Безпека об'єктів критичної енергетичної інфраструктури в умовах гібридної війни.

Олена Ткаченко
Заступниця генерального директора
Консалтингова компанія «СІДКОН»

Загрози об'єктам критичної енергетичної інфраструктури

Різноманітність загроз, кількість яких постійно збільшується, створює велику реальну небезпеку в процесі захисту критичних об’єктів інфраструктури. Зокрема, нові вразливості для критичної інфраструктури проявилися з розвитком інформаційних технологій. Тому захист життєво-важливих суспільних структур та інститутів є ключовим питанням, яке потребує комплексного підходу.

Загрози безпеці

1. Загрози тероризму як фактор необхідності формування нових підходів щодо безпеки суб'єктів підприємництва;

2. Внутрішні загрози (з боку персоналу);

3. Кримінальні посягання (загальнокримінальна злочинність);

4. Інформаційні загрози: крадіжки корпоративних даних, корпоративний шпіонаж, інсайдерська розвідка, зловживання доступом, витік інформації;

5. Сучасні тенденції реалізації корпоративних загроз шляхом Web-атак, можливостей кібертероризму та кібершпіонажу;

6. Цілеспрямований підрив ділової репутації для дискредитації структури. Інформаційні війни, інформаційний тероризм (медіа-тероризм) та інші недобросовісні методи, що застосовуються у інформаційному протистоянні;

7. Політичні ризики;

8. Корупція в органах державної влади та управління.

Загрози безпеці

Міжнародний стандарт ISO/IEC 27032:2012 «Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки» (Information technology – Security techniques – Guidelines for cybersecurity) визнає **найпоширенішими такі кіберзагрози**:

- атаки соціального інжинірингу;
- хакінг (злом комп'ютерної системи);
- поширення шкідливого програмного забезпечення («шкідливих програм» / комп'ютерних вірусів – malware);
- упровадження шпигунських програм;
- дія інших потенційно небажаних програмних кодів.

Кібератаки на критично важливі енергетичні об'єкти у світі

Кібератака на атомні об’єкти південнокорейської корпорації KHNP в 2014 році

В рамках атаки співробітникам та партнерам АЕС, що належить KHNP, розіслали лист з шкідливим кодом через електронну пошту. В результаті вдалося заразити комп’ютери та викрасти дані щодо ядерних об’єктів KHNP.

Під час другої стадії атаки був зламаний веб-сайт компанії, що дозволило отримати персональні дані та облікові записи колишніх співробітників, що, в свою чергу, призвело до витоку даних щодо приватного життя співробітників корпорації.

Таким чином, зловмисники хотіли заразити комп’ютери у внутрішній мережі компанії шляхом відправки листів, які мали визвати довіру у співробітників.

На даному етапі вдалося вчасно виявити і зупинити інцидент, що дозволило корпорації уникнути збитків.

Кібератаки на критично важливі енергетичні об'єкти у світі

Досить відомою є масштабна кампанія з кібершпигунства – Red October («Червоний жовтень»), основними цілями якої були дипломатичні та урядові відомства, а також наукові організації різних країн світу, приватні компанії, які діють у сферах енергетики, зокрема ядерної, нафтової та газової, космосу та торгівлі.

Цей вірус унікальний тим, що, за попередніми оцінками, він почав діяти ще у 2007 р., а вперше був виявлений лише наприкінці 2012 р. (офіційно повідомлено про його викриття у січні 2013 р.).

Red October не був вірусом «сліпого пошуку»: для зараження систем зловмисники розсилали фішингові листи, адресовані конкретним отримувачам певної організації. Найбільше від вірусу постраждали країни колишнього СРСР, Східної Європи, а також низка держав у Центральній Азії.

Експерти так і не змогли надати однозначної відповіді щодо можливих замовників і виконавців зазначеної кібератаки.

За підрахунками експертів, за п’ять років своєї роботи Red October зміг передати своїм авторам сотні терабайт чутливої інформації.

Кібератаки на критично важливі енергетичні об'єкти у світі

Великобританія та Сполучені Штати виявили серйозні кібератаки Росії проти енергетичного сектору у всьому світі.

Вони виявили історичну злоякісну діяльність ФСБ, спрямовану проти критичних IT-систем та національної інфраструктури в Європі, Америці та Азії.

