Наукова бібліотека СумДПУ імені А. С. Макаренка

Бібліографічний огляд

КІБЕРБЕЗПЕКА – ЦЕ ВАЖЛИВО У СУЧАСНОМУ СВІТІ

Суми 2025

Глобальний інформаційний простір упродовж кількох останніх десятиліть став ареною боротьби між світовими державами-лідерами за отримання переваги у вирішенні проблем і конфліктів. Процеси глобалізації та невпинний розвиток інформаційних технологій породили нові загрози національній безпеці, насамперед терористичні та кібернетичні, виникнення кібертероризму, безпосередньо пов'язаного з рівнем науково-технічного прогресу.

Поява кібертероризму, що розглядається фахівцями як різновид технологічного тероризму та визнаний одним із найнебезпечніших видів кіберзлочинності, зумовлена переходом до електронного управління технологічними процесами.

Комп'ютерна безпека – це сукупність проблем у галузі телекомунікацій та інформатики, пов'язаних з оцінкою і контролюванням ризиків, що виникають при користуванні комп'ютерами та комп'ютерними мережами і розглядуваних з точки зору конфіденційності, цілісності і доступності.

Закон України «Про основні засади забезпечення кібербезпеки України» дає таке визначення: *«Про основні засади забезпечення кібербезпеки України» дає таке визначення: «кібернетична безпека (кібербезпека) – це стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі; кібернетичний простір (кіберпростір) – це середовище, яке виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем»*.

Об'єктами кібербезпеки та кіберзахисту є:

1) конституційні права і свободи людини і громадянина;

2) суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;

3) держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;

4) національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;

5) об'єкти критичної інфраструктури.

В свою чергу об’єктами кіберзахисту є:

1) комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань;

2) об’єкти критичної інформаційної інфраструктури;

3) комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.

Загроза для кібербезпеки – це умисна спроба отримати доступ до системи окремого користувача або цілої організації. Зловмисники постійно вдосконалюють свої методи атак, щоб уникати виявлення й використовувати нові вразливості. Однак деякі з цих методів досить поширені, і до них можна підготуватися.

Сучасний світ як ніколи оснащений великою кількістю засобів зв’язку. Світову економіку формують люди, які спілкуються, перебуваючи в різних часових поясах, і отримують доступ до важливої інформації звідусіль.

Кібербезпека стимулює продуктивність і впровадження інновацій, що дає користувачам змогу впевнено працювати та спілкуватись онлайн. Правильні рішення й процеси дають компаніям і державним установам змогу користуватися технологіями для покращення спілкування й надання послуг, не ризикуючи постраждати від атак.

Основні положення та визначення кіберпростору, основні напрями розвитку теорії кіберпростору, основи спілкування у кіберпросторі, економічна діяльність у кіберпросторі, особливості побудови пошукових систем, особливості побудови та функціонування соціальних мереж, соціальне, психологічне та культурне середовище кіберпростору, війна як один з основних способів протиборства в інформаційному та кіберпросторі наведено у посібнику:

Основи кіберпростору, кібербезпеки та кіберзахисту [Текст] : навчальний посібник / [автори: В. М. Богуш, В. В. Богуш, В. Д. Бровко, В. П. Настрадін]. - Київ : Ліра-К, 2022. - 553 с.

Навчальний посібник створений за результатами детального аналітичного вивчення сучасної міжнародної та національної нормативно-правової бази щодо сфери забезпечення кібербезпеки на міжнародному, державному рівні та на рівні організації. Він складається з трьох частин і чотирнадцяти розділів.

У першій частині здійснений аналіз основних напрямів розвитку теоретичних основ побудови та дослідження кіберпростору. Сформульовані загальні підходи щодо побудови, розвитку і використання інфраструктури кіберпростору та сервісів кіберпростору, а також методів та засобів дослідження соціологічної та психологічної сфери кіберпростору з метою виявлення загроз безпеці кіберпростору.

У другій частині на основі системного підходу викладені методологічні та теоретичні основи забезпечення безпеки особистості, суспільства та держави у кіберпросторі, що охоплює кіберінфраструктуру, кіберсервіси, соціологічні та психологічні сфери, пов’язані з діяльністю людей. Наведені теоретичні та методологічні основи запобігання кіберзлочинності, кібертероризму, кіберконфліктам і кібервійнам на основі впровадження методів та засобів забезпечення кібербезпеки.

