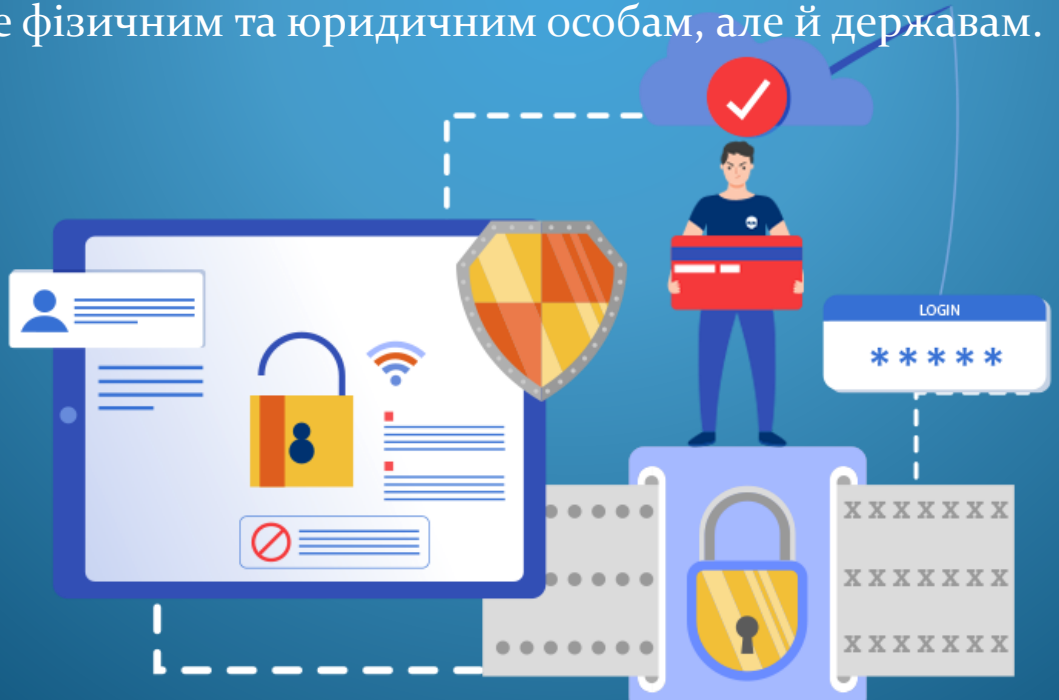
Кібербезпека у XXI столітті

Бібліотека ДУІТЗ ©

В епоху інформаційних технологій неможливо відчувати себе захищеним у кіберпросторі. З розвитком технологій стрімко зростає кількість злочинів у цій сфері, а тому з впевненістю можна стверджувати, що саме «кіберзлочини» у XXI столітті будуть одними з найчисельніших. В Україні та в усьому світі щороку здійснюють десятки тисяч злочинів з використанням інформаційно-комунікаційних технологій, програмних, програмно-апаратних засобів, інших технічних і технологічних засобів та обладнання. Щодня у людей та компаній крадуть персональні дані, кошти з рахунків, збирають безліч конфіденційної та комерційної інформації, блокують діяльність тощо. Це не дивно, адже кіберпростір – безмежний, а досвідчені хакери мають всі необхідні навички та засоби, щоб залишатися в ньому інкогніто. Сьогодні кібератаки шкодять не лише фізичним та юридичним особам, але й державам.



Щорічно у світі проводять сотні заходів різних рівнів щодо обговорення актуальних проблем кібербезпеки. В літературних словниках постійно з'являються нові визначення: кіберрозвідка, кібертероризм, кібершпигунство, кібервійна, кібероборона тощо. 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. Україна, як і всі країни світу, щодня зіштовхується з викликами у сфері кібербезпеки. За останні роки державні установи неодноразово були атаковані з кіберпростору. В Україні на законодавчому рівні приймають відповідні закони та нормативні акти, які регулюють відносини в цій сфері.

Станом на початок 2022 р. до правової основи кібербезпеки України входять такі нормативно-правові акти: Конституція України, Кримінальний кодекс України, закони України «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основи національної безпеки» та інші закони, Доктрина інформаційної безпеки України, Конвенція Ради Європи про кіберзлочинність та інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України. Відповідно до українського законодавства, кібербезпека – це захищеність життєво важливих інтересів людини й громадянина, суспільства та держави у процесі використання кіберпростору. Кібербезпека – це реалізація заходів із захисту мереж, програмних продуктів та систем від цифрових атак. В Україні політика щодо кібербезпеки покладається на низку державних органів, а саме на Державну службу спеціального зв'язку та захисту інформації України, Національну поліцію України, Службу безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України. В кожному із зазначених органів діють відповідні підрозділи.

Кібербезпека – це реалізація заходів із захисту мереж, програмних продуктів та систем від цифрових атак. В Україні політика щодо кібербезпеки покладається на низку державних органів, а саме на Державну службу спеціального зв'язку та захисту інформації України, Національну поліцію України, Службу безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України. В кожному із зазначених органів діють відповідні підрозділи.

