"Безпека та захист інформаційного простору "

(надходження І півріччя 2024)

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

Брацук І. Міжнародно-правове регулювання забезпечення інформаційної безпеки в рамках ООН / І. Брацук, С. Кавин // Вісник Київського національного університету імені Тараса Шевченка. Серія: Юридичні науки. – 2023.– № 1(125). – С. 21-26.

Р/1276

Стаття присвячена аналізу та вивченню правових механізмів ООН у сфері забезпечення інформаційної безпеки. Проаналізовано особливості функціонування інституційно-правового механізму інформаційного захисту в рамках координації ООН у контексті багатовекторної системи міжнародної безпеки та правового регулювання міжнародного співробітництва. Обґрунтовано доцільність розробки інтегрованої, скоординованої інформаційної політики міжнародних організацій та інституцій з метою уніфікації підходів до забезпечення інформаційної безпеки. Проведено узагальнення основних проблем, що виникають у міжнародному правовому регулюванні боротьби у сфері забезпечення інформаційної безпеки й основних загроз міжнародному миру в інформаційному просторі та запропоновано шляхи їхнього вирішення. Узагальнено принципи міжнародної інформаційної безпеки, виокремлено основні тенденції розвитку кіберзагроз у сучасному інформаційному просторі та заходи, необхідні для їх нейтралізації. Аналізуються особливості функціонування інституційно-правового механізму кіберзахисту в контексті законодавчої регламентації міжнародного співробітництва між міжнародними організаціями та інституціями. Зокрема, проведено аналіз основних механізмів правового забезпечення кіберзахисту інформаційного простору з метою їхньої інтеграції в єдину міжнародну систему правового інформаційного поля.

Глобенко С. Становлення й розвиток правового поля України щодо захисту інформаційного простору держави / С. Глобенко // Науковий вісник: Державне управління. – 2023. – № 2(14). – С. 64-79.

Р/1443

Наведено результати дослідження чинної нормативно-правової бази України, згідно з якою унормовано питання захисту інформаційного простору держави в умовах сьогодення. З'ясовано, що захист суверенітету, територіальної цілісності та національної безпеки є ключовими завданнями для будь-якої держави, у тому числі й України. Конкретизовано виклики й загрози у сферах інформаційної та кібербезпеки, зокрема щодо відсутності цілісної державної інформаційної політики. З'ясовано, що внаслідок своєї комплексності мають враховуватися різні аспекти життєдіяльності суспільства і держави, в тому числі економічні, енергетичні, інформаційні, кібернетичні, екологічні, продовольчі, охорони здоров'я, освіти та культури тощо. Зазначено про важливість дотримання моральних та етичних норм під час створення й поширення медійного контенту з урахуванням обмежень для захисту національної безпеки та інформаційної безпеки держави. Встановлено необхідність уніфікації норм чинного правового поля задля створення єдиного інформаційного простору для забезпечення безпеки інформаційної взаємодії та зміцнення національної системи стійкості.

Горліченко С. Особливості формування технічних каналів витоку інформації від сучасних ІКС / С. Горліченко // Безпека інформації. – 2023. – Т. 29, № 2. – С. 80-87.

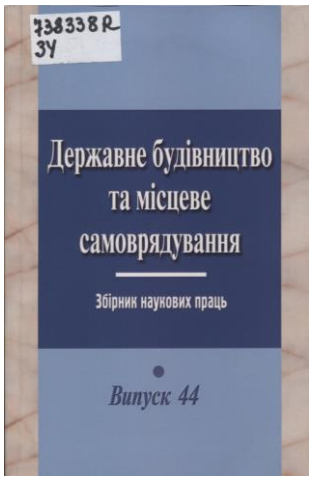
Р/1408

Інформаційно-комунікаційні системи постійно розвиваються і вдосконалюються, впроваджуючи нові технології і можливості. Однак, разом з стрімким розвитком з 'являється також і більша загроза безпеці інформації. Тому важливо вдосконалювати методи та алгоритми технічного захисту ІКС для забезпечення їх захищеності та безпеки. Було проведено аналіз різних підходів до визначення сутності терміну "витоки інформації", а також проведена систематизація інформації щодо класифікації технічних каналів, через які відбувається витік інформації. Вивчено сутність процесу формування технічних каналів витоку інформації, висвітлено різноманітні методи захисту інформації від таких витоків. Також ***було проаналізовано міжнародне та внутрішнє законодавство, яке регулює сферу захисту інформації, зокрема в Україні.*** Акцентовано увагу на важливості забезпечення безпеки інформації під час дії військового стану в Україні. В контексті сучасних викликів та загроз, пов'язаних з кібербезпекою, наголошено на необхідності зміцнення заходів захисту інформації, щоб забезпечити належний рівень захисту в умовах воєнного стану та потенційних загроз. Запропоновано подальший розгляд завдання щодо обґрунтування захищеності джерел конфіденційної інформації від витоку технічними каналами для всіх видів її аналого-цифрового перетворення, що реалізують сучасні ІКС, на основі заданих гранично допустимих ризиків інформаційної безпеки.

Дейнека О. Р. Дослідження проблем класифікації та безпечного зберігання даних / О. Р. Дейнека, О. І. Гарасимчук // Безпека інформації. – 2023. – Т. 29, № 3. – С. 147-153.

Р/1408

З розвитком технологій і ростом обсягів даних все більше постає проблема, як ці дані класифікувати та організувати їх безпечне зберігання. *Мета даної статті* полягає в ознайомленні з аналізом та потребами безпечного зберігання даних за наступними критеріями: обсяг даних, термін зберігання, доступність та швидкодія, безпека та конфіденційність. Технологічний прогрес, а також економічні чинники змінюють сучасні тенденції зберігання даних у напрямку хмарних рішень, а особливо у розподіленні між різними гравцями збереження даних із використанням хмарних рішень для пониження ризиків втрати. В даній статті ми проаналізували джерела загроз для великих даних, а саме кіберзлочини, соціальний інжиніринг, фізичні та внутрішні загрози, віруси та шкідливе програмне забезпечення. Проаналізовані основні принципи конфіденційності та безпечного зберігання великих обсягів даних.



738338 R
35

Державне будівництво та місцеве самоврядування [Текст] : збірник наук. праць / Нац. акад. правових наук України, НДІ держ. буд-ва та місцевого самоврядування. - Харків : Право.

Вип. 44. - Харків, 2023. - 428 с. - Бібліогр. наприкінці ст. Текст укр., англ. Дод. тит. арк. англ.

Зі змісту:

Мукомела І. В. **Кібернетичний тероризм як загроза національній безпеці в умовах війни Росії проти України.** – С. 316-327.

Стаття присвячена теоретико-правовому аналізу сутності кібернетичного тероризму в контексті російсько-української війни. Розкривається зміст поняття кібертероризму та його законодавче закріплення. Зосереджено увагу на трьох типах наступальних інформаційних операцій, які проводять кібертерористи в умовах війни Росії проти України. Висвітлено напрями протидії кібертероризму в Україні.

Науменко А. В. **Кібербезпека, як невід'ємний елемент сучасної державної політики України.** – С. 391-407.

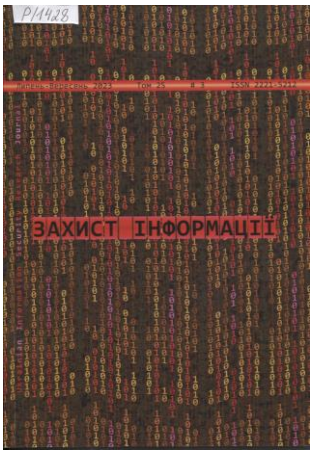
У статті проаналізовано поняття «кібербезпека» та досліджено національне та міжнародно-правове регулювання цієї сфери. Вказано основні напрями та цілі розвитку кіберсфери в Україні. Досліджено внутрішньодержавні інституції та міжнародні організації, що здійснюють та допомагають в реалізації політики кібербезпеки. Наведено міжнародний досвід, а саме досвід Естонії з реалізації та функціонування кіберзахисту, виділено корисні для України рекомендації. З'ясовано проблемні питання, що потребують вирішення для ефективного функціонування політики кібербезпеки в Україні.

Зубок В. Ю. Кібербезпека критичної інфраструктури в законодавстві України та в директиві (ЄС) 2022/2555 / В. Ю. Зубок, А. В. Давидюк, Т. М. Клименко // Електронне моделювання. – 2023. – Т. 45, № 5. – С. 54-66.

Р/518

Наведено галузі, сектори та основні критерії визначення критичних об'єктів, стан кібербезпеки яких підлягає особливому контролюванню, зокрема, з боку державних органів. Також представлено відомі світові підходи до визначення критичної інфраструктури та вимог до її кіберзахисту.

Проаналізовано основні положення Директиви (ЄС) 2022/2555, відомої як NIS2, її відмінності від попередньої директиви NIS. Показано класифікацію об'єктів з особливим контролем кібербезпеки, галузі та сектори, розширення відносно старих положень для порівняння з українським законодавством і практикою і для подальшої оцінки обсягів та напрямків робіт з гармонізації українських нормативно-правових актів з документами Європейського Союзу.



Курій Є. Розробка методології оцінки відповідності стандарту ISO 27001/ Є. Курій, В. Сусукайло, І. Опірський // Захист інформації. – 2023. – Т. 25, № 3. – С. 132-139.

Р/1428

Даний науковий документ пропонує розробку методології оцінки відповідності організацій новій версії стандарту ISO 27001, яка була представлена в кінці 2022 року.

Висока значущість інформаційної безпеки в сучасному світі вимагає від компаній адаптувати свої практики та політики до нових вимог стандарту. Автори аналізують останні дослідження у галузі впровадження стандарту ISO 27001 та недоліки релевантних матеріалів для оцінки відповідності.

Методологія включає аналіз нових вимог стандарту, порівняння їх із зіставленням існуючих практик організацій, визначення «гепів» (розривів / невідповідностей) між ними, розробку плану впровадження змін та моніторингу відповідності. Запропоновані рекомендації допоможуть організаціям забезпечити ефективний перехід на новий стандарт, мінімізувати ризики і зберегти високий рівень інформаційної безпеки. Ця методологія є актуальним інструментом для організацій, що прагнуть адаптувати свої практики і політики до нової версії стандарту ISO 27001 та підтримувати безпеку своєї інформації на високому рівні. Дана розробка враховує унікальні потреби організацій та сприяє їхньому успішному впровадженню нових практик і вимог інформаційної безпеки.

Ця стаття має на меті допомогти читачам зрозуміти складність та важливість проведення початкової оцінки на невідповідність перед впровадженням стандарту та висвітлити ефективність застосування детального чекліста під час проведення аналізу на невідповідності. Для підтримки дослідження був проведений детальний аналіз літератури та статей, що стосуються впровадження стандарту ISO 27001 в організаціях.

Механізми безпеки в хмарному середовищі на базі міжнародних стандартів / Л. В. Дакова, С. Ю. Даков, Н. В. Блаженний [та ін.] // Зв'язок. – 2022. – № 4(158). – С. 9-16.

Р/776

Удосконалено стандартизований функційний підхід до процедури оцінювання відповідності, ґрунтуючись на специфіці функціонування хмарних технологій. Здійснено огляд сучасних фреймворків, які використовуються для оцінювання та сертифікації надавачів хмарних послуг (НХП), щодо відповідності вимогам загальновизнаних стандартів безпеки.

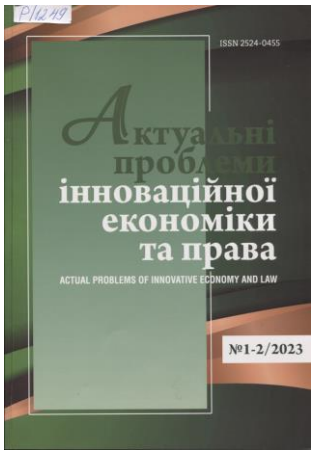
Запропоновані рівні гарантій передбачають розроблення особливих вимог стосовно забезпечення безпеки інформаційних систем НХП відповідно до класифікації критичності систем і даних потенційних споживачів хмарних послуг.

Керуючись нормативними актами, нормами міжнародних стандартів і вже розглянутими національними схемами з оцінювання кібербезпеки хмарних продуктів, сервісів і послуг, сформульовано узагальнений список вимог до безпеки надавачів хмарних послуг, який охоплює всі необхідні умови та відповідає запропонованим рівням гарантій.

Здійснено оцінювання відповідності стандартам безпеки, яке є відправною точкою для визначення політики інформаційної безпеки та боротьби із загрозами, що притаманні хмарним сервісам.

Запропоновано розподіл на три рівні гарантій безпеки, яким має відповідати НХП під час оцінювання відповідності залежно від бізнес-потреб користувачів і критичності даних, котрі обробляє та зберігає хмарна інформаційна система. Розроблено узагальнену схему вимог безпеки до НХП, побудовану на основі загальновідомих фреймворків, яка бере до уваги різнорівневий підхід до гарантій безпеки, розподілену відповідальність за дотримання перелічених вимог залежно від моделі функціонування і визначає компоненти архітектури хмари, що є чутливими до тих чи інших умов.

У статті поєднано всі найкращі стандарти Сполучених Штатів Америки та Європейського Союзу, а також найкращі практики безпеки для використання хмарного середовища, яке вважається найнебезпечнішим з погляду інформаційної безпеки, але зручним для використання.



Микитюк В. О. Нормативне регулювання захисту персональних даних як онлайн права кожної людини / В. О. Микитюк, С. О. Микитюк // Актуальні проблеми інноваційної економіки та права = Actual Problems of Innovative Economy and Law. – 2023. – № 1-2. – С. 94-99.

Р/1249

Правове регулювання онлайн прав людини є вимогою нової інформаційної ери і полягає у необхідності створення відповідних правових засобів – норм права, виражених у нормативних актах, що дозволяє правильно зрозуміти механізм їх правового регулювання, подолати труднощі їх захисту, реалізованості в офлайн середовищі. Зміна цінностей, стереотипів поведінки людини, зокрема і в онлайн просторі, призвели до необхідності підвищення рівня захисту персональних даних, вдосконалення механізму їх правового регулювання.

Правове регулювання персональних даних як онлайн права кожної людини полягає у їх упорядкуванні, організації та вдосконаленні положень шляхом створення, зміни, доповнення або скасування правових норм (нормативне регулювання), оскільки його здійснюють правотворчі органи у межах власної компетенції. Важливим аспектом такого нормативного регулювання є орієнтація на норми європейського права, які встановлюють загальні правила і стандарти захисту персональних даних, є зрозумілими і доступними як для організацій, що їх збирають і обробляють, так і для користувачів, а процес зберігання даних є доступним для перевірки з боку органів

контролю і нагляду. Поступово, з моменту нормативного закріплення захисту персональних даних як складової частини права на приватність, воно набуло фундаментального значення і отримало правове регулювання як важливого онлайн права кожної людини на рівні міжнародного законодавства (конвенції, регламент), так і національного (окремий закон). Але враховуючи положення проведеного дослідження все ще підлягають вирішенню окремі питання, такі як оновлення українського законодавства до європейських норм і стандартів, розповсюдження знань про необхідність захисту персональних даних, створення чітких правил онлайн захисту персональних даних для всіх суб'єктів, що залучаються до відповідного процесу.

Опірський І. Р. Дослідження безпеки стандарту Wi-Fi Protected Access 3 (WRA3) / І. Р. Опірський, Н. В. Максимів, М. В. Женчур // Безпека інформації. – 2023. – Т. 29, № 1. – С. 21-31.

Р/1408

Wi-Fi технологія є дуже актуальною у наш час, оскільки бездротовий зв'язок став необхідною складовою нашого повсякденного життя. Wi-Fi дозволяє підключатися до Інтернету на різних пристроях, таких як смартфони, планшети, ноутбуки, телевізори та інші. Крім того, Wi-Fi технологія постійно розвивається та вдосконалюється. Нові стандарти технології, такі як 802.11ax (Wi-Fi 6), дозволяють покращити швидкість передачі даних та забезпечити більшу стійкість до перешкод та інтерференції. Однак, разом з популярністю Wi-Fi технології з'являється також і більша загроза безпеці мережі. Тому важливо вдосконалювати безпекові методи та алгоритми шифрування Wi-Fi мережі для забезпечення її захищеності та безпеки.

Дослідження вразливостей протоколів бездротового зв'язку Wi-Fi WPA2 та WPA3 є дуже актуальним у зв'язку з тим, що бездротові мережі є незмінною складовою сучасного світу. Так як, хакерські атаки на бездротові мережі стали розповсюдженими, дослідження вразливостей WPA2 та WPA3 є дуже важливим для забезпечення безпеки мережі Wi-Fi. Адже, вразливості протоколів WPA2 та WPA3 можуть бути використані зловмисниками для отримання несанкціонованого доступу до мережі та отримання конфіденційної інформації, такої як паролі та дані користувачів. В цій статті буде розглянуто такі теми, як вразливості захисту WI-FI мереж за допомогою WPA2 та WPA3, основні засоби захисту від атак та порівняльна характеристика цих двох методів захисту.

737397 R
621.39

Планування та електромагнітна сумісність в безпроводових інфокомунікаціях [Текст] : навч. посіб. для здобувачів ступеня бакалавра за спец. 172 "Телекомунікації та радіотехніка" / [Ільченко М. Ю., Наритник Т. М., Капштик С. В. та ін.] ; відп. ред. Правило В. В. ; Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського". - Київ : КПІ ім. І. Сікорського, [Вид-во "Політехніка"], 2023. - 348 с. : граф., табл., фот. - Бібліогр.: с. 346-347. Авт. зазнач. на звороті тит. арк. та с. 348.

Описано головні принципи та методи управління використанням радіочастотного спектру, забезпечення електромагнітної сумісності у безпроводових системах, що використовують різні діапазони частот.

Наведено основні формули для розрахунку показників електромагнітної сумісності різноманітних систем та мереж радіозв’язку.

Посібник ґрунтується на нормативних документах Міжнародного союзу електрозв’язку в галузі використання радіочастотного ресурсу, міжнародних та національних нормативних документах.

Савченко В. А. Забезпечення стійкості кібероборони держави в умовах збройного конфлікту / В. А. Савченко // Сучасний захист інформації. – 2023. – № 3(55). – С. 6-11.