У третій – визначені загальні завдання побудови та впровадження технологій та засобів захисту інфраструктури кіберпростору, основні напрями дослідження середовища кібербезпеки організації та розробки загальних підходів її

кіберзахисту, загальної методології обґрунтування засобів, заходів та технологій кіберзахисту організації, процесу побудови системи її кіберзахисту.

Посібник містить словник додаткових термінів і понять, покажчик ключових термінів і понять. Наведені також англійські еквіваленти термінів і понять, а також їхня етимологія, тобто визначення походження слова шляхом співставлення його зі спорідненими словами тієї або іншої мови. Це дозволяє досить докладно окреслити предметну частину кіберпростору, кібербезпеки та кіберзахисту та використовувати посібник як тлумачний словник.

Кібербезпека розроблена як галузь інформаційної безпеки, яка включає в себе різноманітні заходи та технології для захисту від різних кібернетичних загроз. Серед них – хакерські атаки, віруси, шпигунське програмне забезпечення та інші досить небезпечні ситуації. Методи з забезпечення конфіденційності, цілості та доступності інформації та комп'ютерних ресурсів наведено у посібнику:

Лісовська, Ю. П. Кібербезпека: ризики та заходи [Текст] : навчальний посібник / Ю. П. Лісовська. – Київ : Кондор, 2021. – 268 с.

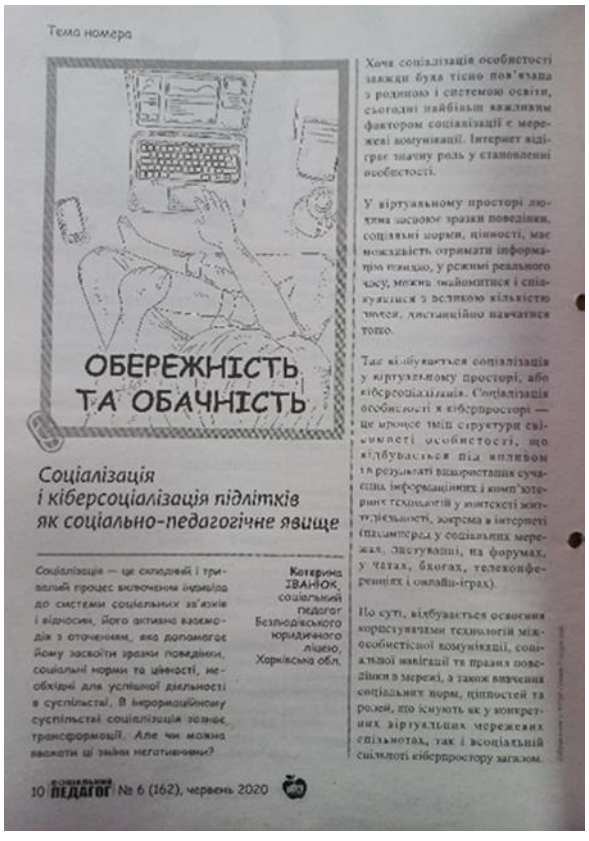
У навчальному посібнику розкрито кібербезпеку як інноваційну систему віртуальності сучасного інформаційного простору. Показано правову ентропію як кібербезпекове явище якісно нового семантичного стану особи, держави та суспільства в процесі їх самовизначення.

Акцентовано, що кібербезпекове управління інвестиційним ризиком є якісним забезпеченням антикорупційної інфраструктури України та країн світу. При цьому автор передбачає нову загрозу – аерокосмічний тероризм. В результаті цього, мають бути створені якісно нові наносупутники.

У сучасному інформаційному суспільстві система забезпечення кібербезпеки України створюється і розвивається відповідно до Конституції України та інших нормативно-правових актів, що регулюють суспільні відносини в електронній сфері. Основу даної системи складають органи, сили та засоби забезпечення кібербезпеки, які застосовують комплекс адміністративно-правових, інформаційно-аналітичних, організаційно-управлінських, та інших заходів, спрямованих на забезпечення стійкого функціонування системи державного управління.