Повністю захиститися від кібератак неможливо. Проте виконання хоча б мінімальних правил техніки безпеки в мережі значно підвищить шанси, що ваші дані не будуть викрадені зловмисниками. Отже, пропонуємо ознайомитися з основними правилами:

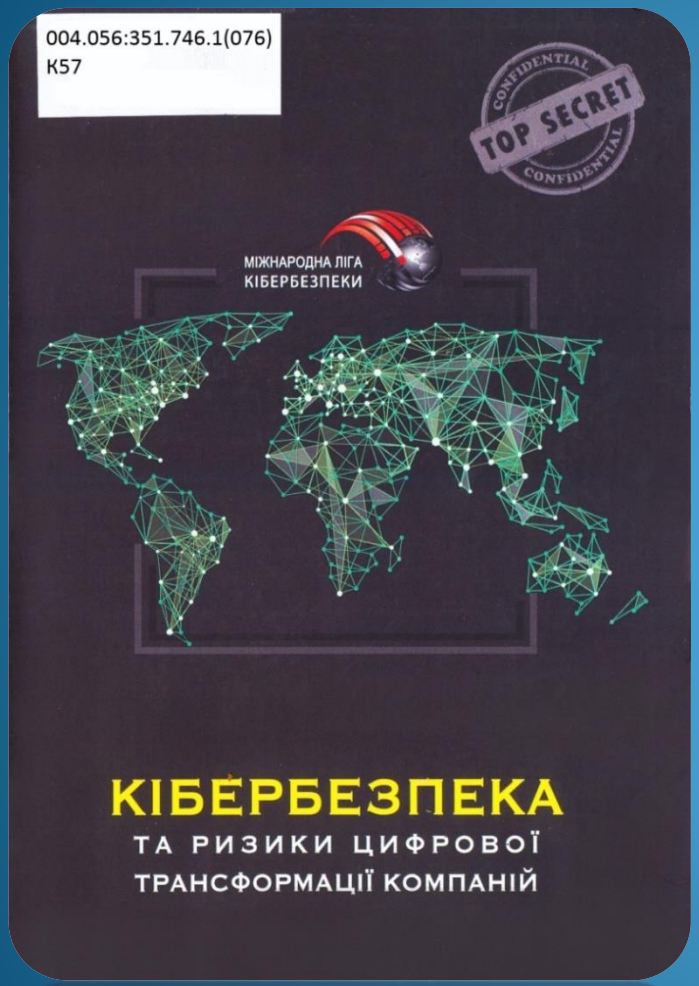
- користуватися виключно офіційним ПЗ і вчасно його оновлювати;
- не завантажувати програмне забезпечення з ненадійних джерел;
- використовувати антивірусні програми для роботи з комп'ютерами;
- нікому не передавати особисті персональні дані (пін коди карток, CVV коди, паролі до акаунтів тощо), навіть якщо вам намагаються вказати на необхідність таких дій з метою вирішення певного питання;
- не здійснювати платіжних операцій у відкритій, незахищеній мережі Wi-Fi;
- намагатися користуватися двофакторною аутентифікацією;
- не відкривати файли та листи від підозрілих джерел;

не переходити на підозрілі посилання та за спливаючими вікнами;

- не заходити на ненадійні сайти та не завантажувати з них жодне ПЗ;
- не вставляти у свій комп'ютер флешки та зовнішні диски, якщо не довіряєте джерелу;
- періодично здійснювати резервне копіювання важливої інформації;
- тримати свої гаджети в полі зору, коли перебуваєте у місцях, де до них можуть отримати доступ сторонні особи.

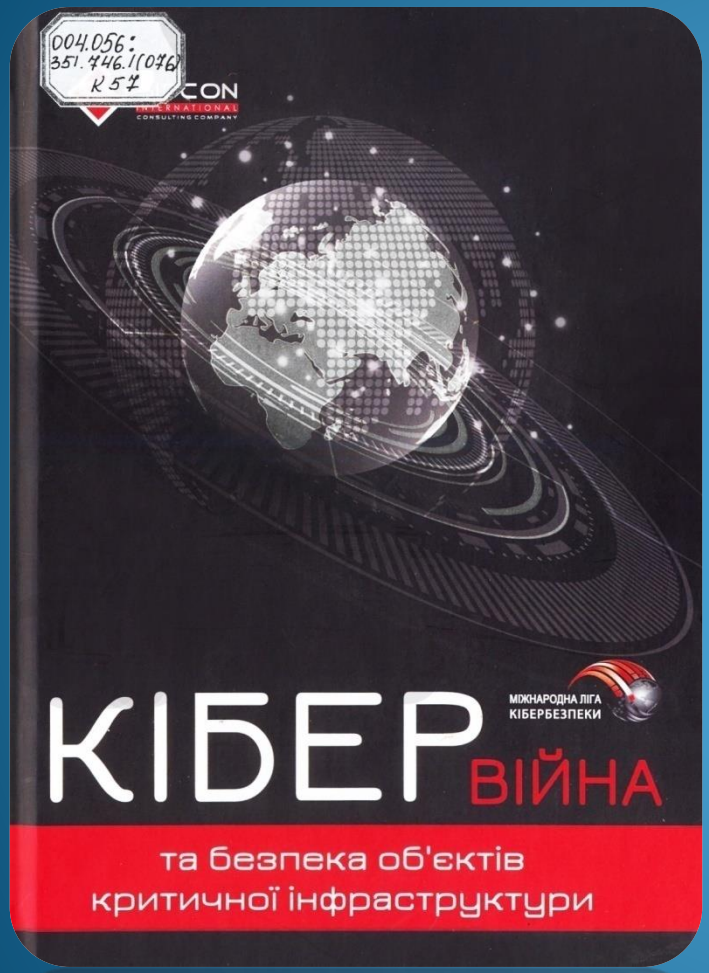
Когут, Ю. І. Цифрова трансформація економіки та проблеми кібербезпеки : практ. посіб. / Ю. І. Когут. – Київ : Сідкон, 2021. – 368 с.