P/2300

Стаття присвячена проблемі стійкості кібероборони національної безпеки в контексті сучасних збройних конфліктів.

У роботі розглядаються ключові аспекти, які становлять загрозу для кібербезпеки держави, включаючи кібератаки, кібершпигунство і кіберсаботаж.

Стаття аналізує необхідність розвитку кіберінфраструктури, підготовки кадрів та кризового плану для відновлення після кібератаки. Також розглядається роль державних інституцій у забезпеченні кібербезпеки, включаючи розробку нормативного регулювання і співпрацю з приватним сектором та академічними установами. Крім того, стаття висвітлює міжнародний аспект стійкості кібероборони і важливість співпраці між державами та дотримання міжнародних норм і правил у кіберпросторі.

Робота закінчується висновками щодо важливості спільних зусиль національних та міжнародних громадських структур для забезпечення сталої кібербезпеки в умовах збройних конфліктів.

Толюпа С. Формування системи кіберзахисту для інтегрованої галузевої інформаційної системи України сектору національної кібербезпеки / С. Толюпа, Л. Сліпачук // Безпека інформаційних систем і технологій. – 2023. – № 1(6). – С. 37-42.

P/1227

Розкрито та висвітлено передбачений склад, структуру заходів і засобів, які увійдуть до комплексної системи захисту інтегрованої галузевої інформаційної системи України (ІГІСУ) сектору національної кібербезпеки. Описано специфіку і стратегічну цінність залучених ресурсів, якими оперуватиме створена система кіберзахисту.

Зазначено, що система кіберзахисту ІГІСУ передбачає задіяти комплекс взаємопов'язаних засобів і заходів, виконання яких необхідне й достатнє для повноцінного захисту ІГІСУ, для протистояння зовнішнім несанкціонованим системам доступу (НСД) тощо.

Акцентовано увагу на відповідності передбаченої системи кіберзахисту міжнародним критеріям і стандартам захисту подібних керівних систем для країн НАТО, зокрема і кібербезпековому стандарту міністерства оборони США (TCSEC – "Помаранчева книга"); міжнародним критеріям і стандартам захисту подібних керівних систем інших провідних країн світу, зокрема, міжнародному технічному стандарту ISO/IEC 15408 "Загальні критерії оцінювання безпеки ІТ", який ратифікувало багато країн; настановам і рекомендаціям міжнародної організації NCSS (National Cyber Security Strategies) для країн – партнерів НАТО, що передбачені Стратегією національної кібербезпеки та розроблені міжнародними експертами з питань національної кібербезпеки, науковцями та європейськими радниками з міжнародної кібербезпеки в контексті проекту Програма НА ТО SPS "Наука заради миру та безпеки"; національним технічним стандартам України.

У межах цієї статті детально показано повний асортимент загальнообов'язкових ресурсів та інструментів, які передбачені для забезпечення кібербезпеки спроектованої ІГІСУ сектору національної кібербезпеки, та які включають п'ять рівнів кіберзахисту (організаційний, програмний, апаратно-технічний, інженерно-технічний, додатковий фізичний).

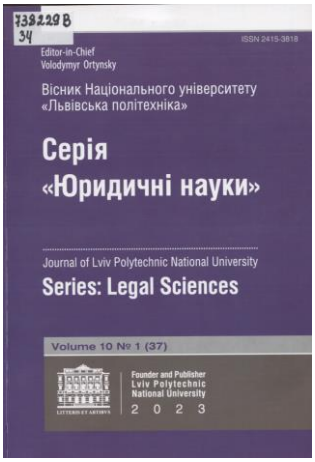
737730 В
32

Харківський національний університет імені В. Н. Каразіна.
Вісник Харківського національного університету імені В. Н. Каразіна [Текст] / [зб. наук. пр.]. - Харків : [ХНУ ім. В. Н. Каразіна]. - (Питання політології).
№ 39. - Харків, 2021. - 138 с. - Бібліогр. наприкінці ст. Текст укр., рос. та англ.

Зі змісту:

Зінченко О. І. **Європейська регіональна система протидії кібертероризму: політичні, інституційні та правові механізми**. – С. 118-122.

Розглянуто сучасний етап розвитку кібертероризму в Європі. Прогресуванню цього явища сприяє мережа «Інтернет», яка має суттєвий вплив на всі сфери суспільного життя, надаючи величезну кількість інформації будь-якому користувачеві та заохочуючи висвітлення такої інформації та її поширення. Виявлено фактори, що ускладнюють процес протистояння кібертероризму, доведено, що сучасний кібертероризм є складовою частиною гібридних воєн і одним із дієвих важелів досягнення політичних цілей на міжнародній арені. Розкрито політичні, інституційні та правові механізми протидії кібертероризму в європейській регіональній системі кібербезпеки. Показуються способи та методи здійснення кібератак, а також можливості європейської регіональної системи протидії їм. Ця проблема висвітлюється на міжнародному рівні, вказуються документи, які передбачають методи протидії. Розглядається досвід передових країн у боротьбі із кібертероризмом. Зазначається, що особливістю кібертероризму є прагнення атакуючих зробити ефектний терористичний акт не тільки з небезпечними наслідками для інфраструктури та населення, а й зі значним суспільним резонансом. Однак кіберзлочинці постійно вдосконалюють свою діяльність, з'являються все нові форми вчинення тероризму в мережі Інтернет, нові способи залякування населення, нові методи впливу на свідомість людей. Разом із тим і структура кіберзлочинності помітно різниться в різних країнах залежно від характеру і ступеня розвитку в них інформаційних технологій, поширення мережі Інтернет, використання електронних сервісів і електронної комерції. Зазначене зумовлює необхідність постійного оновлення, вдосконалення та коригування чинного антитерористичного національного, регіонального і міжнародного законодавства.



738229 В
34

Юридичні науки [Текст] : зб. наук. пр. Vol. 10 № 1 (37) / відповідальний ред. Ортинський Володимир Львович. - Львів : Вид-во Львів. політехніки, 2023. - 304 р. : граф. - (Вісник Національного університету "Львівська політехніка" : наук. журнал / Національний університет "Львівська політехніка"). - Бібліогр. наприкінці ст. Текст кн. укр. та англ.

Зі змісту:

Крикавська І. **Нормативно-інституційне забезпечення цифровізації та кібербезпеки системи державного управління в ЄС.** – С. 148-152. – Текст англ.

Зауважено, що на сучасному етапі Інтернет є інструментом, який використовується в багатьох видах діяльності, особливо в системі державного управління, що збільшує можливість посягань у кіберпросторі та зростання ризиків, що з цим пов'язані. Розглянено нормативно-правове та інституційне забезпечення цифровізації та кібербезпеки системи державного управління в ЄС. Досліджено семантичне наповнення термінів "діджиталізація", "кібербезпека" та "е-урядування".

Присвячено увагу сферам цифровізації та кібербезпеки в урядуванні ЄС. Проаналізовано показники Індексу цифрової економіки та суспільства, нормативну основу роботи Агентства Європейського Союзу з кібербезпеки.

Програмні системи захисту інформації

Андрощук А. В. Захист від DDOS-атак на мовах програмування Java та C# / А. В. Андрощук // Технології та інжиніринг. – 2023. – № 3(14). – С. 9-14.

P/1733

Мета. Проаналізувати і порівняти можливості кіберзахисту у Java та C# та визначити переваги та недоліки кожної мови з точки зору безпеки програмного забезпечення.
Методика. В основу розробки системи ефективних засобів кіберзахисту було покладено основні механізми кіберзахисту, доступні у мовах програмування Java та C#, такі як виключення, контроль доступу, шифрування даних та перевірка вводу.
Результати. В ході дослідження було проведено аналіз загроз та вразливостей, що стосуються програм, написаних на мовах програмування Java та C#. Було виявлено, що такі загрози, як ін'єкція SQL-запитів, вразливості XSS (міжсайтовий скриптінг), вразливості переповнення буфера та інші, можуть становити серйозну загрозу для безпеки програмного забезпечення.

Для захисту програм від цих загроз було розглянуто основні механізми кіберзахисту, доступні у мовах програмування Java та C#. Серед них були виокремлені виключення, контроль доступу, шифрування даних та перевірка вводу. Ці механізми можуть бути використані для запобігання різним видам атак та злому програмного забезпечення.

Порівняно можливості кіберзахисту у Java та C# та визначено переваги та недоліки кожної мови з точки зору безпеки програмного забезпечення.

Зроблено висновки про важливість кіберзахисту на мовах програмування Java та C# та надано рекомендації для розробників програмного забезпечення стосовно свідомого підходу до кіберзахисту та використання відповідних методів та технік для забезпечення безпеки своїх програм.

Говорущенко Т. Інформаційна технологія прогнозування рівня якості програмного забезпечення / Т. Говорущенко, Ю. Войчур, Д. Медзатий // Радіоелектронні і комп'ютерні системи. – 2023. – № 3(107). – С. 238-254. – Текст англ.

P/1769

Метою даного дослідження є розв'язання цієї задачі шляхом розроблення інформаційної технології прогнозування рівня якості програмного забезпечення на основі вимог. Запропонована інформаційна технологія прогнозування рівня якості програмного забезпечення на основі вимог забезпечує аналіз атрибутів якості у вимогах, відображає залежність характеристик якості від атрибутів, формує кількісну оцінку характеристик якості, відображає залежність якості від її характеристик, формує кількісну оцінку якості, виконує прогнозування рівня якості, надає всі перераховані сервіси одночасно, в комплексі, а модель, методи та засіб, які лежать в основі ІТ, належать до спільних методологічних підходів та інтегруються між собою, тобто задовольняє всі вісім визначених критеріїв одночасно. Запропонована система прогнозування рівня якості програмного забезпечення на основі вимог є засобом розробленої інформаційної технології прогнозування рівня якості програмного забезпечення на основі вимог, який забезпечує аналіз вимог, на основі якого надає користувачу прогнозовані оцінки восьми характеристик якості ПЗ, геометричну інтерпретацію значень характеристик якості ПЗ, комплексний показник прогнозованої якості ПЗ та висновок про рівень якості майбутнього ПЗ, на основі якого можна виконати порівняння наборів вимог до ПЗ та обґрунтований вибір набору вимог для подальшої реалізації. Розроблені у

статті інформаційна технологія прогнозування рівня якості програмного забезпечення на основі вимог та система прогнозування рівня якості програмного забезпечення на основі вимог забезпечують можливість порівняння наборів вимог до ПЗ, обґрунтованого вибору вимог для подальшої реалізації якісного ПЗ (як показали експерименти, це лише один з чотирьох пропонованих наборів), а також відмови або доопрацювання невдалих наборів вимог, за якими неможливо розробити якісне ПЗ.

738194 R
51

Кривий, Сергій Лук'янович.
Вступ до математичних основ захисту інформації [Текст] : навч. посіб. / С. Л. Кривий ; Київський нац. ун-т імені Тараса Шевченка. - [Київ] : ВПЦ Київський університет, 2022. - 352 с. : рис., табл.

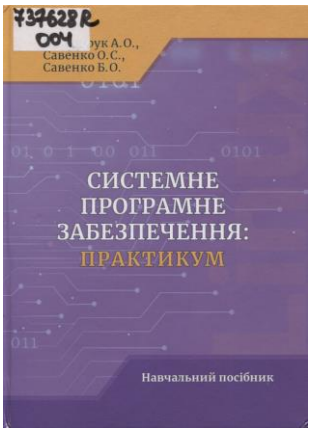
Розглянуто основні математичні поняття, на базі яких будують криптографічні системи: основи теорії складності обчислень, алгебраїчні структури (групи, кільця, поля), елементи теорії чисел, теоретико-числові функції та алгоритми їхнього обчислення, елементи теорії імовірностей та інформації. Описано класичні системи обміну ключами, електронного підпису та взаємної автентифікації, а також симетричні й асиметричні криптографічні системи (класичні й сучасні). Подано прості способи генерації випадкових чисел.

738018 R
004

"Моделювання і комп'ютерна графіка" [Текст] : зб. матер. Восьмої міжнар. наук.-техн. конф., 11-14 квітня 2023 р. : присвяч. 100-річчю з дня народження Льва Петровича Фельдмана / ДВНЗ "Донец. нац. техн. ун-т", Ін-т проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Вінниц. нац. техн. ун-т, Штутгартський ун-т (м. Штутгарт, ФРН) [та ін.]. - Луцьк ; Київ : ДВНЗ "ДонНТУ", 2023. - 199 с. : граф., рис., табл. - Текст кн. укр. та англ. мов. - Бібліогр. наприкінці ст.

Зі змісту:

Гільгурт С. Я. **Оперування наборами патернів баз даних сигнатур реконфігуровних систем захисту інформації.** – С. 56-60.
Розглянуто формалізований опис набору патернів баз даних сигнатур, що дозволяє ефективно оперувати технічними характеристиками сигнатурних систем технічного захисту інформації на базі ПЛІС, таких як системи виявлення вторгнень. Запропоновано відповідну техніку впорядкування патернів в наборі.



737628 R
004

Нічепорук, Андрій Олександрович.
Системне програмне забезпечення: практикум [Текст] : навч. посібник / Нічепорук А. О., Савенко О. С., Савенко Б. О. - Хмельницький : [ХНУ], 2023. - 168 с. : рис., табл. - Бібліогр.: с. 164-166 (41 назва).

Розглянуті способи та методи практичної реалізації основних механізмів взаємодії і синхронізації між процесами в операційній системі Linux.

Принцип і метод синтезу систем обману для виявлення зловмисного програмного забезпечення і комп'ютерних атак / А. Каштальян, С. Лисенко, Б. Савенко [та ін.] // Радіоелектронні і комп'ютерні системи = Radioelectronic and Computer Systems. – 2023. – № 4(108). – С. 112-151. – Текст англ.

Р/1769

Об’єктом дослідження в роботі є системи обману. Результати цієї роботи розвивають елементи теорії та практики створення таких систем.

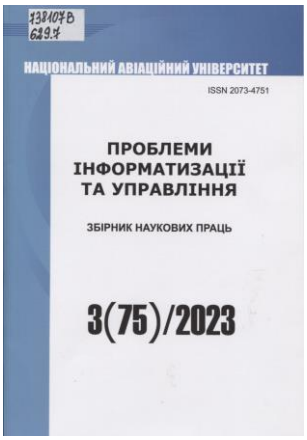
Особливе місце серед засобів виявлення та протидії зловмисному програмному забезпеченню та комп’ютерним атакам займають системи обману. Ці системи заплутують зловмисників, але теж потребують постійних змін та оновлень, оскільки з часом особливості їх функціонування стають відомими.

Тому, актуальною є проблема створення систем обману, функціонування яких залишалось би незрозумілим для зловмисників.

Для вирішення цієї проблеми в роботі пропонується новий принцип синтезу таких систем. Оскільки формування таких систем буде на базі комп’ютерних станцій корпоративної мережі, тоді систему позиціоновано як мультикомп’ютерну.

В системі запропоновано використовувати комбіновані приманки та пастки для створення хибних об’єктів атак. Всі компоненти такої системи формують тіньову комп’ютерну мережу. В роботі розроблено принцип синтезу мультикомп’ютерних систем з комбінованими приманками і пастками та контролером прийняття рішень для виявлення та протидії зловмисному програмному забезпеченню та комп’ютерних атакам.

738107 В
629.7



Проблеми інформатизації та управління [Текст] : зб. наук. пр. / Нац. авіац. ун-т, Ф-т комп'ютерних наук та технологій. - Київ : [НАУ].

Вип. 3(75). - Київ, 2023. - 100 с. : іл., табл. - Бібліогр. наприкінці ст. Текст кн. укр., англ.

Зі змісту:

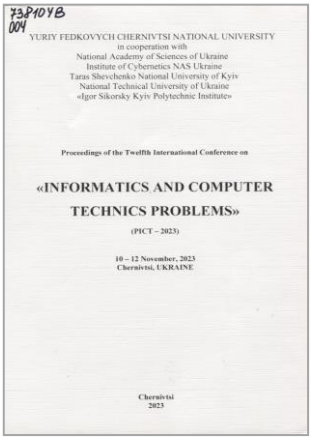
Гнатюк С. О., Бердибаєв Р. Ш., Богун А. М, Сидоренко В. М., Положенцев А. А., Жигаревич О. К. **Інтеграційна шина даних для ефективного функціонування системи управління подіями інформаційної безпеки.** – С. 29-40.

Кількість кіберзагроз у сфері ІКТ постійно збільшується, тому розробка нових засобів для забезпечення безпеки є дуже важливим і актуальним науковим завданням.

Серед таких засобів варто відзначити SIEM системи, які спрямовані на аналіз подій та управління інцидентами з метою запобігання негативним наслідкам та зменшення шкоди від кіберзагроз для користувачів.

У попередніх дослідженнях автори провели аналіз існуючих SIEM систем та типів баз даних для них, а також розробили нову архітектуру хмарної SIEM системи.

Наступним кроком є дослідження Enterprise Service Bus (ESB). У статті було визначено роль ESB у концепції архітектури Service-Oriented Architecture (SOA), визначені її функції та переваги. Також автори проаналізували найпопулярніші сучасні рішення ESB та надали рекомендації щодо впровадження розвиненої SIEM системи на об'єктах критичної інфраструктури. Розроблений ESB компонент для ефективного функціонування SIEM систем на об'єктах КІ забезпечить цілу низку переваг, такі як широкий спектр роз'ємів і масштабованість рішення, гнучка маршрутизація даних, гарантована доставка інформаційних повідомлень, організація захищеного каналу передачі, централізоване управління, можливість моніторингу та діагностики стану передачі, а також можливість інтеграції зі сторонніми чергами повідомлень. Крім того, у дослідженні було сформовано специфікацію для SIEM системи в критичній інфраструктурі.