Кіберсоціалізація – процес оволодіння навичками користування інтернетом, різноманітними програмними продуктами для комунікації в віртуальній мережі, а також за допомогою чат-ботів та віртуальних співрозмовників, наслідком якого є специфічна соціалізація особистості. Соціалізація і кіберсоціалізація підлітків як соціально-педагогічне явище розглядається у статті:

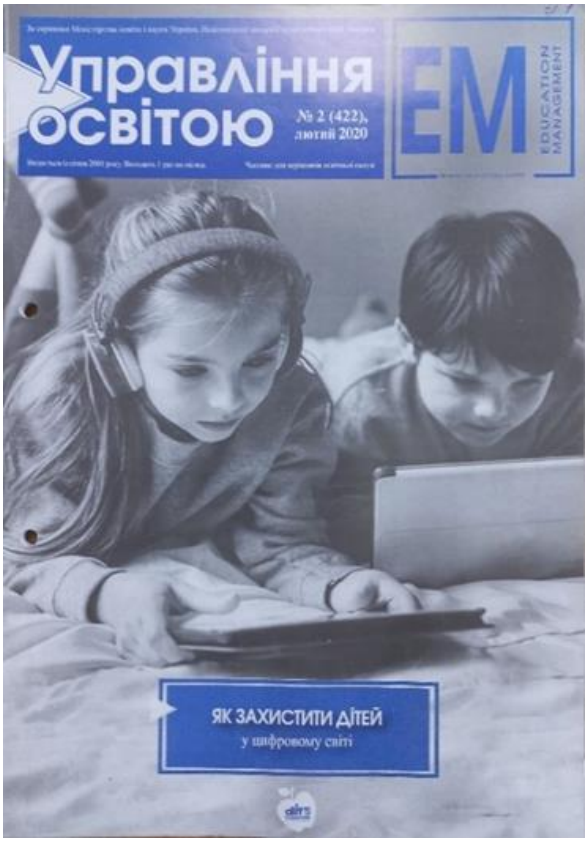
Іванюк, К. Обережність та обачність [Текст] : соціалізація і кіберсоціалізація підлітків як соціально-педагогічне явище / К. Іванюк // Соціальний педагог. – 2020. – № 6, червень. – С. 10-15.



У статті описуються вплив інформаційних технологій на свідомість підлітків, зокрема зміну структури свідомості, а також соціалізацію, що зазнає трансформації під впливом соціальних мереж. Автор розглядає проблему залежності підлітків від соціальних мереж, незадоволеність підлітків реальністю несе загрозу кібербулінгу, сексстингу та ін.

Кіберсоціалізація, життя в новій віртуальній реальності, Інтернет-залежна людина, п’ять основних типів інтернет-залежності детально розглядається в статті:

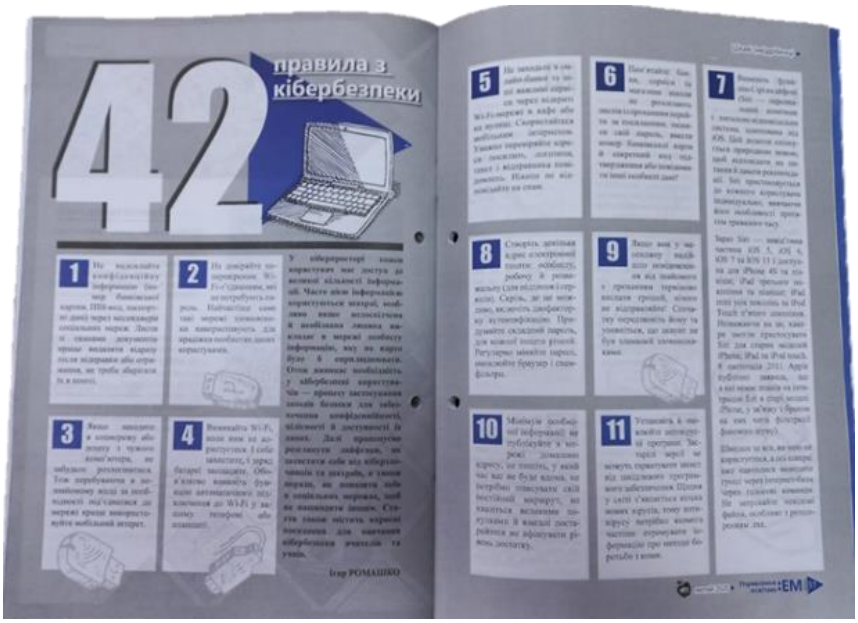
Бугайчук, А. Кіберсоціалізація [Текст] : життя в новій віртуальній реальності / А. Бугайчук // Управління освітою. – 2020. – № 2, лютий. – С. 24-44.



