 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Текст кн. укр., англ., рос. мов. Дод. тит. арк. англ.

Зі змісту:

Гулак Г. М., Лахно В. А., Адилжанова С. А. **Метод раціонального керування системами кіберзахисту та забезпечення гарантоздатності радіотехнічних систем.** – С. 62-68.

В статті визначається можливість застосування модифікованого генетичного алгоритму для вирішення завдання раціонального вибору апаратно-програмних засобів захисту інформації (ЗЗІ) і динамічного керування конфігураціями засобів на різних рівнях безпеки гарантоздатних радіотехнічних систем (ГРС), а також інформаційних систем (ІС).

Кіберпростір: тенденції розвитку // Оборонний вісник. – 2021. – № 4. – С. 16-19.

Р/1134

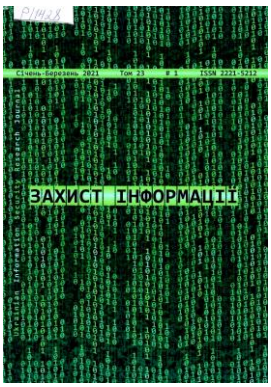
Розділи статті:

- Формування спільних підрозділів для проведення кібероперацій
- Інтеграція кібернетичного потенціалу в усі бойові сфери на тактичному рівні
- Інтеграція кібероперацій, кіберрозвідки та можливостей кінетичного удару встановлює вимоги до новітніх систем управління боєм
- Космічні активи, що відіграють вирішальну роль у кіберопераціях, потребують наявність систем й захисту
- Кіберпідрозділи – невід'ємна частина концепції багатодоменної оперативної групи (MDO).

Кіндзерський Ю. В. Кібербезпека та становлення цифрової економіки: проблеми взаємозв'язку / Ю. В. Кіндзерський // Економічний вісник Дніпровської політехніки. – 2020. – № 3. – С. 18-26.

Р/1790

Розкрито значення кібербезпеки у формуванні цифрової економіки. Проаналізовано рівень готовності країн до захисту даних у кіберпросторі за «Глобальним індексом кібербезпеки» (Global Cybersecurity Index, GCI) та «Національним індексом кібербезпеки» (National Cyber Security Index, NCSI), розкрито особливості їх складових. Акцентовано увагу на оцінці впливу кібербезпеки на рівень розвитку цифрової економіки. Виявлено проблему волатильності взаємозв'язку між кібербезпекою та рівнем цифрового розвитку крізь призму показників розвитку ІКТ і мережевої готовності.



Концептуальні засади впровадження організаційно-технічної моделі кіберзахисту України / О. Потій, А. Семенченко, Д. Дубов [та ін.] // Захист інформації. – 2021. – Т. 23, № 1. – С. 47-60.

Р/1428

У статті запропоновано концептуальні засади впровадження організаційно-технічної моделі кіберзахисту. Зокрема, визначені її місія, мета, призначення та цілі. Вперше визначені сили та засоби кіберзахисту. Розглянуто архітектуру організаційно-технічної моделі кіберзахисту, яка являє собою структуровану систему, яка складається з трьох інфраструктур кіберзахисту.

732178 R
004

Корченко, Анна Олександрівна.
Технології виявлення та попередження кібератак [Текст] : навч. посіб. / А. Корченко, В. Гребенюк ; Національний авіаційний університет. - Київ : НАУ, 2021. - 108 с. : граф., рис., табл. - Бібліогр.: с. 108.

У навчальному посібнику сформована класифікація сучасних атак, запропоновані базові характеристики для систем виявлення вторгнень та проведений аналіз програмних і програмно-апаратних засобів та систем виявлення вторгнень.

Котух Є. В. Типи владних відносин у стратегії кібербезпеки // Інвестиції: практика до досвід. – 2021.– № 11. – С. 98-102.