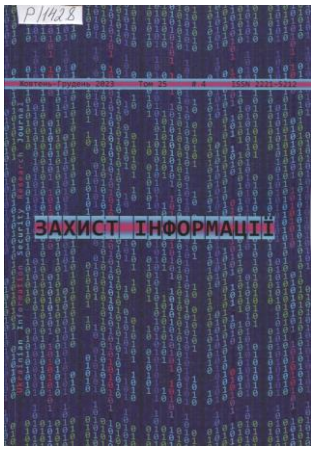
738104 В
004

Проблеми інформатики та комп'ютерної техніки (ПІКТ-2023) [Текст] = Informatics and Computer Technics Problems (PICT-2023) : праці XII Міжнародної науково-практичної конференції, Чернівці, 10-12 листопада, 2023 / Ін-т кібернетики імені В. М. Глушкова НАН України, Київ. нац. ун-т імені Тараса Шевченка, Нац. техн. ун-т України "КПІ імені Ігоря Сікорського", Чернівецький нац. ун-т імені Юрія Федьковича. - Чернівці : [ЧНУ], 2023. - 200 с. : іл., табл. - Загол. обкл. : Proceedings of the Twelfth International Conference on "Informatics and computer technics problems". - Бібліогр. наприкінці ст. Текст укр., англ. Обкл. англ.

Зі змісту:

Олар О. Я., Никифорюк А. М. **Плагін для захисту користувацьких даних у веб-браузерах.** – С. 53-55.

Розроблено плагін для захисту користувацький даних у веб-браузерах, який доповнює можливості та функції веб-браузера. Запропонований плагін додає новий та покращує наявний функціонал на вебсайтах. Забезпечені різні види захисту даних, включаючи блокування різноманітних технологій, які дозволяють сайтам відстежувати дії користувачів та ідентифікувати їх, захист від відстеження, маскування передавання даних, збереження конфіденційності та приватності тощо. Для забезпечення стабільної та надійної роботи плагіна виконано тестування плагіну в різних браузерах.



Програмне забезпечення щодо кіберзахисту держави від кібератак / Н. Блавацька, М. Браіловський, В. Козюра, В. Хорошко // Захист інформації. – 2023. – Т. 25, № 4. – С. 184-191.

Р/1428

Захист об'єктів критичної інфраструктури держави від кібератак, тим більше в умовах бойових дій, вимагає від державних органів вжити ефективних заходів кіберзахисту. В основі таких заходів лежить розробка державних цільових програм кіберзахисту. При формуванні вимог до сучасних систем кіберзахисту необхідно вирішити ряд завдань, до основних з яких відносяться визначення характеристик впливу кібератак на системи кіберзахисту, кількісних показників ефективності систем захисту реалізації кіберзагроз та оптимального розподілу обмежених ресурсів на реалізацію ефективного кіберзахисту.

На основі модифікації відомих методів цільової оцінки альтернатив у роботі розробляється метод підтримки прийняття рішень при формуванні комплексних цільових програм кіберзахисту об'єктів критичної інфраструктури в умовах реалізації противником кібератак, різних загроз та ризиків.

Основна ідея запропонованого підходу до аналізу впливу кібератак при виконанні програми з кіберзахисту є у тому, що події, які сприяють кібератакам, розглядаються як складова частина системи кіберзахисту, тобто як вплив зовнішнього середовища. Тому такі моделі кібератак включають у ієрархію цілей програми кіберзахисту, установлюються їх зв’язки з іншими системами та цілями державних цільових програм. Ефективність таких програм оцінюється при умові наявності кібератак з урахуванням їх ймовірних характеристик. Запропоновані моделі кібератак та ризиків. Моделлю кібератаки є проект програми, що включається у ієрархію цілей комплексної програми, яка описується степенем та вірогідністю реалізації. Модель ризика будується з двох компонентів: фактора ризика, який описується випадковим процесом, та деякою фіктивною ціллю – індикатором ризику.

Тестування захищеності сучасних інформаційних систем: вибір ефективних методів та сценаріїв для різних об'єктів тестування / С. В. Легомінова, Д. І. Рабчун, Р. І. Драгунцов, М. М. Запорожченко // Сучасний захист інформації. – 2023. – № 4(56). – С. 84-90.

Р/2300

Сучасні виклики у сфері кібербезпеки вимагають глибокого розуміння та ефективного застосування різних видів тестування захищеності. Тестування захищеності, як один із основних елементів стратегії кібербезпеки, вимагає систематичного підходу та вибору оптимальних сценаріїв тестування відповідно до конкретних потреб та особливостей ІТ інфраструктури організації. З ростом різноманітності кіберзагроз і технік атак, важливо розглядати та порівнювати різні види тестування захищеності для визначення їх ефективності у різних сценаріях. *Метою статті* є розробка рекомендацій для фахівців із кібербезпеки щодо вибору ефективних методів оцінювання рівня захисту, шляхом використання різних сценаріїв тестування захищеності ІТ інфраструктури. У статті виконано аналіз та класифікацію різних видів тестування захищеності з метою вибору найефективніших методів та сценаріїв для різних систем. Розроблено матрицю вибору, яка допомагає систематизувати процес вибору методів та сценаріїв тестування відповідно до конкретних об'єктів тестування. Кожен об'єкт має свої особливості та формує відповідні вимоги до тестування, і вибір методів повинен бути адаптований до цих унікальних аспектів для забезпечення максимальної ефективності заходів безпеки. Застосування відповідних методів, таких як сканування вразливостей, пентест, аналіз вразливостей, Red teaming та соціально-інженерне тестування, у поєднанні з конкретними сценаріями, дозволяє ефективно виявляти та усувати недоліки та вразливості ІТ інфраструктури та її компонентів. На основі виконаного аналізу, надаються практичні рекомендації щодо вибору оптимальних стратегій для конкретних сценаріїв тестування.

Толюпа С. Математична модель взаємовідносин системи керування інформаційною безпекою / С. Толюпа, С. Штаненко // Безпека інформаційних систем і технологій. – 2023. – № 1(6). – С. 28-36.

Р/1227

Результативне розв'язання задач аналізу і синтезу систем керування інформаційною безпекою не можна забезпечити одними лише способами простого опису їхньої поведінки в різних умовах – системотехніка виявила проблеми, які потребують кількісного оцінювання характеристик. Ті дані, що отримані експериментально або шляхом математичного моделювання, повинні розкривати властивості систем керування інформаційною безпекою. Основним у них є ефективність, під якою розуміють ступінь відповідності результатів захисту інформації поставленій меті. Остання, залежно від наявних ресурсів, знань розробників та інших факторів, може бути досягнута тією або іншою мірою, причому можливі альтернативні шляхи її реалізації. У ряді публікацій авторами запропоновано основи категорійного апарату теорії множин, які дозволяють пояснити процес взаємовідносин множин загроз і множин системи захисту інформації, що дозволяє будувати різні математичні моделі з метою аналізу систем інформаційного обміну в системах критичного застосування. Нині створення систем керування інформаційною безпекою неможливе без дослідження й узагальнення світового досвіду побудови інформаційних систем та їхніх складових підсистем, одними з ключових серед яких є системи захисту інформації та протидії вторгненням в інформаційну систему. Складовими математичного забезпечення таких систем є моделі процесів нападу на механізми захисту та блокування або знищення самих кіберзагроз. Базою таких моделей є математичний апарат, який має забезпечити адекватність моделювання процесів захисту інформації за будь-яких умов впливу кіберзагроз. Під час визначення математичного апарату необхідно чітко розуміти, як будуються ті або інші множини кіберзагроз та як здійснюються взаємовідносини самих множин кіберзагроз, множин елементів системи захисту та множин систем виявлення кібератак, які мають контролювати правильність роботи процесу захисту інформації. У статті проаналізовано різні варіанти побудови моделей системи керування інформаційною безпекою та створено математичну модель, яка враховує внутрішні взаємозв'язки різних підмножин складових системи захисту інформації за впливу кіберзагроз.

Телекомунікаційні мережі та інформаційно-комунікаційні технології

Аналіз загроз мережевого трафіку рівнів моделі OSI для динамічного розрахунку RTO в контексті боротьби з DDoS атаками / Г. І. Гайдур, С. О. Гахов, М. В. Сич, В. Є. Дмітрієв // Телекомунікаційні та інформаційні технології. – 2023. – № 3(80). – С. 12-21.

P/1921

В статті проведено огляд актуальних загроз мережевої безпеки, з точки зору аналізу мережевого трафіку на різних рівнях моделі OSI. Розглянуто різновиди атак розподіленої відмови в обслуговуванні (DDoS) та їх вплив на протокол керування передачею (TCP), зокрема, на важливий параметр – час очікування повторної передачі (RTO). Розкрито основні алгоритми та методи розрахунку RTO, включаючи адаптивні стратегії з залученням машинного навчання та штучного інтелекту для оптимізації стека TCP/IP.

Зокрема, надано інформацію щодо роботи алгоритму розрахунку RTO, який є важливим для надійності передачі даних через TCP. Описано, як цей алгоритм адаптивно змінює значення RTO в залежності від стану мережі та вимірюваних значень RTT (часу проходження всього шляху). Також наведено формули, які використовуються для розрахунку RTO з різними параметрами.

Додатково, розглянуто можливості використання методів машинного навчання та аналізу даних для виявлення та запобігання DDoS атак. Пояснено, як сучасні технології дозволяють використовувати ці методи для мінімізації хибно позитивних виявлень шкідливих пакетів трафіку та підвищення ефективності захисту інформаційних систем.

Приведено приклад програмних та апаратних засобів, що використовуються для практичної реалізації алгоритмів в пристроях передачі даних по Ethernt підключенню.

Дана робота дає уявлення про сучасні проблеми та виклики, які існують в сфері захисту мережевої безпеки в умовах зростаючого числа DDoS атак.

Аналіз факторів уразливості технології WEB 3.0 / О. В. Вишнівський, О. В. Зінченко, Ю. І. Катков [та ін.] // Наукові записки Державного університету телекомунікацій. – 2023. – № 2(4). – С. 73-84.

P/872

Стаття присвячена критичним аспектам під час впровадження технології Web-3.0. Ставиться завдання: на основі аналізу впровадження технології Web-3.0 для вирішення множини завдань, а саме: децентралізації на основі блокчейну; створення загальної доступності; підвищення довіри сайтам; підвищення безпеки персональної інформації від хакерів; забезпечення справжній власності на інформацію авторів; відсутність цензури; поліпшення соціальної взаємодії; використання інтернет речей сумісно з віртуальною або доповненою реальністю; застосовування штучного інтелекту – розглянути експлойт нульового дня для Web-3.0. Експлойт нульового дня показує, що постачальник або розробник щойно дізналися про уразливість і вони мають «нуль днів» її виправлення. Атака нульового дня відбувається внаслідок використання зловмисниками уразливості (критичних місць) до того, як розробникам вдалося її виправити. Для вирішення цього завдання в статті: зроблено опис основних відмінностей архітектури побудови Web-3.0 від Web-2.0; виконаний аналіз завдань Oprah Winfrey Network архітектури Web-3.0; розглянуто можливості: зовнішнього інтерфейсу (дизайн та інтерфейс веб-програм), серверної частини (ґрунтується на децентралізованих технологіях, насамперед, dApp, яка використовує переваги блокчейна: прозорість, надійність та незмінність даних), бази даних (зберігає дані про користувачів, їх повідомлення, теги та коментарі); виконано аналіз можливих загроз та уразливості внаслідок впровадження технології Web-3.0 до початку експлойту нульового дня.

На основі виконаного аналізу робляться висновки: що уразливість пов’язана з масштабованістю, обмеженою пропускною спроможністю транзакцій та обчислювальної потужності, безпекою, складністю, сумісністю; що Web-3.0 створює багато умов, які можуть бути корисні людям, але впровадження нових можливостей Web-3.0 призводить до появи нових загроз або уразливості, які можуть бути використані зловмисниками для нанесення шкоди людям. Це вимагає розглянути можливий вплив загроз, визначити можливі уразливості в технології Web-3.0 до початку експлойту нульового дня, тобто вимагає необхідність дослідження можливості появи нових уразливих місць.

Бабенко Т. Інтелектуальна модель класифікації мережних подій із кібербезпеки / Т. Бабенко, А. Бігдан, Л. Мирутенко // Безпека інформаційних систем і технологій. – 2023. – № 1(6). – С. 61-69.

Р/1227

Через збільшену складність сучасних комп'ютерних атак, виникає потреба у фахівцях із безпеки не тільки для виявлення шкідливої активності, але і для визначення відповідних кроків, які проходитиме зловмисник у ході виконання атаки. Незважаючи на те, що виявлення експлойтів і вразливостей зростає з кожним днем, розроблення методів захисту просувається помітно повільніше за розроблення методів нападу. Саме тому це все ще залишається відкритою дослідницькою проблемою.

У цій статті представляємо дослідження у галузі ідентифікації мережних атак із використанням нейронних мереж, зокрема багатошарового персептрона Румельхарта, для виявлення та прогнозування майбутніх подій мережної безпеки на основі попередніх спостережень.

Для забезпечення якості процесу навчання й отримання бажаного узагальнення моделі використано 4 млн записів, накопичених протягом 7 днів Канадським інститутом кібербезпеки. Наш результат демонструє, що моделі нейронних мереж, що базуються на багатошаровому персептроні, можуть використовуватися після уточнення для виявлення та прогнозування подій мережної безпеки.

Вахула О. Дослідження проблематики безпеки в хмарних середовищах та вирішення з застосуванням підходу "безпека як код" / О. Вахула, І. Опірський // Захист інформації. – 2023. – Т. 25, № 3. – С. 113-122.

Р/1428

‘‘Безпека як код”– це підхід організації безпеки в хмарних середовищах, який полягає на методі інтеграції контролів безпеки, політик та кращих практик безпосередньо в процеси розробки та розгортання програмного забезпечення. Процес інтеграції включає трансформацію вимог безпеки та конфігурацій в програмний код, який в свою чергу вважається невід’ємною частиною повного життєвого циклу розробки програмного забезпечення. Вбудовуванням мір безпеки в код, скріпти, шаблони та автоматизовані робочі процеси, організація забезпечує, що є чітко визначені контролі безпеки, які консистентно та примусово будуть застосовані на всіх операційних фазах створення програмного забезпечення (розробка, тестування, впровадження, підтримка).

В даній статті розглянуто основні проблеми побудови безпеки в хмарних середовищах та їх причини, також розглядає складові та принципи підходу ‘‘Безпека як код”, приклад реалізації з поясненням, переваги даного підходу, а також роль DevSecOps. Ця стаття має на меті допомогти читачам зрозуміти важливість підходу ‘‘Безпека як код”, як одного з найефективніших методів організації безпеки в хмарних середовищах. Так, як хмарні середовища продовжують розвиватися та поширюватися, а загрози стають все більш складними, підхід ‘‘Безпека як код” являє собою основну стратегію для проактивного захисту цифрових активів. Ця публікація слугує посібником для розуміння, впровадження та отримання переваг від підходу ‘‘Безпеки як код”, надаючи уявлення про майбутній ландшафт безпеки хмарних середовищ та важливу роль автоматизації та інтеграції у вирішенні сучасних викликів безпеки. Для підтримки дослідження було проведена широкий аналіз літератури та статей, які надають інформацію про підхід ‘‘Безпека як код” та його застосування.

Визначення ступеня захищеності інформації в соціальних мережах в залежності від профілю зв'язків між абонентами / В. М. Ахрамович, С. Г. Чупрун, О. Р. Стефурак, Р. В. Придибайло // Сучасний захист інформації. – 2023. – № 4(56). – С. 22-32.

Р/2300

Ще до виникнення соціальних мереж було з'ясовано який вплив дають особі оточуючі її люди. При цьому було визначено, що дуже часто найбільш корисним для особи є не близьке оточення суб'єкта (сильні зв'язки), а люди, з якими суб'єкт спілкується «поверхово» (слабкі зв'язки). Люди, які не входять у вузький кластер близьких друзів і знайомих, відкривають перед особистістю корисну інформацію – ту інформацію, якою особистість не володіє, в силу того, що зі слабкими зв'язками у суб'єкта комунікації менше загальних контактів. При цьому виникає інша проблема – проблема захищеності інформації, до якої можуть отримати доступ зовсім невідомі люди, які не входять до близького оточення суб'єкта. Для розробки методики оцінки захищеності інформації в соціальних мережах було відшукано рішення системи захисту в соціальних мережах з урахуванням дії специфічного параметру – сили зв'язків між абонентами, провести наочний аналіз поведінки системи. На відміну від класичного підходу, створена лінійна математична модель, знайдено стаціонарну позицію системи, отримано рівняння гармонічного осцилятора з затухаючою амплітудою. Визначено власну частоту коливань, період та коефіцієнт демпфування системи захисту. Зроблено висновок, що, виходячи з умов співвідношення дисипації і власної частоти коливань величини, загасання останньої до певного значення здійснюється періодично, з затухаючою амплітудою, або за експоненціально загасаючим законом. В результаті досліджень лінійної моделі захисту на основі диференціальних рівнянь встановлено, що системи захисту соціальної мережі нелінійні.

Гніденко М. П. Напрямки оптимізації комплексів захисту корпоративної мультисервісної мережі зв'язку / М. П. Гніденко, С. О. Сєрих, А. Г. Захаржевський // Телекомунікаційні та інформаційні технології. – 2023. – № 2(79). – С. 4-12.

Р/1921

З метою визначення напрямків оптимізації комплексів захисту корпоративної мультисервісної мережі і загальних підходів до її здійснення розглянута модель мережі зв'язку, що побудована по ієрархічному принципу. Визначено місце корпоративної мережі в складі мережі зв'язку. Зазначено, що більш раціональним підходом до забезпечення захисту інформації слід вважати етап проектування, коли можливо передбачити і реалізувати заданий рівень захисту. Запропоновано загальний алгоритм проектування корпоративної мережі, який складається з наведених в статті етапів. На першому етапі проведено вибір і обгрунтування загальної топології захищеної корпоративної мережі адаптованої до вимог її користувачів. Визначені напрямки комунікаційного трафіку між відправником і одержувачем інформації через мережу.

Гніденко М. П. Підвищення безпеки програмно-визначених мереж (SDNs) / М. П. Гніденко, С. В. Прокопов, М. М. Гніденко // Наукові записки Державного університету телекомунікацій. – 2023. – № 2(4). – С. 54-65.