У статті розглядається кіберпростір, як новий простір для організації життєдіяльності людини і який висуває до неї певні вимоги, та впливає на її соціалізацію. Також автор описує переваги киберсоціалізації у сучасної молоді та виділяє основні ризики кіберсоціалізації. Значну увагу автор приділяє інтернет-феноменам, таким як тролінг, кібербулінг та кіберхарасмент.

42 правила з кібербезпеки, що актуальні як для дітей так і для дорослих користувачів інтернетом наведено в статті:

Ромашко, І. 42 правила з кібербезпеки [Текст] / І. Ромашко // Управління освітою. – 2020. – № 2, лютий. - С. 50-56.



У статті наведено рекомендації, щодо захисту від кіберзлочинців та шахраїв, а також поради, як поводити себе в соціальних мережах, щоб не нашкодити іншим. Стаття містить корисні посилання для навчання кібербезпеки вчителів та учнів.

У процесі кіберсоціалізації в людини виникає низка нових, фактично кіберонтологічних очікувань та інтересів, мотивів і цілей, потреб і установок, а також форм психологічної та соціальної активності, безпосередньо пов'язаних з кіберпростором.

Віртуальне середовище, поряд з природним, просторово-географічним, соціальним, культурним, ландшафтно-архітектурним тощо – відіграє значну роль як у повсякденному житті сучасної людини, так і в професійній діяльності.

Технології захисту і збереження інформації детально описано у навчальному посібнику:

Технології захисту інформації [Текст] : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король ; під заг. ред. С. Е. Остапова. – Київ : Новий світ-2000, 2020. – 500 с.

Навчальний посібник містить систематичний опис основ захисту інформації. Він складається зі вступу, тринадцяти розділів і лабораторного практикуму.

Перший розділ присвячено основним поняттям та визначенням курсу захисту інформації.

У другому розділі вивчаються основні поняття політики інформаційної безпеки, аналізуються моделі загроз і модель порушника, подано методику оцінки ризиків підприємства.

Розділи з третього по дев'ятий містять основи криптографічного захисту інформації, де розглядається симетрична й асиметрична криптографія, хешувальні алгоритми та електронний цифровий підпис, елементи криптоаналізу, основні напрямки розвитку сучасної криптографії.

У наступних розділах описані механізми та протоколи керування криптографічними ключами, методи та пристрої забезпечення безпеки, а також моделі захисту й використання механізмів контролю доступу.

У сучасних умовах Україна є об'єктом безперервного інформаційно-психологічного впливу, що обумовлено її геополітичним положенням і наявністю політичних, економічних та інших інтересів щодо нашої держави з боку розвинених країн та сусідніх держав, що зумовлює велику ймовірність втягнення її в інформаційну війну.

Національна безпека держави має стійку залежність від інформаційної безпеки та кібербезпеки, яка постійно зростає із розвитком інформаційних технологій.

Інформаційна безпека та кібербезпека держави, а також кіберпростір як середовище, в якому все частіше відбувається протиборство між суб'єктами міжнародних відносин описано в посібнику:

Інформаційна безпека та кібербезпека держави [Текст] : навчальний посібник / Н. М. Титова, Н. М. Рідей, В. П. Настрадін, М. М. Присяжнюк, С. М. Мамченко, С. В. Артюх, Р. О. Яворська ; під заг. ред. Н. М. Титова. – Київ : Ліра-К, 2024. – 224 с. – Режим доступу: https://jurkniga.ua/contents/informatsiyna-bezpeka-ta-kiberbezpeka-derzhavi.pdf?srsltid=AfmBOopXt2d2nIoHIga1p2xMkxZAiWHEPc8gL8TObwz-FCJa3HsJTIt5

Посібник містить теоретичні матеріали та правові основи з діяльності по забезпеченню інформаційної безпеки та кібербезпеки держави, значна увага приділена місцю медіа у проведенні інформаційної політики та спеціальних інформаційних операцій (інформаційно-психологічних операцій).