Національний центр кібербезпеки (NCSC) вважає, що центр 16 FSB, також відомий псевдонімами хакерської групи «Energetic Bear», «Berserk Bear» and «Crouching Yeti», здійснив шкідливу програму кіберактивності, спрямовану на критично важливі комп'ютерні системи та національні інфраструктури в Європі, Америці та Азії, за даними британського уряду.

https://www.infobae.com

Кібератаки на критично важливі енергетичні об'єкти у світі

Кібератаки на енергетичні компанії України

У грудні 2015 року на українські підприємства “Прикарпаттяобленерго” та “Київобленерго” була здійснена масштабна кібератака, яка призвела до відключення підстанцій, залишивши понад 310 тисяч споживачів без електроенергії. Кібератака була реалізована завдяки інтегрованому підходу, а саме: мережа попередньо була заражена за допомогою електронних листів, в яких був розташований шкідливий код. Після цього було зламано автоматизовану систему диспетчерського управління, що дозволило віддалено відключити підстанцію. Елементи інформаційної інфраструктури також були вимкнені, інформація про сервери та робочі станції була знищена.

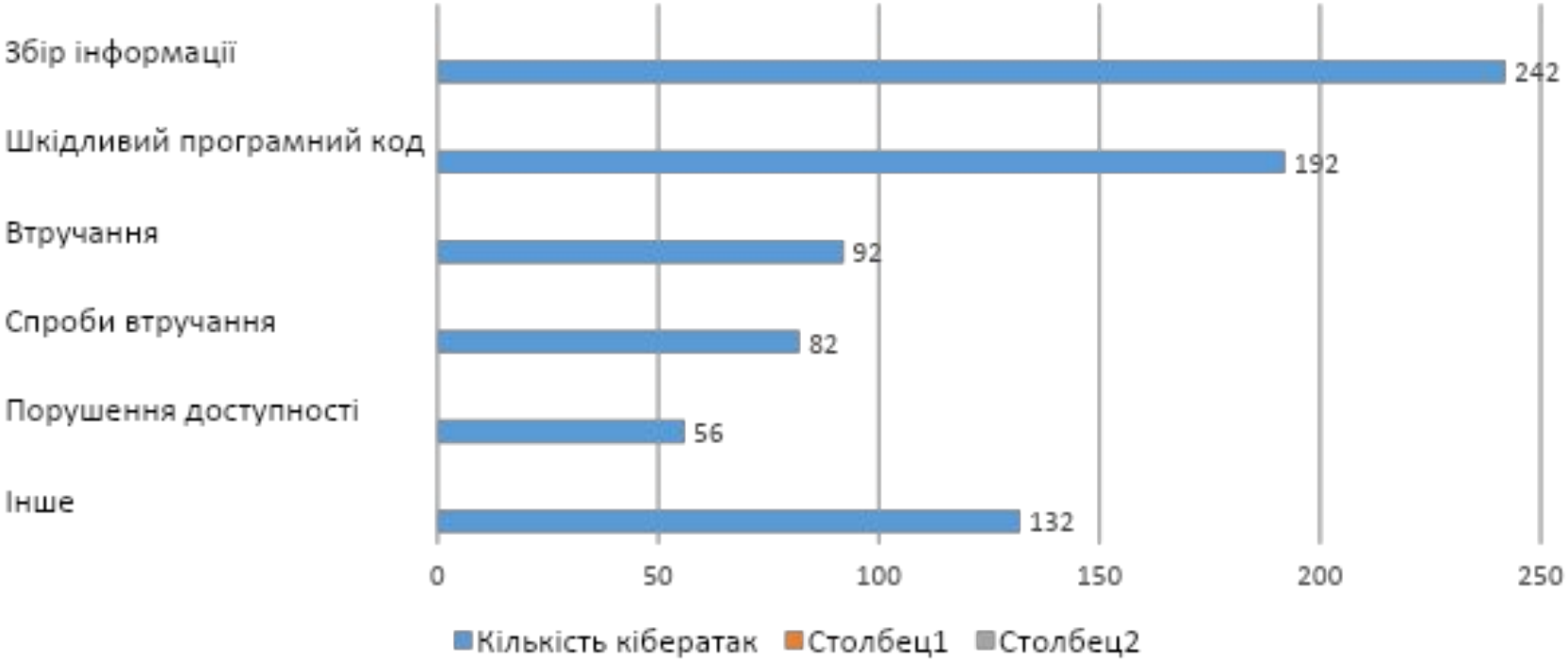
Кібератаки на критично важливі енергетичні об'єкти у світі

Кібератаки на енергетичні компанії України

Друга кібератака відбулася в ніч з 17 на 18 грудня 2016 року. У результаті кібератаки на підстанції “Північна” стався збій роботи автоматичних систем управління. Таким чином частина мешканців правого берегу Києва, а також прилеглих населених пунктів області залишились без світла на 1 годину і 15 хвилин. Іншої суттєвої шкоди не було зафіксовано, а дана кібератака була прикладом можливостей хакерського угруповування.