Р/872

Програмно-визначена мережа (SDN) – нова парадигма, яка порушує вертикальну інтеграцію в традиційних мережах, щоб забезпечити гнучкість програмування мережі через (логічне) централізоване керування мережею. У роботі представлені різні загрози безпеці, які вирішуються SDN, і нові загрози, які виникають в результаті впровадження SDN. Нещодавні атаки на безпеку та контрзаходи в SDN також підсумовані у формі таблиць. Також надано опитування щодо різних стратегій, які реалізуються для досягнення енергоефективності та безпеки мережі через впровадження SDN. Щоб передбачити майбутню еволюцію цієї нової парадигми, було обговорено основні поточні дослідницькі зусилля, виклики та тенденції досліджень у цій галузі. Завдяки цій роботі дослідники та студенти можуть мати більш повне розуміння архітектури SDN, різних атак на безпеку та заходів протидії.

Захаржевський А. Методологія побудови захищених інфокомунікаційних мереж спеціального призначення на базі каналів загального доступу / А. Захаржевський // Information technologies and electronic engineering = Інфокомунікаційні технології та електронна інженерія. – 2023. – Vol. 3, № 2. – P. 53-63.

Р/1042

У статті вирішено нове актуальне наукове завдання щодо формування методології побудови перспективних захищених інфокомунікаційних мереж спеціального призначення. Проаналізовано архітектуру побудови та вперше подано нову класифікацію інфокомунікаційних мереж за функціональною декомпозицією. Визначено зміст структурних складових мережі на рівні "мережа", "система", "інфокомунікаційна мережа". Розроблено новий функціональний опис образу перспективної мережі та її якості. На основі аналізу міжнародних та спеціальних стандартів вперше запропоновано декомпозицію сфери застосування в інфокомунікаційних мережах мережі спеціального призначення. Запропоновано нові наукові підходи до проектування захищених інфокомунікаційних мереж спеціального призначення, які передбачають функціонально-структурний та структурно-функціональний підхід. Відповідно до запропонованих підходів у роботі подано перелік та описання моделей побудови інфокомунікаційних мереж спеціального призначення. Розкрито їх зміст, обмеження щодо застосування, переваги та недоліки окремих моделей. Сформовано нове наукове завдання на проектування перспективної захищеної інфокомунікаційної мережі спеціального призначення на основі каналів загального доступу та подано його загальний опис.

737819 R
004

Захист мовленнєвої інформації [Текст] : науково-практичний посібник / МВС України, Державний науково-дослідний ін-т ; [упорядники: Смерницький Дем'ян Вікторович, Яковенко Олександр Васильович, Мусієнко Дмитро Іванович]. - Київ : [Видавництво Людмила], 2023. - 358 с. : граф., табл., рис. - Бібліогр.: с. 248-254 (70 назв), в додатках та у виносках.

Спеціальна техніка для правоохоронної діяльності: науково-технічне та правове забезпечення.

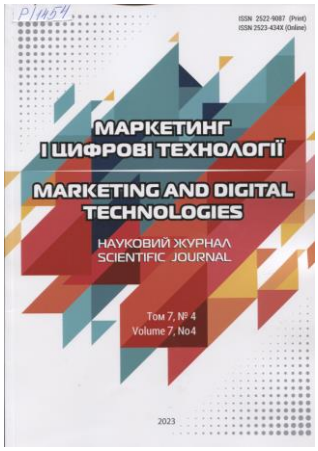
У посібнику викладено теоретичні основи розповсюдження звуку в приміщеннях та на відкритому просторі щодо його можливого перехоплення пристроями запису. Висвітлено основні характеристики сучасних акусто-електричних перетворювачів мовленнєвої інформації, що можуть використовуватися в закладних пристроях, їх переваги та недоліки. Розглянуто результати досліджень провідних світових учених у сфері розпізнавання мовленнєвої інформації в умовах впливу зовнішніх шумів. Наведено способи захисту мовленнєвої інформації в приміщеннях та методологію розрахунків ефективності їх використання.

Інтеграція послуг безпеки в архітектурі системи керування телекомунікаціями / Л. Н. Беркман, О. Г. Варфоломеєва, Г. Ф. Колченко [та ін.] // Зв'язок. – 2022. – № 4(158). – С. 3-8.

Р/776

Розглянуто основні завдання щодо забезпечення безпеки системи керування телекомунікаційними мережами України. Проаналізовано стандарти та іншу нормативну документацію з питань інформаційної безпеки телекомунікацій і систем керування ними. Особливу увагу приділено питанням керування безпекою як складової функціональної архітектури системи керування

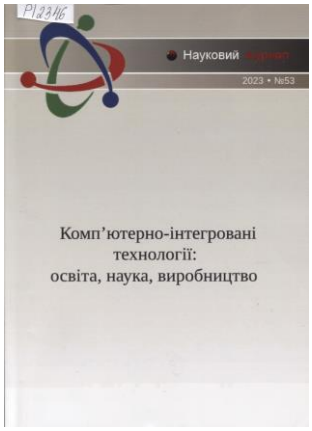
телекомунікаціями згідно з концепцією побудови мережі керування телекомунікаціями TMN. Визначено особливості впровадження послуг безпеки для кінцевих або проміжних вузлів телекомунікаційних мереж. Проведено порівняння ієрархічної моделі надання послуг безпеки з моделлю взаємодії відкритих систем 0SI. Запропоновано практичну модель організації безпеки системи керування телекомунікаційними мережами. Досліджено основні переваги та недоліки інтеграції послуг безпеки на нижніх та верхніх протокольних рівнях.



Карандін О. В. Роль соціальних мереж в обороноздатності країни / О. В. Карандін // Маркетинг і цифрові технології. – 2023. – Т. 7, № 4(158). – С. 106-116.

Р/1454

В дослідженні розглядається важливість та вплив соціальних мереж на обороноздатність країни. Досліджено їхню роль у формуванні позитивного іміджу оборонних сил та зміцненні патріотичних настроїв серед населення. Аналізується використання соціальних мереж для забезпечення інформаційної безпеки та захисту від кіберзагроз. Також висвітлюється їхній внесок у ефективну реакцію на кризові ситуації та динаміку використання в армійських стратегіях країн зі складною геополітичною обстановкою. Це дослідження може бути корисним для вчених, які цікавляться сучасними аспектами використання соціальних мереж у сфері оборони, а також для практиків, які бажають оптимізувати використання цих інструментів для підвищення обороноздатності своєї країни.



Кардашук В. С. Проблеми захисту інформації у віртуальних приватних мережах та відбиття атак на WEB-додатки / В. С. Кардашук, К. Я. Бортник, Н. В. Багнюк // Комп'ютерно-інтегровані технології: освіта, наука, виробництво. – 2023. – № 53. – С. 117-124.

Р/2346

У статті розглянуті сучасні проблеми захисту інформації у віртуальних приватних мережах, що використовують технологію VPN, стосовно масштабованості, гнучкості адміністрування, вимог до підключень та вартості. Для реалізації дослідження відбиття атак на WEB-додатки за допомогою евристичного методу проаналізована та досліджена нейронна мережа адаптивної-резонансної теорії. Запропонована модифікована структура, алгоритм навчання нейронної мережі та рішення щодо усунення недоліків її роботи. В результаті дослідження намічені подальші шляхи удосконалення алгоритму навчання нейронної мережі, що направлені на збільшення кількості відбиття атак на WEB-додатки.

738007 R
007

Климаш, Михайло Миколайович.

Системи передавання інформації [Текст] : підручник / М.М. Климаш, Р.С. Колодій, Ю.В. Пиріг ; Нац. ун-т "Львів. політехніка". - Львів : Вид-во Львів. політехніки, 2023. - 548 с. : граф., рис., табл. - (Серія "Електронні комунікації" = Телекомунікаційні системи і мережі ; вип. 1). - Бібліогр.: с. 519-523.

У підручнику висвітлено основні поняття теорії функціонування та методи побудови систем передавання інформації, наведено основні відомості щодо технологій частотного та цифрового мультиплексування

синхронної і асинхронної ієрархій з подальшим передаванням трактами телекомунікаційних мереж, а також розглянуто перспективи подальшого розвитку систем передавання у ракурсі новітніх технологій транспортування даних. Наведена інформація допоможе читачеві зрозуміти принципи роботи сучасних телекомунікаційних систем і надасть необхідні знання для розвитку та вдосконалення технологій у цій галузі.

Клімович С. Методологія маскування трафіку у спеціалізованій мережі передачі даних / С. Клімович // Захист інформації. – 2023. – Т. 25, № 3. – С. 107-112.

Р/1428

У зв'язку зі зростаючими загрозами в кібербезпеці, існує необхідність в розробці нових підходів (нової методології) маскування трафіку для уникнення виявлення та аналізу трафіку з боку несанкціонованих осіб. Маскування трафіку дозволяє приховувати характеристики переданих даних, такі як джерело, призначення, тип та об'єм, шлях та інші метадані, що надають змогу ідентифікувати та аналізувати комунікацію. Це може бути особливо корисним у випадках, коли необхідно зберегти приватність користувачів або запобігти виявленню конфіденційної інформації. Сучасні методи аналізу трафіку постійно вдосконалюються, тому виникає потреба в розвитку нових підходів до маскування у відповідності до змін в технологіях аналізу даних. Актуальність роботи пов’язана з тим, що дії адміністратора спеціалізованої мережі щодо забезпечення безпеки її функціонування спрямовані на розв’язання двох взаємопов’язаних завдань, а саме: забезпечення скритного функціонування мережі і виявлення фактів стороннього втручання (виявлення дій сторонніх осіб). Обидва завдання суворо регламентовані керівними документами, но кінцевий результат залежить від глибини розуміння посадовою особою існуючої проблеми, ступеня володіння методологією забезпечення безпеки функціонування спеціалізованої мережі, наявних матеріальних (в тому числі фінансових) засобів та наявного часового ресурсу. В роботі проведено аналіз існуючих підходів до забезпечення маскування трафіку в мережі, наведено алгоритми (варіанти програмної реалізації) механізмів маскування та виявлення факту маскування трафіку в спеціалізованій мережі передачі даних.

Козловський В. В. Метод забезпечення надійності одноканальних безпроводових телекомунікаційних мереж при умові мінімізації обсягу задіяних ресурсів / В. В. Козловський, Б. М. Залевський // Наукоємні технології. – 2023. – № 2(58). – С. 165-171.

Р/2289

Одним з елементів забезпечення стабільного і надійного процесу передачі корисних даних є завдання підтримання надійності одноканальних безпроводових телекомунікаційних мереж.

В статті проаналізовано та визначені найбільш оптимальні по мінімізації задіяного ресурсу топологічні схеми побудови телекомунікаційної мережі, обґрунтовано метод забезпечення надійності відносно поданих схем та розроблено метод забезпечення надійності одноканальної безпроводової телекомунікаційної мережі, приведеної по побудові до оптимальних топологічних схем.

Встановлено, що топологічні схеми «точка-точка», «шина», «дерево» є найбільш оптимальними по побудові за критерієм мінімізації затрат на їх побудову. Обґрунтовано, що найбільш прийнятим методом забезпечення надійності топологічних схем побудови одноканальної безпроводової телекомунікаційної мережі є метод резервування. Розроблено методичний підхід забезпечення надійності телекомунікаційною мережею, який передбачає комплексну оцінку всіх факторів, процедуру еквівалентного приведення складних елементів та схем топологічної побудови телекомунікаційної мережі до одного еквівалентного елементу з відповідним показником надійності та процедуру вертикальної та горизонтальної декомпозиції топологічної схеми на елементарні підсистеми.

Коробейніков Ф. О. Онтологія цілей і задач резильєнтності для організаційного рівня систем захисту інформації / Ф. О. Коробейніков // Електронне моделювання. – 2023. – Т. 45, № 5. – С. 67-80.

Р/518

Досліджено онтологію високорівневих конструктів резильєнтності в контексті побудови систем захисту інформації на організаційному рівні. Описано принципи взаємодії цих конструктів з елементами структури управління організацією та її активами. Процес визначення критичних функцій організації та пов'язаних із ними ризиків виокремлено як ключовий етап впровадження резильєнтності на організаційному рівні. Сформульовано припущення, що в структурах, де одна організація агрегує кілька підрозділів або взаємопов'язаних організацій, як елементів нижчих рівнів ієрархії, резильєнтність усієї системи не може бути просто визначена як агрегат резильєнтності її складових частин.

Лемешко А. В. Безпека даних в Україні за допомогою використання технології VPN / А. В. Лемешко, С. О. Новіченко, А. В. Недавній // IT synergy. – 2022. – Issue 2(3). – P. 28-42. – Текст укр.

Р/1973

На сьогоднішній день важко уявити світ без вільного доступу до Інтернету. На жаль, уряди деяких країн на законодавчому рівні обмежують доступ до тих чи інших ресурсів, що, в свою чергу, збільшує попит на розвиток та використання VPN технологій та сервісів. Деякі користувачі використовують VPN для анонімності в мережі Інтернет та отримання доступу до заблокованих ресурсів. Інші – користуються даною технологією для захисту особистої інформації. Під час вибору VPN-сервісу деякі користувачі керуються якістю послуг, які будуть надаватись, а інші – їх вартістю. Власники VPN-сервісів постійно вдосконалюють якість своїх послуг та впроваджують нові технології.

Попит на VPN-сервіси, після початку повномасштабного російського вторгнення, в Україні виріс в рази – не тільки за рахунок блокування українських медіа ресурсів, а й за рахунок появи IT-армії України. Завдяки чому деякі VPN-сервіси почали безкоштовно надавати доступ українцям до своїх серверів.

VPN має декілька рівнів захисту такі як: шифрування даних, аутентифікація джерела даних, перевірка хешу, що в свою чергу забезпечує конфіденційність передаваємих даних в Інтернеті. В сумісності, це все допомагає підвищити рівень захисту особистих даних користувачів.

Громадяни України, котрі залишаються на тимчасово окупованих територіях, в більшій мірі, мають доступ тільки до російського медіа простору, за рахунок того, що українські ресурси блокуються, а операторів зв'язку «глушать» та знищується їх інфраструктура. За допомогою VPN-сервісів вони можуть отримати доступ до українського медіапростору.

Лисецький Ю. М. Інформаційна безпека корпоративних баз даних / Ю. М. Лисецький, Д. Й. Калбазов // Математичні машини і системи. – 2023. – № 3(158). – С. 31-37.

Р/1052

Щодня компанії по всьому світу збирають та генерують велику кількість даних. Тепер інформація прийняла цифрову форму та зберігається в автоматизованих цифрових базах даних, використання яких дає можливість обробляти великі масиви даних, що були важкодоступними для обробки раніше. Важливим для економічної безпеки підприємства є захист корпоративних баз даних та інформації в них, який містить фізичний захист; захист продуктивності та їх моніторинг; захист даних від знищення чи пошкодження; контроль доступу; облік нових даних, які з'являються в інфраструктурі. З огляду на те, що до баз даних мають доступ користувачі різних типів та рівнів доступу (внутрішні користувачі, системні адміністратори, підрядники та партнери, Machine-to-Machine комунікації), вони можуть зловживати наданим доступом у таких напрямах: зловживання та використання надмірних прав доступу; зловживання об'єктивно необхідними правами доступу; зловживання правами, які не використовуються. Слабо контрольований процес видачі прав доступу до баз даних, як правило, формує надмірні права доступу, що завжди створює надлишковий ризик для інформаційної безпеки. До заходів безпеки відносять, по суті, за-

провадження процесу видачі та обліку виданих доступів, видачу мінімально необхідних прав доступу та впровадження механізму контролю й блокування виданих доступів. У статті розглянуто такі види загроз для баз даних, як SQL Injections і NoSQL injection атаки; низький рівень деталізації подій баз даних; витік через резервні копії; вразливості та налаштування; DDoS-атаки і методи протидії цим загрозам. Наведено, що найбільш дієвим способом захисту баз даних є впровадження Imperva DBS та Imperva WAF – спеціалізованих програмно-апаратних комплексів, розроблених для захисту баз даних. Застосування Imperva DBS допоможе вирішити усі ключові завдання захисту баз даних і забезпечить повну видимість та контроль їх використання в інфраструктурі підприємства.

Лукова-Чуйко Н. Удосконалення методу виявлення та локалізації нелегальних точок доступу до бездротової мережі об'єктів інформаційної діяльності / Н. Лукова-Чуйко, Т. Лаптєва // Безпека інформаційних систем і технологій. – 2023. – № 1(6). – С. 21-27.

Р/1227

Широке використання мобільних пристроїв привело до збільшення підключень до інтернету і розгортання нових бездротових локальних мереж. Згідно з останніми дослідженнями компанії Cisco, до кінця 2023 р. в усьому світі користувачами інтернету стануть 66 % населення Землі. До глобальної мережі будуть підключені більше 28 млрд пристроїв. В останні два десятиліття ми стали свідками народження і розвитку технології, яка істотно змінила нашу роботу і життя, – IEEE 802.11, також відому як Wi-Fi. Технологія Wi-Fi є улюбленим способом підключення до інтернету через простоту використання і гнучкість. Для підключення до бездротової мережі лише необхідно перебувати в радіусі її дії. Тобто споживачі і бізнес будуть усе більше покладатися на мобільні мережі. Однак слід зазначити, що кожна нова можливість цифровізації також дає нові можливості кіберзлочинцям і тому проблема безпеки бездротових мереж нині є однією з головних проблем IT-технологій. Неминуче поширення бездротових мереж і зростаючий трафік у цих мережах, може призвести до безлічі інцидентів інформаційної безпеки. Основні загрози спрямовані на перехоплення, порушення конфіденційності і цілісності переданих даних, здійснення атак на доступність вузлів каналу передачі та їхню підміну. У статті проведено аналіз існуючих методів виявлення несанкціонованих точок доступу до інформації. Удосконалено метод виявлення та локалізації несанкціонованих точок доступу до інформації, яка циркулює у бездротовій мережі на об'єктах інформаційної діяльності. Проведено натурне моделювання виявлення несанкціонованого втручання в інформаційну бездротову мережу підприємства. Натурне моделювання підтвердило точність локалізації відкритої точки доступу до інформації у мережі Wi-Fi – до 2 м. Це дозволить своєчасно виявляти та локалізувати несанкціоновані точки доступу до інформації у бездротовій мережі підприємств та установ.

