СИСТЕМА КІБЕРБЕЗПЕКИ УКРАЇНИ ТА ОНОВЛЕННЯ ОСВІТНЬОЇ ПРОГРАМИ МАГІСТРАТУРИ ЗА СПЕЦІАЛЬНІСТЮ «КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ»

sidcon.com.ua

Фундаментальним державним документом, який став першим етапом розвитку національної системи кібербезпеки України стала Стратегія кібербезпеки України, яка була схвалена у березні 2016 року. Ухвалення даної Стратегії спонукало до процесів поглиблення в питаннях забезпечення кібербезпеки та змін в законодавстві. У 2021 році була прийнята оновлена Стратегія кібербезпеки України на 2021-2025 роки.

Згідно зі Стратегією, викликами для України у сфері кібербезпеки є:

- активне використання кіберзасобів у міжнародній конкуренції;
- змагальний характер розвитку засобів кібербезпеки в умовах швидких прогресуючих змін інформаційно-комунікаційних технологій, зокрема хмарних та квантових обчислень, 5G-мереж, великих даних, Інтернету речей, штучного інтелекту тощо;
- мілітаризація кіберпростору та розвиток кіберзброї, що дає можливість приховано проводити кібератаки для підтримки бойових дій і розвідувально-підривної діяльності у кіберпросторі;
- вплив пандемії COVID-19 на економічну діяльність та соціальну поведінку, що спричинив стрімку трансформацію і організацію значного сегмента суспільних відносин у дистанційному режимі з широким використанням електронних сервісів та інформаційно-комунікаційних систем;
- упровадження нових технологій, цифрових послуг та механізмів електронної взаємодії громадян з державою, що здійснюється безсистемно в частині заходів з кібербезпеки та без належної оцінки ризиків.

Нормативно-правові акти України у сфері кібербезпеки

Законодавчі та концептуальні акти

- Закон України «Про основні засади забезпечення кібербезпеки України».
- Стратегія кібербезпеки України.
- Постанова Кабінету міністрів України «Про затвердження загальних вимог до кіберзахисту об’єктів критичної інфраструктури».
- Закон України «Про інформацію».
- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».
- Закон України «Про державну таємницю».
- Закон України «Про електронні документи та електронний документообіг».
- Доктрина інформаційної безпеки.
- Закон України «Про національну безпеку України».
- Стаття 15 КУ. Контроль за законністю заходів із кібербезпеки України.

Міжнародні нормативно-правові акти у сфері кібербезпеки

Серія стандартів ISO / IEC

- ISO/IEC27000:2019 - Інформаційні технології - Методи і засоби забезпечення безпеки - Системи управління інформаційною безпекою - Загальні відомості і словник
- ISO/IEC 27001:2013 - Інформаційні технології - Методи захисту - Системи управління інформаційною безпекою – Вимоги
- ISO/IEC 27002:2013/COR 2:2015 - Інформаційні технології - Методи захисту - Звід рекомендованих правил для управління інформаційною безпекою
- ISO/IEC 27003:2017 - Інформаційні технології - Методи безпеки - Системи управління інформаційною безпекою – Керівництво
- ISO/IEC 27004:2016 - Інформаційні технології - Методи безпеки - Управління інформаційною безпекою - Моніторинг, вимір, аналіз і оцінка
- ISO/IEC 27005:2018 - Інформаційні технології - Методи безпеки - Управління ризиками інформаційної безпеки
- ISO/IEC 27006:2015/AMD 1:2020 - Інформаційні технології - Методи безпеки - Вимоги до органів, які проводять аудит і сертифікацію систем управління інформаційною безпекою
- ISO/IEC 27007:2020 - Інформаційна безпека, кібербезпека і захист конфіденційності - Настанови щодо здійснення аудитів систем управління інформаційною безпекою
- ISO/IEC 15408-1:2009 - Загальні критерії оцінки захищеності інформаційних технологій
- ISO/IEC TS 27008:2019 - Методи безпеки - Вказівки для оцінки засобів контролю інформаційної безпеки
- ISO27032 – Інформаційні технології. Методи захисту
- ISO 27035 – Управління інцидентами
- ISO 22301 – Системи управління неперервністю бізнесу
- ISO31000 – Ризик-менеджмент

Міжнародні нормативно-правові акти у сфері кібербезпеки

Інші міжнародні стандарти

- Стандарт кібербезпеки ANSI/ISA 62443
- Стандарт безпеки даних індустрії платіжних карт (PCI DSS)
- COBIT5 (Control Objectives for Information and Related Technologies) / Цілі управління інформаційними та суміжними технологіями
- Система управління ризиками підприємства COSOERM2017
- TheCISCriticalSecurityControlsforEffectiveCyberDefensev7.1 / Важливі заходи безпеки Центральна безпека Інтернету для забезпечення ефективних кіберзахистів