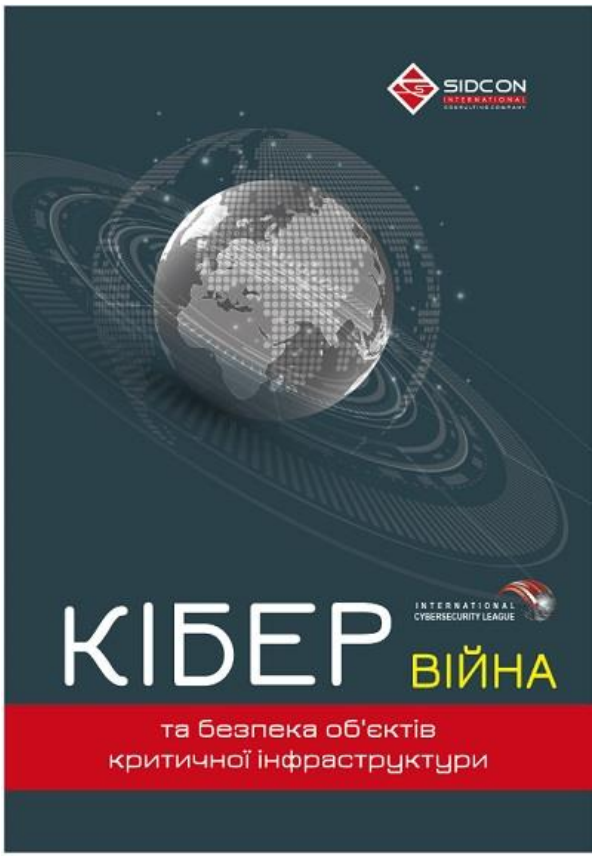
Видання складається з розділів: інформаційна безпека та кібербезпека в системі національної безпеки України; виклики та загрози національній безпеці України у сферах інформаційної безпеки та кібербезпеки; загрози людині в інформаційній сфері; засоби медіа та влада: особливості співпраці в царині забезпечення інформаційної безпеки держави; проблеми інформаційної безпеки: журналістські практики, російська пропаганда; маніпулятивний вплив у медіа.

Використання інформаційно-комунікаційних технологій як силового вирішення міждержавних суперечностей стає більш небезпечною загрозою

міжнародному миру й безпеці, національним інтересам держав. В епоху новітніх інформаційних технологій кіберпростір стає середовищем, в якому все частіше відбувається протиборство між суб'єктами міжнародних відносин у вигляді здійснення кібервійн, інформаційних, мереживоцентричних, асиметричних, гібридних війн.

Кібервійна та безпека об'єктів критичної інфраструктури розглядається у монографії:

Когут, Ю. Кібервійна та безпека об'єктів критичної інфраструктури [Текст]: [монографія] / Ю. Когут. – Київ : Сідкон, 2021. – 332с.



У книзі розкриті та проаналізовані питання створення системи безпеки та стійкості критичної інфраструктури для протидії гібридним загрозам в умовах стрімкого зростання кіберризиків для функціонування критичної інфраструктури. Надано дієві рекомендації для розбудови державних можливостей гарантувати безпеку суспільства в умовах реалізації багаточисельних гібридних загроз у світі.

Посібник розроблено для практичного використання у процесі діяльності критично важливих об'єктів з метою зниження та нейтралізації загроз безпеці їх функціонування, а також прийняття ефективних управлінських рішень.

Критична інфраструктура – це об'єкти, які є надзвичайно важливими для функціонування суспільства та економіки країни. До такої інфраструктури відносяться в першу чергу об'єкти оборони, а також ті, що забезпечують життєво важливі послуги та комунікацію.

Кібератаки, можуть здійснюватися як на критичну інфраструктуру будь-якої країни, так і на державні сайти цієї країни.

У зв'язку з розвитком нових технологій рівень кібервійни постійно вдосконалюється. Деякі держави починають приділяти захистові від кібервійни належну увагу – виділяють необхідні кошти для організації систем захисту і підтримують спеціальні підрозділи, основною задачею яких є вдосконалення інтернетної безпеки країни та захисту від нападів.

Кібервійни, кібертероризм, кіберзлочинність. Концепції, стратегії, технології розглянуто у монографії:

Когут, Ю. Кібервійни, кібертероризм, кіберзлочинність. Концепції, стратегії, технології [Текст]: [монографія] / Ю. Когут. – Київ : Сідкон, 2022. – 284с.