738224 В
37

Луцький національний технічний університет.
Студентський науковий вісник [Текст] = Student Scientific Bulletin = Studencki Biuletyn Naukowy : [фаховий] наук. зб. / [гол. ред. Лютак Олена Миколаївна]. - Луцьк : [Вид-во "Вежа -Друк"], 2023 - .
Вип. 49. - Луцьк, 2023. - 431 с. : граф., рис., табл. - Текст кн. укр. та англ. мов. - Бібліогр. в кінці ст.

Зі змісту:

Павленко А. В. **Виявлення та аналіз найвразливіших місць веб-ресурсів.** – С. 123-135.
У даній статті виконаний опис найпопулярніших вразливостей веб-ресурсів, вказані місця на які націлені атаки зловмисників, також пропонуються засоби для виявлення та аналізу вразливостей, а саме OpenVAS та ElasticSearch. OpenVAS вибрано, тому що він має ряд істотних переваг, серед існуючих засобів для виявлення вразливостей. Виконано встановлення та показано технологію роботи даних систем.

Модифікація моделі репутації та довіри в задачах інформаційної безпеки Grid-систем для стійкості до загрози "зловмисні групи хвостів" / О. В. Семенов, С. О. Сєрих, В. В. Василенко, М. П. Гніденко // Наукові записки Державного університету телекомунікацій. – 2023. – № 1(3). – С. 46-56.

Р/872

З розвитком електронної комерції в Інтернет довірі стали приділяти підвищену увагу. Клієнти повинні довіряти продавцю, оскільки передають йому особисті дані, а продавець повинен довіряти клієнтові для того, щоб надавати йому свої послуги.

В Grid-системах ключовою ідеєю є спільне використання ресурсів, тому виникає необхідність у взаємній довірі користувачів і постачальників ресурсів.

В Grid-системах невеликого розміру всі учасники знаходяться у відношенні повної довіри. Наприклад, в Українському Академічному Grid-сегменті всі учасники належать до НАН України, і на цій підставі виникає повна довіра. Але в більш масштабних Grid-системах учасники найчастіше можуть бути безпосередньо не пов'язані один з одним, і існує ризик того, що хтось з учасників виявиться недобросовісним і зловмисним. Зменшити ці ризики і покликані механізми довіри.

738458 R
355

Національна академія Державної прикордонної служби України імені Богдана Хмельницького.

Збірник наукових праць Національної академії Державної прикордонної служби України [Текст]. - Хмельницький : Вид-во НАДПСУ. - (Військові та технічні науки).

№ 2,3 (85). - Хмельницький, 2021. - 336 с. : табл. - Бібліогр. наприкінці ст. Текст кн. укр., англ.

Зі змісту:

Андрощук О., Коваленко О., Тітова В., Чешун В., Поляков А. **Удосконалення систем захисту інформації в комп'ютерних мережах Державної прикордонної служби України.** – С. 5-21.

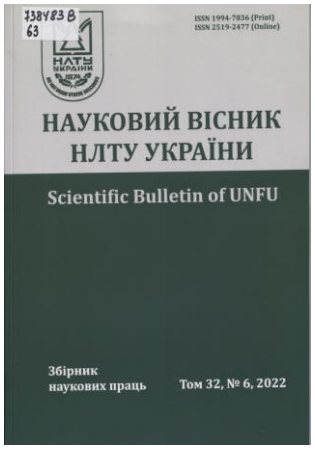
У статті представлені результати аналізу науково-технічної літератури і відкритих нормативно-розпорядчих документів міжнародного, національного і відомчого рівнів, присвячених процесу функціонування систем захисту інформації від несанкціонованого доступу до автоматизованих інформаційних систем в комп’ютерних мережах із застосуванням міжмережевих екранів.

На прикладі типових систем захисту інформації від несанкціонованого доступу розглянуті функціональні можливості діючих складових захисту інформації.

Виявлено недоліки та визначено основні аспекти удосконалення підсистем управління доступом даних до комп’ютерних мереж Державної прикордонної служби України на основі використання нових інформаційно-телекомунікаційних технологій, що пов’язані з підвищенням реальної захищеності автоматизованих інформаційних систем.

Визначено основні принципи забезпечення безпеки локальних мереж і автоматизованих інформаційних систем Державної прикордонної служби України. Безпека автоматизованих інформаційних систем повинна періодично аналізуватися й переоцінюватися.

Як перспективну технологію запропоновано мережеві екрани “наступного покоління” “Fortigate” та “Cisco ASA”, які засновані на застосуванні комплексного підходу.



738483 В
63

Національний лісотехнічний університет України.
Науковий вісник НЛТУ України [Текст] = Scientific Bulletin of UNFU : збірник наук.-техн. праць. - Львів : [РВВ НЛТУ України].
Т. 32, № 6. - Львів, 2022. - 96 с. : граф., рис., табл. - Бібліогр. наприкінці ст. Текст кн. укр., англ. Дод. тит. арк. англ.

Зі змісту:

Дяк Т. П., Грицюк Ю. І., Горват П. П. **Проблема виявлення фейкових новин на веб-сайтах мережі Інтернет.** – С. 78-94.
Проаналізовано наявні підходи до вирішення проблеми виявлення фейкових новин у мережі Інтернет, розглянуто екосистему новин як бізнес-модель їхньої появи, ознайомлення та поширення, що передбачає комплекс взаємопов'язаних сутностей – виробників новинної інформації її користувачів і розповсюджувачів, які сукупно можуть вирішити різноманітні завдання потенційних учасників на єдиному інтегрованому полі. З'ясовано, що мережа Інтернет має очевидні переваги над традиційними ЗМІ у розповсюдженні новин, такі як миттєвий доступ читачів до потрібної інформації, безкоштовне її розміщення, відсутність обмежень у стилі подання та різноманітність формату – текстова, графічна та мультимедійна. Однак, їхня неврегульованість будь-яким редакційним наглядом, а також державними органами з інформаційної безпеки призвели до того, що пересічному читачу часто важко визначити достовірність інформації в деяких опублікованих новинах. Встановлено, що серед вітчизняних фахівців заслуговують уваги ґрунтовні публікації в основному професійних журналістів, у яких вони висвітлюють як різну хибну інформацію, так і повну дезінформацію. Не відстають від них і молоді дарування, які у своїх критичних дописах розвінчують міфи про силу і міць північного сусіда, а також різні фейки про ті чи інші резонансні події. Зазначену проблему за останнє десятиліття з успіхом почали досліджувати закордонні вчені, які домоглися чималих результатів як у практичному, так і теоретичному планах. Досліджено, що головним завданням виявлення фейкових новин є автоматизована їх ідентифікація на ранніх стадіях появи, а також відсутність або мала кількість так званої позначеної (маркованої) інформації для машинного навчання відповідних моделей, призначених для ідентифікації фейкових новин, а також подальшого їх аналізу. З'ясовано, що за терміном екосистемне мислення знаходиться деякий світогляд, цілеспрямоване мислення та відповідні дії людей, залучені в цій системі. Екосистема новин як бізнес-модель їхньої появи, ознайомлення та поширення, передбачає комплекс взаємопов'язаних сутностей – виробників новинної інформації, її користувачів і розповсюджувачів, які сукупно можуть вирішити різноманітні завдання потенційних учасників на єдиному інтегрованому полі.

738133 R
004

Пашорін, Валерій Іванович.
Безпека інформаційних систем [Текст] : навч. посіб. / В. І. Пашорін, Ю. В. Костюк ; Державний торговельно-економічний університет. - Київ : [Держ. торг.-екон. ун-т], 2023. - 376 с. - Бібліогр.: с. 372-375.

У навчальному посібнику розглянуто сучасні напрями забезпечення безпеки інформаційно-телекомунікаційних систем. Викладено технічні, криптографічні, програмні методи і засоби захисту інформації. Формулюються проблеми вразливості сучасних інформаційно-телекомунікаційних систем, розглядаються питання захисту інформації в розподілених інформаційних системах, організаційно-правове забезпечення захисту інформації. Розглянуті загальні питання технологій збереження даних в єдиному інформаційному просторі та впровадженню функцій протидій кіберзлочинності, здатності організовувати та підтримувати

комплекс заходів щодо забезпечення безпеки інформаційної та кібербезпеки, з урахуванням їхньої юридичної та економічної обґрунтованості, технічної реалізації, запобігання можливих зовнішніх впливів, імовірних загроз, а також запобігання розголошенню, витоку і неправомірному оволодінню інформацією, застосування технологій захисту інформаційно-телекомунікаційних систем.

737946 В
629.7

Проблеми інформатизації та управління [Текст] : зб. наук. пр. / Нац. авіац. ун-т, Ф-т комп'ютерних наук та технологій. - Київ : [НАУ].
Вип. 2(74). - Київ, 2023. - 102 с. : іл., табл. - Бібліогр. наприкінці ст. Текст кн. укр., англ.

Зі змісту:

Безвершенко Є. І., Гузій М. М. **Моделі інформаційних конфліктів в інфокомунікаційних системах.** – С. 9-13.
У проведеному дослідженні виконано системний аналіз моделей інформаційної конфліктної взаємодії в інфокомунікаційних системах (ІКС). Інфраструктура ІКС реалізується сукупністю телекомунікаційних та інформаційно-обчислювальних систем (ТКС/ІОС). Аналіз наукових публікацій показує актуальність проблеми удосконалення існуючих та розробки нових методів управління процесами захисту інформації в динамічних умовах інформаційного протиборства з урахуванням невизначеності інформації про дії супротивника, необхідності розробки теоретичних основ, наукових методів і моделей управління захистом інформації в ІОС. На сучасному етапі співіснують декілька підходів до моделювання інформаційних конфліктів, які відтворюють специфічні особливості реалізації конфліктного компоненту. Їх можна умовно розділити на підходи, що засновані на точному описанні, та підходи, які базуються на продукційних або ігрових моделях. Математичну модель динаміки інформаційного конфлікту в ТКС/ІОС представлено загальновідомою системою рандомізованих рівнянь динамічної зміни ймовірностей станів конфліктуючих систем. Важлива особливість інформаційного конфлікту полягає у невизначеності використання виділеного ресурсу оперуючими системами. Визначені методологія та етапи дослідження взаємодії захищених інформаційних систем, що функціонують в середовищі інформаційного конфлікту в ТКС/ІОС.

Столяр А. Л. **Аналіз сучасних методів виявлення аномалій в комп'ютерних мережах.** – С. 91-100.
Проаналізовано визначення поняття аномалії, коротко описано причини їх виникнення та можливий вплив на комп'ютерні мережі. Розглянуто три типи аномалій: поодинокі (точкові), контекстуальні та групові аномалії. Також описано на основі яких характеристик відбувається виявлення аномальної поведінки. Наведено класифікації методів виявлення аномалій, які описано в науковій літературі. Розглянуто стандартні статистичні методи, методи на основі кластеризації та методи на основі класифікації.

Руденко Н. В. Дослідження безпеки та приватності систем Інтернету речей у мережах мобільного зв'язку / Н. В. Руденко, І. В. Луцюк, А. П. Сутик // Зв'язок. – 2023. – № 6(166). – С. 19-22.

Р/776

Дослідження безпеки та приватності систем Інтернету речей (IoT) у мережах мобільного зв'язку є актуальною та важливою темою в сучасному світі. Зростання популярності та використання IoT-пристроїв, підімкнених до мобільних мереж, створює нові можливості для комунікації, але також вносить важливі виклики, пов'язані з безпекою та захистом приватності.

Мобільні мережі, зокрема 4G і 5G, надають з'єднання для безлічі IoT-пристроїв, від розумних термостатів та вимикачів світла до медичних

пристроїв та автомобілів. Однак із кожним новим підімкненим пристроєм зростає потенційна загроза для безпеки мережі та захисту особистих даних користувачів.

У статті проаналізовано різні аспекти безпеки та приватності в контексті IoT у мобільних мережах. Розкрито потенційні загрози та вразливості, а також заходи, які можуть бути вжиті для зменшення ризику.

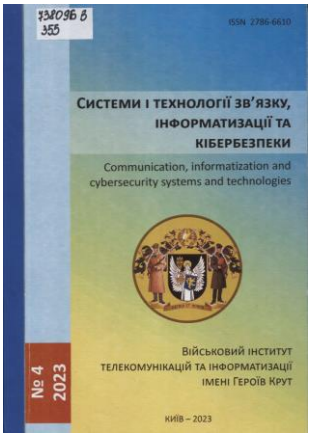
Особливу увагу приділено підвищенню усвідомленості щодо проблем безпеки та приватності в IoT і мобільних мережах, із сприянням подальшому дослідженню та розробленню заходів для забезпечення безпеки та конфіденційності в цьому напрямку.

Синтез моделі соціальних санкцій для забезпечення стійкості віртуальних спільнот у соціальних мережах в умовах антагоністичного середовища / С. Євсеєв, Ю. Тимонін, С. Веретюк [та ін.] // Захист інформації. – 2023. – Т. 25, № 3. – С. 139-146.

Р/1428

Швидка інтеграція віртуальних комунікацій у суспільне життя актуалізує потребу у створенні безпечного й комфортного середовища для комунікації користувачів віртуальних спільнот. *Метою дослідження* є підвищення рівня інформаційної безпеки соціальних віртуальних груп шляхом обґрунтування та формалізації особливостей застосування інструментів соціального контролю для управління динамікою віртуальної спільноти в інформаційному просторі. На основі моделей Моно та популяційної динаміки формалізовано процес еволюції віртуальної спільноти в умовах антагоністичного середовища, а також функціонал управління та забезпечення стійкістю віртуальної спільноти в соціальних інтернет-сервісах. Параметрами моделі визначено вплив частки деструктивних публікацій, які становлять загрозу інформаційній безпеці соціальній спільноті; глибина комунікації акторів досліджуваної спільноти з учасниками антагоністичної спільноти; показники якості контенту. У дослідженні набули подальшого розвитку компоненти соціального контролю в соціальних інтернет-сервісах та класифікація порушників інформаційної безпеки.

738096 В
355



Системи і технології зв'язку, інформатизації та кібербезпеки [Текст] = Communication, informatization and cybersecurity systems and technologies : [зб. наук. праць] / [за заг. ред. В. А. Романюка] ; М-во оборони України, Військовий ін-т телекомунікацій та інформатизації ім. Героїв Крут. - Київ : [Військовий ін-т телекомунікацій та інформатизації ім. Героїв Крут], 2023 - .

№ 4. - Київ, 2023. - 126 с. : граф., рис., табл. - Текст кн. укр. та англ. мов. - Бібліогр. наприкінці ст.

Зі змісту:

Субач І. Ю., Власенко О. В. **Архітектура інтелектуальної SIEM-системи для виявлення кіберінцидентів у базах даних інформаційно-комунікаційних систем військового призначення.** – С. 82-92.

У статті розглянуто актуальні завдання кіберзахисту баз даних інформаційно-комунікаційних систем. Проаналізовано ефективність поточних заходів щодо захисту баз даних і зроблено висновок, що існуючі системи не враховують багаторівневість захисту, що є критичним аспектом у сфері кібербезпеки. Запропоновано забезпечення кіберзахисту баз даних із використанням інтелектуальних можливостей SIEM-систем. Пропонується новий підхід до архітектури SIEM-системи, який враховує різні рівні контуру захисту інформаційно-комунікаційної системи. Розроблена архітектура надає можливість ефективно виявляти та реагувати на кібератаки на всіх рівнях захисту: від операційної системи до баз даних. Основним аспектом дії архітектури є багаторівневий захист бази даних, що дозволяє ефективно виявляти та реагувати на кібератаки. Запропонований підхід включає додавання джерел даних із застосунків різних рівнів контуру захисту інформаційно-комунікаційної системи, модуля аналізу даних про події в базі даних, який функціонує на основі застосування методів теорії нечітких множин та нечіткого логічного виводу

та модуля кореляції правил для покращення виявлення кіберінцидентів. А також інтеграцію OLAP-технологій для отримання глибокого аналітичного погляду на стан безпеки бази даних. Запропонована архітектура для виявлення кіберінцидентів дозволяє підвищити ефективність за показником точності виявлення кіберінцидентів, пов'язаних із функціонуванням бази даних інформаційно-комунікаційної системи.

Результатом дослідження є покращення можливостей SIEM-системи у виявленні та реагуванні на кіберінциденти у сфері бази даних інформаційної системи військового призначення. Подальшим напрямком досліджень є побудова моделі функціонування системи кіберзахисту бази даних інформаційно-комунікаційної системи.

Сметанін К. Кластерний підхід побудови мереж як спосіб забезпечення відповідного рівня кібербезпеки інформаційно-комунікаційної системи / К. Сметанін // Безпека інформації. – 2023. – Т. 29, № 1. – С. 6-10.

Р/1408

Взаємодія між суб'єктами сучасного суспільства невід'ємно пов'язана з надійним функціонуванням комп'ютерних інформаційних систем і мереж. Безпека та якість обслуговування (англ. Quality of service, QoS) є двома ключовими мережевими послугами для забезпечення безпеки зв'язку (відповідно до українського національного стандарту ДСТУISO/IEC 27000:2017). Якість є ключовою вимогою, і з подальшим розвитком комп'ютеризованих інформаційних систем і мереж швидко зростають додаткові вимоги до безпеки. Характеристики безпеки, рівні обслуговування та вимоги до керування всіма мережевими службами мають бути визначені та включені до будь-якої угоди про надання послуг мережі. Інтенсивний розвиток комп'ютерних інформаційних систем і мереж підвищив уразливість системи та в рази збільшив можливість кібернетичних атак. Тому управління мережевою безпекою є ключовим елементом функціонування комп'ютерних систем і мереж. Вразливості безпеки в маршрутизаторах, балансувальниках і операційних системах міжмережевого екрану, такі атаки як «відмова в доступі» і «відмова в обслуговуванні» на ключові мережеві вузли і сервери, зміна параметрів і вторгнення в маршрутизатори тощо, впливають на доступність ресурсів і якість обслуговування. Такі питання, як забезпечення ключових параметрів QoS, захист пакетів даних, запобігання атакам вторгнень і атакам на відмову в обслуговуванні, – це лише деякі з питань, які необхідно вирішити, щоб забезпечити безпечний розподіл ресурсів, доступ і безпечні шляхи передачі, захист вмісту та кінцеві – завершення надання QoS. Механізми безпеки та QoS не є незалежними. Вибір механізму безпеки впливатиме на продуктивність QoS і навпаки. Задоволення вимог щодо якості обслуговування вимагає використання механізмів безпеки для забезпечення належного рівня обслуговування та виставлення рахунків. Неправильний вибір механізмів безпеки знизить продуктивність ретельно побудованої мережі, або інформаційно-комунікаційної системи (далі ІТС), а неправильний вибір рівнів обслуговування призведе до витоку інформації. Тобто оптимальний баланс параметрів QoS допомагає зменшити витік інформації. Таким чином в даній статті запропоновано кластерний підхід побудови мережі для своєчасного виявлення та реагування на кіберзагрози, а також несанкціонований доступ до критичних компонентів мережі який в свою чергу є необхідною складовою для забезпечення високого рівня кібербезпеки всієї ІТС.