Посібник підготовлений на базі більш ніж 20-тирічного практичного досвіду та практичної роботи автора у сфері кібербезпеки та корпоративної безпеки бізнесу. Він містить унікальні авторські напрацювання із захисту бізнесу та державних систем від сучасних кіберзагроз в умовах процесів діджиталізації в економіці та суспільстві. В посібнику акумульовані теоретичні знання та практичний досвід, розкриті питання забезпечення кібербезпеки. Посібник стане в нагоді державним управлінцям, керівникам та власникам бізнесу, науковцям, студентам.



Кібербезпека та ризики цифрової трансформації компаній : практ. посіб. / Ю. І. Когут. – Київ : Сідкон, 2021. – 372 с.

У посібнику вперше системно проаналізовано загрози безпеці держави, суспільства, бізнесу та особистості у кіберпросторі, в т. ч. кіберзлочини як окремий вид кіберзагроз та запропоновані технології протидії та боротьби з ними. У посібнику автор проаналізував загрози кібербезпеці, актуальні проблеми національної та міжнародної кібербезпеки, методи боротьби з кібертероризмом, системи захисту інформаційного простору України. Посібник буде корисним власникам та керівникам бізнесу, спеціалістам сфери цифрової трансформації, державним посадовцям, науковцям у сфері кібербезпеки.



Когут, Ю. І. Кібервійна та безпека об'єктів критичної інфраструктури : практ. посіб. / Ю. І. Когут. – Київ : Сідкон, 2021. – 332 с.

У книзі розкриті та проаналізовані питання створення національної системи безпеки та стійкості критичної інфраструктури для протидії гібридним загрозам в умовах стрімкого зростання кіберризиків для функціонування критичної інфраструктури. Кібероперації можуть використовуватися як засіб впливу на об’єкти цивільної інфраструктури, при цьому кіберзагрози постійно еволюціонують. В посібнику детально розглянуто досвід провідних зарубіжних країн щодо створення кібервійськ, національних структур, які забезпечують кібербезпеку на високому рівні. Посібник адресований фахівцям з безпеки, а також студентам, аспірантам, викладачам вузів, які готують фахівців з безпеки.

Когут, Ю. І. Кібертероризм (історія, цілі, об'єкти) : практ. посіб. / Ю. І. Когут. – Київ : Сідкон, 2021. – 304 с.

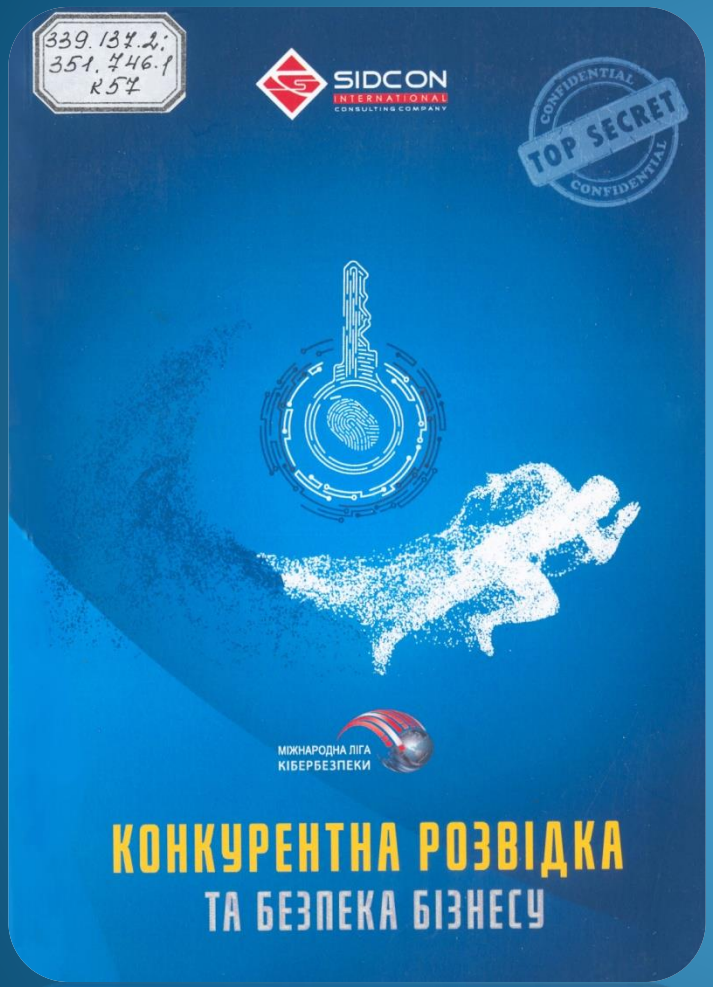
У посібнику приведені ефективні системні заходи протидії кібертероризму та забезпечення кібербезпеки критично важливих об'єктів інфраструктури, державних та приватних підприємств в епоху цифрової економіки. Жертвами кібертероризму у віртуальному просторі стали виступати не тільки окремі користувачі мереж, а й цілі держави. Зі зростанням використання інформаційних технологій зростає і використання їх у злочинних цілях та з корисливою метою. Повноцінне функціонування системи кібербезпеки має забезпечуватися комплексом організаційних, технічних, нормативно-правових заходів. Посібник рекомендується до використання власникам та керівникам бізнесу, керівникам державних підприємств, компаній, банків, державним посадовцям, науковцям у сфері кібербезпеки, студентам тощо.