В книзі розкриті питання щодо основних концепцій, технологій та стратегій кібервійн, асиметричних, гібридних, мережевих, інформаційних війн, засад теорії проведення спеціальних інформаційних операцій, проблем та перспектив застосування кіберзброї в сучасній мережевій війні, загроз застосування штучного інтелекту, теоретико-правових аспектів кібертероризму, напрямів та способів використання кіберпростору в терористичних цілях, нових викликів і стратегій протидії кіберзлочинності.

Кіберзлочинність – це будь-яка злочинна діяльність, яку здійснюють у цифровому просторі. Часто ми уявляємо кіберзлочинність як «хакерство», що в цьому контексті означає несанкціоноване проникнення у цифрове середовище, але ж у цифровому всесвіті існує багато інших типів злочинів, в тому числі фізичних.

До категорії «кіберзлочинів» відноситься багато речей – від торгівлі дитячою порнографією або незаконного зняття коштів з рахунку клієнта за допомогою інсайдера в банку до крадіжки вихідного коду. Успішно вчинений кіберзлочин часто виявляє порушення права на конфіденційність. Наприклад, коли компанія неналежним чином зашифрувала особисті дані, і їх було викрадено, це є порушенням правил конфіденційності користувачів з боку компанії та водночас кіберзлочин з боку тих, хто викрав дані.

Кіберзлочинність спричиняє астрономічні фінансові втрати, які, однак, вкрай важко передбачити або прорахувати.

Когут, Ю. Цифрова трансформація економіки та проблеми кібербезпеки [Текст]: [монографія] / Ю. Когут. – Київ : Сідкон, 2021. – 368с.

Представлений практичний посібник є першим українським виданням, в якому акумульовані теоретичні знання та практичний досвід, системно розкриті питання та приведені технології забезпечення кібербезпеки в процесі цифрової трансформації державних та приватних структур в епоху четвертої промислової революції – Індустрії 4.0.

На цей час здатність здобувати, аналізувати та використовувати інформацію у сфері інформаційної та кібернетичної безпеки мають велике значення з декількох ключових причин, серед яких можна виділити зростання кількості даних, цифрову трансформацію бізнесу, суспільства, держави, збільшення загроз і ризиків від кіберзлочинності, залежність багатьох сфер життя від інформаційних технологій.

Підприємства, організації, державні установи активно впроваджують цифрові технології для покращення ефективності та конкурентоспроможності своєї роботи. Це призводить до збільшення кількості цифрових пристроїв, точок доступу, які потенційно можуть бути використані для кібератак.

Кібернапад та кібервторгнення можуть завдати величезних збитків або спричинити значні руйнування критичної інформаційної інфраструктури на будь-якому рівні. Це стосується насамперед кібератак на об’єкти енергетичної, транспортної та військової інфраструктури, під час яких виводяться з ладу об’єкти управління постачанням, керування логістикою тощо.

Законодавство України визначає: «Кібертероризм – терористична діяльність, що здійснюється у кіберпросторі або з його використанням». Що стосується природи кібертероризму, то він якісно відрізняється від загальноприйнятого поняття тероризму, зберігаючи лише стержень цього явища і ознаки. Кібертероризм, його історія, цілі та об'єкти розглядаються у монографії:

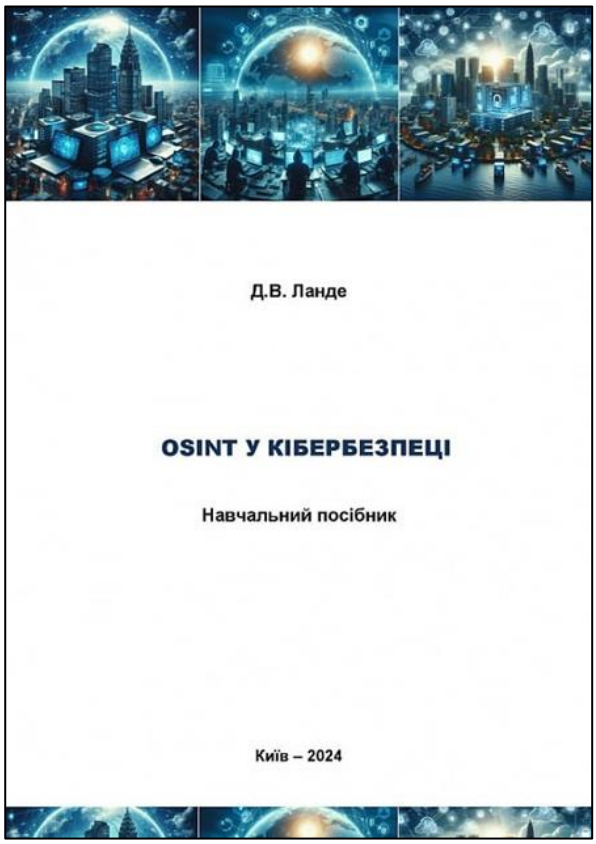
Когут, Ю. Кібертероризм. Історія, цілі, об’єкти [Текст]: [монографія] / Ю. Когут. – Київ : Сідкон, 2021. – 304с.