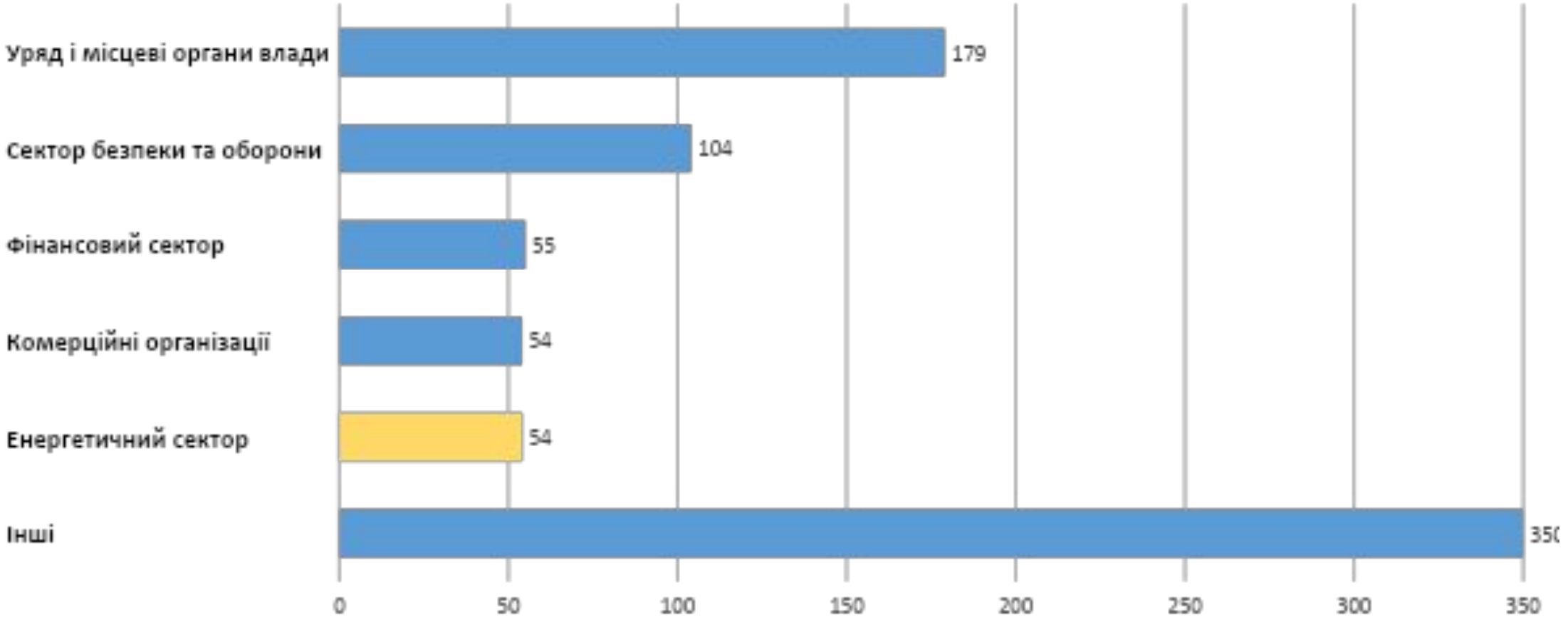
Найпоширеніші методи кібератак

За інформацією від Державної служби спеціального зв’язку та захисту інформації України, за перші чотири місяці війни відбулося 796 кібератак на інфраструктуру України.



SIDCON INTERNATIONAL CONSULTING COMPANY

Кількість кібератак за секторами



56% населення світу проживає в містах чи населених пунктах міського типу. Це говорить про те, що **енергія є критичною для існування всіх інших інфраструктур**. Усі інші системи залежать від енергії - від підзарядки мобільного телефону до роботи АЗС, водопостачання та виробництва. **Майже все потребує енергії**. З такою урбанізацією, згідно з попередніми дослідженнями вчених, жодна країна у світі не витримує більше місяця загального відключення від електроенергії.

Відсутність стійкої пропозиції енергетичних послуг призведе до хаосу навіть у розвиненій країні. Наслідки можуть бути найгіршими.

Ось чому альтернативні джерела виробництва енергії, децентралізація надання енергетичних послуг розробляються можливості надання автономного живлення для приватних будинків.

- ***Що теоретично може вимкнути хакерів? Наприклад, чи можуть ядерні електростанції зупинитися?***
- Теоретично може все вимкнути.

Атомні електростанції взагалі не підключені до Інтернету, але це не означає, що вони захищені від кібератак.

