"Безпека та захист інформаційного простору "

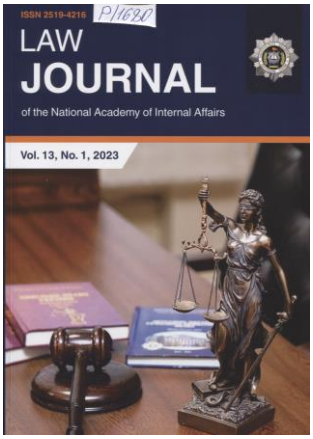
(надходження II півріччя 2023)

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

Американські штати борються за обмеження доступу дітей до соціальних мереж / © 2023 CQ-Roll Call, Inc., розповсюджене Tribune Content Agency, LLC // Бізнес і безпека. – 2023. – № 1(149). – С. 57.

Р/1070

Кілька штатів просувають законодавство, яке обмежує доступ дітей до Інтернету та використання соціальних мереж, створюючи ще одне потенційне протистояння між штатами та Конгресом щодо технологічної політики.



Антіпова О. Стратегічні комунікації як складова інформаційної безпеки держави / О. Антіпова // Law Journal of the National Academy of Internal Affairs = Юридичний часопис Національної академії внутрішніх справ. – 2023. – Vol. 13, No. 1. – P. 44-52. – Текст англ.

Р/1680

Становлення інформаційного суспільства на сучасному етапі означене активним процесом інфообміну та комунікативної взаємодії на різних рівнях – на міжособистісному, між соціальними групами; верствами, країнами. Крім конструктивних характеристик, цей процес означений низкою ризиків, які постають перед інформаційною безпекою держав та спрямовані на порушення прав і свобод людини, підривання усталених демократичних традицій та авторитету на геополітичній мапі світу. Це засвідчує актуальність дослідження стратегічних комунікацій як запоруки надійності безпекового сектору.

З огляду на зазначене, *метою статті* є вивчення особливостей комунікативної взаємодії на стратегічному рівні в контексті інформаційної безпеки держави.

Ключовими загрозами, які постають перед інформаційною безпекою в контексті комунікативної взаємодії на стратегічному рівні, є використання агресивної риторики, продукування потоків неправдивої інформації, поширення фейкового контенту, міфотворчість і намагання переписати історію.

Розглянуто сутність російських інформаційних кампаній, які проводяться засобами дезінформації, та досвід країн ЄС та Балтії щодо протидії їм.

Українські реалії засвідчили раціональність побудови стратегічних комунікацій на основі довіри суспільства до суб'єктів продукування інформації, з огляду на що, крім| представників дипломатичного корпусу та представників сектору безпеки, активними учасниками цього процесу мають бути експерти з числа науковців та громадянське суспільство загалом.

Практична цінність результатів полягає в тому, що їх може бути використано для визначення шляхів побудови національної системи стратегічних комунікацій та створення інституції з координації цієї діяльності на міжвідомчому рівні.

736877 R
31

Боднар, Ірина Романівна.

Основні критерії інформаційної політики України [Текст] : монографія / І. Р. Боднар ; Центральна спілка споживчих товариств України, Львівський торговельно-економічний ун-т. - Львів : Вид-во Львів. торг.-екон. ун-ту, 2023. - 144 с. : граф., табл. - Бібліогр.: с. 118-134.

У монографії досліджуються проблеми та окреслені перспективні напрями інформаційної політики України. Особлива увага приділена аналізу сучасного стану розвитку інформаційної сфери та інформаційної політики в Україні. Висвітлюються основні тенденції глобалізації інформаційних процесів. Запропоновані перспективи розвитку процесів інформатизації в Україні. Розглядаються концепції інформаційної політики України. Визначені пріоритетні напрями державної політики у сфері розвитку цифрової економіки.

Глобенко С. Інформаційний простір держави та проблеми забезпечення його захисту в Україні / С. Глобенко // Науковий вісник: Державне управління. – 2023. – № 1(13). – С. 195-210.

Р/1443

Досліджено проблематику державної політики в інформаційній сфері з акцентом на гарантуванні інформаційної безпеки, значний інтерес до якої продиктований сучасною суспільною дійсністю. Розглянуто погляди щодо забезпечення національної безпеки і оборони держави в умовах новітніх загроз і викликів в аспекті необхідності досягнення максимально можливої стійкості як окремих її складових, так і самої системи в цілому. Виокремлено особливості національного інформаційного простору та з'ясовано основні проблеми його подальшого розвитку з урахуванням забезпечення безпеки особи, суспільства, держави як одного із основоположних факторів функціонування механізму держави, який характеризується значним рівнем комплексності й багатоаспектності, що нині в умовах України потребує пошуку максимально ефективних управлінських рішень. Проаналізовано роль і місце України у загальносвітових рейтингах безпекових спроможностей у сфері захисту інформаційного простору, відповідних механізмів державного управління, а також основних чинників, які впливають на ці процеси. Узагальнено й систематизовано фактори формування державної системи інформаційної безпеки, напрями імплементації стратегічних планів та відповідних заходів з питань забезпечення безпеки в інформаційній сфері в умовах надзвичайних і кризових явищ, наведено теоретичні й прикладні аспекти перспектив подальшого розвитку інформаційного простору держави і забезпечення його захисту в умовах України.

736778 В
623

Державний науково-дослідний інститут випробувань і сертифікації озброєння та військової техніки.

Збірник наукових праць Державного науково-дослідного інститут випробувань і сертифікації озброєння та військової техніки [Текст] : науково-теоретичний та науково-практичний збірник наукових праць. - Черкаси : [Євгенок О. О.], 2022 - .

Вип. 4(14). - Черкаси, 2022. - 176 с. : граф., рис., табл. - Бібліогр. наприкінці ст. - Алф. покажч.: с. 176. Текст укр. та англ. мов.

Зі змісту:

Кучеренко Ю. Ф., Александров О. В., Носик А. М., Камак Д. О. **Методологічні основи інформаційної безпеки країни з урахуванням умов сучасного періоду її державотворення.** – С. 99-109.

У статті наведені методологічні основи інформаційної безпеки держави як однієї з складових національної безпеки України. Детально розкриті складні умови сучасного періоду процесу державотворення в Україні, що визначаються впливом низки негативних зовнішніх та внутрішніх факторів, а саме: процесом формування нової політичної географії у світі; поширенням впливу національних рухів на відносини між країнами та в середині суспільства; здійснення повномасштабного військового вторгнення з боку російської федерації; загострення міждержавних економічних та територіальних суперечностей; зростання кількості внутрішніх конфліктів етнічного і релігійного характеру на території країни; зріст злочинності та корупції в державі; боротьба різних партій та громадських організацій за лідерство між собою; неконтрольоване розповсюдження зброї; низький економічний стан країни та зниження рівня життя більшості населення країни тощо. Представлена система інформаційної безпеки держави, визначені основні її складові та розкриті джерела, що класифіковані за групами впливу на її базову основу, яка представляє собою інформацію. Розкритий механізм необхідності адаптації системи захисту інформаційної сфери від зміни зовнішніх та внутрішніх факторів впливу на неї.

737367 R
35

Збірник нормативних документів та матеріалів з питань законного перехоплення інформації в Україні [Текст] : [наук.-практ. вид.] / [уклад.: Чечіль Ю. О., Кавешніков П. О., Говоруха В. І., Сивобородько А. В.] ; Служба безпеки України, Укр. НДІ спец. техніки та судових експертиз СБУ. - Київ : ІСТЕ СБ України, 2023. - 280 с. : табл. - Бібліогр.: с. 278-279. Уклад. зазнач. на звороті тит. арк.

Збірник містить нормативні документи з питань законного перехоплення інформації в Україні, а також розроблені Українським науково-дослідним інститутом спеціальної техніки та судових експертиз Служби безпеки України технічні вимоги, програми та методики випробувань у сфері забезпечення реалізації функції законного перехоплення.

Методичний посібник з кібербезпеки для військових та держслужбовців // Бізнес і безпека. – 2023. – № 1(149). – С. 47-56.

Р/1070

Матеріал підготовлено спільно з Департаментом контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБУ. Матеріал постійно оновлюється та доповнюється.

736777 В
34

Повітряне і космічне право. Юридичний вісник [Текст] : наукові праці Національного авіаційного ун-ту / Нац. авіац. ун-т. - Київ : [НАУ]. **№ 1(66).** - Київ, 2023. - 220 с. - Бібліогр. наприкінці ст. Текст укр., англ.

Зі змісту:

Юровський А. Г. **Поширення недостовірної інформації про особу в мережі Інтернет: актуальні питання судового захисту.** – С. 140-147.

Метою статті є розгляд актуальних питань судового захисту поширення недостовірної інформації про особу в мережі Інтернет, у тому числі щодо публічних осіб, на основі вивчення й узагальнення

доктринального доробку юридичної науки, чинного законодавства України та судової практики. Методологічною основою дослідження є загальнонаукові та спеціальні методи наукового пізнання. Результати: було зроблено висновок про те, що останнім часом національні суди у більшості випадків відмовляють у задоволенні позовних вимог та не визнають інформацію, яка поширюється через мережу Інтернет, недостовірною та не зобов'язують її спростовувати, оскільки в більшості випадків суди вважають судження відносно позивачів оціночними і такими, що критикують особу, однак наклеп при цьому відсутній, що позбавляє осіб отримати належний захист та сатисфакцію в судовому порядку. Обговорення: в огляді судової практики щодо справ про захист честі, гідності та ділової репутації Касаційний цивільний суд у складі Верховного суду зазначав, що національним судам необхідно знаходити правильний баланс або пріоритет як для правової та демократичної держави між двома конституційно гарантованими правами: правом на свободу думки і слова, правом на вільне вираження своїх поглядів та переконань, з одного боку, та правом на повагу до людської гідності, гарантіями невтручання в особисте і сімейне життя, судовим захистом права на спростування недостовірної інформації про особу, з другого боку. Саме в цьому суть правильного вирішення дифамаційного спору. Автор статті з цим цілковито погоджується.

Правові механізми забезпечення інформаційної безпеки України в умовах гібридної війни / С. В. Легомінова, Ю. В. Щавінський, Т. М. Мужанова [та ін.] // Телекомунікаційні та інформаційні технології. – 2023. – № 1(78). – С. 101-110. – Текст англ.

Р/1921

У статті зроблений аналіз вітчизняних досліджень стану та особливостей нормативно-правового забезпечення інформаційної безпеки у порівнянні із зарубіжними країнами. За результатами аналізу визначені основні проблеми законодавчого забезпечення інформаційної безпеки, що є актуальними для багатьох країн світу. Вони полягають у розбіжності міжнародних правил поведінки в кіберпросторі, що не дозволяє ефективно застосовувати правові механізми для сумісних дій, вказують на недостатню ефективність посилення норм відповідальності за порушення інформаційної безпеки в умовах гібридної війни. Визначені особливості правового регулювання забезпечення інформаційної безпеки та шляхи вирішення проблем, які полягають у розробленні та впровадженні законодавчих норм, що регулюють діяльність в мережі Інтернет, у тому числі й у національному сегменті, та повинні включати особливі вимоги до провайдерів мережевого зв'язку та інших суб'єктів, які забезпечують функціонування мережі в умовах воєнного стану. Визначена потреба у законодавчому закріпленні особливих механізмів інформаційної безпеки для організації здійснення превентивних законодавчих заходів з метою попередження кібератак та інформаційного впливу на суспільство в особливих умовах гібридної війни, які включають особливості функціонування суб'єктів інформаційної безпеки в умовах воєнного стану, посилення співпраці з міжнародною спільнотою у відповідності з міжнародними угодами. Запропоновано врахування факторів для забезпечення ефективного нормативно-правового забезпечення в умовах гібридної війни. Визначена необхідність проведення наукових досліджень з розробки пропозицій щодо вдосконалення вітчизняного законодавства на основі міжнародних угод та імплементації їх положень в національне законодавство щодо забезпечення інформаційної безпеки.

Сопілко І. Соціально-правові основи інформаційної безпеки держави, суспільства й особи в Україні / І. Сопілко, Л. Рапацька // Scientific Journal of the National Academy of Internal Affairs = Науковий вісник Національної академії внутрішніх справ. – 2023. – Vol. 28, № 1. – P. 44-54.

Р/2375

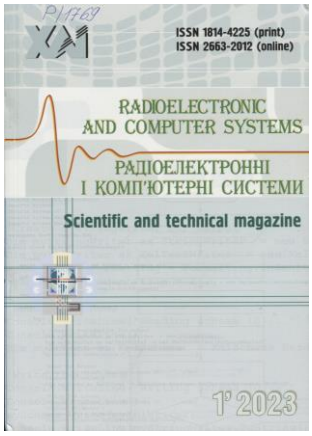
Україна зазнає військової агресії у зв'язку із повномасштабним вторгненням росії, яка використовує також інформаційну зброю. Тому актуальною є проблема забезпечення достатньо високого рівня інформаційної безпеки в Україні. *Мета дослідження* – висвітлити суть й особливості поняття «інформаційна безпека», пов'язаних із нею

термінів, здійснити всебічний аналіз чинного нормативно-правового масиву з питань забезпечення надійного рівня інформаційної безпеки як основи національної безпеки.

Доведено важливість забезпечення інформаційної безпеки на рівні кожного окремого суб'єкта як підґрунтя для існування українського інформаційного суспільства та засобу протидії агресивним діям Російської Федерації. Обґрунтовано важливість забезпечення достатнього рівня кібербезпеки як визначального елемента інформаційної оборони, надання якого має бути максимально узгодженим із державною інформаційною політикою.

Окреслено потенційні наслідки недотримання надійного рівня інформаційної та кібербезпеки на фоні повномасштабного вторгнення, а саме: повалення влади, крах репутації України на міжнародній арені, хаотичні процеси в суспільстві та зростання рівня його невдоволення, економічна криза та людські жертви.

Схарактеризовано наявний стан забезпеченості інформаційної безпеки в країні та запропоновано шляхи його вдосконалення.



Стрєлкіна А. Методологія оцінювання задоволеності вимогами на ранніх стадіях процесу розроблення програмного забезпечення / А. Стрєлкіна, А. Тецький // Радіоелектронні і комп'ютерні системи. – 2023. – № 1(105). – С. 197-206. – Текст англ.

Р/1769

Отриманим ***результатом*** є методологія кількісного оцінювання рівня задоволеності вимогами з урахуванням різних характеристик вимог на початку етапу розроблення. Дане дослідження є значним і необхідним, тому що в більшості випадків попередні дослідження не пропонують вичерпних кількісних та вимірних методів визначення ступеня задоволеності вимогами до тих чи інших характеристик. Також показано використання створеної методології з реальними вимогами. Додатково наведено рекомендації щодо посилення рівня задоволеності вимогами. ***Висновок.*** Запропонована методологія є розширюваною, на відміну від інших, а це означає, що характеристики та шкала оцінок можуть фактично змінюватись в залежності від вимог, цілей та інших особливостей ІТ-проекту.

736818 В
623

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

№ 4 (71). - Київ, 2022. - 160 с. : граф., рис., табл. - Бібліогр. наприкінці ст. Текст кн. укр., англ. Дод. тит. арк. англ.

Зі змісту:

Козубцов І. М., Козубцова Л. М. **Методика розрахунку ефективності функціонування системи захисту інформації й кібербезпеки в інформаційно-комунікаційних системах та оцінювання вкладу окремих показників.** – С. 31-44.