Дана робота є першим українським виданням, в якому системно розкриті питання феномену кібертероризму в світі та нові ризики, пов’язані з цим явищем, на рівні держави, суспільства, бізнесу та особистості; приведений перелік системних заходів для забезпечення кібербезпеки в процесі трансформації державних та приватних структур в епоху цифрової економіки. Кібертероризм використання комп’ютерних та телекомунікаційних технологій (насамперед, інтернету) в терористичних цілях.

Наприклад, акти, спрямовані на залякування з метою досягнення політичних результатів, або завдання шкоди комп'ютерним мережам, особливо персональним комп'ютерам, підключеним до Інтернету, за допомогою таких засобів, як комп'ютерні віруси.

Повномасштабна війна в Україні показала, наскільки потужним інструментом є OSINT (з англ. Open source intelligence) – розвідка на основі відкритих джерел, а саме концепція, методологія й технологія добування та використання військової, політичної, економічної та іншої інформації з відкритих джерел (мережі Instagram, Facebook, російські ресурси vk, «однокласніки» та livejournal та TikTok) без порушення законів. Використовується для ухвалення рішень у сфері національної оборони та безпеки, розслідувань тощо. Детально розглядається у навчальному посібнику:

Ланде, Д. OSINT у кібербезпеці [Текст] : навчальний посібник / Д. Ланде – Київ : ТОВ «Інжиніринг», 2024. – 552с.



Навчальний посібник присвячено розгляду ключових аспектів розвідки у відкритих джерелах, розвідувального циклу та його окремих етапів, процесів планування, збирання, обробки та аналізу розвідувальної інформації та доведення цільової інформації та висновків до замовника.

Детально розглядаються і аналітичні аспекти OSINT, включаючи комп'ютерну лінгвістику, методи інформаційного аналізу, засоби формування звітів. Крім того, велику увагу приділено використанню в рамках OSINT мереж та графових баз даних для аналізу та візуалізації такої інформації.

Сьогодні немає завдання, важливішого за перемогу України в усіх трьох традиційних просторах війни. Проте разом із перемогою над ворогом на землі, на морі й у повітрі, звільненням українських міст і сіл від окупанта, поверненням на всій нашій землі мирного життя й розвитку навряд чи колись в найближчому майбутньому настане мир у ще одному просторі – просторі комп'ютерних мереж, систем і даних або, як тепер його заведено спрощено називати, у кіберпросторі.

Україна сьогодні не лише успішно захищається від кібератак, а й атакує ворога у відповідь. І хоча це – новий вид війни не лише для України, а й для всього світу, ми вже маємо з чим порівнювати і свої успіхи, і свої невдачі. Перегони кіберозброєнь детально описується у монографії:

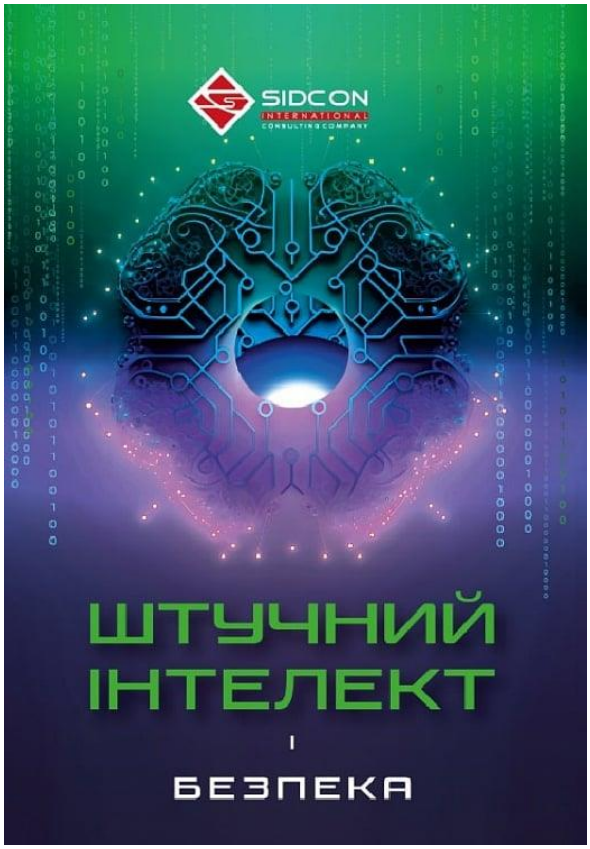
Перлрос, Н. Ось таким, як мені кажуть, буде кінець світу: перегони кіберозброєнь [Текст]: [монографія] / Н. Перлрос – Харків : Фоліо, 2024. – 576с.