Когут, Ю. І. Корпоративна безпека : практ. посіб. / Ю. І. Когут. – Київ : Сідкон, 2021. – 460 с.

Розглядаються теоретико-прикладні проблеми й питання: управління сферою національної безпеки України, державної безпеки, воєнної безпеки, економічної безпеки, захисту державної таємниці, захисту інформації, інтелектуальної власності, екології. Сучасним та актуальним завданням, яке стоїть перед компаніями державного та недержавного сектору економіки, є вихід на нові ринки та їх освоєння. Таким чином, корпоративна безпека впливає на економічну, інформаційну, продовольчу та інші види безпеки держави і бізнесу та є одним з факторів забезпечення національної безпеки України. Посібник орієнтований на власників бізнесу, наукових і науково-педагогічних працівників, аспірантів, студентів.

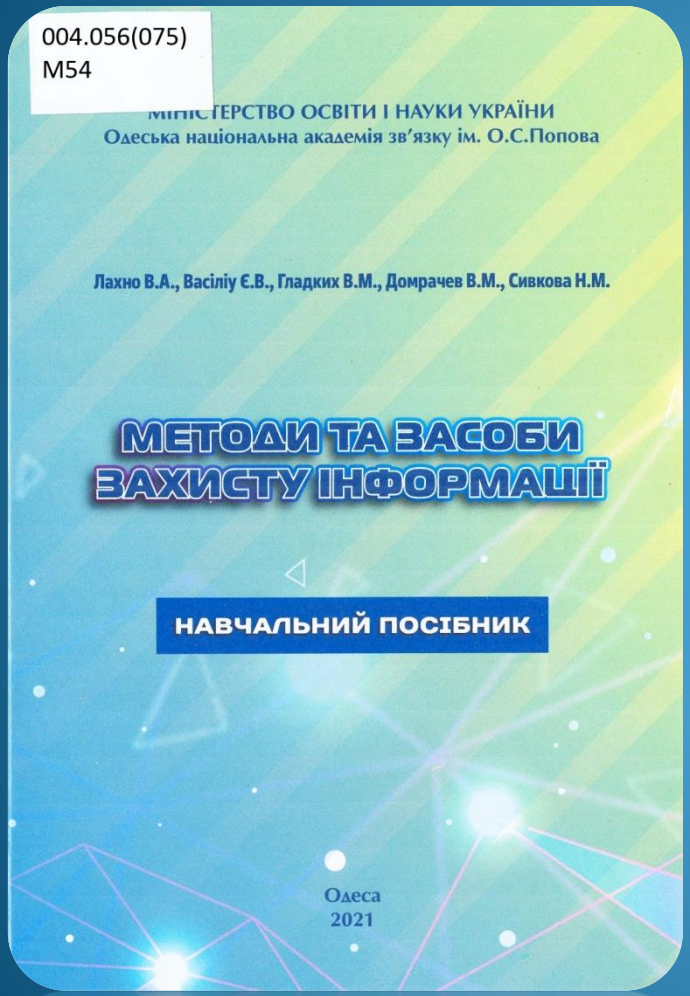
Корпоративна безпека для власників бізнесу в сучасних умовах / наук. ред. Ю. І. Когут. – Київ : Сідкон, 2018. – 276 с.

У посібнику розглядаються концептуальні положення, основні напрями та практичні рекомендації щодо забезпечення корпоративної безпеки в сучасних умовах. Розкривається сутність і стан інформаційної, економічної та корпоративної безпеки України. Проведено ідентифікацію загроз безпеці компаній і банків в умовах економічної кризи. Показано шляхи забезпечення безпеки національних компаній, запропоновано механізми забезпечення сучасної системи безпеки підприємництва. Посібник розрахований на власників і менеджмент українського бізнесу, викладачів, аспірантів та студентів.



Когут, Ю. І. Конкурентна розвідка та безпека бізнесу / Ю. І. Когут. – Київ : Сідкон, 2021. – 318 с.

У практичному посібнику викладені сучасні пріоритетні технології та інструменти конкурентної розвідки. Ці технології показали свою ефективність при використанні у низці провідних вітчизняних та зарубіжних компаній та отримали визнання на конференціях та семінарах з питань безпеки та захисту бізнесу. Посібник адресований фахівцям з безпеки, студентам економічних вузів та вузів, які готують фахівців з економічної та національної безпеки.