Р/2124

Стратегія кібербезпеки охоплює як захист державних інтересів у кіберпросторі, так і проведення більш широкої безпекової політики шляхом використання багатьох можливостей, які пропонує кіберпростір. У статті досліджено типологію владних відносин у стратегії кібербезпеки. Розглядаючи кібербезпеку в кожній

з чотирьох категорій влади (примусовій, інституційній, структурній та продуктивній), встановлено, що вони не обов'язково взаємовиключні. Доведено, що примусова влада стосовно кібербезпеки надає можливості для безпосереднього контролю одного актора з боку іншого; інституційна влада надає можливість опосередкованого контролю над акторами за посередництва інститутів; структурна влада визначає соціальні можливості та інтереси шляхом реалізації державно-приватних партнерських відносин; продуктивна влада дає можливість з'ясувати, яким чином системи знань та дискурсивні практики функціонують у мережах соціальних сил, породжених кібербезпекою.

Кравець І. Хакери та ковбаса: чи загрожує кібератака вашому сніданку / І. Кравець // Agroexpert. – 2021. – № 7(156). – С. 52-53.

Р/2278

У попередніх статтях ми дедалі частіше порушували тему саме кібербезпеки, що в часи тотальної цифровізації якось залишилася на задньому плані. Хоча саме ця тематика потребує значної уваги, як з боку ІТ-фахівців, так і обізнаності серед кожного аграрія. Бо так чи інакше кожен день ми починаємо з гаджетів: переглядаємо знімки з дронів, дивимось індекси вегетації, прогноз урожаю, бухгалтерські звіти та багато іншої інформації. І всі ці терабайти персональних даних потребують захисту. Чому? Бо це є ваш цифровий актив. А ви ж не хочете втрачати свої активи.

Кузьменко О. В. Економіко-математичне моделювання ефективності національної системи протидії кібершахрайствам та легалізації кримінальних доходів на основі методів аналізу виживання / О. В. Кузьменко, Т. В. Доценко, Л. О. Скринька // Науковий вісник Мукачівського державного університету. Серія: Економіка. – 2021. – Т. 8, № 1. – С. 144-153.

Р/2057

У статті проведено бібліометричний аналіз публікацій, присвячених проблемі ефективності кібершахрайства та протидії легалізації незаконних коштів, за допомогою побудови бібліометричної карти ключових слів, з використанням програмного забезпечення VOSviewer. Це дозволило виділити 7 кластерів основоположних категорій аналізу кібершахрайства. А зміни векторів досліджень науковців показала візуалізаційна карта контекстуально-часового виміру досліджень ефективності кібершахрайств у виданнях бази даних Scopus. У роботі досліджено ефективність національної системи протидії кібершахрайствам та легалізації кримінальних доходів на основі таблиць виживання.

Леонов Б. Д. Методичне забезпечення заходів з класифікації, ідентифікації та фіксації кіберзлочинів / Б. Д. Леонов, В. С. Серьогін // Інформація і право. – 2021. – № 1(36). – С. 99-105.

Р/844

Стаття присвячена аналізу напрямів удосконалення методичного забезпечення експертних досліджень програмних засобів, призначених для негласного доступу до комп'ютерної інформації. В межах статті досліджуються актуальні питання методичного забезпечення заходів з класифікації, ідентифікації та фіксації кіберзлочинів на базі запропонованих методичних підходів у сфері протидії кіберзлочиності.

Лисенко С. М. Метод оцінки ризику інформаційної безпеки кіберфізичних систем на основі взаємозалежності вразливостей / С. М. Лисенко, А. С. Кондратюк // Комп'ютерні системи та інформаційні технології = Computer Systems and Information Technologies. – 2020. – № 2. – С. 54-58.

Р/1110

У статті представлено новий метод оцінки ризику інформаційної безпеки кіберфізичних систем на основі взаємозалежності вразливості. У роботі представлено метод оцінки ризику атак на кіберфізичні системи, який уможливлює кількісне визначення ризиків. Крім того, враховано рівень імовірності успішної атаки обчислюється з урахуванням взаємозалежного взаємозв'язку між вразливістю, а рівень впливу атаки враховує наслідки на кіберфізичну систему, що спричинюються в результаті кібератак.