Книга «Ось таким, як мені кажуть, буде кінець світу: перегони кіберозброєнь» – це журналістський подвиг. Спираючись на багаторічний досвід підготовки аналітичних матеріалів і проведення сотень інтерв'ю, колишня репортерка New York Times, яка на разі працює в провідному американському агентстві з кібербезпеки CISA, Ніколь Перлрос стягує завісу з тіньового ринку, розкриваючи серйозну загрозу, що насувається на кожного з нас. У книзі публікувано розлогі аналітичні матеріали щодо ключових кіберзлочинів останнього десятиріччя – атак російських хакерів на атомні станції, аеропорти й нафтохімічні заводи; розслідувала резонансну кібератаку представників КНДР на Sony Pictures, аналізувала кіберзлочини Ірану до низки американських нафтових компаній і банків, а також об'єктів критичної інфраструктури США.

Останніми роками у світі одне з провідних місць у структурі досліджень посідає проблематика технологій штучного інтелекту. Штучний інтелект використовується у вразливих сферах суспільства, таких як судова система, критична інфраструктура, відеоспостереження, та інше.

Необхідність забезпечення кібербезпеки у застосуванні штучного інтелекту описується у могографії:

Когут, Ю. Штучний інтелект і безпека [Текст]: [монографія] / Ю. Когут. – Київ : Сідкон, 2024. – 294с.



Книга присвячена актуальним векторам та проблемам розвитку штучного інтелекту як інструментарію безпеки та інтелектуальної зброї майбутнього. Також викладені напрацювання практичної спрямованості щодо потенціалу, сучасних трендів і перспектив інтегрування штучного інтелекту у різні сфери господарської діяльності і життєдіяльності суспільства та людини.

Значна увага приділена аналізу потенційної небезпеки штучного інтелекту і можливі наслідки його виходу з-під контролю людини.

Штучний інтелект (ШІ) відіграє важливу роль у кібербезпеці. Спочатку, ШІ використовував прості правила для відстеження мережевого трафіка та дій користувачів. Ці правила, створені людьми, допомагали виявляти підозрілу активність, але мали обмеження.

Надійна кібербезпека стала як ніколи важливою в сучасну цифрову епоху, оскільки бізнес-лідери намагаються бути на крок попереду в умовах, що постійно змінюються. Як і в багатьох інших сферах, роль штучного інтелекту (ШІ) у

кібербезпеці, ймовірно, стане більш помітною. Кіберзлочинність справила безпрецедентний вплив на бізнес у різних галузях.

Очікується, що у 2027 році ринкова вартість штучного інтелекту в кібербезпеці досягне 46,3 мільярда доларів США. Компанії, що займаються кібербезпекою ШІ, пропонують значні переваги, надаючи організаціям безцінні інструменти для навігації в кібербезпеці та більшої гнучкості перед викликами, що виникають у зв'язку з кіберзагрозами.

Кібербезпека та боротьба з кіберзлочинністю у XXI столітті – це одні з найбільш важливих питань, які потребують глибокого аналізу, розробок та впровадження високотехнологічних рішень з метою запобігання та викриття кіберзагроз.

Шановні читачі!

Деякі книги, представлені в огляді є в фондах Наукової бібліотеки університету.

За більш повною інформацією пропонуємо звернутися до мережі інтернет та Електронного каталогу бібліотеки

https://library.sspu.edu.ua/

Матеріал підготувала

бібліотекар ІІ категорії Міщенко М. І.