Метою статті є обґрунтування пропозицій щодо вибору окремих показників оцінювання здатності функціонування системи захисту й кібербезпеки інформації в інформаційно-комунікаційних системах спеціального зв'язку з частковими показниками ефективності. Результатом дослідження стало обґрунтоване рішення нового науково-практичного завдання з обґрунтування показників ефективності функціонування системи захисту інформації й кібербезпеки за результатами аналізу щорічних звітів інцидентів кібербезпеки. Уперше запропоновано окремі показники оцінювання здатності (ефективності) функціонування системи захисту й кібербезпеки інформації в інформаційно-комунікаційних системах спеціального зв'язку.

Харківський національний університет Повітряних Сил імені Івана Кожедуба.

Збірник наукових праць Харківського національного університету Повітряних Сил [Текст] = Scientific Works of Kharkiv National Air Force University : щоквартальне наукове видання / Міноборони України. - Харків : Видавництво ХНУПС імені Івана Кожедуба.

Вип. 2 (72). - Харків, 2022. - 76 с. : рис., табл. - Дод. тит. арк. англ. - Бібліогр. наприкінці ст. - Алф. покажч.: с. 76. Текст кн. укр., англ.

Зі змісту:

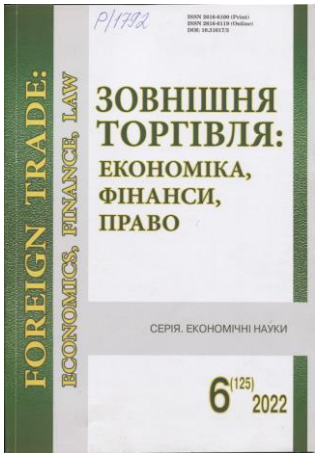
Кучеренко Ю. Ф., Власік С. М., Сальник О. В., Воробйов О. Г. **Методологічні аспекти щодо розробки системи захисту інформації в системах управління військового призначення.** – С. 65-70.

У статті наведені методологічні основи щодо необхідності розвитку теорії та практики забезпечення надійного функціонування різних систем управління військового призначення в інформаційному просторі держави в умовах повномасштабної агресії Російської Федерації проти України, як одних з головних елементів інформаційної безпеки держави.

Детально розкриті як зовнішні, так і внутрішні фактори впливу на інформацію, що циркулює при функціонуванні систем управління військового призначення в сучасних умовах жорсткого протиборства в інформаційній сфері. Розкрита необхідність забезпечення надійного функціонування систем управління військового призначення за рахунок розробки та впровадження системи захисту інформації, що циркулює в них.

Наведені методологічні аспекти щодо розробки системи захисту інформації в даних системах: визначені основні вимоги та завдання до них, розкриті їх функціональні складові, наведені джерела загроз для інформації, що циркулює в даних системах та визначені основні їх порушення. Розкритий механізм необхідності відповідності системи захисту інформації в системі управління військового призначення основним принципам при їх створенні, з урахуванням зміни зовнішніх та внутрішніх факторів (методів, алгоритмів, засобів, користувачів) впливу на неї.

Показано, що запобігання впливу на інформаційний простір нашої країни та основні його елементи, як то системи управління військового призначення, особливо в умовах ведення повномасштабної збройної агресії з боку Російської Федерації є першочерговим завданням сучасного етапу, вирішення якого забезпечить надійне їх функціонування та виконання завдань за призначенням на належному рівні.



Чубаєвський В. Світова практика управління подіями інформаційної безпеки корпорацій / В. Чубаєвський // Зовнішня торгівля: економіка, фінанси, право. – 2022. – № 6. – С. 73-82.

Р/1792

Проблема. Центральним процесом у системі управління інформаційною безпекою корпорацій є процес «Управління подіями». Тільки компетентна організація цього процесу може забезпечити належний рівень усієї послідовності етапів ефективного функціонування системи захисту корпоративної інформації, що охоплює всі дії протягом усього життєвого циклу події інформаційної безпеки; від планування, навчання та підвищення обізнаності до виявлення, реагування та навчання на подіях інформаційної безпеки.

Метою статті є теоретико-методичне обґрунтування доцільності запровадження процесу Управління подіями інформаційної безпеки в контексті аналізу світової практики системи захисту корпоративної інформації.

Програмні системи захисту інформації

Білобровець І. В. Технологія виявлення мережевих загроз з використанням програмного забезпечення Zabbix / І. В. Білобровець, Г. Г. Найман // Сучасний захист інформації. – 2023. – № 2(54). – С. 19-28.

Р/2300

В статті проведено аналіз проблеми забезпечення інформаційної безпеки підприємства та необхідності застосування систем моніторингу. Проаналізовано сучасні існуючі системи моніторингу та принципу виявлення загроз. Доведено, що для виявлення загроз та підвищення інформаційної безпеки актуально використовувати програмне забезпечення Zabbix. Визначено призначення, характеристику та основні можливості Zabbix. Наведено приклади застосування програмного забезпечення для виявлення атак. На основі досліджень проведених в статті розроблено технологію виявлення загроз із застосуванням Zabbix і плагіну для нього. Показано ефективність застосування розробленої технології для виявлення загроз.

737188 В
355

Військовий інститут Київського національного університету імені Тараса Шевченка.
Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка [Текст] : збірник наукових праць. - Київ : [ВІКНУ].
Вип. № 77. - Київ, 2022. - 184 с. : іл. - Алф. покажч.: с. 175. - Бібліогр. наприкінці ст. Текст кн. укр., англ.

Зі змісту:

Міночкін Д. А., Нсер А. М. **Програмні методи моніторингу мережевої безпеки.** – С. 125-133.
В роботі розглянуто програмні методи моніторингу мережевої безпеки (NSM – Network Security Monitoring). Із зростанням і швидким розвитком мобільного зв'язку, великих даних і технологій штучного інтелекту ми вступаємо в еру мобільного Інтернету. З безперервною інтелектуалізацією мережевої безпеки та інфраструктури інформаційних технологій, вони широко використовуються в галузі промислового контролю, що робить мережеву безпеку все більш відкритою. В даний час спостерігається зростання кількості інформаційних загроз та факторів, що призводять до нестабільного функціонування мереж передачі даних. Одним із компонентів забезпечення інформаційного захисту мереж є програмні комплекси, призначені для виявлення шкідливої чи підозрілої активності – методи моніторингу мережевої безпеки (NSM). Методи моніторингу мережевої безпеки (NSM) використовуються для моніторингу та обміну даними по мережі щодо подій, пов'язаних з інформаційною безпекою.
У статті наведено визначення методів моніторингу мережевої безпеки, їх класифікація, цикл NSM та їх опис. Розглянуто деякі з найвідоміших і широко використовуваних багатомодульних рішень NSM. Найвідомішими прикладами таких комбінацій є IDS/IPS, SEM/SIEM і UTM. Моніторинг мережевої безпеки перевіряє, чи працюють перші лінії захисту, надає можливість усунути загрози, перш ніж вони завдадуть реальної шкоди. Якщо в системі є вразливість, NSM дозволяє зрозуміти, де ці вразливості та як запобігти атакам.

Волошко Д. С. Технологія виявлення простих вірусів у програмному коді / Д. С. Волошко, Д. Є. Гамза, Є. С. Смолєв // Сучасний захист інформації. – 2023. – № 2(54). – С. 35-40.

Р/2300

У даній статті розглянуто питання виявлення простих вірусів у програмному коді. Віруси можуть завдати значної шкоди програмному забезпеченню, тому важливо попередити їхнє поширення та

виявляти їх вчасно. Для виявлення вірусів можна використовувати різні методики, такі як вірус сканери, статичний аналіз коду, аналіз поведінки програмного коду та інші. При виявленні вірусів в програмному коді важливо звертати увагу на контекст виявлення та досвід експерта з безпеки програмного забезпечення. Виявлення вірусів у програмному коді є важливим етапом в забезпеченні безпеки програмного забезпечення та може допомогти запобігти шкоді, яку можуть завдати віруси.

Єсіна М. В. Моделі загроз для хмарних послуг / М. В. Єсіна, В. В. Онопріенко, А. В. Толок // Радіотехніка. – 2023. – Вип. 212. – С. 36-41.

Р/908

Хмарні послуги стали популярними завдяки своїм перевагам над традиційними обчисленнями. Хмара дає можливість отримувати віддалений доступ до програмного забезпечення, обладнання та інших послуг. Це дозволило компаніям бути більш продуктивними і зробило можливою віддалену роботу. Хмарні послуги мають менше вимог до обладнання та інфраструктури, що знижує витрати на утримання та підтримку інформаційних технологій. Майбутній успіх організацій буде залежати від обсягу впровадження хмарних обчислень у свою роботу. За прогнозами витрати на хмарні IT-технології будуть зростати та у 2025 р. будуть перевищувати витрати на традиційні IT-технології. Безпека хмарних послуг стає критичною проблемою, оскільки все більше компаній завершують свою цифрову трансформацію. Незважаючи на велику кількість переваг, хмарні послуги також стикаються зі своїми власними загрозами та викликами безпеки. Оскільки хмарні послуги зберігають та обробляють значну кількість конфіденційної інформації, злам хмари може призвести до витоку даних, що може стати на шляху розвитку бізнесу та завдати значної шкоди репутації компанії. Існують ризики, зв'язані з недоступністю хмарних послуг у випадку технічних проблем та залежності від зовнішніх провайдерів. Тому, підприємства повинні ретельно оцінювати потенційні загрози та приймати відповідні заходи для захисту своїх даних та бізнесу в цілому при використанні хмарних послуг. Існує багато методів, які допоможуть визначити, наскільки ваша організація готова до зростаючої кількості загроз. Моделювання загроз один з методів прогнозування та підготовки до можливих загроз. Використання фреймворків моделювання дозволяє розподілити ресурси та спланувати можливі дії під час атаки. Існує багато фреймворків моделювання, але важливо пам’ятати, що ці фреймворки мають свої переваги та недоліки, тому вибір залежить від контексту та потреб конкретної системи. Аналіз, оцінка та порівняння існуючих методів моделювання та захисту від загроз у хмарних послугах є основною метою цієї статті.

Єсіна М. В. Огляд загроз безпеці та цілісності даних у хмарних обчисленнях / М. В. Єсіна, А. А. Кравченко, С. О. Кравченко // Радіотехніка. – 2023. – Вип. 212. – С. 30-35.

Р/908

Хмарні обчислення стали невід’ємною частиною нашого життя, і сьогодні їх використовують майже усюди. Взагалі, хмарні обчислення являють собою концепцію надання IT ресурсів у вигляді послуг. Розрізняють дві моделі хмарних обчислень – розгортання, що відрізняються за типом управління хмарою та доступу до неї та рівнем безпеки, і моделі обслуговування, які відрізняють за рівнем надання послуг – це впливає, окрім іншого, на рівень відповідальності постачальника і споживача послуг. Хмарні сервіси почали набувати своєї популярності у 2009 р., і з кожним роком попит на них лише зростав у геометричній прогресії. Особливо великої популярності вони набули під час пандемії у 2019 р., коли люди повинні були залишатись вдома, не зупиняючи при цьому робочих процесів, і зараз, в постковідні часи, вони теж залишаються популярними через їх зручність, високу доступність, легку масштабованість та економію коштів. Через розповсюджену експлуатацію послуг хмарних обчислень виникає необхідність високого рівня безпеки. На жаль, у великій популярності є свої мінуси – окрім того, що слідкувати за безпекою віддаленого

середовища складніше, ніж за збереженістю локального комп'ютера, існує ще безліч загроз. Люди використовують технології хмарних обчислень у великих обсягах, наприклад, на роботі, в особистих цілях та інше, так як вони мають велику довіру до цих технологій. Саме це є причиною необхідності підтримувати безпеку на високому рівні і весь час її вдосконалювати. Загрози безпеки хмарних обчислень зазвичай поділяють на загрози конфіденційності, цілісності та доступності. Щоб запобігти втраті довіреної інформації провайдери послуг мають забезпечити її цілісність. Користувачі хочуть бути впевнені в тому, що їх дані не попадуть до рук зловмисника або на сторонні сервіси. Тож, дана стаття розглядає найбільш поширені загрози безпеки і цілісності даних в хмарних обчисленнях та існуючі методи, що на різних рівнях та за допомогою різних інструментів запобігають цим вразливостям та можливим проблемам.

Засоби протидії загрозам для інтелектуальних систем від безфайлового зловмисного програмного забезпечення / Ю. І. Катков, О. В. Зінченко, С. С. Цибульник, Ю. О. Вітенко // Зв'язок. – 2022. – № 3(157). – С. 3-11.

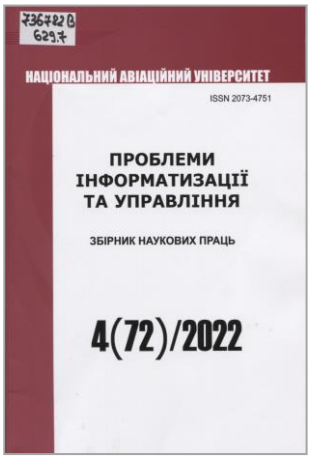
Р/776

Розглянуто актуальне питання пошуку засобів протидії загрозам для інтелектуальний систем від безфайлового зловмисного програмного забезпечення. Поставлено задачу: для своєчасної локалізації та мінімізації можливих збитків від впливу загроз (уразливостей, атак) від безфайлового зловмисного програмного забезпечення на критичні об'єкти IT-інфраструктури інтелектуальних систем підприємства потрібно визначити найкращий напрям створення методів їм своєчасного виявлення. У статті показано, що інтелектуальна система підприємства має вразливість та критичність від слабкого впливу загроз (уразливостей, атак) зловмисника на критичні об'єкти IT-інфраструктури підприємства. Наслідком цього є загострення протиріч між складністю методів захисту об'єктів критичної IT-інфраструктури підприємства від шкідливого програмного забезпечення, зокрема безфайлового зловмисного програмного забезпечення, та їх результативністю з погляду своєчасної локалізації та мінімізації можливих збитків від впливу загроз. Але розв'язання цього протиріччя можливе завдяки створенню гнучких організаційним структур спостереження за синергетичними уявленнями процесу адаптації інтелектуальних систем підприємства до загроз від безфайлового зловмисного програмного забезпечення. Показано, що передусім є потреба в постійному вдосконаленні методів виявлення впливу загроз в напрямі їх передбачення. Для цього, ґрунтуючись на виконаний аналіз алгоритму дії безфайлового зловмисного програмного забезпечення через набори експлойтів, шкідливі макроси Microsoft Word та скомпрометоване мережне обладнання, визначено механізм впливу на PowerShell операційних систем Windows, Unix. На основі цього механізму запропоновано дії щодо захисту від безфайлових шкідливих програм. Для реалізації цих дій показано, в який спосіб можливо здійснювати пошук макросів, виявляти та підтверджувати наявність безфайлових загроз. Запропоновано застосування перевірки інформаційної безпеки підприємства за допомогою методів аудиту. Як основний метод аудиту рекомендовано використовувати методологію моделювання атак хакерів Red Teaming та методи тестування penetration testing. Розглянуто способи їх вживання.

Мусієнко Д. Безпека використання месенджерів / Д. Мусієнко // Бізнес і безпека. – 2023. – № 2-3(150). – С. 58-65.