Солодкий-Солодаренко В. Д. Порівняльний аналіз сучасних технологій забезпечення відмовостійкості комп'ютерних систем / В. Д. Солодкий-Солодаренко // Зв'язок. – 2022. – № 4(158). – С. 29-33.

Р/776

Хмарні застосунки на вимогу є однією з технологій, що стрімко розвиваються та користуються великим попитом на ринку. Зі збільшенням кількості комп’ютерних систем і вимог до бізнес-аналітики в реальному часі потенційні клієнти таких послуг звертаються до постачальників послуг «обчислення на вимогу». У ситуації, коли клієнт надсилає запит у роботу, цей запит розгортається

на комп'ютерній системі в центрі оброблення даних постачальника послуг. При цьому немає стовідсоткової впевненості, що завдання буде виконано, а не провалено через брак ресурсів або через відмову програмного забезпечення. Проблеми відмовостійкості та високої доступності зараз є найбільш гострими в цій сфері. Проаналізовано та зіставлено сучасні технології відмовостійкості та високої доступності. Порівняно сучасні моделі системи високої доступності та інструменти для її впровадження. Виявлено недоліки сучасних моделей та засобів упровадження відмовостійкості. Розроблено рекомендації щодо застосування підходів, які допоможуть усунути розглянуті недоліки в різних випадках.

Сосновий В. О. Безпека мережі з використанням рекурентної нейромережі / В. О. Сосновий, І. В. Замрій // Зв'язок. – 2022. – № 5(159). – С. 21-24.

Р/776

Зростання кількості кібератак та шкідливих програм, що спостерігається останнім часом, яскраво свідчить про те, що наявних контрзаходів проти цього явища все ще недостатньо. Хакери стають дедалі обережнішими у своїх підходах передусім завдяки розробленню все якіснішого програмного забезпечення, насамперед – аби уникнути виявлення.

Відтак, дедалі очевиднішою стає потреба в ефективному автоматизованому вирішенні кібербезпеки, якого можна досягти за допомогою глибинних нейронних мереж.

У статті досліджено ефективність повторюваних нейронних мереж (Recurrent Neural Networcs, RNN) для боротьби в кіберпросторі. Проведений експеримент показує, що RNN з довготривалою короткочасною пам'яттю (Long Short-Term Memory, LSTM) працює набагато краще, ніж класичні алгоритми машинного навчання (SUM і Random Forest) з точністю відповідно 99,70,98,55 та 99,42%. Це можливо, оскільки RNN мають вбудовану пам'ять, яка може запам'ятати кілька попередніх станів і неявно виокремити характерні риси, сховану складну структуру та комплекс послідовного зв'язку в даних, який допоможе досягти кращої точності.

Сосновий В. О. Розробка структури нейронної мережі для аналізу виявлення вторгнень / В. О. Сосновий, Н. О. Лащевська // Телекомунікаційні та інформаційні технології. – 2023. – № 4(81). – С. 101-109.

Р/1921

Належні рішення безпеки в інформаційно-комунікаційному світі мають вирішальне значення для забезпечення безпеки мережі, забезпечуючи захист мережі в режимі реального часу від уразливостей мережі та використання даних. Ефективна стратегія виявлення вторгнень здатна використовувати цілісний підхід для захисту критично важливих систем від несанкціонованого доступу чи атак.

В роботі розглянуто останні наукові досягнення та дослідження стосовно аналізу виявлення вторгнень в мережу з використанням методів машинного навчання (МН).

В статті описано комплексне рішення безпеки на основі машинного навчання (МН) для виявлення вторгнень в мережі з використанням комплексної контрольованої структури МН і методів вибору функцій ансамблю. Крім того, надано порівняльний аналіз кількох моделей МН і методів вибору функцій. В статті розроблено загальний механізм виявлення та досягнення вищої точності з мінімальною частотою помилкових позитивних результатів (ЧПР).

В статті використовуються набори даних і результати показують, що модель виявлення може успішно ідентифікувати 99,3% вторгнень із найменшою кількістю помилок у 0,5%, що відображає кращі показники продуктивності порівняно з існуючими рішеннями.

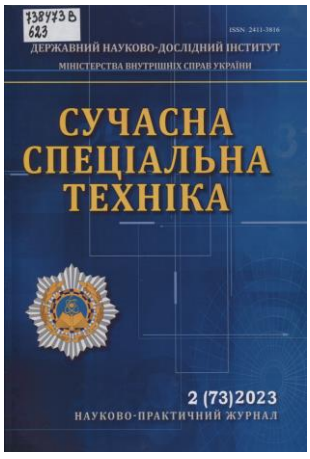
В статті об'єднано вибір функцій ансамблю та підходи машинного навчання ансамблю як механізм виявлення в СВВ для виявлення мережевих аномалій. Проведено експериментальне дослідження з наборами функцій, отриманими з дев'яти методів вибору функцій, а потім об'єднано ці набори функцій, щоб отримати мінімальну кількість функцій за допомогою

голосування більшості. Проведено порівняльний аналіз наборів функцій. Використано контрольовані методи, які ефективніші з збалансованим набором даних. Щоб зробити навчальний набір даних збалансованим, спочатку було вибрано тип даних (доброякісні або атакуючі) з мінімальною кількістю екземплярів даних у цьому навчальному наборі даних. Реалізовано алгоритм вибору функцій ансамблю та класифікації ансамблю, щоб покращити загальну продуктивність запропонованої моделі машинного навчання. Запропоновані перспективи розвитку подальших досліджень.

Стратегія побудови безпровідної мобільної системи зв'язку в умовах радіоелектронної протидії / О. Серков, О. Касілов, Б. Лазуренко [та ін.] // Радіоелектронні і комп'ютерні системи. – 2023. – № 2(106). – С. 160-170. – Текст англ.

Р/1769

Предметом дослідження в статті є процеси побудови системи мобільного зв’язку, що працює в умовах радіоелектронної протидії. *Мета* – розробка рекомендацій щодо побудови безпровідної мобільної системи зв’язку, що ефективно працює у складній завадовій електромагнітній обстановці. В основу стратегії побудови системи мобільного безпровідного зв’язку покладено використання угруповання маловисотних БПЛА з застосуванням технології надширокосмугових сигналів, які циркулюють в каналах управління та зв’язку із інтеграцією до її структури елементів прийняття рішення. Завдання дослідження полягає в забезпеченні усталеної та безпечної роботи безпровідної мобільної системи зв’язку в умовах організованої радіоелектронної протидії. В роботі використовувалися методи аналітичного, часового позиційно-імпульсного кодування та нечіткого логічного висновку для прийняття рішень щодо передачі обслуговування у мережі. Отримані наступні результати. Розроблена стратегія побудови безпровідної мобільної системи зв’язку в умовах радіоелектронної протидії. Показано, що для отримання високої завадостійкості каналів управління і зв’язку та захисту інформації від перехоплення слід застосовувати технологію безпровідного надширокосмугового зв’язку, яка дозволяє забезпечити великі обсяги та швидкості передачі інформації. Запропоновано технічне рішення щодо конструкції надширокосмугової приймально-передавальної антенної системи. Причому, рекомендовано використовувати результати обробки даних у нечіткій системі прийняття рішень для передачі обслуговування між вузлами мобільної мережі в умовах завад.



738473 В
623

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

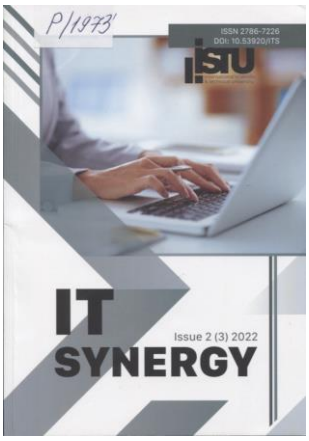
№ 2 (73). - Київ, 2023. - 114 с. : граф., рис., табл. - Бібліогр. наприкінці ст. Текст кн. укр., англ. Дод. тит. арк. англ.

Зі змісту:

Розорінов Г. М., Сірченко І. А., Неня О. В., Фесенко М. А., Березненко Н. М. **Оцінка залишкового ризику при забезпеченні функціонування захищеної мережі розповсюдження аудіовізуального контенту.** – С. 33-44.

Запропоновані підходи до оцінки величини залишкового ризику системи захисту мережі розповсюдження аудіовізуального контенту, зокрема оцінки можливого рівня заподіяної шкоди.

Розроблено моделі процесів захисту функціональних властивостей захищеності системи, для чого проаналізовано взаємодію атак на функціональні властивості мережі із засобами протидії цим загрозам. Визначено математичні співвідношення для оцінки кількісних характеристик. Знайдено ті елементи, через які захищеність контенту є найбільш вразливою для загроз.



Ткаченко О. М. Модель прогнозування безпеки мережі за допомогою нейронних мереж / О. М. Ткаченко, В. О. Сосновий // IT synergy. – 2022. – Issue 2(3). – P. 43-54. – Текст укр.

P/1973

В статті розглянуто чотири алгоритми, а саме алгоритм SVM, алгоритм нечіткої кластеризації, алгоритм кластеризації K-Means і алгоритм Аргіогі. Деталізуємо 4 різних кроки безпеки користувачів мережі та їх контролю доступу статті є розробка надійної моделі прогнозування безпеки мережі. Розроблена модель виявлення вторгнень, побудована з використанням нейронних мереж. Модель виявлення вторгнень виявляє аномалії та атаки на основі зловживання. Модель виявлення вторгнень також виконує три типи завдань класифікації. Завдання включають класифікацію між появою атаки чи звичайним випадком, класифікацією між різними типами атаки чи звичайним випадком. Модель виявлення вторгнень також показує точність класифікації, час виконання та обсяг використання пам'яті. Цілями моделі виявлення вторгнень є висока точність, малий час виконання та мінімальний обсяг використання пам'яті. Модель виявлення вторгнень, побудована за допомогою нейронних мереж, відповідає цілям високої точності, малого часу виконання та мінімального використання пам'яті.

Федоренко А. А. Аналіз методів виявлення вразливостей WEB-ресурсів до SQL-ін’єкцій / А. А. Федоренко, Б. І. Осадчий, В. В. Коржик // Сучасний захист інформації. – 2023. – № 3(55). – С. 57-61.

P/2300

Ця стаття розглядає проблему вразливостей до SQL-ін'єкцій у веб-додатках та використання автоматизованих сканерів для виявлення цих вразливостей. Вона починається з опису SQL-ін'єкцій та їх наслідків, а також ручної перевірки на вразливості. Далі стаття аналізує різні автоматизовані сканери вразливостей, включаючи Acunetix, Burp Suite, Nessus, OpenVAS, SQLMap, OWASP ZAP та Nikto. Для кожного сканера наведені переваги та недоліки, а також рівень деталізації та функціональні можливості. Стаття закінчується висновками, які підкреслюють важливість розуміння ризиків SQL-ін'єкцій та використання правильних інструментів для їх виявлення. Наголошується на тому, що автоматизовані сканери не є універсальним рішенням, і вони повинні супроводжуватися ручною перевіркою та аналізом. Стаття вказує на необхідність постійного оновлення сканерів та комбінації автоматизованих та ручних методів для забезпечення найвищого рівня безпеки. Вона надає читачам корисний огляд різних аспектів та аспектів використання автоматизованих сканерів вразливостей до SQL-ін'єкцій у веб-додатках.

Фільтрація забороненого контенту / А. В. Лемешко, К. Ю. Шульженко, А. Ю. Березовський, В. С. Галета // Зв'язок. – 2022. – № 6(160). – С. 14-16.

P/776

Актуальність цього дослідження полягає в необхідності фільтрації контенту з високою точністю через створення оптимальних варіацій архітектур нейронних мереж. Наявні сьогодні рішення дають низьку точність фільтрації, що призводить до блокування потенційно безпечного контенту. Повна відсутність фільтрації призведе до того, що неповнолітні користувачі та інші вразливі групи отримають до нього доступ, що неприпустимо.

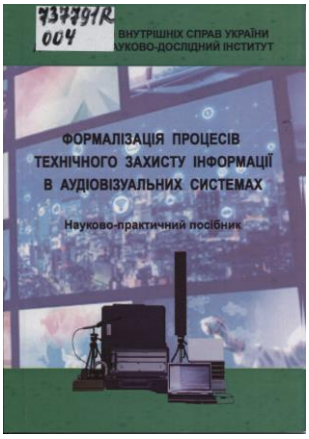
Об’єктом дослідження є процеси фільтрації контенту.

Предметом дослідження є методи і технології побудови нейронних мереж для фільтрації контенту.

Мета статті полягає в підвищенні точності фільтрації контенту через розроблення архітектури нейронної мережі.

Як засіб розроблення системи було вибрано PyCharm та мову програмування Python. Інструментами розроблення були вибрані бібліотеки SciPy та Keras, бібліотека для імпорту та експорту даних Pickle та бібліотека для роботи з алгоритмами нейронних мереж Sckit-learn.

Результатом роботи є побудована архітектура нейронної мережі для фільтрації забороненого контенту.



737791 R
004

Формалізація процесів технічного захисту інформації в аудіовізуальних системах [Текст] : наук.-практ. посібник / [Г. М. Розорінов, І. А. Сірченко, Д. В. Смерницький та ін.] ; МВС України, Держ. наук.-дослід. ін-т. - Бібліогр.: с. 72-76. Авт. зазнач. на с. 77 та 78.

У науково-практичному посібнику висвітлено питання розроблення ефективної системи захисту аудіовізуального контенту з формалізацією процесу захисту, у тому числі шляхом розроблення його моделі. Крім того, розглянуто оцінку ефективності такої системи через призму показників досягнутого рівня захищеності, зокрема величини залишкового ризику системи захисту мережі розповсюдження аудіовізуального контенту та можливого рівня заподіяної шкоди.

738087 B
51

Харківський національний університет імені В. Н. Каразіна.
Вісник Харківського національного університету імені В. Н. Каразіна [Текст] = Bulletin of V. N. Karazin Kharkiv National University eng : [зб. наук. пр.]. - Харків : [Вид-во ХНУ імені В. Н. Каразіна]. - (Математичне моделювання. Інформаційні технології. Автоматизовані системи управління).

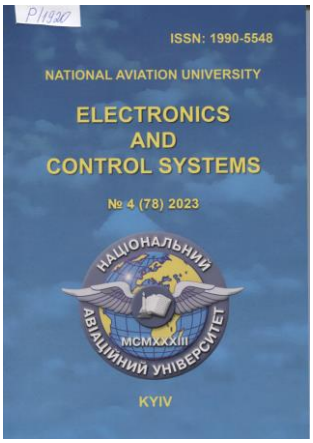
Вип. 54. - Харків, 2022. - 60 с. : граф., рис., табл. - Бібліогр. наприкінці ст. Текст укр., англ. Паралел. назва англ.

Зі змісту:

Дейнега Т. С., Сватовський І. І. **Дослідження застосування алгоритмів штучного інтелекту в системах виявлення/запобігання вторгнень.** – С. 16-26.

Проведено аналіз необхідності та доцільності використання алгоритмів та технологій штучного інтелекту на основі нейронних мереж та нечіткої логіки у системах виявлення та запобігання вторгнень у мережу. Сучасні атаки на мережу відрізняються здатністю змінювати свої характеристики та способи дії майже у реальному часі. Застарілі експертні системи захисту мережі, які засновані на понятті «правило-дія», вже не можуть впоратися з даними видами атак, тому що їм потрібен певний час на обробку інформації про нову атаку та занесення її до своєї бази даних.

У роботі пропонується модель системи виявлення/запобігання вторгнень на основі використання нейронної мережі, що навчається на тестовій вибірці, яка створюється за алгоритмами нечіткої логіки. Алгоритм навчання нейронної мережі заснований на методі навчання з вчителем та методі зворотного поширення помилки. Таким чином, повна процедура навчання нейронної мережі вимагає від користувача мати лише дамп перехопленого мережевого трафіку для його подальшої обробки згідно алгоритму створення тестової вибірки. Результати оцінки і практичного тестування запропонованої моделі показують, що подібна схема захисту мережі від атак може працювати досить надійно і використовуватись в якості системи виявлення/запобігання вторгнень для локальних та глобальних мереж.



Sineglazov V. M. Twitter Fake News Detection Using Graph Neural Networks = Розпізнавання фейкових новин у Twitter за допомогою графових нейронних мереж / V. M. Sineglazov, K. I. Bylym // Electronics and Control Systems. – 2023. – № 4(78). – P. 26-33.

Р/1920

Цю статтю присвячено інтелектуальному обробленню текстової інформації з метою виявлення фейкових новин. Для розв'язання поставленого завдання запропоновано використання глибоких графових нейронних мереж. Виявлення фейкових новин з урахуванням уподобань користувачів доповнено більш глибокими топологіями графових нейронних мереж, що включають в себе Hierarchical Graph Pooling with Structure Learning, для покращення операції згортки графа і захоплення більш багатих контекстних зв'язків у графах новин. У статті представлено можливості розширення фреймворку виявлення фейкових новин з урахуванням уподобань користувачів за допомогою глибоких графових нейронних мереж для покращення розпізнавання фейкових новин. Оцінка на наборі даних FakeNewsNet (підмножина Gossipcop) з використанням фреймворків PyTorch Geometric і PyTorch Lightning демонструє, що розроблена глибока модель графової нейронної мережі досягає 94% точності в класифікації фейкових новин. Результати показують, що більш глибокі графові нейронні мережі з інтегрованими текстовими та графовими функціями пропонують перспективні варіанти для надійного і точного виявлення фейкових новин, прокладаючи шлях до підвищення якості інформації в соціальних мережах та за їх межами.