Лисенко С. М. Проектування та розроблення інтелектуального агента виявлення кіберзагроз та ШПЗ в корпоративних мережах / С. М. Лисенко, Т. М. Кисіль, Р. В. Щука // Вісник Хмельницького національного університету. Серія: Технічні науки. – 2020. – № 5. – С. 89-94.

Р/1055«Т»

В роботі представлено інтелектуальний агент виявлення кіберзагроз та ШПЗ в корпоративних мережах, який представляє програмну систему із можливістю виявлення відомих та невідомих кібератак, ШПЗ мережного та хвостового типу, а також здатністю продукувати множину сценаріїв безпеки для забезпечення резильєнтності КС в умовах кіберзагроз.

730225 R
004

Методи і алгоритми захисту інформаційних ресурсів комп'ютерних систем [Текст] : навч. посібник / Джулій В. М., Кльоц Ю. П., Муляр І. В., Чешун В. М. - Хмельницький : [ХНУ] , 2021. - 175 с. : іл. - Бібліогр.: с. 169-170.

Подані поняття технологій захисту інформаційних ресурсів комп'ютерних систем, види інформаційних загроз і атак, методи та засоби керування безпекою, способи і критерії оцінки ефективності систем захисту інформації, базові криптографічні методи захисту, способи аутентифікації інформаційних повідомлень тощо.

Муравський В. Класифікація стейкхолдерів (користувачів) облікової інформації для цілей кіберзахисту підприємства / В. Муравський, В. Муравський, О. Шевчук // Вісник економіки. – 2021. – № 1(99). – С. 83-96. – Текст англ.

Р/1236

У процесі дослідження актуальності варіативних кіберзагроз для різних видів стейкхолдерів використані загальнонаукові емпіричні, логічні та історичні методичні прийоми пізнання дійсності. Дослідження базуються на основі загальних методів вивчення економічних процесів, фактів та явищ з позиції бухгалтерського обліку та кібербезпеки підприємств. Інформаційною базою дослідження стали історичні документи щодо класифікації стейкхолдерів, наукові праці вітчизняних та зарубіжних учених у частині поділу користувачів облікової інформації на види тощо.

Опірський І. Розслідування кіберзлочинів за допомогою приманок у хмарному середовищі / І. Опірський, В. Сусукайло, С. Василишин // Безпека інформації. – 2021. – Т. 27, № 1. – С. 20-26.

Р/1408

Ця стаття досліджує можливості приманок в хмарних середовищах. Аналізує проблему розслідування кіберзлочинів у хмарах. Визначає та вивчає відповідні технології, що використовуються фахівцями з кібербезпеки під час розслідування кіберзлочинів. Визначає переваги використання приманок у хмарній інфраструктурі. Для хмарних середовищ загрозою номер один є порушення даних. Неадекватне управління доступом, у хмарному середовищі, загроза, що може призвести до компрометації хмарної системи.

Оцінювання ефективності рішень в системах захисту інформації / В. Ю. Тітова, О. С. Андрощук, В. С. Орленко [та ін.] // Вісник Хмельницького національного університету. Серія: Технічні науки. – 2020. – № 5. – С. 307-310.

Р/1055«Т»

В даній статті розглянуто відомі методи оцінювання ефективності рішень. Проаналізовано можливість їх використання для оцінювання ефективності рішень, що приймаються системами захисту інформації стосовно класифікації та визначення загроз.

Побудова систем виявлення кібератак за допомогою прихованої марківської моделі / С. Толюпа, І. Пархоменко, Л. Терейковська, В. Квасніков // Технічні науки і технології. – 2021. – № 1(23). – С. 53-61.

Р/1125

Одним із найбільш перспективних напрямів підвищення якості аналізу даних є використання їх у системах виявлення мережевих кібератак методом виявлення аномалій.

У результаті проведених досліджень обґрунтовано можливість формування шаблонів нормальної поведінки мережевих об'єктів комп'ютерних систем на основі однорідного ланцюга Маркова з послідовними переходами.