Р/1070

Безпека в тому чи іншому месенджері – річ дуже мінлива. У світі кожної хвилини з'являється нове програмне забезпечення для зчитування особистих переписок та доступу до персональних даних. Убезпечити себе від кожної з них – неможливо. Та досить часто ми віддаємо свої дані добровільно і навіть не розуміємо цього. Тож, яким би безпечним не був месенджер на програмному рівні, доступ до вашої інформації можна отримати не тільки технічних шляхом, але й за допомогою інтелектуального злому.



736782 В
629.7

Проблеми інформатизації та управління [Текст] : зб. наук. пр. / Нац. авіац. ун-т, Ф-т кібернетики, комп'ютерної та програмної інженерії. - Київ : [НАУ].
Вип. 4 (72). - Київ, 2022. - 76 с. : іл., табл. - Бібліогр. наприкінці ст.

Зі змісту:

Антонішин М. В., Міснік О. І., Цуркан В. В. **Способи тестування уразливостей мобільних програмних застосунків.** – С. 4-12.

Проаналізовано застосовність способів тестування уразливостей мобільних програмних застосунків. Показано їхню орієнтованість на задоволення настанов відкритого проекту забезпечення безпеки вебзастосунків. Це зведено до застосування керівництва з тестування і стандарту верифікування безпеки мобільних програмних застосунків. За ними виокремлено статичний і динамічний способи тестування уразливостей. Водночас встановлено обмеженість практичного застосування даних способів у зв’язку з неоднозначною належністю сценаріїв до статичного або динамічного тестування, наприклад; експортованих компонентів, MSTG-STORAGE-6, нестандартних сертифікатів, сертифікату SSL-пінінгу, MSTG-NETWORK-4. Цим обумовлено актуальність аналізування застосовності способів тестування уразливостей мобільних програмних застосунків. Результатами існуючих досліджень підтверджено узагальнену орієнтованість на задоволення настанов відкритого проекту забезпечення безпеки вебзастосунків. На їхній основі забезпечено повноту сценаріїв тестування і, як наслідок, сформульовано рекомендації для зменшення витоку конфіденційної інформації. Зосереджено увагу на протидії атакам критично важливих програмних застосунків. Окрему увагу приділено розширенню можливостей розроблених засобів тестування уразливостей використанням відповідних фреймворків.

Розробка засобів інформаційного захисту для систем оптичного розпізнавання тексту / К. Ю. Дергачов, Л. О. Краснов, В. О. Білозерський, А. Я. Зимовин // Радіоелектронні і комп'ютерні системи. – 2022. – № 2(102). – С. 159-177. – Текст англ.

Р/1769

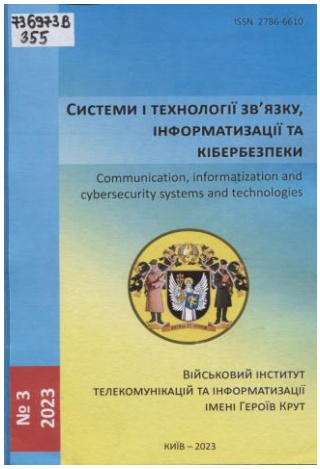
Мета роботи – сформулювати концепцію створення сучасного простого та надійного методу захисту інформації при її передачі каналами зв'язку, визначити об'єктивні критерії якості його роботи, ***створити набір алгоритмів для реалізації запропонованого методу та програмне забезпечення для проведення експериментальних досліджень.*** За результатами цих досліджень необхідно оцінити ефективність практичного використання запропонованого методу як у плані надійності кодування/декодування даних, що передаються, так і в плані скритності фактів передачі інформації.

Отримано такі результати. Сформульовано універсальну концепцію створення та використання сучасних методів захисту інформації в системах оптичного розпізнавання текстів при передачі конфіденційних даних по відкритих каналах зв'язку. Визначено основні критерії якості цих систем. Запропоновано новий оригінальний комбінований метод кодування повідомлень, що передаються, за допомогою QR-кодів з подальшим маскуванням фактів передачі даних різними способами LSB-стеганографії. ***Для проведення експериментальних досліджень було розроблено програмне забезпечення для розпізнавання текстів, яке базується на програмі оптичного розпізнавання символів (OCR) Tesseract версії 4.0. Програма написана мовою Python з використанням сучасних ресурсів бібліотеки OpenCV.*** Програмно реалізована методика оцінки ефективності роботи алгоритмів кодування даних і скритності сеансів зв'язку. Наведено приклади роботи системи та результати тестування програмного забезпечення в режимі кодування та потайної передачі повідомлень.

Розробка програмного засобу для еволюційного декодування блокових кодів / О. М. Комар, В. О. Дробик, М. А. Штомпель, В. П. Лисечко // Телекомунікаційні та інформаційні технології. – 2023. – № 1(78). – С. 74-81.

Р/1921

Представлено підхід до розробки програмного засобу для еволюційного декодування блокових кодів. Розглянуто ключові етапи процесу проектування даного програмного засобу. Обґрунтовано застосування мови програмування Python при програмній реалізації еволюційного декодування блокових кодів. Визначено, що дана мова програмування забезпечує достатньо просту та функціональну реалізацію обчислень у скінченних полях та процедур еволюційної оптимізації вбудованими компонентами та бібліотеками. Наведено узагальнені етапи еволюційного декодування деякого блокового коду. Показано, що спочатку здійснюється жорстке декодування, а потім виконується еволюційний пошук кодового слова на основі найбільш надійного базису породжувальної матриці блокового коду. Запропоновано функціональну діаграму, що заснована на опрацюванні основних етапів декодування блокових кодів з використанням процедур еволюційної оптимізації. Дана діаграма ілюструє пропонований спосіб реалізації програмним засобом необхідних функцій компонентами еволюційного декодеру. Розроблена архітектура програмного засобу еволюційного декодування блокових кодів. Пропонована архітектура передбачає використання наявних бібліотек блокових кодів, обчислень у скінченних полях, еволюційної оптимізації та розробленого функціоналу декодеру. Розглянуто призначення окремих блоків та програмних модулів даного програмного засобу. Результати роботи доцільно застосовувати для підвищення достовірності передавання інформації у існуючих та перспективних системах радіозв'язку. Також отримані результати можуть бути використані при проведенні експериментальних досліджень характеристик різних типів блокових кодів, що знаходять застосування у сучасних електронних комунікаціях.



736973 В
355

Системи і технології зв'язку, інформатизації та кібербезпеки [Текст] = Communication, information 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 - .

№ 3. - Київ, 2023. - 186 с. : граф., рис., табл. - Текст кн. укр. та англ. мов. - Бібліогр. наприкінці ст.

Зі змісту:

Фесьоха В. В., Кисиленко Д. Ю., Нестеров О. М. **Аналіз спроможності існуючих систем антивірусного захисту та покладених у їхню основу методів до виявлення нового шкідливого програмного забезпечення у військових інформаційних системах**. – С. 143-151.

У статті вирішується завдання аналізу спроможності існуючих антивірусних систем та покладених у їх основу методів до виявлення нового шкідливого програмного забезпечення в інформаційних системах критичної інфраструктури, зокрема сектору сил оборони держави. Зазначено, що офіційні дані розробників антивірусних систем часто не підтверджують задекларований рівень точності виявлення нового шкідливого програмного забезпечення на практиці. До того ж, у більшості випадків задекларований показник точності виявлення нового шкідливого програмного забезпечення є вищим за аналогічний показник виявлення відомого шкідливого програмного забезпечення, що свідчить про тестування розглянутих антивірусних систем у специфічних умовах, занадто відмінних від реальних.

Описано властивості нового шкідливого програмного забезпечення з метою пошуку найбільш відповідного йому класу комп'ютерних вірусів. Класи поліморфних (олігоморфних) та

метаморфних вірусів демонструють найбільш повну відповідність зазначеним властивостям, що дозволяє стверджувати про їх значну частку у застосуванні нового шкідливого програмного забезпечення.

Наведено характеристику методів виявлення шкідливого програмного забезпечення, які завдяки своїм властивостям спроможні певною мірою адаптуватися до метаморфної (поліморфної) їх природи. Найбільш повну відповідність демонструють методи, в основу яких покладено теорію нечіткої логіки.

Запропоновано напрям удосконалення існуючих антивірусних систем щодо підвищення адаптивності до виявлення нових (поліморфних, метаморфних) класів шкідливого програмного забезпечення. Отримані результати доцільно розглядати, як підґрунтя для реалізації нових підходів до виявлення шкідливого програмного забезпечення з метою ідентифікації раніше невідомих його екземплярів, що дозволить значно підвищити ефективність забезпечення кібербезпеки сучасних інформаційних систем та мереж.

737234 В
62

"Харківський політехнічний інститут". Національний технічний університет.

Вісник Національного технічного університету "Харківський політехнічний інститут" [Текст] = Bulletin of the National Technical University "KhPI". Series: New solutions in modern technology : зб. наук. пр. - Харків : НТУ "ХПІ". - (Нові рішення в сучасних технологіях).

№ 1(15). - Харків, 2023. - 103 с. : іл., табл. - Бібліогр. наприкінці ст. Текст кн. укр., англ.

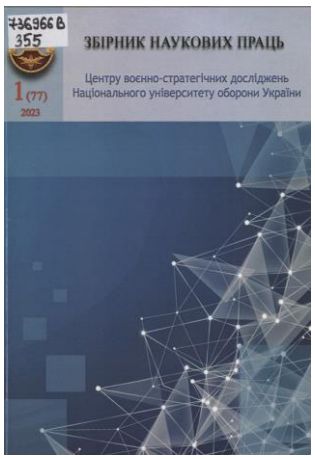
Зі змісту:

Цибульник С. О., Зубарський Д. О., Півторак Д. О. **Прикладне програмне забезпечення для зберігання персональної інформації.** – С. 53-59.

У сучасному світі персональну інформацію будь-якої людини можна умовно розділити на дві великі категорії: загальна та особлива. Як можна зрозуміти з назви, перша категорія відповідає за той тип даних, які можна знайти у загальному доступі, а саме: прізвище, ім'я, по-батькові, підпис, місце та дата народження, громадянство, сімейний стан, освіта, банківські реквізити, тощо. Подібне різноманіття персональних даних потребує різних методів та автоматизованих засобів зберігання.

Сьогодні все частіше приватні та державні установи відмовляються від зберігання інформації у паперовому вигляді. Це пояснюється низьким рівнем безпеки таких сховищ, які можуть постраждати від вогню, води, шкідників, тощо. Показано, що цифрове зберігання інформації дозволяє позбутися подібних проблем. Персональні дані, які зберігаються в електронному вигляді, найчастіше можна відновити навіть при втраті пристрою, з якого здійснювався доступ до них. Одним із основних видів персональної інформації в сучасному суспільстві є дані для входу: логін та пароль. Саме тому було розроблено алгоритмічне та програмне забезпечення автоматизованої системи збереження персональних даних користувача. Дана система має надати можливість користувачу генерувати стійкі до стандартних методів зламу паролі та зберігати їх у базі даних. Розроблення автоматизованої системи проходило з використанням архітектурного шаблону MVC, який є одним з варіантів реалізації багаторівневої архітектурної моделі. Для детального проектування та кодування обрано об'єктно-орієнтовну мову програмування зі статичною строгою типізацією Java. Також прийнято рішення розробити автоматизовану систему у вигляді веб-додатку за допомогою використання фреймворка Spring.

У ході процесу розроблення спроектовано локальну базу даних, в якій зберігатимуться персональні дані у вигляді логінів та паролів, які ввів користувач або згенерувала сама система. Розроблено алгоритм генерації стійких до зламу стандартними методами паролів. Також використано алгоритми хешування, як додатковий захист головного пароля від веб-додатку. Створено графічний інтерфейс, який дозволяє користувачу отримати доступ до основних функцій автоматизованої системи.

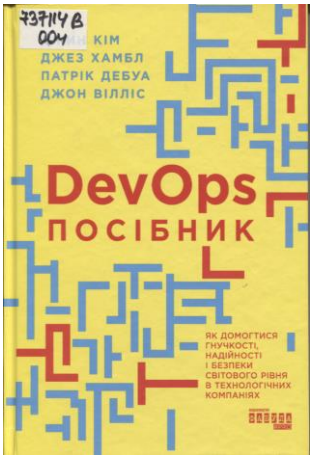


736966 В
355

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. 1(77). - [Київ], 2023. - 140 с. : граф., рис., табл. - Бібліогр. наприкінці ст. Текст кн. укр., англ.

Зі змісту:

Рибидайло А. А., Галаган В. І., Васюхно С. І., Мулявка А, С., Руденська Г. В. **Порядок організації створення спеціального програмного забезпечення для інформаційних систем військового призначення.** – С. 69-78.
Розглянуто стратегії розроблення програмного забезпечення. Обґрунтовано підхід до порядку розроблення програмного забезпечення для інформаційних систем військового призначення з урахуванням умов ведення відповідного проекту.
"Основна увага приділена процедурі вибору моделі життєвого циклу. Вибір моделі життєвого циклу програмного забезпечення є важливим етапом у створенні програмного продукту. Для визначення раціональної моделі необхідно врахувати низку факторів та зосередитися на розробленні продукту згідно з вибраною моделлю. Періодичне оцінювання прогресу та ризиків дасть змогу вносити необхідні зміни та забезпечити успішне завершення проєкту".



737114 В
004

DevOps. Посібник: Як домогтися гнучкості, надійності і безпеки світового рівня в технологічних компаніях [Текст] / Джин Кім, Джез Хамбл, Патрік Дебуа і Джон Вілліс. - [Харків] : Видавничий Дім "Фабула", [2023]. - 384 с. : табл., рис. - Покажч. : с. 362-379.

Ні для кого не є секретом, що існує тісна взаємозалежність між розробкою і використанням програмного забезпечення. Саме цим і користується низка практик, що отримали загальну назву DevOps і мають своєю метою допомогти організаціям швидше та якісніше створювати та оновлювати програмні продукти і послуги. Ця методологія зосереджена на узгодженні розробки і постачання програмного забезпечення із його використанням, і це завдання зазвичай вирішується за допомогою автоматизації процесів і стандартизації середовищ розробки з метою забезпечення швидкої підготовки релізів.
«Посібник із DevOps», створений четвіркою маститих фахівців, що стояли біля витоків цієї методології, не тільки познайомить читача-професіонала з ідеологією і практикою цього руху, а й надасть безліч корисних порад у питаннях організаційних змін і тіснішої співпраці між різними типами працівників, об’єднання та автоматизації різних процесів, їх швидшого та частішого виконання, системного адміністрування, автоматизації процесів постачання та ін. Загалом, DevOps охоплює весь процес постачання програмного забезпечення, перетворюючи його на більш передбачуваний і динамічний, надійний та ефективний. Завдяки цьому значно скорочуються терміни виходу ПЗ на ринок, підвищується якість продукції, знижується кількість відмов і збоїв, скорочується час внесення змін і виправлення помилок.
Отже, немає нічого дивного в тому, що цей підхід набув широкої популярності серед інженерів і менеджерів найпрогресивніших світових компаній у сфері IT.

Телекомунікаційні мережі та інформаційно-комунікаційні технології

Аналіз технологій побудови мережі передавання даних із високими вимогами щодо інформаційної безпеки, надійності та затримки / В. О. Власенко, Ю. В. Щавінський, М. М. Запорожченко, В. С. Тищенко // Зв'язок. – 2023. – № 3(163). – С. 8-15.