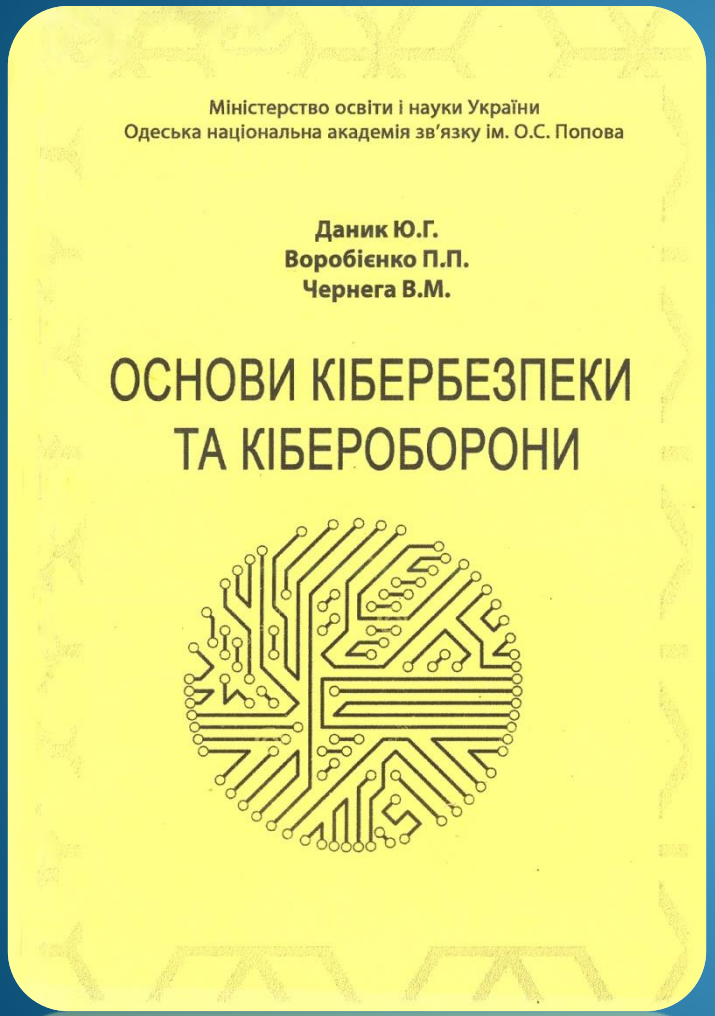


Методи та засоби захисту інформації : навч. посіб. / В. А. Лахно, Є. В. Василіу, В. М. Гладких [та ін.]. – Київ; Одеса : ЦП «Компринт», 2021. – 444 с.

У навчальному посібнику розглядаються сучасні методи та засоби захисту інформації, зокрема, викладені питання управління безпекою та управління доступом, архітектура і моделі безпеки, методи забезпечення безперервності бізнесу і відновлення після аварій, методи розробки безпечного програмного забезпечення. Матеріал в посібнику викладено згідно зі стандартом вищої освіти України, містить теоретичний і тестовий матеріал. При написанні посібника використано досвід та напрацювання авторів в галузях інформаційної безпеки, захисту інформації, розробки прикладного програмного забезпечення та дослідження провідних вчених в галузі кібернетичної безпеки. Призначений для студентів, аспірантів, викладачів вишу за спеціальністю 125 «Кібербезпека».

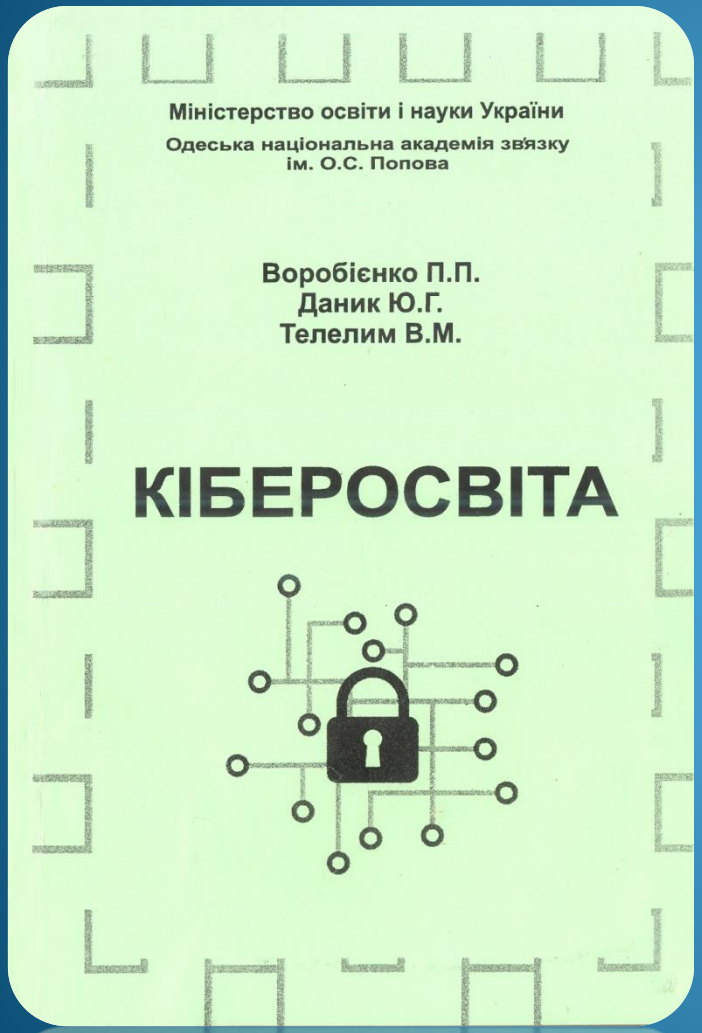
Наукоемкие технологии в инфокоммуникациях: обработка информации, кибербезопасность, информационная борьба : монография / под общ. ред. В. М. Безрука, В. В. Баранника. – Харьков : Лидер, 2017. – 600 с.