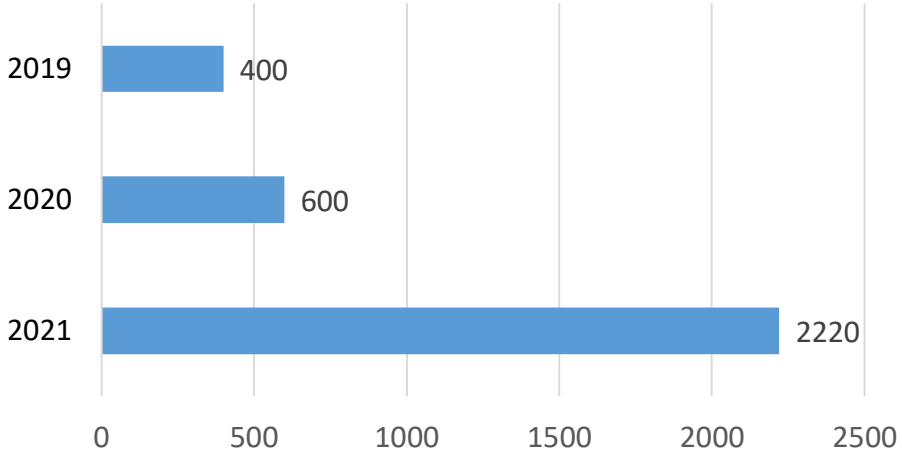
Європейський Союз. Загальні положення про кібербезпеку

- ПОСТАНОВА (ЄС) 2019/881 Європейського Парламенту та Ради від 17 квітня 2019 року про ENISA (Агентство Європейського Союзу з кібербезпеки) і про сертифікацію кібербезпеки інформаційних і комунікаційних технологій і скасування Регламенту (ЄС) № 526/2013 (Закон про кібербезпеку)
- Директива (ЄС) 2016/1148 Європейського Парламенту та Ради від 6 липня 2016 року про заходи щодо забезпечення високого загального рівня безпеки мережі та інформаційних систем по всьому Союзу
- Рекомендація КОМІСІЇ (ЄС) 2017/1584 від 13 вересня 2017 року про скоординоване реагування на великомасштабні інциденти і кризи в області кібербезпеки
- Рекомендація КОМІСІЇ (ЄС) 2019/534 від 26 березня 2019 року. Кібербезпека мереж 5G Стійкість, стримування і оборона: створення міцної кібербезпеки для ЄС
- Директива 2002/58 / ЕСЕВРОПЕЙСКОГО ПАРЛАМЕНТУ І РАДИ від 12 липня 2002 року щодо обробки персональних даних і захисту конфіденційності в секторі електронних комунікацій (Директива про конфіденційність і електронних комунікаціях)
- ПОСТАНОВА (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб при обробці персональних даних і про безкоштовне переміщення таких даних і скасування Директиви 95/46 / ЕС (Загальні правила захисту даних)
- ПОСЛАННЯ КОМІСІЇ ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ І РАДИ щодо сприяння захисту даних за допомогою технологій підвищення конфіденційності
- Стратегія кібербезпеки Європейського Союзу: Відкритий, безпечний і надійний кіберпростір
- Зміцнення Європейської системи кіберустійкості і розвиток конкурентоспроможної та інноваційної індустрії кібербезпеки
- Конвенція про кіберзлочинність 23.XI.2001 р

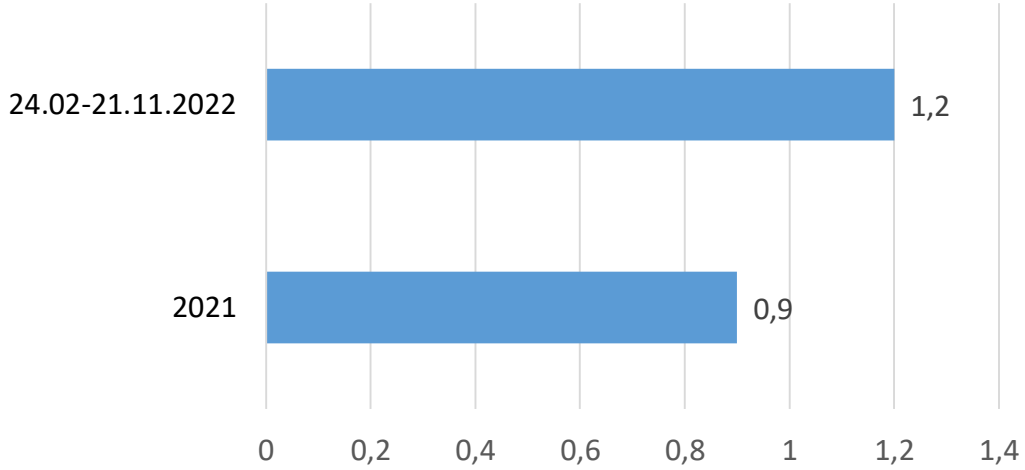
Проблеми кібербезпеки України

- Нестача висококваліфікованих фахівців у сфері кібербезпеки;
- Низький рівень обізнаності суспільства щодо кіберзагроз та кіберзахисту;
- Недосконалість державно-приватного партнерства у сфері кібербезпеку;
- Недосконалість законодавства у сфері кібербезпеки;
- Активний зріст кількості кібератак на державний та приватний сектори, в тому числі на енергетику.