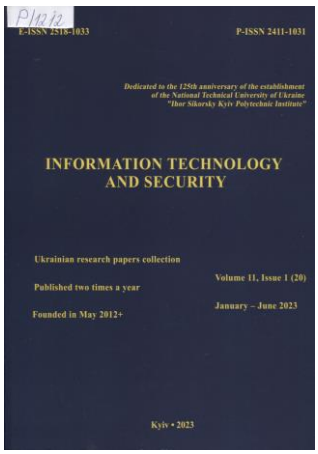
Р/776

Наукову статтю присвячено аналізу сучасних підходів і технологій у побудові мереж передавання даних, спрямованих на забезпечення інформаційної безпеки, надійності та мінімальної затримки.

Обґрунтовано потребу в комплексному врахуванні факторів, які впливають на ефективність мережі із зосередженням уваги на надійності та безпеці. Аналіз мереж дає можливість створити інфраструктуру, яка відповідатиме вимогам сучасного інформаційного середовища, комплексно брати до уваги переваги та недоліки кожної технології мережі в процесі побудови. Для математичного оцінювання надійності мережі передавання даних запропоновано марковську модель, яка базується на теорії марковськик процесів.

Розроблена мовою програмування Python із використанням бібліотек модель дає змогу кількісно оцінити надійність мережі передавання даних, зважаючи на різні фактори відмов, переводів між станами та відновлення. Модель дозволяє прогнозувати стани мережі та планувати превентивні організаційні і технічні заходи щодо забезпечення надійності та безпеки через постійно зростаючі вимоги до якості обслуговування і захисту конфіденційної інформації. Аналіз методів затримки передавання інформації виявив залежність швидкості і обсягу інформації, що передається, від багатьох факторів, зокрема пропускної здатності, навантаження мережі, типу та швидкості з'єднання, оброблення даних вузлами мережі.

У дослідженні визначено потребу в комплексному відпрацюванні систем оцінювання та створенні загальної моделі оцінювання.



Ахрамович В. Метод розрахунку захищеності інформації в соціальних мережах в залежності від кількості співтовариств / В. Ахрамович // Information Technology and Security. – January-June 2023. – Vol. 11, Iss. 1(20). – P. 15-26.

Р/1212

Розроблена математична модель (лінійна система диференціальних рівнянь) та проведено дослідження моделі захисту персональних даних від кількості співтовариств та інтенсивності передачі даних в соціальних мережах.

Розглянута лінійна система захисту інформації в соціальних мережах у математичному розумінні цього терміну. При описі лінійними моделями об'єкт, хоча б приблизно, має бути лінійним. Такий підхід дозволяє достатньо просто розглянути математичні моделі. Якщо таке явище не спостерігається, необхідне дослідження системи захисту на лінійність.

Досліджено залежності: величини потоку інформації в соціальній мережі від складових захисту інформації, кількості персональних даних, та швидкості потоку даних; захищеності системи від розмірів системи (як і від кількості персональних даних); загроз безпеки інформації від кількості співтовариств, а також враховано: Z_p – коефіцієнт, що відображає вплив заходів щодо захисту інформації; C_v – коефіцієнт, що відображає вплив швидкості витоку даних; $C_к$ – коефіцієнт, що відображає вплив кількості даних на їх витік, C_{d2} – коефіцієнт, що відображає вплив розмірів

системи на захищеність; C_{dl} – коефіцієнт, що відображає вплив захищеності на витік даних; $m_к$ – кількість зв'язків у соціальних мережах; $n_к$ – кількість вершин у соціальних мережах; a –параметр a може служити для налагодження алгоритму розбиття мережі. Отримано рішення – рівняння гармонічного осцилятора, яке розпадається на три випадки: дорезонансна зона, резонансна та зарезонансна. Таким чином, ***досліджено вплив параметрів кількості співтовариств на параметри системи захисту соціальної мережі. Таке дослідження корисне та важливе з точки зору захисту інформації в мережі, оскільки параметри кількості співтовариств значно впливають, до 100 %, на показник захисту.*** В результаті досліджень встановлено, що системи захисту соціальної мережі нелінійні.

737400 R
004

Безпека мобільних пристроїв [Текст] : наук.-практ. посібник / [упоряд.: М. Г. Вербенський, В. О. Криволапчук. Д. В. Смерницький та ін.] ; МВС України, Держ. наук.-дослід. ін-т. - Київ : ["Вид-во Людмила"], 2023. - 100 с. : граф., рис., табл. - (Серія "Кібербезпека"). - Бібліогр.: с. 97-99 та у виносках. Упоряд. зазнач. на с. 100 та звороті тит. арк.

У посібнику викладено питання захисту мобільних пристроїв від хакерських атак. Проведено класифікацію та узагальнено ризики, пов'язані з використанням мобільних пристроїв. Розглянуто підходи двох найбільших виробників операційних систем для мобільних пристроїв щодо заходів, які вживаються для протидії хакерським атакам. Значну увагу приділено питанням захисту мобільних пристроїв користувачем. Надано детальні рекомендації щодо налаштувань мобільних пристроїв під керуванням операційних систем Androd та iOS. Підібрано низку корисних програм для цих операційних систем, використання яких покращить стійкість мобільного пристрою до хакерських атак.

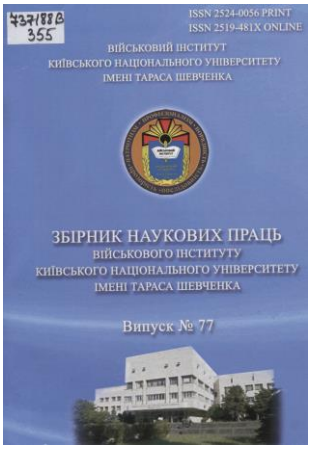
Бучик С. С. Аналіз і розпізнання мережних відмов в інформаційній мережі / С. С. Бучик, С. В. Толюпа, О. В. Кітура // Зв'язок. – 2023. – № 2(162). – С. 37-42.

Р/776

У статті показано, що кожна інформаційна система має свої особливості, зумовлені сферою її застосування. Важливість і відповідальність задач, розв'язуваних за допомогою систем у реальному масштабі часу, зумовили високі вимоги до надійності цих систем, а відмова всієї інформаційної системи або її окремих компонентів може призвести до негативних наслідків. В основу розпізнання мережних відмов покладено принцип визначення за системою продукцій характеру мережних відмов. Цей принцип реалізовано діалоговою процедурою в межах байєсівського підходу, який дає змогу нагромаджувати інформацію, що надходить із різних джерел, з метою підтвердження (не підтвердження) певної гіпотези.

Розроблено стратегію керування логічним висновком, керувальними параметрами якої є поточна ймовірність істинності гіпотез, межі їх зміни і ваги асоційованих із цими гіпотезами ознак. Облік поточної ймовірності гіпотез і меж їх зміни дає змогу в процесі висновку, по-перше, фокусувати увагу на найбільш перспективній (імовірній) гіпотезі, а по-друге, припиняти висновок, досягнувши верхнього порогу, що уможливить скорочення кількості ознак, котрі перевіряються, і в такий спосіб скоротити час діалогу. Крім цього, досягнувши нижнього порогу, гіпотеза від-кидається як неправдоподібна і в процесі висновку більше не бере участі, що також призводить до скорочення часу розпізнання.

Облік ваг ознак у процесі логічного висновку дає змогу передусім перевіряти ті ознаки, які максимально збільшують імовірність правдоподібності гіпотез. Загалом, розроблена стратегія, на відміну від класичної схеми, породжує цілеспрямований процес перевірки правдоподібності гіпотез, що зумовлює скорочення часу розпізнання.



737188 В
355

Військовий інститут Київського національного університету імені Тараса Шевченка.

Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка [Текст] : збірник наукових праць. - Київ : [ВІКНУ].

Вип. № 77. - Київ, 2022. - 184 с. : іл. - Алф. покажч.: с. 175. - Бібліогр. наприкінці ст. Текст кн. укр., англ.

Зі змісту:

Лєнков С. В., Джулій В. М., Солодєєва Л. В. **Метод протидії поширенню та виявлення шкідливої інформації в соціальних мережах**. – С. 103-116.

В роботі проведено дослідження задачі виявлення та протидії поширенню у соціальних мережах шкідливої інформації, в тому числі «фейкових новин». Особливо гостро стоїть необхідність протидії поширенню у соціальних мережах таких новин, що породжують хвилі паніки, які виникають під час пандемії. На теперішній час – війна в Україні. Фейкові новини поширюються у соціальних мережах у шість разів швидше, ніж правдиві дописи. Російська пропаганда стала одним з головних елементів війни в Україні, її якісно закамуфльовано під вигляд матеріалів західних ЗМІ – DW, CNN або BBC.

З метою підвищення ефективності системи протидії в Інтернет-мережах вирішена задача розробки відповідного підходу підвищення обґрунтованості прийнятого рішення на протидію поширенню та виявлення шкідливої інформації за рахунок збільшення числа параметрів, що враховуються при виборі інформаційного об’єкта впливу та дійових контрзаходів. Вирішення поставленої задачі, досягається за рахунок проведення ранжування контрзаходів та аналізу джерел мережі шкідливої інформації. Запропонований метод протидії та виявлення в соціальних мережах поширенню шкідливої інформації, ґрунтується на використанні запропонованих моделей, алгоритмів, забезпечує, на відміну від аналогів, аналіз інформації соціальних мереж; формування списків інформаційних об'єктів впливу для проведення протидії об'єктам, сортування інформаційних об’єктів; надання оператору системи протидії пропонованого та альтернативних варіантів з обґрунтуванням вибору.

737189 В
355

Військовий інститут Київського національного університету імені Тараса Шевченка.

Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка [Текст] : збірник наукових праць. - Київ : [ВІКНУ].

Вип. № 78. - Київ, 2023. - 156 с. : іл. - Алф. покажч.: с. 147. - Бібліогр. наприкінці ст. Текст кн. укр., англ.

Зі змісту:

Лєнков С. В., Джулій В. М., Берназ А. М., Муляр І. В., Пампуха І. В. **Метод прогнозування вразливостей інформаційної безпеки на основі аналізу даних тематичних інтернет-ресурсів**. – С. 123-134.

Аналіз проведеного дослідження поточного стану в області інформаційної безпеки показує, що темпи розвитку інформаційних та комп'ютерних технологій значно випереджають процес створення програмно-апаратного забезпечення в області інформаційної безпеки. Пріоритетними, в даній ситуації, є задача аналізу, класифікації, виявлення діючих механізмів та засобів проведення атак і загроз інформаційній безпеці системи, які можуть призвести до отримання несанкціонованого доступу до конфіденційних даних, порушення функціонування інформаційної системи, визначення заходів протидії атакам та загрозам, оцінка заданої шкоди, розробка нормативно-правової бази, механізмів захисту та критеріїв інформаційної безпеки системи протидії. На сьогодні не існує єдиного підходу до вирішення проблеми захищеності інформаційно-

пошукових систем, стосовно предметних областей: розробниками програмно-апаратного захисту інформації пропонуються відповідні компоненти на вирішення конкретних задач; забезпечення надійного захисту інформаційних ресурсів потребує реалізації відповідних технічних та організаційних заходів в комплексі, що супроводжуються розробкою відповідної документації. Більшість (учасних програмно-апаратних систем виявлення комп'ютерних загроз та атак працюють із використанням підходів сигнатурного аналізу та фіксації інтернет-мережевих аномалій. Дані підходи мають недоліки, пов'язані із використанням потужних обчислювальних ресурсів на їх реалізацію, при виявленні нових комп'ютерних загроз мають низьку ефективність. Метод прогнозування вразливостей інформаційної безпеки на основі даних інтернет-ресурсів, заснований на нечіткому логічному виводу, семантичному та статистичному аналізі, відрізняється можливістю виявлення вразливостей та загроз до їх реалізації, дозволяє описувати закономірності інформаційного процесу наповнення тематичних ресурсів новими текстовими повідомленнями, що відображається на якості прогнозування.

Реалізований в інформаційно-аналітичній системі алгоритм прогнозування вразливостей та загроз безпеки інформації на основі аналізу потоку даних тематичних ресурсів дозволяє автоматизувати інформаційний процес виявлення нових вразливостей, загроз, надає фахівцям інформаційної безпеки можливість оцінити своєчасно ступінь захищеності ресурсів та при необхідності вжити відповідних заходів щодо нейтралізації можливих загроз та вразливостей, тим самим підвищити інформаційну безпеку обчислювальних комп'ютерних систем від реалізації нових мережевих комп'ютерних атак.

737190 В
355

Військовий інститут Київського національного університету імені Тараса Шевченка.

Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка [Текст] : збірник наукових праць. - Київ : [ВІКНУ].

Вип. № 79. - Київ, 2023. - 198 с. : іл. - Алф. покажч.: с. 189. - Бібліогр. наприкінці ст. Текст кн. укр., англ.

Зі змісту:

Лєнков С. В., Джулій В. М.,Мірошніченко О. В., Браун В. О., Прохорський С. І. І**нформаційно-аналітична система прогнозування вразливостей та загроз інформаційної безпеки.** – С. 114-127.

В роботі запропоновано структурну схему інформаційно-аналітичної системи прогнозування вразливостей та загроз інформаційної безпеки.

Реалізований в інформаційно-аналітичній системі алгоритм прогнозування вразливостей та загроз безпеки інформації на основі аналізу потоку даних тематичних інтернет-ресурсів дозволяє автоматизувати інформаційний процес виявлення нових вразливостей, загроз, надає фахівцям інформаційної безпеки можливість оцінити своєчасно ступінь захищеності ресурсів та при необхідності вжити відповідних заходів щодо нейтралізації можливих загроз та вразливостей, тим самим підвищити інформаційну безпеку обчислювальних комп'ютерних систем від реалізації нових мережевих комп'ютерних атак.

Проведено аналіз систем нечіткого логічного виводу, сучасних засобів обробки великих об'ємів даних, засобів морфологічного аналізу тексту, редакторів онтологій. Для проведення логічного моделювання інформаційної системи прогнозування вразливостей та загроз інформаційної безпеки побудовані UML-діаграми діяльності, послідовності дій, класів. Для фізичного моделювання системи розроблено UML-діаграми розгортання та компонентів.

Обґрунтовано можливість реалізації інформаційно- аналітичної системи прогнозування вразливостей та загроз безпеки інформації на основі аналізу текстових повідомлень тематичних інтернет-ресурсів з використанням наступних програмних продуктів: СКБД MySQL, редактор онтології – Protege, системи нечіткого логічного виводу – Fuzzy Logic Designer, засобів морфологічного аналізу даних – Mystem. Для проведення оцінки отриманих результатів обчисленні показники MAPE, MAE, RMSE для значень прогнозування виникнення вразливостей та загроз інформаційної безпеки, а також розраховані на їх основі згладжені часові рядки з періодом три та п'ять діб.

Гиренко І. Удосконалений метод побудови двосторонніх границь показників надійності обладнання інформаційно-комунікаційної мережі при обмеженій вихідній інформації / І. Гиренко, І. Кононова, Ю. Щиголь // Information Technology and Security. – January-June 2023. – Vol. 11, Iss. 1(20). – P. 84-95.