Монография содержит материалы по актуальным направлениям наукоемких инфокоммуникационных технологий. Стремительное развитие отраслей информатизации и коммуникации обусловило кардинальные изменения в обществе, государстве. Третья часть книги содержит результаты исследований в области кибербезопасности, защиты информации и информационной борьбы. Включены новые подходы относительно защиты статических и динамических информационных ресурсов для системы критической инфраструктуры. Рассматриваются вопросы планирования и управления в инфокоммуникационных сетях, хранения, обработки, интеллектуализации инфокоммуникационного пространства, обработки информации, кибербезопасности. Монография представляет интерес специалистам в области инфокоммуникаций, ученым, преподавателям и студентам.



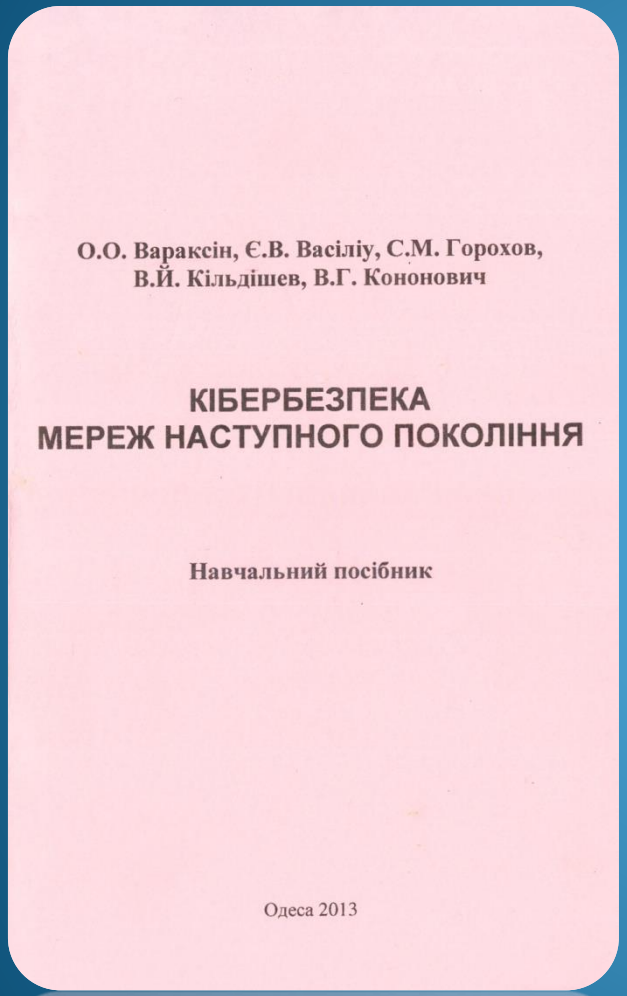
Даник, Ю. Г. Основи кібербезпеки та кібероборони : підручник / Ю. Г. Даник, П. П. Воробієнко, В. М. Чернега. – Одеса : ОНАЗ ім. О. С. Попова, 2018. – 228 с.

У підручнику викладено сутність і зміст кібербезпеки. Розглянуто роль і місце кібербезпеки у системі національної безпеки держави. Надано аналіз побудови системи кібербезпеки. Розглянуто широке коло питань зі складових кібербезпеки, їх аналізу і дій для їх всебічного забезпечення. Приділено значну увагу технологіям дій у кіберпросторі. Підручник буде корисним для студентів, науково-педагогічних працівників, докторантів, військових і цивільних фахівців, що працюють у галузі кібербезпеки.