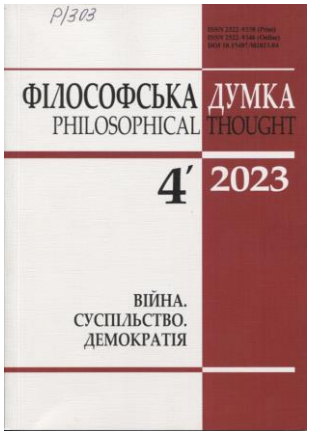
Інформаційне протиборство у воєнних конфліктах. Інформаційно-психологічна безпека

Базарний С. Класифікація методів аналізу та моделей соціальних мереж в інтересах інформаційної операції / С. Базарний // Безпека інформації. – 2023. – Т. 29, № 2. – С. 61-66.

Р/1408

Інформаційна війна, яку веде противник проти України не менш небезпечна, ніж безпосередні бойові дії на лінії зіткнення. Враховуючи досвід широкомасштабної збройної агресії російської федерації проти України, можна дійти висновку, що ворог намагається підривати єдність українського суспільства, довіру громадян до влади та збройних сил. Соціальні мережі є сучасним та потужним інструментом розповсюдження спеціальних інформаційних матеріалів для ведення психологічного впливу на противника. Методи аналізу та моделі соціальних мереж викликають інтерес у науковців під час проведення досліджень в межах виконання бойових (спеціальних) завдань. Аналіз інформації у соціальних мережах про поведінку, особисті відомості, думки та погляди агентів соціальних мереж необхідний для проведення інформаційних операцій. Для аналізу даних у соціальних мережах існує багато застосунків, за допомогою яких проводиться моделювання інформаційних потоків, процесів взаємодії агентів всередині мережі, прогнозування їх поведінки, розрахунки параметрів та візуалізація графа мережі. За допомогою інформаційно-технічної системи або спеціалізованого програмного забезпечення, можна керувати великою кількістю облікових записів через адміністратора групи та впливати на поведінку інших агентів. З метою підвищення ефективності психологічного впливу агентів соціальних мереж на цільові аудиторії, необхідна розробка моделей соціальних мереж для вивчення закономірностей розповсюдження спеціальної інформації та встановлення зв'язків і взаємодії агентів з цільовою аудиторією противника. В даній статті проведена класифікація методів аналізу соціальних мереж, описані основні показники, що характеризують соціальні мережі, розглянуті моделі соціальних

мереж. Для візуалізації отриманих результатів, щодо проведення класифікації методів та моделей розроблені та представлені структурні схеми. Перспективою подальшого дослідження є розробка грифової нейронної мережі (graph neural networks), яка дозволить моделювати взаємодії та властивості графів для оцінювання рівня психологічного впливу в інтересах інформаційних операцій. Ця модель може використовувати методи графових згорток (graph convolutions), які базуються на локальних операторах для аналізу структури мережі.



Борисенко Є. Інформаційна війна крізь призму комунікативної теорії: спроба аналізу / Є. Борисенко // Філософська думка. – 2023. – № 4. – С. 21-38.

Р/303

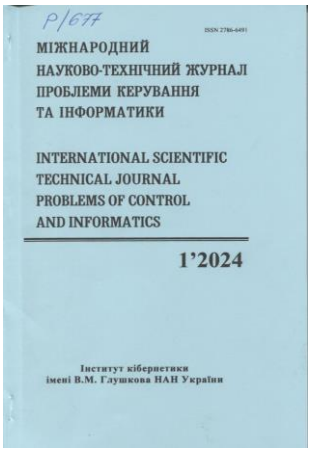
Сучасна інформаційна доба привносить зміни у всі явища людського життя. Наприклад, змінюється характер воєн, що з фактичного поля бою переносяться в інфопростір – тобто стають гібридними. Перевагу здобуває той, чий наратив стає домінантним у глобальному інформаційному просторі. Російсько-українська війна є виразним прикладом новітнього протистояння. Воно відбувається між двома абсолютно протилежними позиціями, компроміс між якими є неможливим. Цей конфлікт є глибоко екзистенційним, адже росія різко заперечує існування України як самостійної держави та як нації загалом, про що свідчить як риторика держави-агресора, так і численні її воєнні злочини. Однак ця війна триває не лише між двома сторонами. Відмовляючи Україні в її існуванні, ворог також кидає виклик і тим цінностям, які відстоюють українці та на засадах яких прагнуть розбудовувати власну країну. І такими є цінності вільного демократичного світу. Отже, росія протистоїть не лише одній країні, а всім тим, хто також поділяє демократичні цінності. Саме тому інформаційна війна починає сягати далеко за кордони України. Ми спостерігаємо вплив росії, чия пропаганда впливає на порядок денний багатьох провідних країн Заходу. Використовуючи як класичні ЗМІ (газети, радіо, телебачення), так і нові (спільноти в соцмережах, блоги тощо), вона втручається у глобальний інформаційний простір. Інтернет лише ще більш проблематизує поширення достовірної інформації та сприяє пропаганді, адже тепер контроль над потоком інформації майже відсутній. Цю проблему констатує Ю. Габермас, зазначаючи, що кожен тепер є потенційним автором, над яким до того ж відсутній контроль редакції. Тому в умовах, коли ЗМІ тяжіють до розважальності, а більшість інформації ллється безконтрольним потоком, триває війна за людські уми. Тож сучасна ситуація стає викликом для комунікативної теорії, яка навчилася правильно визначати діагнози, однак ще не запропонувала свого варіанту виходу з кризи. Допис Габермаса «Війна та обурення» поки що є лише свідченням радше неспроможності його філософії відповісти на реальні виклики.

738261 R
35

Державне будівництво та місцеве самоврядування [Текст] : збірник наук. праць / Нац. акад. правових наук України, НДІ держ. буд-ва та місцевого самоврядування. - Харків : Право.
Вип. 43. - Харків, 2022. - 454 с. - Бібліогр. наприкінці ст. Текст укр., англ. Дод. тит. арк. англ.

Зі змісту:

Бруслик О. Ю., Мукомела І. В. **Ведення інформаційної війни в період російського вторгнення в Україну (стаття перша).** – С. 165-178.
Стаття присвячена дослідженню теоретичних основ інформаційної війни, а також практичному її веденню в світлі російської агресії в Україні. Авторами зроблений загальний аналіз інструментів ведення інформаційної війни. Зроблена спроба продемонструвати хід інформаційної експансії та засобів ведення війни, наративів із одночасним їх семантичним аналізом. Робиться висновок про те, що вже зараз можна говорити про повну перемогу України в інформаційній війні, що є важливою передумовою для перемоги на полі бою.



Нікітін А. В. Особливості побудови, асимптотичний аналіз та комп'ютерна реалізація для багатовимірної моделі інформаційної боротьби в умовах пуассонової апрокисмації / А. В. Нікітін, Б. В. Красюк // Міжнародний науково-технічний журнал Проблеми керування та інформатики. – 2024. – № 1. – С. 24-33.

Р/677

Модель Лотки-Вольтерра, яка визначає взаємодію між «хижаком» і «жертвою», – одна з ключових типів моделей, що описують різноманітні процеси в прикладній математиці, соціальних науках та економіці. Пропонувалося застосувати цей підхід до моделювання інформаційної війни. Існуючі підходи розглядають соціальну спільноту з постійною кількістю осіб N_0, які можуть стати об'єктом n-типів інформаційних загроз. Наприклад, це може бути загроза негативної зміни поглядів членів спільноти за допомогою передачі інформації, поданої у двох різних формах. Важливо зауважити, що типи інформації можуть мати як позитивний, так і негативний характер, але найбільш цікавим є випадок антагоністичних точок зору, поширення яких викликає поляризацію суспільства і породжує питання про переможця в інформаційній війні. Позначення $N_1(t)$, $N_2(t)$, ..., $N_i(t)$ вказують на кількість «прихильників» типів загроз, які прийняли нову інформацію, ідеї, норми тощо, залежно від часу t. Крім розрахунку для n-типів інформаційних загроз, розроблена програма дозволяє динамічно змінювати вхідні параметри середовища, стрибків, а також кожного окремого типу інформаційної загрози. Пуассонівська апроксимація може використовуватися для доповнення процесу моделювання інформаційної війни шляхом врахування стрибків, наприклад, відображення реакції спільноти на появу компроментуючої інформації відносно конкретного типу інформаційної загрози. Наведено програмну реалізацію розрахунку для моделі інформаційної війни n-типів інформаційних загроз. Доведено доцільність такого методу оцінки процесу інформаційної боротьби. Модель у поєднанні з програмною реалізацією дозволяє відслідковувати швидкість поширення того чи іншого виду інформації, контролювати швидкість поширення залежно від зміни параметрів середовища, що дасть змогу ефективно реагувати на загрози.

737682 В
32

Політологічний вісник [Текст] = Politology Bulletin : збірник наук. праць / голов. ред. О. В. Батрименко ; Київський нац. ун-ті імені Тараса Шевченка. - [Київ] : [ВАДЕКС].
Вип. 89. - Київ, 2022. - 240 с. : іл. - Бібліогр. наприкінці ст.

Зі змісту:

Батрименко О. В. **Роль соціальних медіа у російсько-українській інформаційній війні.** – С. 124-132.
У статті викладені результати системного дослідження ролі соціальних медіа у висвітленні подій російсько-української війни, які є одним з актуальних інструментів у веденні інформаційного протиборства між Україною та країною-агресором. Стверджується, що соціальні медіа сприяють подоланню традиційних бар'єрів для масової комунікації. Таким чином, збільшується не лише обсяг доступної інформації, але й кількість активних акторів інформаційно-комунікаційних процесів. До останніх сьогодні належать не лише офіційні органи державної влади, а усі небайдужі громадяни.

Наголошується на відмінності між стратегіями, використовуваними РФ та Україною щодо соціальних мереж та платформ. Так, держава-агресор жорстко лімітує доступ своїх громадян до незалежних джерел, забороняючи останні на своїй території, при цьому активно використовує соціальні медіа для пропаганди та дезінформації як на території своєї країни, так і далеко за її межами. В Україні соціальні медіа, насамперед, застосовуються для миттєвого донесення

актуальної інформації до громадян, поширення правдивого наративу серед власного населення та за межами держави. При цьому наголошується, що використання соціальних медіа у інформаційній війні має як свої переваги, так і недоліки. Так, швидкість та доступність є виразними плюсами, а ось до мінусів можна зарахувати проблему достовірності та множинності наративів.

Розроблено низку порад для споживачів контенту соціальних мереж, які можуть допомогти уникнути омани.

738268 R
33

Теоретичні та прикладні питання економіки [Текст] : зб. наук. праць / Київ. нац. ун-т імені Тараса Шевченка, Екон. ф-т, Каф. економіки підприємства. - Київ : [ТОВ ЦП "КОМПРИНТ"], 2023 - .

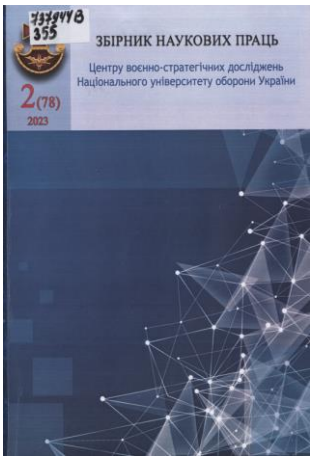
Вип. 1 (46). - Київ, 2023. - 155 с. : граф., рис., табл. - Бібліогр. наприкінці ст. Текст укр., англ. мов.

Зі змісту:

Варналій З. С., Федченко О. П., Пампуха І. В., Лаврінчук О. В., Микитюк О. П. **Управління неструктурованими даними при дослідженні впливу засобів масової інформації на соціальну безпеку людини в умовах гібридної війни.** – С. 4-16.

Важливим елементом аналізу стану соціальної безпеки людини в умовах гібридної війни є вивчення та оцінка структури і динаміки розвитку громадської думки в визначених регіонах країни. Одним з найбільш серйозних способів оцінки громадської думки і прогнозування її змін є, поряд з соціологічними дослідженнями – моніторинг впливу засобів масової інформації на населення регіону.

У зв'язку з швидким кроком прогресу та розвитком геоінформаційних систем спеціалісти компанії Esri (США) комплексно підійшли до проблеми сумісного використання неструктурованих даних та геоінформаційних систем. Для вирішення цієї проблеми був створений модуль Locate XT. Новий додатковий модуль ArcGIS LocateXT призначений для пошуку, вилучення та нанесення на карту даних зі звичайного тексту, включаючи географічні координати в різних форматах, назви місць та іншу пов'язану з місцем розташування інформацію.



737944 B
355

Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського.

Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України [Текст] : [наук. вид.] / [голов. ред. Загорка Олексій Миколайович]. - [Київ] : [ЦВСД НУОУ імені Івана Черняховського].

Вип. 2(78). - [Київ], 2023. - 144 с. : граф., рис., табл. - Бібліогр. наприкінці ст. Текст кн. укр., англ.

Зі змісту:

Прокопенко О. С., Федорієнко В. А., Кульчицький О. С. **Підхід щодо виявлення і аналізу інформаційних загроз національній безпеці України у системі стратегічних комунікацій.** – С. 35-43.

Розглянуті питання концептуальних положень системи стратегічних комунікацій і запропоновано методичний підхід щодо своєчасного виявлення, аналізу та оцінювання інформаційних загроз національній безпеці держави у воєнній сфері.

738255 В
355

Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського.

Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України [Текст] : [наук. вид.] / [голов. ред. Загорка Олексій Миколайович]. - [Київ] : [ЦВСД НУОУ імені Івана Черняховського].

Вип. 3(79). - [Київ], 2023. - 146 с. : граф., рис., табл. - Бібліогр. наприкінці ст. Текст кн. укр., англ.

Зі змісту:

Інформаційна війна завжди починається до проведення військової операції, триває паралельно з нею та після її завершення. З 2014 року інформаційне середовище активно використовується Російською Федерацією для поширення пропаганди та дезінформації, а у 2022 році цей процес масштабувався та постійно зазнає змін та перетворень. На сьогодні агресор активно використовує малі групи в соціальних мережах для укорінення своїх наративів, які він реалізовує через поширення фейків, дезінформації, негативної пропаганди, маніпуляцій тощо. У статті надані рекомендації щодо нівелювання негативного впливу.

Кібербезпека – проблема XXI століття

Кіберстатистика в Україні. Сучасний стан / А. В. Давидюк, В. Ю. Зубок, Ю. Є. Хохлачова [та ін.] // Безпека інформації. – 2023. – Т. 29, № 2. – С. 53-60.

Р/1408

З розвитком кіберзахисту в Україні збільшуються і технічні спроможності для забезпечення безпеки інформації. Новітнє обладнання здатне збирати великі масиви даних для аналізування потенційних загроз кібербезпеці. Інтеграція аналізу цих даних в процеси кіберзахисту дасть змогу попередити виникнення ряду кіберінцидентів. Водночас існує імовірність того, що суб'єкти забезпечення кібербезпеки під час виконання власних функцій збирають одні і ті ж самі набори даних інформації, що значно зменшує ефективність їх інформаційного обміну та пов’язаних процесів. З огляду на зазначене, доцільним є впровадження процесів кіберстатистики, що має на меті диференціювати функції суб'єктів забезпечення кібербезпеки за наборами даних, які вони використовують у власній діяльності. Така диференціація допоможе визначити існуючі проблеми в процесах цих суб'єктів та сприятиме впровадженню уніфікованих підходів до збору та аналізування даних в сфері кібербезпеки. Таким чином розробка та впровадження методики збору та оброблення даних кіберстатистики дасть змогу оптимізувати процеси забезпечення кібербезпеки.

Кількісна оцінка кіберзахищеності інформації / В. Хорошко, Ю. Хохлачова, Н. Вишневська, О. Чобаль // Захист інформації. – 2023. – Т. 25, № 2. – С. 70-76.

Р/1428

Створення, впровадження та експлуатація комп’ютерних систем привело до виникнення нових проблем в сфері безпеки інформації. Кіберзахист інформаційних технологій повинен за своїми характеристиками бути відповідним масштабам загроз і ризиків. Відхилення від цього правила приведе до значних збитків. Для кожної комп'ютерної системи (КС) має бути свій оптимальний рівень кіберзахищеності, який необхідно постійно підтримувати. Нажаль до цього часу не існує адекватної методики оцінки кількісного рівня кіберзахищеності. Основними проблемами, які необхідно вирішити для розробки математичних основ кількісного аналізу кіберзахищеності та визначення його рівня є: визначення функціональної залежності між методами атаки на КС і

методами КЗ; розробка критерію оцінки рівня КЗ, виходячи з усієї сукупності її кількісних характеристик; визначення методики обґрунтування пріоритетних заходів, спрямованих на забезпечення заданого рівня кіберзахищеності інформації. Запропонована методика дасть можливість для використання нових методів обробки інформації з метою оцінки її кіберзахищеності, які раніше не застосовувались.

Кузьменко А. О. Методика аналізу та прогнозування кіберінцидентів на основі методу головних компонент / А. О. Кузьменко, Н. Л. Веселков // Сучасний захист інформації. – 2023. – № 4(56). – С. 75-83.

Р/2300

В статті розглянуто теоретичні аспекти методу головних компонент, його застосування для аналізу даних про кіберінциденти та побудови прогностичних моделей. Окрема увага приділена експериментальним результатам, їх аналізу та обговоренню з метою підвищення ефективності методики прогнозування кіберінцидентів. Ця стаття спрямована на вдосконалення інструментів та підвищення рівня кібербезпеки шляхом застосування новітніх методів аналізу даних та прогнозування подій у кіберпросторі. Корисність методу головних компонент при аналізі даних кіберінцидентів ґрунтується на можливості зменшення обсягів аналізу інформації та визначення найбільш суттєвих факторів кіберінцидентів. Перевагою описаного методу аналізу статистики кіберінцидентів є те, що він може застосовуватись незважаючи на характер розподілу випадкових величин – показників інцидентів. Завдяки основним властивостям методу головних компонент він достатньо успішно може бути використаний для прогнозування статистики кіберінцидентів, забезпечуючи при цьому найменшу похибку прогнозу. Загальна модель ризику кіберінцидентів комплексно враховує вплив на кібербезпеку усього спектру технічних, організаційних та людських чинників та будується на основі схеми виникнення кіберінциденту, у якій кожен інцидент пов'язується з передумовою його виникнення. Зазначений підхід дозволяє здійснювати аналіз безпосередніх причинно-наслідкових зв'язків, що мають місце в процесі інциденту та виявляти як основні, так і приховані причини та види подій, що призводять до кіберінцидентів на підставі статистичних даних. Наведений у статті приклад демонструє прикладну спрямованість компонентного аналізу, зокрема для задач прогнозу числа вихідних показників кіберінцидентів за, порівняно малим числом допоміжних (латентних) змінних, що виражають причини цього явища, візуалізації багатовимірних даних та виділення типоутворюючих ознак кіберінцидентів.