730285 В
338

Проблеми економіки та управління [Текст] = Economics & Management Issues : зб. наук. пр. / Львівська політехніка, Національний університет. - Львів : Вид-во Львів. політехніки, 2020. - 186 с. : граф., рис., табл. - (Вісник / Львівська політехніка, Національний університет ; vol. 4, № 2). - Бібліогр. наприкінці ст. - Текст кн. укр., англ. мов.

Зі змісту:

Шандрівська О. Є., Шинкаренко Н. В. **Прикладна оцінка ризиків у системі забезпечення безпеки соціально-економічних процесів у кіберпросторі.** – С. 94-105.
З'ясовано вплив ключових тенденцій сучасності на формування превентивних та адаптивних механізмів забезпечення інформаційної та кібернетичної безпеки підприємств.

Розробка ефективних методів та засобів отримання й захисту інформації: фізична модель біосенсора та кодування даних / А. Білецький, О. Ключко, В. Шутко, І. Морозова // Захист інформації. – 2021. – Т. 23, № 2. – С. 90-101.

Р/1428

Метою виконаної роботи є детальна характеристика технічних пристроїв – біосенсорів як елемента біомедичних інформаційних систем, аналіз електричних інформаційних сигналів на виході біосенсора, можливості кодування ним інформації та можливості захисту даних у такій системі.

Статистичне дослідження стану кіберзахисту критичної інфраструктури України / О. О. Бакалинський, Ю. І. Циплинський, І. В. Нечаєва, В, О. Дубок // Електронне моделювання. – 2021. – Т. 43, № 1. – С. 67-80.

Р/518

Наведено результати виконання доручення прем'єр-міністра України щодо опитування про стан кіберзахисту, яке було проведено в рамках виконання підготовчих заходів до "Огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом".

730412 R
004

Сучасні інформаційні технології в кібербезпеці [Текст] : монографія / [Довбиш А. С., Ободяк В. К., Шелехов І. В. та ін.] ; за ред. В. К. Ободяка, І. В. Шелехова ; Сумський державний університет. - Суми : Сумський державний університет, 2021. - 348 с. : граф., рис., табл. - Бібліогр. наприкінці розд. - Авт. зазнач. на звороті тит. арк. та у змісті.

У монографії розглянуто питання квантової криптографічної технології, управління ризиками інформаційної безпеки, виявлення шкідливого програмного забезпечення, стандартизації та термінології кібербезпеки і підготовки студентів за спеціальністю "Кібербезпека".

Значну увагу приділено вирішенню завдання інформаційно-екстремального синтезу системи виявлення кібератак у рамках розробленого авторами методу машинного навчання.

732190 R
004

Сучасні інформаційні технології і системи [Текст] : монографія / [В. П. Бурдаєв, Н. Г. Аксак, М. В. Кушнарьов та ін.] ; за заг. ред. В. С. Пономаренка ; Харк. нац. екон. ун-т ім. С. Кузнеця. - Харків : [ФОП Бровін О. В.], 2021. - 182 с. : граф., рис., табл. - Бібліогр. наприкінці глав. - Авт. зазнач. на звороті тит. арк. та с. 174-181.

В монографії розглянуті сучасний стан та перспективи розвитку сучасних інформаційних технологій і систем різних видів прикладного характеру. Монографія представляє інтерес як для фахівців, сфера діяльності яких безпосередньо пов'язана з розробкою прикладних інформаційних технологій і систем, так і для більш широкого кола фахівців.

Сучасні комплекси пост-квантової безпеки державних електронних інформаційних ресурсів / А. О. Корченко, Є. В. Іванченко, Н. В. Кошкіна [та ін.] // Безпека інформації. – 2021. – Т. 27, № 1. – С. 27-52.

Р/1408

Мета роботи. Виходячи з актуальності проблеми забезпечення національної безпеки України в умовах ведення інформаційних і гібридних війн, метою роботи є удосконалення систем спеціального призначення за рахунок побудови комплексів КЗІ пост-квантової безпеки державних електронних інформаційних ресурсів. Реалізовано проекти розробки та впровадження програмно-технічних комплексів та апаратних засобів КЗІ для надавачів електронних довірчих послуг Збройних сил України, Міністерства внутрішніх справ, Державної прикордонної служби, Державної податкової служби України, Національного банку України, Приватбанку, Укрсіббанку, Альфа банку тощо, включно по два технологічні центри сертифікації ключів для Центрального засвідчувального органу України та засвідчувального центру Національного банку України. Таким чином, розроблені програмно-технічні комплекси та апаратні засоби КЗІ створили безпечне пост-квантове довкілля для державних електронних інформаційних ресурсів.