Р/1212

При дослідженні питань забезпечення заданої надійності обладнання інформаційно-комунікаційної мережі, важливим напрямком є розроблення ефективних методів оцінки інтенсивності виникнення збоїв та їх впливу на процеси функціонування мережі. Вирішення задач оцінки та забезпечення надійності може стикатися з невизначеністю вихідної інформації через обмежену можливість отримання великої кількості досліджень випадкових величин, які визначають безвідмовність, ремонтопридатність та процес функціонування системи, що необхідні для оцінки ступеня збігу теоретичних та статистичних розподілів. Зазвичай можна точно визначити лише значення математичного очікування та дисперсії випадкової величини на основі результатів випробувань або даних експлуатації.

Метою дослідження є розробка удосконаленого методу оцінки надійності обладнання інформаційно-комунікаційної мережі в умовах, коли окремі функції розподілу вихідних випадкових величин невідомі, а визначені тільки лише перший та другий їхні початкові моменти. У статті представлено удосконалений аналітичний метод, який використовується для отримання розрахункових співвідношень, необхідних для створення двосторонніх оцінок показників надійності комунікаційного обладнання інформаційно-комунікаційної мережі. У цьому методі враховуються стійкі відмови та збої в умовах апріорної невизначеності. Основна ідея запропонованого удосконаленого методу полягає у виокремленні типових функціоналів, які відображають основні показники надійності комунікаційного обладнання з часовим і (або) структурним резервуванням. Ці функціонали будуть розраховані на повній вихідній інформації та надалі використовуватись для отримання точних нижніх та верхніх границь при відомих початкових моментах розподілу вихідних випадкових величин на першому етапі. На другому етапі будуть отримані двосторонні оцінки показників надійності, застосувавши граничні значення відповідних функціоналів. Досліджено, що збої можуть значно погіршувати показники надійності, навіть якщо використовується структурне та часове резервування.

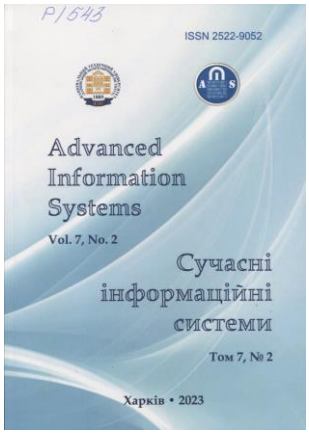
Гринкевич Г. О. Побудова захищеної інфокомунікаційної мережі в умовах інформаційно-технічних впливів на елементи мережі зв'язку з пам'яттю / Г. О. Гринкевич, А. Г. Захаржевський // Телекомунікаційні та інформаційні технології. – 2022. – № 4(77). – С. 4-13.

Р/1921

Досліджено питання побудови захищеної інфокомунікаційної мережі в умовах інформаційно-технічних впливів на елементи мережі зв'язку з пам'яттю.

Представлено методику побудови захищеної інфокомунікаційної мережі в умовах інформаційно-технічних впливів на елементи мережі зв'язку з пам'яттю. Були обґрунтовані можливість здійснення переходу від об'єктового захисту кореспондентів та елементів мережі зв'язку до групового захисту, а також підвищення ймовірності передачі даних у випадку блокування розповсюдження деструктивних інформаційно-технічних впливів та вузлів їхніх джерел.

Виявлено, що забезпечення стійкості інформаційного потоку можна досягти, по-перше, шляхом підвищення захищеності кореспондентів та елементів мережі зв'язку через кероване фізичне розташування трактів передачі та отримання інформації, що унеможливлює наявність фізичного шляху для здійснення деструктивних впливів. По-друге, можна забезпечити підвищення ймовірності передачі даних, зменшення часу передачі та навантаження на пропускну здатність ліній зв'язку при реконфігурації мережі, відмов та перевантажень її елементів завдяки використанню пам'яті телекомунікаційного обладнання у процесі передачі даних.



Даценко С. С. Біометрична автентифікація, що використовує згорткові нейронні мережі / С. С. Даценко, Г. А. Кучук // Сучасні інформаційні системи = Advanced Information Systems. – 2023. – Т. 7, № 2. – С. 87-91. – Текст анг.

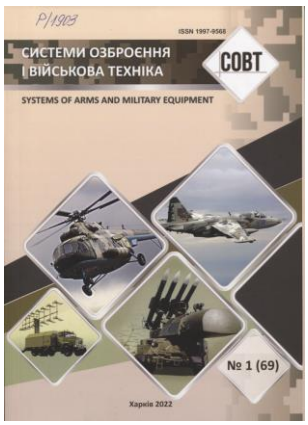
Р/543

Актуальність. Криптографічні алгоритми та протоколи є важливими інструментами сучасної кібербезпеки. Вони використовуються в різних додатках, від простого програмного забезпечення для шифрування комп'ютерної інформації до складних інформаційних і телекомунікаційних систем, які реалізують різні електронні довірчі служби. Розробка повних біометричних криптографічних систем дозволить використовувати персональні біометричні дані як унікальний секретний параметр замість необхідності запам'ятовувати криптографічні ключі або використовувати додаткові пристрої аутентифікації. *Об'єкт дослідження* – процес генерації криптографічних ключів з біометричних зображень обличчя людини з реалізацією нечітких екстракторів. *Метою даної статті* є дослідження нових методів генерації криптографічних ключів із біометричних зображень за допомогою згорткових нейронних мереж та гістограми орієнтованих градієнтів.

Захаржевський А. Г. Розроблення алгоритмів оцінювання стану захисту інформації засобами мережних ресурсів ІК-мережі зв'язку / А. Г. Захаржевський, А. О. Макаренко // Зв'язок. – 2022. – № 3(157). – С. 26-30.

Р/776

Описано один із підходів до створення системи оцінювання стану захисту інформації (ОСЗІ), яка може бути використана як для оцінювання інформаційної безпеки (ІБ) типової інформаційної системи (ІС), так і для аналізу особливої системи підприємств телекомунікаційної та інших галузей. Розроблено алгоритми оцінювання стану захисту інформації засобами мережних ресурсів інфокомунікаційної мережі зв'язку. У процесі розроблення алгоритму для опису ймовірнісних характеристик істини гіпотези використовуватимемо поняття «коефіцієнта впевненості». З огляду на комплексне оцінювання ІБ інформаційної системи доходимо висновку, що створення ОСЗІ стає можливим, виправданим, доцільним та необхідним кроком. У цьому разі одним із найважливіших етапів є розроблення алгоритму взаємодії користувача та самої системи, яка в остаточному варіанті унаочнюватиме деяке програмне забезпечення. Взаємодіючи з програмним інтерфейсом, користувач працює з механізмом здобуття результатів аналітичного оцінювання, в якому вибираються категорії даних та база даних (БД). У процесі координування дій користувача та ОСЗІ для досягнення різноманітних, незалежних цілей та завдань різні зони взаємодії всередині ОСЗІ визначаються потребами та вимогами до реалізації цих зон. Існують два етапи визначення зон взаємодії між користувачами ІС та ОСЗІ. Алгоритм взаємодії користувача з ОСЗІ охоплює чотири етапи, протягом яких виробляються кілька запитів від системи та відповідей від користувача. Такий опис алгоритму взаємодії користувача та системи може бути фундаментом для розроблення логіки роботи ОСЗІ.



Концепція реструктуризації інформаційного простору на основі кількісної ознаки для підвищення ефективності кодування відеоданих в інфокомунікаційних системах спеціального призначення / О. П. Мусієнко, І. М. Тупиця, Я. О. Боровенський, В. О. Новічков // Системи озброєння і військова техніка. – 2022. – № 1(69). – С. 34-43.

Р/1903

Досліджуються сучасні методи кодування відеозображень, що активно використовуються в інфокомунікаційних системах спеціального призначення. Аналізуються проблемні аспекти використання алгоритмів

сімейства JPEG в процесі кодування відеоданих з позиції забезпечення збереження семантичної складової в умовах необхідного рівня компресійних характеристик. Пропонується принципово новий підхід до процесу обробки відеоінформації, основною відмінною рисою якого є відсутність необхідності переходу від просторового до частотного представлення зображення. Сутність підходу полягає у реструктуризації даних відеоінформаційного ресурсу за кількісною ознакою, що враховує семантичне навантаження елементів відеопослідовності. В ролі інструменту для реструктуризації інформаційного простору виступає кількісний показник, що враховує статистичні закономірності та кореляційні зв'язки елементів. Це дозволяє створити умови для управління якістю реконструйованого відеозображення в умовах забезпечення необхідного рівня компресійних характеристик за рахунок додаткового усунення психовізуальної надмірності повідомлення. Перевагами запропонованої концепції реструктуризації інформаційного простору кодованих даних є створення умов для покращення компресійних характеристик у порівнянні з існуючими алгоритмами в умовах забезпечення необхідного рівня якості.

Крючкова Л. П. Інфокомунікаційні мережі як об'єкт навмисних деструктивних електромагнітних впливів / Л. П. Крючкова, Д. О. Тарасенко // Зв'язок. – 2023. – № 2(162). – С. 21-24.

Р/776

Навмисні деструктивні електромагнітні впливи, сформовані на основі наявних технічних засобів, є ефективним видом сучасних радіоелектронних інформаційно-технічних впливів на інфокомунікаційні мережі. *Мета публікації* – розгляд уразливостей сучасних інфокомунікаційних мереж від навмисних деструктивних електромагнітних впливів, під якими розуміють навмисне створення в злочинних або терористичних цілях потужного електромагнітного впливу на електронні та електричні системи для порушення їхнього функціонування. Навмисні деструктивні електромагнітні впливи спрямовуються на руйнування інформаційних потоків, що циркулюють між елементами мережі; зниження швидкості інформаційного обміну між елементами системи керування, що істотно збільшує тривалість циклу керування і, як наслідок, знижує ефективність керування мережею; забезпечення достатньо масованого і довготривалого виведення з ладу мережних технічних засобів.

Міночкин Д. Розподілені обчислення в безпроводових телекомунікаційних системах спеціального призначення: ефективність та перспективи / Д. Міночкин // Information Technology and Security. – January-June 2023. – Vol. 11, Iss. 1(20). – P. 115-121.

Р/1212

Дослідження присвячене аналізу застосування технологій розподілених обчислень в безпроводових телекомунікаційних системах. У роботі розглядається концепція хмарних мереж радіодоступу (C-RAN) і їх використання для покращення продуктивності і зниження витрат операторів зв'язку. Розглядається логічний взаємозв'язок мобільних пристроїв, хмари безпроводової мережі і внутрішніх серверів, а також роль спліт-TCP-проксі в розподіленні з'єднань та підтримці постійного зв'язку між користувачем і внутрішнім сервером хмари. Зазначається, що динамічні операції хмари безпроводової мережі, такі як конфігурація топології і розподіл швидкості передачі даних, забезпечують краще обслуговування на верхньому рівні. Підкреслено важливість знання стану безпроводового каналу для успішної реалізації операцій в C-RAN. Відзначається, що використання розподілених обчислень в безпроводових системах дозволяє зменшити витрати на розгортання та підтримку, забезпечуючи ефективну передачу даних і покращену продуктивність. Отримані результати свідчать про можливість успішного використання технологій розподілених обчислень у безпроводових телекомунікаційних системах. Це відкриває перспективи для операторів зв'язку щодо зниження витрат і покращення якості обслуговування. Дослідження є актуальним у контексті постійного розвитку безпроводових технологій і має потенціал для подальших досліджень і вдосконалення безпроводових телекомунікаційних систем.

Могилевич Д. Аналіз функціональної безпеки обладнання електронних комунікаційних систем / Д. Могилевич, Р. Сбоєв // Information Technology and Security. – January-June 2023. – Vol. 11, Iss. 1(20). – P. 96-105.

Р/1212

На сьогоднішній день обладнання електронних комунікаційних мереж (ОЕКМ) складається з двох взаємопов'язаних компонент. Перший – це апаратний, другий – програмний, від нормального функціонування кожного з яких залежить функціонування мережі загалом. Одним з головних понять, які характеризують здатність мережі виконувати завдання за призначенням є функціональна безпека (ФБ). Це поняття подібне до поняття надійності проте відрізняється, головним чином, тим, що в контексті надійності розглядаються всі можливі відмовні ситуації, а при розгляді ФБ лише ті, які призводять до зриву функціонування певної системи. Так, відмови поділяються на чотири категорії: виявлені безпечні та небезпечні, невиявлені безпечні та небезпечні. З точки зору ФБ розглядаються і становлять загрози лише невиявлені небезпечні. За кількістю небезпечних невиявлених відмов розділяють чотири рівні повноти безпеки. У статті також розглянуто основні міжнародні стандарти, у яких наведені визначення, кількісні характеристики основних параметрів ФБ. Так, до основних параметрів ФБ можна віднести коефіцієнт готовності системи, середній час до відмови, імовірність небезпечної невиявленої відмови. При цьому при аналізу ФБ може бути застосований математичний апарат теорії надійності. Водночас, апаратний компонент ОЕКМ є доволі широко дослідженим, а програмний компонент потребує подальшого вивчення. Також на ФБ програмної складової впливає ряд чинників, як зовнішні (сторонні зловмисні впливи, віруси, відмови апаратної складової тощо), так і внутрішні (системні помилки, алгоритмічні помилки, помилки проектування). Подальше завдання полягає у формуванні методів і заходів, спрямованих на усунення або зменшення впливу впливаючих факторів. Також, оскільки в ОЕКМ широко використовуються різні види програмного забезпечення (ПЗ), переважно системного, то на ньому й необхідно зосередити подальші дослідження.

Можливості авторизації та захисту даних користувача під час розробки хмарних веб-додатків для IoT / М. М. Поліщук, О. В. Семенюк, Л. О. Поліщук , М. В. Ломакін // Комп'ютерно-інтегровані технології: освіта, наука, виробництво. – 2023. – № 52. – С. 94-103.

Р/2346

У статті розглядаються проблеми безпеки та захисту інформації, які створює поширення Інтернету речей. Досліджуються різні підходи та технології для запровадження надійних та безпечних протоколів авторизації пристроїв та збереження конфіденційних даних користувачів. На основі розглянутих технологій і протоколів було спроектовано і розроблено архітектуру системи для керування розумним IoT пристроєм.

Никифоров О. В. Нейромережеві моделі управління процесом функціонування систем захисту інформації / О. В. Никифоров, В. Г. Путятін // Математичні машини і системи. – 2023. – № 2. – С. 34-43.