Кількість нейтралізованих СБУ атак на сайти держорганів:



Кількість кібератак на об’єкти енергетичної інфрастуркутури України (млн. випадків)



Вдосконалення системи кібербезпеки в Україні

Для вдосконалення системи кібербезпеки в Україні, доцільно вдосконалювати та регулярно актуалізувати спеціальність, за якою навчаються майбутні фахівці з кібербезпеки, а саме:

- Вдосконалити існуючі науково-технічні лабораторії для покращення якості практичної підготовки фахівців;
- Вдосконалити систему співпраці з приватним сектором для того, щоб фахівці могли набувати практичних навичок під час навчання;
- Імплементувати навчальні дисципліни, які б охоплювали як технічні, так і інформаційно-психологічні аспекти кібербезпеки незалежно від спеціалізації;
- Розробити навчальні дисципліни, які вивчають забезпечення кібербезпеки на об’єктах критичної інфраструктури (в тому числі критичної енергетичної інфраструктури);
- Оновити навчальні дисципліни з метою їх відповідності провідним міжнародним стандартам кібербезпеки.

Фахівцями компанії Сідкон створено ряд практичних посібників, які розкривають актуальні проблеми кібербезпеки. Також, враховуючи умови сьогодення і актуальні загрози, розроблено серію видань з безпеки об'єктів критичної енергетичної інфраструктури, які також охоплюють питання кібербезпеки.

Кібербезпека та ризики цифрової трансформації компаній

У посібнику вперше систематизовано аналізуються загрози безпеці держави, суспільства, бізнесу та особистості в кіберпросторі в епоху глобальної цифровізації, зокрема кіберзлочинність як окремий вид кіберзагроз, запропоновані технології протидії та боротьби з ними.

Зміст книги «Кібербезпека та ризики цифрової трансформації компаній»

КІБЕРБЕЗПЕКА ТА РИЗИКИ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ КОМПАНІЙ

Зміст

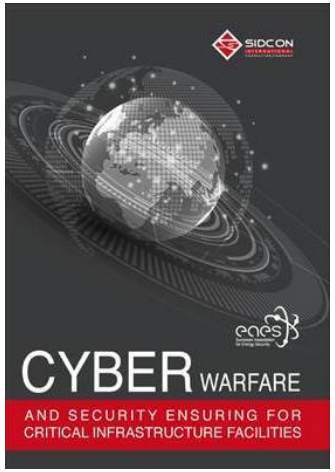
Серія книг з кібербезпеки

Кібертероризм

Цифрова трансформація економіки та проблеми кібербезпеки

Кібервійни, кібертероризм, кіберзлочинність (концепції, стратегії, технології)

Кібервійна та безпека об'єктів критичної інфраструктури



Технології блокчейн та криптовалюта: ризики та кібербезпека

Серія книг з енергетичної безпеки

Цілі та задачі робіт:

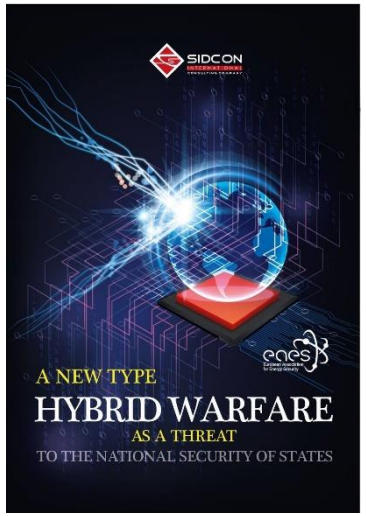
- **привернення уваги світової профільної спільноти до проблеми енергетичних війн та інших загроз об’єктам енергетики,**
- **необхідність посилення захисту та ефективності систем енергетичної безпеки,**
- **розробка та впровадження технологій безпеки для ефективного захисту об’єктів енергетики.**