732554 В
35

Теорія та практика державного управління [Текст] = Theory and Practice of Public Administration : зб. наук. пр. / Нац. акад. держ. упр. при Президентові України, Харк. регіон. ін-т держ. упр. - Харків : [Магістр], 2009 - .
Вип. 1 (72). - Харків, 2021. - 204 с. : граф., табл. - Бібліогр. наприкінці ст. - Текст кн. укр. та англ.

Зі змісту:

Котух Є. В. **Оцінка рівня захисту кіберпростору в публічному управлінні: національний та організаційний виміри.** – С. 31-39.
Проаналізовано сучасний стан та шляхи покращання кібербезпеки у сфері публічного управління на національному та організаційному рівнях, зокрема: збільшення бюджетного фінансування відповідної сфери, стратегічне інвестування в кібераналітику і хмарні технології, створення в організаціях спеціальних підрозділів з кіберзахисту, встановлення сучасного програмного забезпечення та його постійне оновлення, регулярне підвищення кваліфікації працівників, задіяних у питаннях захисту організаційної та персональної інформації.

731916 R
004

Технології виявлення та попередження кібератак [Текст] : лабораторний практикум для здоб. вищ. освіти ОС "Бакалавр" спец. 125 "Кібербезпека" спец. "Системи та технології кібербезпеки" / Національний авіаційний університет ; [А. О. Корченко, В. М. Гребенюк]. - Київ : [НАУ], 2021. - 48 с. : іл. - Бібліогр.: с. 46. - Уклад. зазнач. на звороті тит. арк.

Лабораторний практикум створено відповідно до програми курсу "Технології виявлення та попередження кібератак" та направлено на сприяння засвоєнню набутих знань, умінь і навичок, що формують управлінський профіль фахівця в області Кібербезпеки.

Ткач Ю. Модель захисту кіберпростору CyberSec / Ю. Ткач // Захист інформації. – 2020. – Т. 22, № 4. – С. 206-210.

Р/1428

У статті запропоновано модель захисту кіберпростору CyberSec, що орієнтована на виконання функції "кіберзахисту". Дана модель є функціональною, складається з п'яти етапів, об'єднує в собі низку методів і моделей, є циклічною, а тому дозволяє створити самоналагоджувану систему захисту у кіберпросторі.

Ткаченко В. DLP як захист від цифрових несунів / В. Ткаченко // Сети и бизнес: телекоммуникации и сети – технологии и рынок. – 2021. – № 1(116). – С. 102-107.

Р/1698

Системи запобігання витокам інформації пройшли шлях від захисту електронної пошти до хмар.

Усік В. Досвід розробки та впровадження кіберсистем : Військові кіберспеціалісти швидше виправляють слабкі місця та створюють кіберінструменти для виконання завдань **/** В. Усік // Оборонний вісник. – 2021. – № 9. – С. 17-19.

Р/1134

У Збройних Силах України на цей час відсутні повноцінні спроможності з розробки програмного забезпечення, оскільки у їх складі на сьогодні немає власних підрозділів "програмістів", що змушує звертатися до цивільних підрядників. Схожа ситуація спостерігається і у Збройних Силах деяких інших держав. Однак, у Кіберкомандуванні США є власний погляд на вирішення цієї проблеми.

Хорошко В. Виявлення та оцінювання кібератак в інформаційних мережах із випадковим моментом появи / В. Хорошко, М. Шелест, Ю. Ткач // Технічні науки і технології. – 2021. – № 1(23). – С. 96-102.