Р/1052

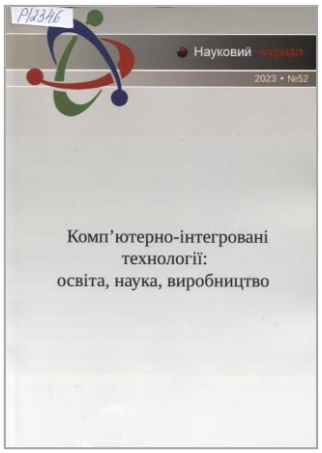
Нейромережеві моделі, які спочатку застосовувалися для моделювання процесів розпізнавання графічних зображень, на цей час знайшли широке використання і в галузі розпізнавання багатопараметричних об'єктів, а також регулювання параметрів роботи складних систем. Таке їх застосування є ефективним стосовно вирішення задач управління інформаційною безпекою. За допомогою нейромереж успішно вирішуються завдання класифікації загроз, вибору параметрів заходів захисту, регулювання режимів роботи інформаційних систем. У науковій літературі помічається велике різноманіття підходів та методів щодо створення штучних нейронних мереж. Це, на початковому етапі проектування систем інформаційної безпеки, коли необхідно визначати основні

параметри створюваного програмного забезпечення, представляє проблему для проектувальника. Прорахунки, зроблені на даному етапі проектування, можуть призвести до невдалого завершення всього проекту. У статті виконаний короткий порівняльний аналіз штучних нейронних мереж, які відрізняються за методами налаштувань (навчання) мережі і за формою її структури. Охарактеризовано застосовність, переваги і недоліки таких методів налаштувань нейромереж, як метод зворотного розповсюдження помилки; генетичний алгоритм; ітеративний алгоритм Уідроу-Хоффа з мінливим кроком; модифікований метод найменших квадратів; метод послідовного навчання. Показано відмінності структури для мереж, призначених для вирішення задач регулювання інформаційних процесів і розпізнавання багатопараметричних об'єктів. Для регулювання процесів структуру нейромережі розглянуто на прикладі нечіткої нейронної мережі ANFIS. Для задач класифікації приведена структура багатошарового персептрона, в якому структура внутрішніх шарів відображає онтологічну мережу розглянутої предметної області. Представлені результати можуть бути використаними при обгрунтуванні виду нейронної мережі, що застосовується для розв'язання конкретної задачі в області інформаційної безпеки.

Острянська Є. В. Класифікація та аналіз вразливостей сучасних інформаційних систем від класичних та квантових атак / Є. В. Острянська, С. О. Кандій, І. Д. Горбенко // Радіотехніка. – 2022. – Вип. 211. – С. 7-21.

Р/908

Завдяки останнім досягненням у квантових технологіях та потенціалу того, що практичні квантові комп'ютери можуть стати реальністю в майбутньому, відновився інтерес до розробки криптографічних технологій, захищених від звичайних та квантових атак. Наразі практично всім асиметричним криптографічним схемам, які зараз використовуються, загрожує потенційна розробка потужних квантових комп'ютерів. Постквантова криптографія є одним із способів боротьби з цією загрозою. Її безпека базується на складності математичних проблем, які вважаються нерозв'язними ефективно – навіть за допомогою квантових комп'ютерів. Безпека інформаційних систем досягається через захист від різноманітних загроз, що використовують вразливості системи. Протоколи безпеки є будівельними блоками безпечного зв'язку. Вони реалізують механізми безпеки для надання послуг безпеки. Протоколи безпеки вважаються абстрактними під час аналізу, але вони можуть мати додаткові вразливості у реалізації. Ця стаття містить цілісне дослідження протоколів безпеки. Розглядаються основи протоколів безпеки, таксономія атак на протоколи безпеки та їх впровадження, а також різні методи та моделі аналізу безпеки протоколів.



Павленко А. В. Виявлення та аналіз найвразливіших місць веб-ресурсів / А. В. Павленко, С. М. Костючко // Комп'ютерно-інтегровані технології: освіта, наука, виробництво. – 2023. – № 52. – С. 85-93.

Р/2346

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.

Самчишин О. Особливості використання соціальних мереж для здійснення кібервпливу / О. Самчишин, Г. Носова // Захист інформації. – 2022. – Т. 24, № 4. – С. 172-177.

Р/1428

У сучасному інформаційному суспільстві широке поширення одержав такий тип віртуальних спільнот як соціальні мережі. Завдання таких соціальних інтернет-сервісів полягає у тому, щоб забезпечити користувачів всіма можливими шляхами взаємодії одне з одним. Соціальні мережі,

окрім виконання функцій підтримки спілкування, обміну думками вирішення своїх професійних потреб, політичних амбіцій, задоволення своїх інтересів у мистецтві, дозвіллі й одержання інформації членами віртуальних спільнот, все частіше стають об'єктами й засобами інформаційного та кібервпливу.

Основними етапами проведення кібероперацій у соціальних інтернет-сервісах, що використовуються найчастіше, вважається: моніторинг відкритих джерел, акаунтів, груп, застосування методів соціальної інженерії і безпосередньо реалізація кібервпливів.

В умовах широкомасштабної війни рф проти України зі значною гібридною складовою, цифрові засоби масової комунікації та соціальні інтернет-сервіси широко використовуються противником для здійснення деструктивного інформаційно-психологічного та кібервпливів на військово-політичне керівництво, особовий склад та населення країни в цілому. Отже, аналіз вразливостей окремого користувача залежно від розміщеної ним інформації у соціальних мережах є актуальним, а розробка методів захисту від деструктивних кібервпливів дасть змогу в подальшому створити ефективну систему виявлення та протидії їм.

737722 В
623

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

№ 1 (72). - Київ, 2023. - 162 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. 58-70.

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

Розроблено моделі процесів захисту функціональних властивостей захищеності системи, для чого проаналізовано взаємодію атак на функціональні властивості мережі з засобами протидії цим загрозам.

Визначено математичні співвідношення для оцінки кількісних характеристик. Знайдено ті елементи, через які захищеність контенту є найбільш вразливою для загроз.

736966 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. 1(77). - [Київ], 2023. - 140 с. : граф., рис., табл. - Бібліогр. наприкінці ст. Текст кн. укр., англ.

Зі змісту:

Кірпічніков Ю. А., Головченко О. В., Андрощук О. В., Петрушен М. В., Розумний О. Д. **Модель оцінювання альтернативних варіантів впровадження інформаційно-комунікаційних сервісів з використанням хмарних технологій для оборонних потреб.** – С. 79-88.

З метою забезпечення переходу від децентралізованої моделі реалізації інформаційно-комунікаційних сервісів для потреб сил оборони до більш динамічних підходів у роботі запропоновано модель експертного оцінювання альтернативних варіантів реалізації зазначених сервісів та розроблено рекомендації щодо їх впровадження на основі хмарних технологій.

Чемерис К. М. Застосування методу вейвлет-аналізу для виявлення атак в мережах / К. М. Чемерис, Л. Ю. Дейнега // Наука і техніка Повітряних Сил Збройних Сил України. – 2022. – № 1(46). – С. 99-107.

Р/2266

Розробка системи виявлення мережевих атак один із найважливіших напрямів у сфері інформаційної безпеки, оскільки постійно збільшується різноманітність комп'ютерних мережевих загроз, реалізація яких може призводити до серйозних фінансових втрат у різних організаціях. Тому розглядаються різні існуючі основні методи вирішення завдань виявлення мережевих атак. Основна увага приділяється розгляду робіт, присвячених методу вейвлет-аналізу виявлення аномалій в мережевому трафіку.

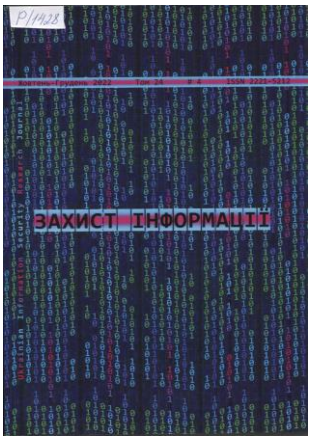
Отримано тестові дані мережевого трафіку з аномаліями для практичного виконання, виконано шумоусунення сигналу для конкретизації даних та зменшення їх розміру, а також застосовано різні методи вейвлет-аналізу для виявлення можливих аномалій та порівняно спектрограми з використанням пакету Wavelet Tools у середовищі Matlab.

Шавловський Я. С. Модельна структура загроз ресурсам інформаційно-телекомунікаційним мережам як базовому активу критично важливого об'єкта інфраструктури / Я. С. Шавловський // Зв'язок. – 2023. – № 1(161). – С. 13-21.

Р/776

Здійснено класифікацію моделей кібератак, спрямованих на комп’ютерні мережі та комплекси і які являють собою найбільшу загрозу. Запропоновано класифікацію, в основу якої покладено основні тенденції практичної реалізації кібератак. Розглядуваний підхід є новим щодо класифікації кібератак на комп’ютерні мережі та комплекси, що обслуговують критично важливі об'єкти інфраструктури, і зважає на десять складових циклу загрози: від комплексного вивчення об'єкта впливу до реалізації кібератаки.

Інформаційне протиборство у воєнних конфліктах. Інформаційно-психологічна безпека



Артемов В. Моделювання інформаційно-психологічного впливу на суспільство / В. Артемов, В. Хорошко, Ю. Хохлачева // Захист інформації. – 2022. – Т. 24, № 4. – С. 183-190.

Р/1428

У статті дається визначення інформаційно-психологічних впливів (ІПВ) і основні шкали їх впливу на соціальні групи суспільства.

Наведено опис моделі, що ведуть до форми нелінійного диференціальне рівняння. В моделі враховано інформаційний вплив на масову свідомість міжособистісної інформаційної взаємодії, засобів масової інформації та ефект забування впливу ІПВ. Показано, що модель має рішення у вигляді узагальненої логістичної кривої. Наведено статистичне розподілення за часом окремих членів соціуму, які підтримують ідеї ІПВ, яка якісно підтверджує формальне рішення моделі. Досліджено окремі випадки моделі, які у всіх випадках підтверджують існування асимптотичного стаціонарного рішення. Наголошено, що розроблення моделі спостерігається в умовах гібридної війни та забезпечення інформаційної безпеки держави, суспільства та кожного окремого члена суспільства, вимагаючи та враховуючи розвиток соціальних мереж.

Ветлицька О. С. Математична модель інформаційної безпеки особистості під впливом медіаінформації / О. С. Ветлицька, Т. М. Мужанова // Сучасний захист інформації. – 2023. – № 2(54). – С. 6-12.

Р/2300

Оскільки засоби масової інформації (ЗМІ) продовжують відігравати дедалі важливішу роль у нашому повсякденному житті, люди стикаються зі зростаючою кількістю ризиків безпеці, пов'язаних із споживанням медіаінформації. Щоб краще зрозуміти фактори, які сприяють індивідуальній безпеці в цьому контексті, у статті пропонується математична модель, яка вивчає зв'язок між кількістю порушень безпеки, обсягом спожитої медіаінформації, рівнем заходів безпеки, вжитих особою, і рівнем медіаграмотності, яким володіє індивід. Наведено рівняння, які представляють ці зв'язки, і запропоновано можливі значення для параметрів моделі. Модель забезпечує структуру для аналізу та покращення індивідуальної безпеки в контексті споживання медіаінформації, і має потенціал для використання в практичних програмах, таких як розробка ефективних кампаній з підвищення обізнаності щодо безпеки та розробка більш безпечних медіа-технологій.

Ветлицька О. С. Модель оцінки впливу соціологічної інформації на поведінку людини в контексті її інформаційної безпеки / О. С. Ветлицька, Т. М. Дзюба // Телекомунікаційні та інформаційні технології. – 2022. – № 4(77). – С. 34-45.

Р/1921

Інформаційно-психологічна безпека визначається як стан захищеності особистості від впливів, здатних проти її волі й бажання змінювати психічний стан й психологічні характеристики індивіда, модифікувати її поведінку і обмежувати свободу формування власної позиції. У багатьох випадках людина, маючи певні свої переконання, в результаті діє «як усі». Щоб пояснити це парадоксальне явище, необхідно дослідити механізм, що лежить в основі такої поведінки. Для цього в статті розглядається математична модель такого механізму та робиться оцінка його адекватності на окремих реальних прикладах.

В статті розглянуто побудову моделі поведінки особистості під впливом інформації, досліджено математичну модель поведінки індивіда, шляхом запровадження кількісних оцінок його ставлення до цього стану, досліджено, як змінюється поведінка індивіда в залежності від результатів соціологічних досліджень. Розглянуто модель поведінки особистості під впливом соціологічної інформації, на прикладі проведення виборів президента, що надало можливість дослідити розроблену модель та проаналізувати її достовірність. Досліджено, що є множиною взаємних впливів на особистість, у якій вирішується проблема вибору, розглянуто суспільний осередок, який впливає на прийняття основних рішень, визначено оцінку ролі телебачення у виборчій кампанії.

736979 R
070

Гібридна війна і журналістика. Проблеми інформаційної безпеки [Текст] : навч. посібник / [авторський колектив: В. О. Жадько, О. І. Клименко, П. П. Куляс та ін.] ; [за заг. ред. В. О. Жадька] ; Національний пед. ун-т імені М. П. Драгоманова. - Київ : Вид-во НПУ імені М. П. Драгоманова, 2018. - 356 с. - Бібліогр. наприкінці глав.

Підготовлений викладачами кафедри журналістики НПУ імені М. П. Драгоманова посібник присвячено питанням інформаційної безпеки, діяльності журналіста в умовах гібридної війни, проблемам медіаосвіти. У книзі чотири розділи, що висвітлюють суть та складові сучасних гібридних протистоянь, їхній інформаційний, інформаційно-психологічний, семантичний, технологічний та силовий аспекти. Видання доповнене термінологічним словником.

Інформаційні заходи шостого етапу інформаційної кампанії Російської Федерації в ході збройної агресії проти України у вересні 2022 року / С. О. Сідченко, С. В. Залкін, К. І. Хударковський, В. В. Бєлімов // Наука і техніка Повітряних Сил Збройних Сил України. – 2022. – № 3(48). – С. 71-80.

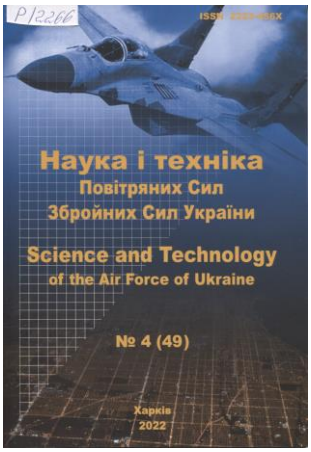
Р/2266

Проаналізовані результати інформаційного (психологічного) впливу на державні інституції та населення рф внаслідок військової поразки на Харківському напрямку, що збігаються з основними стадіями прийняття неминучого. Стадія заперечення полягала у запереченні втрачання збройними силами рф населених пунктів та імітацією нарощування сил в зоні проведення контрнаступу Збройних Сил України, яка здійснювалась переважно в інформаційному просторі. Стадія гніву, яка супроводжувалась ударами крилатими ракетами по цивільній критичній інфраструктурі України. Стадія торгу, яка полягала у звинуваченнях, а також висловленні свого бачення світового порядку та розвитку подій. Стадія депресії, яка полягала у невизначеності подальших кроків щодо проведення спеціальної воєнної операції в Україні. Стадія прийняття, яка полягала у визначенні мети відступу збройних сил рф в ході контрнаступу Збройних Сил України. Висвітлена роль засобів масової комунікації рф у просуванні в інформаційному просторі наративів російської пропаганди, інформаційній підтримці у формуванні парамілітарних утворень з числа засуджених для війни в Україні. Проаналізована електоральна підтримка населенням рф війни в Україні та російської влади за результатами місцевих виборів. У статті зазначається, що інформаційна кампанія рф проти України перенасичена пропагандою, яка, за багатьма ознаками, такими як культ одного лідера та масові заходи на його підтримку, міф про колишню велич імперії та спроби її повернути, героїзація загиблих за щось грандіозне, культивована ненависть до певної групи людей, візуальні ознаки приналежності до певної спільноти, та інше, збігається з пропагандою в Третьому Рейху. Результати дослідження відображають період до 20.09.2022.