Лисецький Ю. М. Підходи до забезпечення інформаційної безпеки / Ю. М. Лисецький, Д. Й. Калбазов // Математичні машини і системи. – 2023. – № 4. – С. 26-32.

Р/1052

У статті проаналізовано підходи до забезпечення інформаційної безпеки, що склалися на сьогоднішній день серед підприємств вітчизняного ринку: ситуаційний, інтеграційний та інтеграційно-інноваційний. Визначено їх відмінності: ситуаційний – це точкове впровадження систем інформаційної безпеки, децентралізація управління, відсутність єдиного підходу до проектування системи захисту, інертність впровадження систем; інтеграційний – наявність служб планування і забезпечення інформаційної безпеки, формування єдиних вимог для інформаційної безпеки, аналіз критичності інформаційних активів, управління ризиками та загрозами, проектування інформаційної безпеки від бізнес-процесів підприємства; інтеграційно-інноваційний – наявність операційних центрів безпеки, центрів оперативного реагування, централізованих систем моніторингу інформаційної безпеки, планування безперервності бізнесу та створення планів аварійного відновлення, формування відмовостійких систем захисту. Наведено існуючі проблеми вибору методів і технологій захисту інформації. Розглянуто способи та засоби ефективного забезпечення інформаційної безпеки підприємства: міжмережеві екрани нового покоління, SIEM-системи, DLP- системи, а також брокер безпеки хмарного доступу – CASB. Його використання для забезпечення інформаційної безпеки у хмари дозволяє вирішувати

такі завдання: контроль доступу; захист даних; виявлення та реагування на загрози; відповідність регуляторним вимогам; моніторинг та аудит; управління політиками безпеки. Проаналізувавши підходи до забезпечення інформаційної безпеки вітчизняних підприємств, можна зробити висновок, що воно має ґрунтуватися на комплексному підході та ефективній інтеграції всіх елементів IT-інфраструктури на різних рівнях їх взаємодії.

Метод формування еталонного субдовкілля для виявлення фішингових URL-адрес / А. Корченко, Є. Іванченко, Ф. Сатибалдієва [та ін.] // Захист інформації. – 2023. – Т. 25, № 2. – С. 82-95.

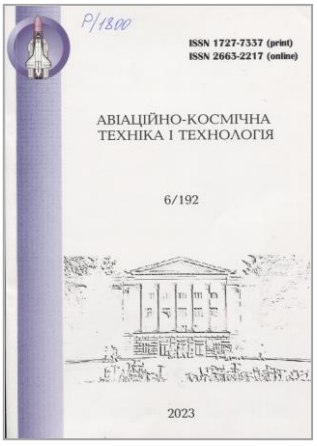
Р/1428

Збільшення та удосконалення кібератак на інформаційні системи зростає щорічно, а використання сучасних систем виявлення вторгнень дозволяє швидко реагувати на нові види кібератак та вдосконалювати існуючі засоби захисту. Такі системи достатньо розвинуті, але для їх ефективної роботи необхідна інформація у режимі реального часу, з використанням якої можливо виявляти підозрілу активність неавторизованої сторони. Таку інформацію можна проаналізувати з використанням експертних підходів. Експертні методи можуть допомогти виявляти нові неочікувані кібератаки. Використання методів, моделей і систем на основі теорії нечітких множин при побудові засобів виявлення аномалій, породжених реалізацією нових кіберзагроз, дозволить удосконалити та зробити більш ефективними існуючі системи виявлення вторгнень. А розробка відповідних технічних рішень, що працюють в нечітких умовах, дозволить виявляти раніше не відомі та модифіковані види кібератак. Також є досить ефективні розробки, які використовуються для вирішення завдань виявлення кібератак, наприклад, низка методів формування еталонного субдовкілля для системи виявлення вторгнень, але вони не орієнтовані на фішингові підходи. Однак, як показує практика, при появі нових загроз та відповідних аномалій, породжених атакуючими діями з невстановленими або нечітко визначеними властивостями, відповідні засоби не завжди залишаються ефективними, тому розробка методів, що дозволяють удосконалити процес отримання нового еталонного субдовкілля для системи виявлення вторгнень, є актуальним завданням. Одним із небезпечних засобів, який направлений на збір конфіденційної інформації, такої як логіни, паролі, фінансові реквізити та інші особисті дані є фішинг. Для цього розроблений метод формування еталонного субдовкілля для виявлення фішингових URL-адрес за рахунок сформованого набору параметрів: кількість країн за IP-адресою, вік домену та експертного оцінювання стану субдовкілля інформаційної системи дозволить формалізувати процес формування параметрів еталонного субдовкілля для вирішення задач, щодо виявлення фішингових URL-адрес.

Митько Л. О. Кібербезпека в енергетиці на тлі швидкого розвитку штучного інтелекту / Л. О. Митько // Електронне моделювання = Electronic Modeling. – 2024. – Т. 46, № 1. – С. 70-77.

Р/518

Розглянуто проблеми захисту інформаційних ресурсів від кібератак державних та приватних підприємств на основі аналізу даних в США за 2022 р. з урахуванням виду кібератаки та оцінок заподіяної шкоди. Аналіз кібератак дозволяє зробити висновок, що безпека інформаційних ресурсів залежить більше ніж на 90 відсотків від людського фактору і саме в цьому напрямку потрібно прикладати максимум зусиль. Покращення захисту інформаційних ресурсів не можливе без використання штучного інтелекту (ШІ). Розглянуто можливості впливу ШІ на кіберзахист енергетичної галузі та запропоновано напрями, що потребують уваги при розробці систем захисту від кібератак, які «приречені» на залучення досягнень ШІ. При цьому враховано, що ШІ не тільки дозволяє підвищити захист від кібератак, але й може зробити комп'ютерні мережі менш захищеними. А надзвичайні можливості нейромереж потребують невідкладного створення погоджених міжнародних протоколів для їх розробників.



Нарожний В. В. Ризик-орієнтоване оцінювання кібербезпеки додатків доповненої реальності з використанням IMECA-аналізу / В. В. Нарожний, В. С. Харченко // Авіаційно-космічна техніка і технологія. – 2023. – № 6(192). – С. 86-94.

Р/1800

Предметом дослідження є метод аналізу загроз, вразливостей та вибору контрзаходів для забезпечення кібербезпеки в додатках доповненої реальності (AR).

Метою є збільшення повноти оцінювання кіберебезпеки додатків AR шляхом використання формалізованої процедури виявлення та аналізу ризиків поширених загроз, вразливостей та типів атак.

Дослідження базується на відомому методі IMECA (аналізу видів, наслідків та критичності втручань), який структурує процедуру аналізу та мінімізації ризиків шляхом введення відповідних контрзаходів для забезпечення прийнятних ризиків кібербезпеки. *Завдання:* обґрунтувати множину основних загроз кібербезпеці, характерних для AR додатків; визначити та описати вразливі до загрузки місця в системах AR; надати детальну класифікацію різних кібератак, спрямованих на платформи AR, враховуючі результати дослідження нещодавніх інцидентів; використати метод IMECA для структурованого опису і аналізу питань кібербезпеки та запропонувати надійні контрзаходи.

738104 В
004

Проблеми інформатики та комп'ютерної техніки (ПІКТ-2023) [Текст] = Informatics and Computer Technics Problems (PICT-2023) : праці XII Міжнародної науково-практичної конференції, Чернівці, 10-12 листопада, 2023 / Ін-т кібернетики імені В. М. Глушкова НАН України, Київ. нац. ун-т імені Тараса Шевченка, Нац. техн. ун-т України "КПІ імені Ігоря Сікорського", Чернівецький нац. ун-т імені Юрія Федьковича. - Чернівці : [ЧНУ], 2023. - 200 с. : іл., табл. - Загол. обкл. : Proceedings of the Twelfth International Conference on "Informatics and computer technics problems". - Бібліогр. наприкінці ст. Текст укр., англ. Обкл. англ.

Зі змісту:

Секція кібербезпека

Ганжело Д. В., Ганжело М. Г., Трембач Д. В. **Принципи безпечного дизайну інформаційних систем.** – С. 193-194.

У статті розглянуто ключові принципи безпеки інформаційних систем на прикладі вже існуючої Платформи для розгортання та супроводу державних електронних реєстів [1].

Д'яченко Л. І., Танащишена І. Є. **Використання Splunk для моніторингу мережі.** – С. 194-196.

В даній роботі розглядаються проблеми, що постають перед адміністраторами мереж, що часто змінюються. Надаються рекомендації щодо кращих практик застосування систем моніторингу інцидентів у мережі та систем для автоматичного аналізу подій. Розглядаються функціональні можливості Splunk, як одного з найкращих продуктів на ринку для автоматизованого аналізу та моніторингу поведінки мережі.

Прохоров Г. В., Ганжело Д. В., Трембач Д. В. **Загальні принципи зберігання резервних копій даних інформаційних систем.** – С. 197-198.

У статті розглянуто ключові принципи резервування даних (бекапів) інформаційних систем на прикладі вже існуючої Платформи для розгортання та супроводу державних електронних реєстів.

Prokhorov G. V., Hanzhelo M. G., Trembach D. V. **Implementation of Security Measures in Information Systems Design.** – P. 198-200.

The article discusses specific steps to ensure the security of information systems using the example of the already existing Platform for the deployment and support of state electronic registers [1].

737811 R
004

Сагун, Андрій Вікторович.
Основи криптографічного та стеганографічного захисту інформації [Текст] : навч. посіб. для студ. спец. 125 - "Кібербезпека", 12 "Інформаційні технології" всіх форм навчання / Сагун А. В., Кулініч О. М., Хайдуров В. В. ; Нац. ун- т біоресурсів і природокористування України. - Київ : [НУБіП України], 2023 - .
Ч. 1 : Криптографічний захист інформації / А. В.Сагун, О. М. Кулініч, В. В. Хайдуров. - Київ, 2023. - 285 с. : іл. - Бібліогр.: с. 262-265.

Зміст навчального посібника відповідає навчальній програмі дисципліни «Основи криптографічного та стеганографічного захисту інформації».

737812 R
004

Сагун, Андрій Вікторович.
Основи криптографічного та стеганографічного захисту інформації [Текст] : навч. посіб. для студ. спец. 125 - "Кібербезпека", 12 "Інформаційні технології" всіх форм навчання / Сагун А. В., Кулініч О. М., Хайдуров В. В. ; Нац. ун- т біоресурсів і природокористування України. - Київ : [НУБіП України], 2023 - .
Ч. 2 : Стеганографічний захист інформації / А. В. Сагун, О. М. Кулініч, В. В. Хайдуров. - Київ, 2023. - 146 с. : іл. - Бібліогр.: с. 129.

Тецький А. Г. Тестування на проникнення компонентів FPGA як сервісу для забезпечення кібербезпеки / А. Г. Тецький // Авіаційно-космічна техніка і технологія. – 2023. – № 6(192). – С. 95-101.

Р/1800

Метою роботи є вдосконалення сучасних методів тестування на проникнення сервісів, що надають послугу FPGA as a Service, для виявлення вразливостей, ліквідація яких підвищує рівень захищеності сервісів та підвищує рівень довіри користувачів до таких сервісів.

Завдання: проаналізувати можливі загрози платформ FPGA as a Service; проаналізувати структуру платформ FPGA as a Service; проаналізувати варіанти використання стандарту проведення тестування на проникнення; запропонувати ключові складові забезпечення кібербезпеки платформ FPGA as a Service.

Відповідно до поставлених завдань, були отримані наступні результати. Проведено дослідження проблем кібербезпеки платформ FPGA as a Service та пропонується комплекс складових забезпечення кібербезпеки платформ FPGA as a Service. Проведено аналіз актуальних загроз кібербезпеки платформ FPGA as a Service.

Розглянуто можливість застосування стандарту проведення тестування на проникнення стосовно сервісів FPGA.

Регулярне проведення аудиту та тестування на проникнення є ключовим елементом стратегії кібербезпеки та допомагає підтримувати довіру клієнтів та користувачів до FPGA сервісів. Запропоновано комплекс складових забезпечення кібербезпеки платформ FPGA as a Service, що відповідає сучаснішим загрозам.

Хорошко В. О. Вибір показників прогнозування кіберзахищеності комп'ютерних систем / В. О. Хорошко, Ю. Хохлачова, Н. Вишневська // Безпека інформації. – 2023. – Т. 29, № 1. – С. 41-47.

Р/1408

В статті запропонований алгоритм вибору показників прогнозування кіберзахищеності комп'ютерних систем.

Процеси кіберзахисту відносяться до випадкових багатовимірних, динамічних нестаціонарних, активних (цілеспрямованих), що ускладнює завдання прогнозування показників кіберзахищеності. Аналіз публікацій показав складність вибору найефективнішого методу прогнозування кіберзахищеності, який полягає у визначенні щодо класифікації методів прогнозування характеристик кожного методу, переліку вимог до ретроспективної інформації. Таким чином, застосування екстраполяції у прогнозуванні завжди передбачає використання будь-яких моделей, тому моделювання є основою для екстраполяції. Прогнозування є досить складним завданням, що підтверджується аналізом причин та факторів, які потенційно впливають на зміни прогнозованого показника.

Вирішення такого завдання, як і будь-якого іншого складного завдання, потребує системного підходу, який допомагає зрозуміти суть проблеми та вибрати адекватні методи його вирішення, а також оцінить причини можливих невдач. Отриманий алгоритм містить багатоповерховість моделі, як у класі лінійних, так і в класі нелінійних за вхідними змінними моделями; виключення окремих членів кращого приватного опису та на основі цього розширення базисного набору аргументів; є оптимальним за обчислювальними витратами для міграційних алгоритмів методу групового обчислювального алгоритму схеми розрахунку критерію іспиту, що ковзає. А також має можливість оцінювати коефіцієнти у моделях як за методом найменших квадратів, так і за методом найменших модулів.

738255 В
355

Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського.

Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України [Текст] : [наук. вид.] / [голов. ред. Загорка Олексій Миколайович]. - [Київ] : [ЦВСД НУОУ імені Івана Черняховського].

Вип. 3(79). - [Київ], 2023. - 146 с. : граф., рис., табл. - Бібліогр. наприкінці ст. Текст кн. укр., англ.

Зі змісту:

Сніцаренко П. М., Саричев Ю. О., Гордійчук В. В., Грицюк В. В. **Кіберстійкість в умовах воєнної агресії РФ: досягнення України та проблемні питання.** – С. 31-38.

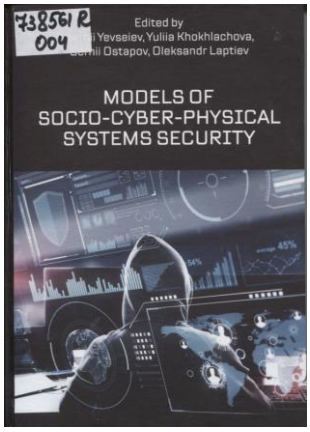
У статті досліджується явище забезпечення кіберстійкості в Україні в умовах широкомасштабної воєнної агресії РФ. Проведено аналіз стану кіберборотьби напередодні та під час вторгнення РФ на територію України. Окреслено характерні закономірні особливості та проблемні питання в інтересах досягнення належної кіберстійкості в Україні в умовах зовнішньої воєнної агресії.

Шуліпа Н. С. Дослідження ефективності застосування мови Python для створення додатків кібербезпеки та захисту інформації / Н. С. Шуліпа, А. В. Мазурик // Сучасний захист інформації. – 2023. – № 3(55). – С. 32-37.

Р/2300

Стаття досліджує можливості мови програмування Python для розв'язання задач кібербезпеки та захисту інформації. Дослідження зосереджується на порівнянні Python з іншими мовами програмування, такими як C++, C#, Java та JS, за їхніми можливостями розробки додатків для аналізу мережі, аналізу даних, інструментів захисту, інструментів для тестування, автоматизації

задач та веб-розробки. Також в статті наводяться приклади коду на Python та JS для розробки шифраторів даних та проведення аналізу мережі, а також описується фреймворк для тестування безпеки OWASP ZAP на Python. Загалом, стаття показує, що Python є потужним інструментом для розв'язання завдань кібербезпеки та захисту інформації, здатним конкурувати з іншими мовами програмування.



738561 R
004

Models of socio-cyber-physical systems security [Текст] : monograph / [authors: Serhii Yevseiev, Yuliia Khokhlachova, Serhii Ostapov and others] ; edited by Serhii Yevseiev, Yuliia Khokhlachova, Serhii Ostapov, Oleksandr Laptiev. - [Kharkiv] : PC TECHNOLOGY CENTER, 2023. - 168 p. : il., fig., tabl. - References.: p. 157-167 (132 назви).

The monograph discusses the methodology for cooperative conflict interaction modeling of security system agents. The concept of modeling the structure and functioning of the security system or critical infrastructure facilities is demonstrated. The method for assessing forecast of social impact in regional communities is presented. Counteracting the strategic manipulation of public opinion in decision-making by actors of social networking services based on the conceptual model for managed self-organization in social networking services are developed. Algorithms for thinning the critical infrastructure identification system and their software are implemented.

The monograph is intended for teachers, researchers and engineering staff in the field of cybersecurity, information technology, social engineering, communication systems, computer technology, automated control systems and economic information security, as well as for adjuncts, graduate students and senior students of relevant specialties.

Figures 60, Tables 32, References 132 items.