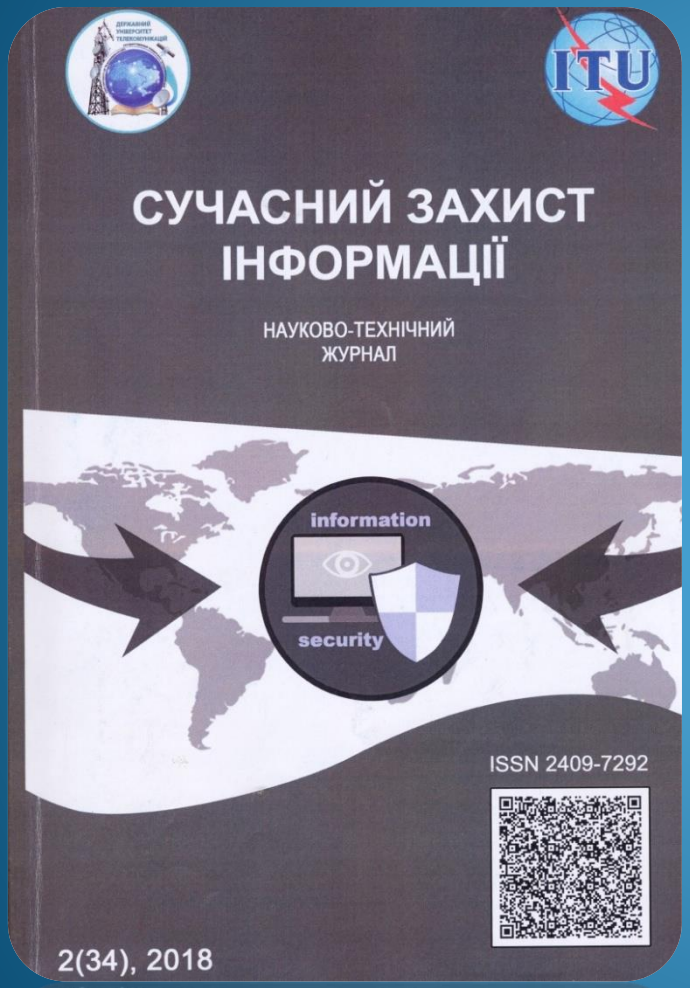
Воробієнко, П. П. Кіберосвіта : монографія / П. П. Воробієнко, Ю. Г. Даник, В. М. Тетелим. – Одеса : ОНАЗ ім. О. С. Попова, 2018. – 208 с. : іл.

У монографії розкрито сутність, зміст і взаємозв'язок кібернетичної та інформаційної безпеки, проведено аналіз формування та розвитку кіберосвіти в Україні та у світі. Для систематизації та удосконалення підготовки у сфері кібербезпеки авторами розроблено варіант реалізації організації системи освіти з питань кібербезпеки. Запропонована цілісна, послідовна, взаємопов'язана та безперервна система підготовки з питань кібербезпеки та кібероборони. Монографія призначена для науково-педагогічних, наукових працівників та фахівців у галузі кібербезпеки.



Кібербезпека мереж наступного покоління : навч. посіб. / О. О. Вараксін, Є. В. Василіу, С. М. Горохов [та ін.]. – Одеса : ОНАЗ ім. О. С. Попова, 2013. – 240 с.

У навчальному посібнику розглянуто основні положення, поняття й визначення, теоретичні засади та практичні аспекти кібербезпеки мереж наступних поколінь. Детально вивчається технологічне управління кібербезпекою. Розглядаються основні цілі, задачі, функції організаційного, правового, технічного, методичного та програмно-апаратного забезпечення кібербезпеки, джерела загроз і засоби їх впливу на об'єкти кібербезпеки. Вивчаються особливості побудови інфокомунікацій та архітектури систем кібербезпеки відповідно до вимог кіберсередовища. Навчальний посібник призначено для студентів, аспірантів, викладачів та працівників підприємств галузі зв'язку.



Боярчук, Р. М. Модель трансформації національної системи кібербезпеки в умовах дії гібридних загроз / В. А. Савченко, О. Й. Мацько, І. В. Новікова [та ін.] // Сучасний захист інформації. – 2020. – № 1. – С. 6-10. – Бібліогр. : 11 найм.

У статті розглядається підхід щодо формування робочого плану трансформації національної системи кібербезпеки України. Основна ідея наведеної методології базується на використанні комбінованої моделі оцінки ризику та досвіду попередніх трансформацій з урахуванням існуючих процесів управління в окремих організаціях. У результаті застосування моделі передбачається одержання плану з комплексом заходів, які слід здійснити для зменшення ризику порушення безпеки як окремого підприємства, так і для національної системи в цілому.

Лагута, В. В. Підвищення якості кібернетичної безпеки в інформаційно-телекомунікаційній системі підприємства / В. В. Лагута // Сучасний захист інформації. – 2020. – № 1. – С. 37-41 : 6 рис. – Бібліогр. : 2 найм.