Левченко О. Особливості антиукраїнського інформаційного (кібер) впливу на Україну / О. Левченко, В. Охрімчук // Захист інформації. – 2022. – Т. 24, № 4. – С. 156-163.

Р/1428

З дня проголошення незалежності України її інформаційний простір, а з розвитком та впровадженням в усі сфери діяльності суспільства інформаційних технологій і кіберпростір постійно перебуває під потужним іноземним інформаційним та кібервпливами. Гібридна війна, розпочата росією 2014 року, змусила Україну переглянути свої підходи до забезпечення інформаційної та кібербезпеки. А з початком широкомасштабного вторгнення дане питання набуло особливої актуальності. Для ведення антиукраїнського інформаційного (кібер) впливу керівництво росії задіяло значні людські, матеріальні і фінансові ресурси, завдяки чому вдалося ефективно "промивати мізки" не тільки більшості своїх громадян, а й частині наших співвітчизників. Тому, на жаль, це призвело до підтримки частиною українських громадян агресивної політики кремля проти України. В статті здійснено аналіз основних інформаційних операцій росії проти України, а також здійснення кібератак на її критичну інформаційну інфраструктуру. В результаті аналізу встановлені особливості антиукраїнського інформаційного (кібер) впливу на Україну.



Напрями розвитку інформаційної кампанії Російської Федерації в ході збройної агресії проти України у вересні–грудні 2022 року / С. О. Сідченко, С. В. Залкін, К. І. Хударковський [та ін.] // Наука і техніка Повітряних Сил Збройних Сил України. – 2022. – № 4(49). – С. 64-79.

Р/2266

У статті висвітлено напрями розвитку інформаційної кампанії Російської Федерації (рф) в ході збройної агресії проти України, зміни основних наративів російської пропаганди та пріоритетів у період з вересня по

грудень 2022 року.

Представлено основні заходи інформаційної кампанії рф щодо легітимізації окупації території України, яка складається з п'ятьох етапів, та надана їх загальна характеристика.

Наведені фейкові результати псевдореферендумів на тимчасово окупованій території України щодо приєднання до рф.

Представлені наративи російської пропаганди в інформаційному просторі щодо зміни основної мети так званої спеціальної військової операції та виправдання збройної агресії проти України.

Висвітлена роль російської пропаганди у формуванні обрису головного ворога Росії в особі "колективного Заходу" та безпосередньо військового блоку НАТО на чолі із США.

У статті представлені додаткові заборони в інформаційному просторі рф, прийняті на законодавчому рівні, та тенденція просування культу смерті для обґрунтування багаточисельних людських втрат Збройних Сил (ЗС) рф та зниження активності російського населення щодо мобілізації як наслідок успішних дій Збройних Сил України.

У статті представлені різноманітні інформаційні заходи рф щодо організації проведення і супроводження комплектування ЗС рф у різні періоди збройної агресії проти України.

Відображені результати роботи російської пропаганди з виготовлення різних пропагандистських творчих продуктів.

Проаналізована електоральна підтримка населенням рф війни в Україні та російської влади за результатами опитування "Левада-центру".

Представлені наративи російської пропаганди на міжнародній арені у 2022 році під час міжнародних заходів та в ході засідань Ради Безпеки ООН з питань навколо України. Визначено, що інформаційна кампанія рф проти України в ході повномасштабного збройного вторгнення виявилась провальною, оскільки агресору не вдалось досягти поставлених цілей.

737681 В
32

Політологічний вісник [Текст] = Politology Bulletin : збірник наук. праць / голов. ред. В. Ф. Цвих ; Київський нац. ун-ті імені Тараса Шевченка. - [Київ] : [ВАДЕКС].

Вип. 88. - Київ, 2022. - 230 с. : іл. - Бібліогр. наприкінці ст. Текст кн. укр., англ.

Зі змісту:

Джус О. А. **Концептуальні основи ведення інформаційної війни в сучасних умовах збройної агресії РФ проти України.** – С. 189-201.

Сунгурова С. Р. **Міжнародний досвід боротьби з політичним насиллям засобами інформаційної війни.** – С. 202-218.

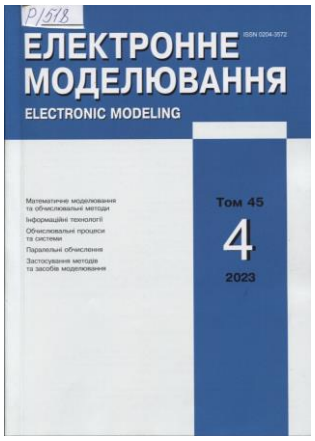
737997 R
31

Сенченко, Оксана Миколаївна.

Інформаційно-мережеві війни: теорія, моделі, алгоритми [Текст] : [наук. вид.] / О. М. Сенченко. - Київ : КВІЦ, 2017. - 332 с. : граф. - Бібліогр. у виносках.

Досліджено аспекти інформаційно-мережевих війн і їх складові: соціальні мережі, технології «керованого хаосу», стратегії непрямої дії і «м'якої сили». Наведено типову модель і мегапроект ведення інформаційно-мережевої війни, розроблено детальні моделі й алгоритми війн у фінансовій, економічній і політичній галузях.

Кібербезпека – проблема XXI століття



Давидюк А. В. Кібердомени в системі національної безпеки України / А. В. Давидюк, Ю. Є. Хохлачова // Електронне моделювання. – 2023. – Т. 45, № 4. – С. 78-87.

Р/518

Ідентифікація кібердоменів має вагоме значення для національної кібербезпеки, оскільки вона забезпечує захист критичної інфраструктури, підвищує ефективність процесів розвідки кіберзагроз та поліпшує ситуаційну обізнаність, сприяє співпраці у сфері кібербезпеки, обміну інформацією, ефективному реагуванню на кіберінциденти та відновленню після кібератак, зміцнює національну обороноздатність, а також підтримує формування державної політики та регулювання. Завдяки всебічному розумінню та забезпеченню безпеки кібердоменів на національному рівні керівництво країни може ефективно протистояти кіберзагрозам, що розвиваються, і забезпечити стійкість і безпеку інформаційних активів і інтересів країни. В дослідженні розглянуто проблему визначення доменів кібербезпеки і кібердоменів. Представлено різні підходи до визначення доменів кібербезпеки. Запропоновано визначити кібердомени на основі сфер відповідальності та основних функцій основних суб'єктів забезпечення кібербезпеки. Впровадження кібердоменів сприятиме підвищенню ефективності процесів кібербезпеки в країні.

Драгунцов Р. І. Моделювання загроз кібербезпеці у зв'язку з масовими відключеннями електропостачання та потенційні заходи протидії / Р. І. Драгунцов, В. Ю. Зубок // Електронне моделювання. – 2023. – Т. 45, № 3. – С. 116-127.

Р/518

Під час російсько-української війни в Україні відбувались масові відключення електропостачання, спричинені російськими атаками на цивільну інфраструктуру, а саме на генеруючі та розподільчі потужності енергосистеми. Ризики, пов'язані з такими відключеннями, охоплюють не лише питання безперебійного функціонування господарства напряму, а і більш складніші аспекти, пов'язані з кібербезпекою. Розглянуто вплив подібних відключень на кібербезпеку інформаційно-комунікаційних систем, а саме ефекти другого порядку, такі як перебої зі спостережністю інформації, порушення цілісності інфраструктури захисту, перевантаження команд моніторингу та реагування хибними тривогами. Всі ці фактори змінюють ландшафт загроз для системи та мають бути враховані в політиці безпеки і, відповідно, при моделюванні загроз. Проведено аналіз прихованих ризиків кібербезпеки, що виникають у зв'язку з масовими відключеннями електропостачання. Наведено можливі підходи до врахування таких факторів ризику при проведенні моделювання загроз, а також способи протидії.

Запорожченко М. М. Місце OSINT в життєвому циклі кібератаки / М. М. Запорожченко // Телекомунікаційні та інформаційні технології. – 2023. – № 1(78). – С. 53-60.

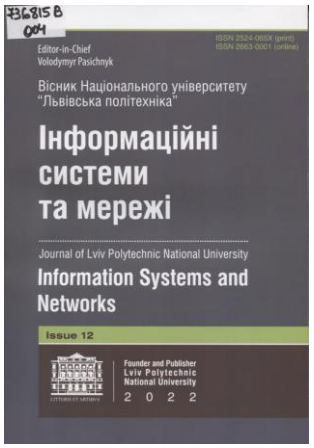
Р/1921

Протягом останніх років можна спостерігати тенденцію до зростання кількості кібератак на організації та окремих користувачів. В багатьох випадках ключовим фактором реалізації інциденту інформаційної безпеки є проведення зловмисником ефективної підготовки до кібератаки: вибір цілі, розвідка, тобто отримання будь-якої інформації, яка може знадобитися при плануванні атаки, озброєння на основі виявлених механізмів захисту, використовуваного програмного та апаратного забезпечення тощо, а також доставка, тобто вибір способу, яким чином шкідливе програмне забезпечення попаде до жертви і які кроки знадобляться для його подальшої активації. Володіння значною кількістю важливої та критичної для організації з точки зору

забезпечення безпеки інформацією надає зловмиснику можливість вибору оптимального сценарію атаки і значно підвищує шанси на її успіх.

Проблема полягає в тому, що сучасні методи та інструменти OSINT дозволяють знайти майже будь-яку інформацію, яка захищена неналежним чином, що значно підвищує ризики особливо для організацій, яким важко контролювати всю інформацію, яка публікується її співробітниками в соціальних мережах, розкривається на інтерв'ю чи випадково потрапляє до Інтернету. Втім, більшість інструментів для розвідки доступні не лише зловмисникам, тому етичні хакери та пентестери також можуть використовувати інструменти OSINT для перевірки вразливих місць організації та вдосконалення її захисту, до того, як цими вразливостями скористаються зловмисники.

В статті досліджені основні методи розвідки на основі відкритих джерел, розглянуто найбільш поширені та найчастіше використовувані інструменти OSINT, проведено опис життєвого циклу кібератаки та визначено етапи, які потребують застосування інструментів OSINT при проведенні аудиту інформаційної безпеки організації та тестів на проникнення.



736815 В
004

Інформаційні системи та мережі [Текст] = Information Systems and Networks : зб. наук. пр. / відп. ред. Володимир Пасічник ; Національний університет "Львівська політехніка". - Львів : Вид-во Львів. політехніки, 2022. - 274 с. : граф., рис., табл. - (Вісник / Національний університет "Львівська політехніка" ; вип. 12). - Бібліогр. наприкінці ст. Текст кн. укр. та англ. мов.

Зі змісту:

Неретін О., Харченко В. **Забезпечення кібербезпеки систем штучного інтелекту: аналіз вразливостей, атак і контрзаходів**. – С. 7-22.

Останніми роками багато компаній почали інтегрувати системи штучного інтелекту (СШІ) в свої інфраструктури. СШІ використовують у вразливих сферах суспільства, таких як судова система, критична інфраструктура, відеоспостереження тощо. Це зумовлює необхідність достовірного оцінювання і гарантованого забезпечення кібербезпеки СШІ. У дослідженні проаналізовано стан справ щодо кібербезпеки цих систем. Класифіковано можливі типи атак і детально розглянуто основні з них. Проаналізовано загрози і атаки за рівнем тяжкості й оцінено ризики безпеки з використанням методу IMECA. Виявлено, що найвищі ризики небезпеки "Змагальних атак" та атак "Отруєння даних", але контрзаходи щодо них не на належному рівні. Зроблено висновок, що існує потреба в формалізації та стандартизації життєвого циклу розроблення та використання безпечних СШІ. Обґрунтовано напрями подальших досліджень щодо необхідності розроблення методів оцінювання і забезпечення кібербезпеки СШІ, зокрема для систем, які надають штучний інтелект як сервіс.

736798 В
004

Інформаційні технології в культурі, мистецтві, освіті, науці, економіці та бізнесі [Текст] : VII Міжнародна науково-практична конференція, 20-21 квітня 2022 р. / М-во освіти і науки України, М-во культури України, Київ. нац. ун-т культури і мистецтв, Українська федерація інформатики [та ін.]. - Київ : [Вид центр КНУКіМ], 2022 - .

Частина 2 : матеріали конференції. - Київ, 2022. - 144 с. : іл. - Бібліогр. наприкінці ст.

Зі змісту:

Інформаційно-екстремальне машинне навчання системи виявлення кібератак / А. С. Довбиш, В. О. Любчак, І. В. Шелехов [та ін.] // Радіоелектронні і комп'ютерні системи = Radioelectronic and computer systems. – 2022. – № 3(103). – С. 121-131. – Текст англ.

Р/1769

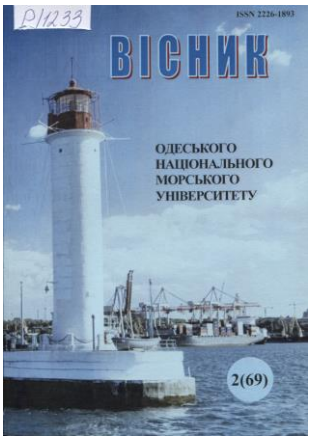
Метою дослідження є підвищення функціональної ефективності машинного навчання системи виявлення кібератак. Розроблено метод інформаційно-екстремального машинного навчання системи виявлення кібератак з оптимізацією контрольних допусків на ознаки розпізнавання, які відбивали властивості трафіка інфокомунікаційної системи.

Метод розроблено в рамках функціонального підходу до моделювання когнітивних процесів природнього інтелекту при формуванні та прийнятті класифікаційних рішень. Такий підхід на відміну від відомих методів інтелектуального аналізу даних, включаючи нейроподібні структури, дозволяє надати системі розпізнавання властивості адаптивності до довільних початкових умов формування навчальної матриці та гнучкості при перенавчанні системи через розширення алфавіту класів розпізнавання. Ідея методу полягає в максимізації інформаційної спроможності системи виявлення атак в процесі машинного навчання.

За результатами інформаційно-екстремального машинного навчання в рамках геометричного підходу побудовано вирішальні правила, практично інваріантні до багатовимірності простору ознак розпізнавання.

Результати комп'ютерного моделювання інформаційно-екстремального машинного навчання системи виявлення атак для розпізнавання чотирьох хостових трафіків різного профілю підтверджують працездатність розробленого методу.

Кібербезпека на морському транспорті / Ю. В. Даус, М. Є. Даус, О. І. Полікарповських, Д. Г. Ларін // Вісник Одеського національного морського університету. – 2023. – № 2(69). – С. 124-133.



Р/1233

Сучасний світ все більше залежить від застосування комп'ютерних технологій.

Застосування таких технологій допомагає знизити собівартість кінцевого продукту, збільшити продуктивність та зменшити вплив людських помилок на виробничі процеси і являється основою прогресу людства. Однак, при цьому зростає кількість кіберінцидентів на морському транспорті, що може призвести до великих втрат, і не тільки грошових, але й екологічних, технологічних та іміджевих.

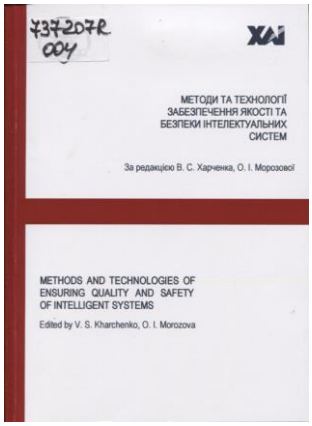
Тому компаніям дуже важливо побудувати систему кіберзахисту на судні, використовуючи цілісну систему захисту, найновіші засоби ідентифікації користувачів та користуватися настановами ІМО.