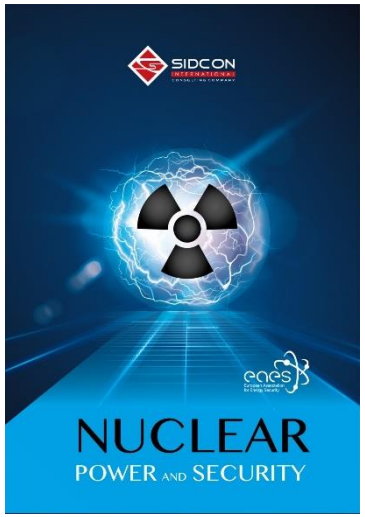
В роботах глибоко аналізуються:

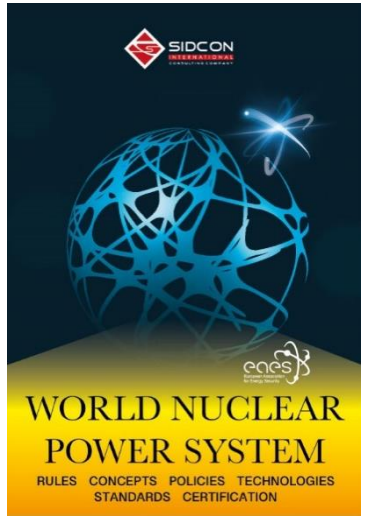
- питання ролі атомної енергетики у світі;
- роль найбільших міжнародних організацій у формуванні глобальної ядерної безпеки;
- загальні нормативні документи та міжнародні стандарти безпеки ядерної енергетики,
- а також пропонується комплекс заходів щодо забезпечення безпеки критичної інфраструктури об'єктів ядерної енергетики.

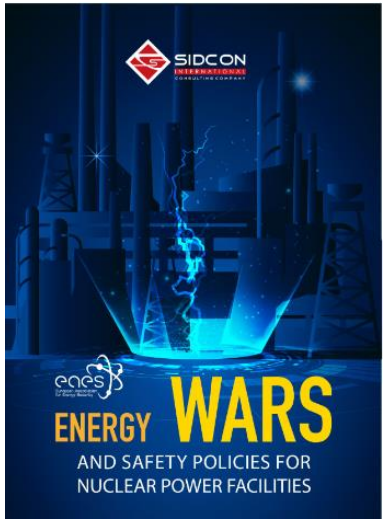
У ряді цих видань вперше в Україні
комплексно висвітлено проблеми енергетичної безпеки, в т.ч.
в сучасних умовах тотальної енергетичної кризи та
воєнних дій з одним із провідних постачальників енергоносіїв для країн ЄС,
створено чіткий алгоритм заходів мінімізації загроз критичній інфраструктурі,
який поєднується теоретичними відомостями та кращими практиками сфери енергетичної безпеки.

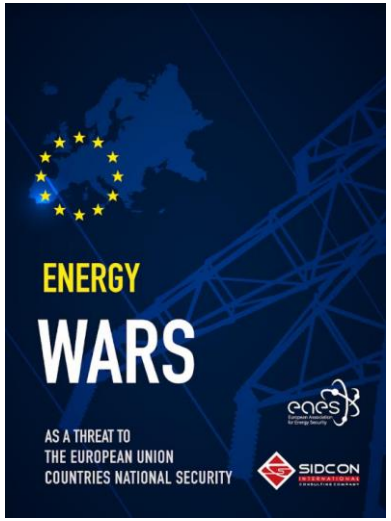
Серія книг з енергетичної безпеки





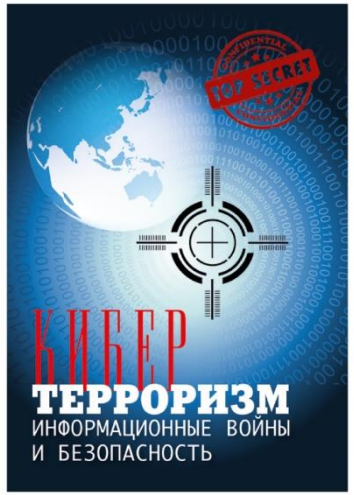


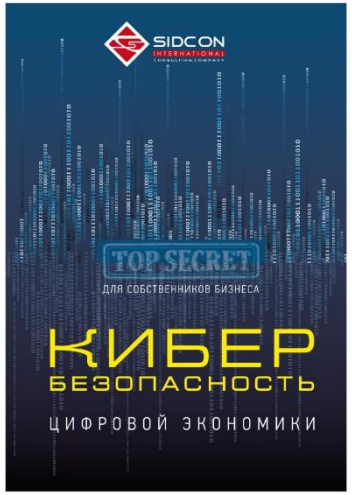




Інші видання

SIDCON INTERNATIONAL CONSULTING COMPANY





ДЯКУЄМО ЗА УВАГУ!

Наші контакти:

Адреса: 03115, Україна, м. Київ, Проспект Перемоги 121-б, оф. 224.
+38 (044) 454-07-92/93
+38 (050) 417 99 39

office@sidcon.com.ua
www.sidcon.com.ua