Р/1125

На основі ймовірнісної оцінки в роботі розкриті оптимальні, послідовні або близькі до них процедури, що дозволяють підвищити кібербезпеку інформації. Розв'язана задача, яка полягала в побудові оптимальної N-усіченої послідовної процедури спільного виявлення кібератак (КА) та оцінки моменту її появи при функції втрат. Проаналізована статистика, пов'язана з усередненим обсягом прогнозу (УОП). Запропоновано загальний вигляд оптимальної процедури послідовного виявлення-оцінювання КА з невідомим моментом появи при зазначених втратах.

Хорошко В. А. Методы распознавания кибератак с учетом мониторинга информационной среды / В. А. Хорошко, Н. Н. Браиловский // Безпека інформації. – 2021. – Т. 27, № 1. – С. 6-12. – Текст рос.

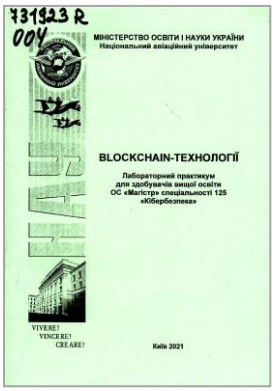
Р/1408

Під час написання даної роботи зроблена спроба викласти в певній логічній послідовності основні аналітичні методи розпізнавання кібернетичних атак в сучасних умовах кібернетичної війни з урахуванням моніторингу інформаційного середовища. Наведено перелік факторів, що підтверджують доцільність застосування методів розпізнавання образів для аналізу даних моніторингу атак. Крім того, розглянуті заходи подібності, які використовуються в алгоритмах ранжування і кластеризації кібератак. Показано, що доцільність їх застосування залежить від конкретних завдань.

Хорошко В. О. Концепція кібербезпеки та моделювання процесів оптимального управління системою кіберзахисту держави / В. О. Хорошко, Ю. Є. Хохлачова, І. В. Кібальчич // Інформатика та математичні методи в моделюванні. – 2020. – Т. 10, № 3-4. – С. 230-242.

Р/2357

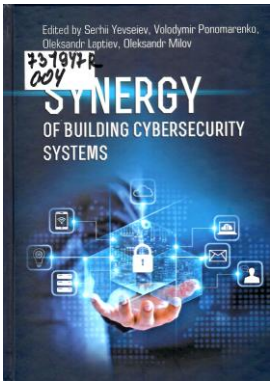
Запропоновано метод моделювання процесів оптимального управління розподіленими системами (якою і є система кібербезпеки держави) на основі системи одномірних диференціальних перетворень, які описують управління хвильовим процесом. Він дозволяє постійно контролювати та коригувати процес управління системою кібербезпеки держави, що дуже важливо щодо забезпечення загальної безпеки держави.



731923 R
004

Blockchain-технології [Текст] : лабораторний практикум для здоб. вищої освіти ОС "Магістр" спец. 125 "Кібербезпека" / Національний авіаційний університет ; [уклад. : С. П. Євсеєв, А. О. Корченко, В. М. Гребенюк]. - Київ : [НАУ], 2021. - 68 с. : рис., табл. - Бібліогр.: с. 62-63. -
Уклад. зазнач. на звороті тит. арк.

Лабораторний практикум створено відповідно до програми курсу "Blockchain-технології" та направлено на сприяння засвоєнню набутих знань, умінь і навичок, що формують управлінський профіль фахівця в області Кібербезпеки.



731947 R
004

Yevseiev, Serhii.
Synergy of building cybersecurity systems [Текст] : monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov. - Kharkiv : PC TECHNOLOGY CENTER, 2021. – 188 p. : рис., табл. - Бібліогр.: с. 165-175. - Текст кн. англ.

The monograph discusses the main types of models used in modeling the behavior of intelligent agents. The originality of the approach associated with the introduction into consideration of the concept of the contour of business processes as an integral object to be protected. The idea of the spatio-temporal structure of the model basis was proposed by the authors, that reflects not only the distribution of the set of models over the corresponding levels of the proposed methodology, but also sets the sequence of their interaction. The application of the developed models to ensure the protection of information and user data in social networks will allow a new look at existing social networks and create new social networks that will provide more reliable security of user data while maintaining usage parameters.