Кібербезпека працівників: чому це не просто важливо, а й життєво необхідно / підгот. редакцією // Охорона праці і пожежна безпека. – 2023. – № 7-8. – С. 10-17.

Р/2325

Тези:

1. *Кібербезпека в Україні: з якими труднощами зіткнулися вітчизняні установи та організації*
2. *Нормативне врегулювання питань кібербезпеки*
3. *Види хакерських атак та їхні наслідки*
4. *Як забезпечити належний рівень кіберзахисту: покрокові алгоритми для роботодавця та працівників.*



737207 R
004

Методи та технології забезпечення якості та безпеки інтелектуальних систем [Текст] = Methods and technologies of ensuring quality and safety of intelligent systems : монографія / за ред. В. С. Харченка, О. І. Морозової ; Нац. аерокосм. ун-т імені М. Є. Жуковського "Харк. авіац. ін-т". - Харків ; [Київ] : [Вид-во "Юстон"], 2023. - 352 с. : іл. - (Проєкт Методологія та інформаційні технології оцінювання та забезпечення безпеки цифрової інфраструктури малих модульних реакторів (Д 503-4/2022-Ф, № Д/Р 0122U000977)) (Проєкт Методи, програмно-апаратні засоби та технології забезпечення гарантоздатності інтелектуальних систем індустріального інтернету речей (Д 503-10/2022-П, № Д/Р 0122U001065)). - Бібліогр. наприкінці розд. Паралел. назва англ.

Монографія базується на результатах досліджень методів і засобів оцінювання та забезпечення безпеки інтелектуальних мобільних систем (ІМС) і систем індустріального інтернету речей (ІІР), які виконано колективом авторів кафедри комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут» та інших університетів. Присвячена аналізу та розвитку принципів, моделей, методів та технологій побудови безпечних ІМС та ІІР. *Бібл. -516 найменувань, рисунків - 112, таблиць - 56.*

The monograph is based on the research results in area of methods and techniques for assessing and providing safety and security intelligent mobile systems (IMS) and systems of industrial Internet of Things (IIoT) that were obtained by author's team of the Computer Systems, Networks and Cyber Security Department, National Aerospace University «Kharkiv Aviation Institute», researchers of other universities and industrial enterprices. It is devoted to the analyzing and developing principles, models, methods, and technologies of designing safe and secure IMSs and IIoT. *Ref. - 516 items, figures -112, tables - 56.*

Міщенко В. Управління кібербезпекою в системі забезпечення національно ускореної стійкості економічного розвитку / В. Міщенко // Економічна теорія. – 2023. – № 1. – С. 47-72.

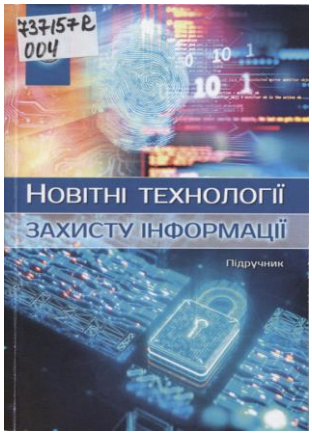
Р/2101

Визначено, що процес організації управління кіберстійкістю повинен ґрунтуватися на розробленні комплексних систем кіберзахисту, які засновані на чітких політиках, правилах і стратегіях раннього виявлення, попередження та мінімізації наслідків реалізації кіберзагроз з використанням широкого спектра технічних, технологічних, організаційних, управлінських і регуляторних заходів. Обґрунтовано необхідність розроблення загальнодержавної стратегії та програми дій

органів влади у сферах законодавства, регулювання, нагляду та контролю за станом кібербезпеки. Доведено, що національна стратегія кіберзахисту повинна передбачати ефективні заходи щодо захисту об'єктів критичної інфраструктури, органів державної влади та населення, а також систему регуляторних і наглядових заходів.

Встановлено, що першочерговим завданням організації та функціонування систем кіберзахисту повинен бути захист цифрових активів і ресурсів підприємств та їхніх клієнтів. З метою посилення інституційної спроможності органів влади для ефективної підтримки національної екосистеми кібербезпеки розроблено структурно-логічну схему взаємодії підприємств і Державного центру кіберзахисту України в процесі обміну інформацією про кіберінциденти, а також наведено практичні рекомендації щодо взаємодії об'єктів критичної інфраструктури та органів державного регулювання, які можуть бути використані з метою забезпечення національно укоріненої стійкості та безпеки економічного розвитку України в умовах гібридної системи "мир-війна".

737157 R
004



Новітні технології захисту інформації [Текст] : підручник / [М. Г. Луцький, В. О. Хорошко, Ю. Є. Хохлачова та ін.] ; Національний авіаційний університет. - Київ : [НАУ], 2023. - 312 с. : граф., табл. - Бібліогр.: с. 308-311.

У підручнику висвітлено комплекс проблем, які виникають під час застосування систем кіберзахисту інформації в інформаційних системах. Розглянуто загальні підходи до застосування систем кіберзахисту інформації. Досліджено структури інформаційного процесу, канали несанкціонованого отримання інформації та загрози їй, а також основи моделювання процесу кіберзахисту та інформаційних процесів у системі кіберзахисту. Запропоновано методи керування доступом до інформації та керування кібербезпекою інформаційних технологій.

Опірський І. Перспективи військового застосування технології блокчейну / І. Опірський, С. Василишин // Безпека інформації. – 2022. – Т. 28, № 2. – С. 57-66.

P/1408

Нові передові технології мають, як правило, величезний вплив на те, як бізнес впроваджує інновації для покращення своїх конкурентних переваг. З моменту появи Інтернету технології блокчейну були визнані одними з вибухових інновацій початку XXI століття. Технологія блокчейну у даний час використовується у фінансових додатках (наприклад, для платежів, обміну валюти, грошових переказів і гаманців, торгових фінансів, ринків, мікроугод, інвестицій, брокерства, страхування), а також в нефінансові додатки (наприклад, управління ідентифікацією в електронному вигляді, автентифікація та авторизація, системи зберігання та доставки даних в електронному вигляді, системи сертифікації, смарт-контракти, розробка додатків, електронне голосування на виборах, управління медичними записами пацієнтів, розподіл робочого навантаження для систем зв'язку, комп'ютерні системи, які мають відповідати вимогам законодавства без втручання людини, Інтернету речей і т. д.). ***І все ж застосування блокчейна найбільш виправдано при вирішенні завдань, пов'язаних в основному із забезпеченням цілісності інформації, що зберігається. Саме тому у цій статті ми розглядаємо перспективи застосування технології блокчейну у військовій справі, аналізуємо її властивості, розглядаємо проблеми та наводимо рішення, які відкриваються з початком використання даної технології.*** Технологія блокчейну здатна підсилити оборонний сектор держави та впровадити додатковий рівень захисту до вже існуючих.

Погасій С. Моделі і методи захисту інформації в кіберфізичних системах / С. Погасій // Безпека інформації. – 2022. – Т. 28, № 2. – С. 67-79.

Р/1408

У статті подано новий підхід забезпечення безпеки інформаційних ресурсів в кіберфізичних системах. Сьогодні таки системи, як правило належать до об'єктів критичної інфраструктури. Як правило такі системи формуються внаслідок комплексування різних елементів технологій мобільного зв'язку, класичних комп'ютерних мереж та систем, а також Інтернет-речей та Інтернет-технологій. В роботі пропонується розгляд формування системи безпеки на основі багатоконтурності, що дозволяє розглядати два контури системи безпеки – внутрішній (фізична інфраструктура кіберфізичних систем) та зовнішній (інфраструктура управляючої системи на основі хмарних технологій). За допомогою розробленого класифікатора загроз на об'єкти критичної інфраструктури забезпечується формування класифікатора зловмисників, у якому визначаються його фінансові та обчислювальні можливості, що дозволяє на основі аналізу загроз своєчасно визначати степені можливості зловмисників, а також його наміри та формувати превентивні заходи захисту. Використання запропонованих моделей захисту на основі моделі Лотки-Вольтери дозволяє враховувати тенденції розвитку сучасних технологій, а також вектор направленості кіберзагроз на об'єкти кричної інфраструктури до яких відносяться сучасні кіберфізичні системи. Для забезпечення безпеки передачі інформації відкритими каналами мережі кіберфізичних систем запропоновані методи захисту інформації на основі постквантових алгоритмів – крипто-кодових конструкцій Мак-Еліса на LDPC-кодах, що дозволяє "закрити" канали передачі даних інфраструктури кіберфізичних систем.

Сверчков Д. О. Аналіз методів і засобів забезпечення кібербезпеки веб-сервісів з використанням штучного інтелекту / Д. О. Сверчков, Г. В. Фесенко // Електронне моделювання. – 2023. – Т. 45, № 2.– С. 61-82.

Р/518

Наведено результати аналізу літературних джерел з питань застосування штучного інтелекту (ШІ) у кібербезпеці. Найбільше уваги приділено джерелам, в яких описано використання застосунків на основі ШІ для аналізу і оцінки існуючих систем на вразливості, а також джерелам, де розглядаються особливості використання вбудованих механізмів ШІ для пошуку, виявлення, класифікації і боротьби з атаками на систему під час її роботи. Визначено типи, вплив та особливості атак на веб-сервіси. Розглянуто особливості застосування ШІ для класифікації веб-сервісів, що тестуються, з метою подальшого обґрунтованого вибору найкращих інструментів забезпечення їх кібербезпеки. Проаналізовано способи використання ШІ у кібербезпеці веб-сервісів під час запровадження вбудованих механізмів і моделей для пошуку, виявлення, класифікації і протидії загрозам. Здійснено порівняння точності використовуваних для виявлення вторгнень методів машинного навчання. Напрями подальших досліджень: розроблення заснованих на використанні ШІ методів моделей та застосунків для аналізу вихідного коду на можливі вразливості веб-сервісу з підтримкою різних мов програмування; розроблення заснованих на використанні ШІ вбудованих у веб-сервіс механізмів пошуку і класифікації загроз.

Субач І. Лексографічний метод рішення багатокритеріальної задачі вибору SIEM-системи для побудови Ситуаційного центру з кібербезпеки / І. Субач, В. Кубрак // Information Technology and Security. – January-June 2023. – Vol. 11, Iss. 1(20). – P. 27-38.

Р/1212

Розглянуто створення Ситуаційного центру з кібербезпеки, його завдання та склад, а також наведено основні технологічні інструменти, які повинні бути включені до ефективного Ситуаційного центру з кібербезпеки. Особлива увага приділена системі управління інцидентами інформаційної безпеки (SIEM), яка є ключовою для Ситуаційного центру з кібербезпеки, тому розглянуто її призначення та основні задачі, які вона повинна вирішувати. Проаналізовано особливості рішення задачі раціонального вибору SIEM-системи . Виділено групи показників, що характеризують ступінь виконання вимог, які пред'являються до SIEM-системи та наведено їх

приклади. Запропоновано застосування теорії нечітких множин для обробки експертної інформації про якісні показники, що характеризують SIEM-систему. Проаналізовано особливості, що стосуються прийняття раціонального рішення щодо вибору SIEM-системи. Виділено групи показників, які можуть допомогти в оцінці ступеня відповідності SIEM-системи вимогам та наведені приклади цих показників. З метою обробки експертної інформації про якісні показники SIEM-системи, було запропоновано використання теорії нечітких множин. Наведено формальну постановку задачі вибору SIEM-системи та запропоновано основні етапи її розв'язання, які включають підготовку початкових даних, вибір методу для рішення багатокритеріальної задачі раціонального вибору SIEM-системи та розробку алгоритму. Запропоновано використання методу нормування кількісних показників SIEM-системи та методу парних порівнянь на основі рангових оцінок для обробки її якісних показників. Розглянуто використання шкали Сааті з 9 бальними значеннями для отримання функцій належності якісних характеристик SIEM-системи на основі експертної оцінки. Розроблений алгоритм побудови функцій належності характеристик SIEM-системи до кожного нечіткого терму. Описано методи вирішення багатокритеріальних задач і запропоновано застосування лексографічного методу для рішення задачі раціонального вибору SIEM-системи в ході побудови Ситуаційного центру з кібербезпеки. Створений та втілений у життя алгоритм його реалізації, і щоб продемонструвати його ефективність, наведено приклад використання для раціонального вибору SIEM-системи. Крім того, надані рекомендації щодо практичного використання отриманих результатів.

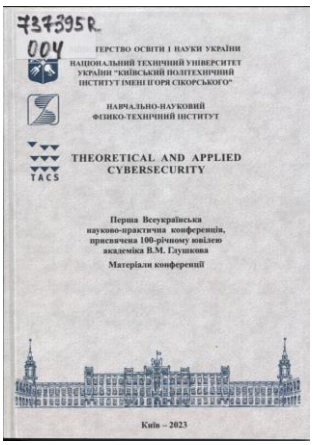
Хворостяний Р. В. Проблеми безпеки та заходи протидії атакам в NFC / Р. В. Хворостяний // Сучасний захист інформації. – 2023. – № 1(53). – С. 39-46.

Р/2300

Технологія Near Field Communication (NFC), широко поширена через зручність у використанні. Разом з тим, NFC уразлива до атак безпеки, таких як людина посередині; відмова в обслуговуванні (DOS) та ін. Ці атаки призводять до витоку важливих даних користувача, що може вплинути на будь-яку організацію, яка використовує програми та технології NFC. У цій статті розглядаються вразливості NFC та різні види атак на NFC. Також у статті розглянуто можливі рішення, які могли б захистити NFC від цих загроз безпеці.

"*Метою цього дослідження* є розгляд механізмів безпеки NFC у їх відповідності до можливих кіберзагроз та вибору раціонального методу протидії таким загрозам".

737395 R
004



Theoretical and Applied Cybersecurity [Текст] : перша Всеукр. наук.-практ. конф., присвячена 100-річному ювілею акад. В. М. Глушкова : матеріали конф. / [редкол.: О. М. Новіков, М. М. Савчук, С. А. Смирнов та ін.] ; Національний технічний університет України "Київський політехнічний інститут ім. Ігоря Сікорського", Навч.-наук. фізико-технічний ін-т. - Київ : КПІ ім. І. Сікорського, 2023. - 266 с. : граф., табл., рис. - Текст кн. укр. та англ. мов. - Бібліогр. наприкінці ст.

Подано матеріали доповідей Першої Всеукраїнської науково-практичної конференції «Theoretical and Applied Cybersecurity», присвяченій 100-річному ювілею академіка В. М. Глушкова (TACS-2023, 26 травня 2023 року, м. Київ, Україна). У збірнику представлені матеріали, присвячені питанням кібернетичної безпеки критичних інфраструктур, моделювання та протидії інформаційним операціям, технологій інформаційно-аналітичних досліджень на основі відкритих джерел інформації. Наведено матеріали з актуальних проблем інформаційної та кібернетичної безпеки, можливості застосування штучного інтелекту, системного аналізу під час забезпечення підтримки прийняття рішень, комп’ютерному моделюванні процесів і систем, актуальні завдання забезпечення інформаційної та кібербезпеки.