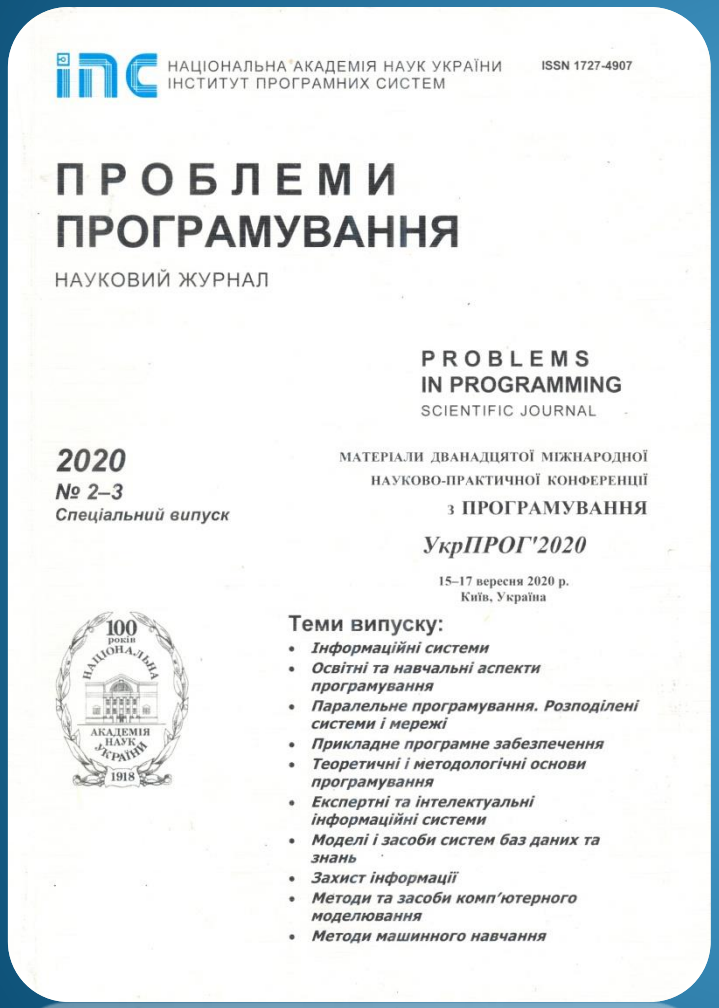
У статті проаналізовано принцип організації системи безпеки з використанням моделі OSI та рекомендації стандарту кібербезпеки ISO 27000. Показано переваги побудови системи безпеки з використанням доменного підходу. Розроблені рекомендації для побудови захищеної комп'ютерної мережі. Захист доцільно будувати по наступним напрямам : захист систем та пристроїв, безпека серверів, забезпечення захисту мережі та фізична безпека.

Давидюк, А. В. Підходи до верифікації артефактів процесу забезпечення кібербезпеки об'єктів критичного призначення / А. В. Давидюк // Електронне моделювання. – 2022. – № 1. – С. 107-117. – Бібліогр. : 25 найм.

З розвитком інформаційних технологій важливим аспектом стабільності функціонування систем критичного призначення стало забезпечення кібербезпеки об’єктів критичної інформаційної інфраструктури. Для захисту інформації законодавством України передбачено побудову комплексних систем захисту інформації та систем управління інформаційної безпеки. Саме виявлення ризиків на етапі проектування дає змогу уникнути більшості помилок та мінімізувати ризики порушення функціонування таких систем.

Ткач, Юлія. Тенденції розвитку сучасного кіберпростору та його захищеності в умовах інформаційного протиборства / Юлія Ткач // Безпека інформації. – 2020. – № 2. – С. 74-79 : рис. – Бібліогр. : 19 найм.

У статті розглянуто актуальне питання формування кіберпростору та особливості його захисту. В умовах, що сьогодні склались, має велике значення підтримка розробки і виробництва в Україні конкурентних інформаційно-комунікаційних засобів та програмного забезпечення, а також застосування таких засобів передусім в оборонному комплексі і об'єктах критичної інфраструктури, з метою протидії інформаційним впливам.



Семенченко, А. І. Організаційно-правові механізми державного управління забезпеченням кібербезпеки та кіберзахисту України: сутність, стан та перспективи розвитку / А. І. Семенченко, В. Л. Плескач, О. А. Заярний [та ін.] // Проблеми програмування. – 2020. – № 2/3. – С. 278-285. – Бібліогр.: 11 найм.

У статті здійснено аналіз організаційно-правових механізмів державного управління забезпеченням кібернетичної безпеки та кібернетичного захисту України. Також надано визначення його сутності, місця в системі стратегічного планування та управління сектором безпеки та оборони, проведено оцінку забезпечення кібернетичної безпеки України.

Савченко, В. А. Основні напрями застосування технологій штучного інтелекту у кібербезпеці / В. А. Савченко, О. Д. Шаповаленко // Сучасний захист інформації. – 2020. – № 4. – С. 6-11. – Бібліогр.: 15 найм.

У статті досліджуються ключові технології штучного інтелекту з метою застосування їх для забезпечення захисту інформації. У якості ключової ідеї застосування засобів штучного інтелекту у кібербезпеці запропоновано використання технологій та методів, які полегшують виявлення та реагування на загрози, використовуючи набори статистичних даних про кібератаки. Пріоритетні сфери застосування штучного інтелекту – забезпечення безпеки мереж і захист даних.

Потій, О. В. Аналіз методів оцінки і управління ризиками кібер- і інформаційної безпеки / Ю. І. Горбенко, О. А. Замула, К. В. Ісірова // Радіотехніка. – 2021. – № 3. – С. 5-24 : рис.; табл. – Бібліогр.: 13 найм.

Ефективність роботи установи, підприємства, компанії, організації безпосередньо залежить від якості і оперативності управління виробництвом. Загальновизнаним чинником при цьому є ефективне застосування інформаційних технологій (ІТ). При цьому застосування ІТ немислимо без підвищеної уваги до питань кібер- і інформаційної безпеки. Руйнування інформаційного ресурсу, його тимчасова недоступність або несанкціоноване використання можуть завдати організації значних збитків. Активна діяльність міжнародних організацій зі стандартизації підтверджує важливість питань забезпечення кібер- і інформаційної безпеки, постійного удосконалення моделей, методів та механізмів безпеки інформаційних технологій.

Дякуємо за увагу!