Євген Володимиров,

заступник міністра енергетики України з питань цифрового розвитку, цифрових трансформацій та цифровізації

30.06.2021

https://ukraine.segodnya.ua

Тенденція до збільшення кількості кібератак на енергетичний сектор

30 червня 2022 року Державна служба спеціального зв’язку та захисту інформації України повідомила про те, що за 4 місяці повномасштабної війни було виявлено майже 800 кібератак, в тому числі і на енергетичний сектор.

Так, пресслужба «Укренерго» повідомила, що з початку повномасштабної війни було зафіксовано 10-кратне збільшення DDos-атак на компанію (50 за 100 днів війни та 5 за останні 3 роки).

Методика формування системи забезпечення безпеки підприємства включає етапи:

1. аналіз зовнішніх та внутрішніх загроз безпеці підприємства та вивчення інформації про минулі кризові ситуації підприємства, їхні причини та шляхи врегулювання;
2. аудит наявних засобів із забезпечення безпеки підприємства та аналіз їх відповідності виявленим загрозам;
3. моделювання комплексної системи безпеки підприємства :
   - розробка плану усунення виявлених під час аудиту недоліків;
   - підготовка пропозицій щодо удосконалення системи безпеки (у тому числі визначення механізмів її забезпечення та розробка організаційної структури управління зазначеною системою);
   - розрахунок усіх видів необхідних ресурсів;
   - планування щомісячних витрат на забезпечення функціонування системи безпеки підприємства;
4. формування / побудова комплексної системи безпеки підприємства;
5. оцінка ефективності сформованої системи, а також визначення шляхів підвищення її результативності.

SIDCON INTERNATIONAL CONSULTING COMPANY

Проведення кібераудиту та розробка системи кіберзахисту

Дозволить:

- оцінити надійність, цілісність та ефективність управління інформаційними процесами та кіберзахисту підприємства;
- розробити ефективну політику інформаційної безпеки та забезпечити її якісне виконання;
- розробити відповідні коригуючі і попереджуючі рішення з метою поліпшення стану інформаційної безпеки та кіберзахисту і формування ефективної СУІБ на підприємстві, зокрема, розробити ключові рекомендації щодо вдосконалення системи управління та забезпечення інформаційної безпеки і кіберзахисту на підприємстві;
- забезпечити надійність збереження інформаційних, фінансових ресурсів підприємства, та на високому рівні підтримувати репутацію підприємства перед клієнтами та професійною спільнотою;
- постійно відслідковувати та оцінювати ризики діяльності з урахуванням цілей діяльності;
- ефективно виявляти найбільш критичні бізнес-ризики та знижати ймовірність їх реалізації;
- ефективно розробляти, впроваджувати та тестувати плани відновлення діяльності;
- забезпечити розуміння питань кібербезпеки керівництвом та всіма працівниками підприємства;
- забезпечити підвищення репутації та ринкової привабливості підприємства;
- знизити ризики рейдерських та інших шкідливих для підприємства атак;
- оптимізувати вартість побудови та підтримання системи кібербезпеки, виконання корпоративних стандартів безпеки ведення діяльності.

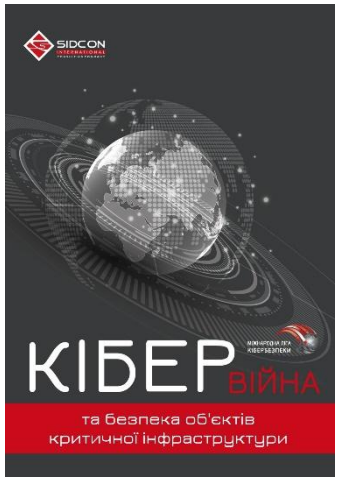
Реалізація та впровадження окремих елементів системи кібербезпеки не є системою кібербезпеки, та означає відсутність такої системи (що робить неможливим дотримання належного рівня безпеки).

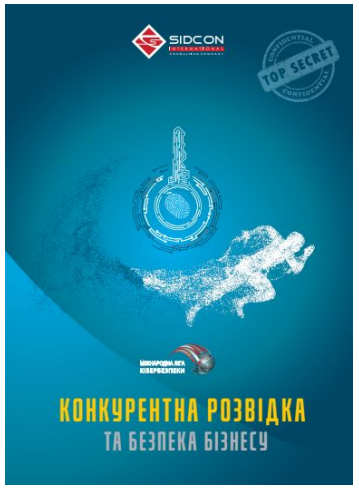
Відсутність впровадженої на підприємстві системи кібербезпеки може призвести до зниження рівня захищеності та втрати активів підприємства, а в деяких випадках – до непоправних наслідків для населення та держави.

Проведення комплексного кібераудиту (методологічний рівень) передбачає опрацювання 112 обов'язкових (згідно міжнародних стандартів) документів СУІБ.

SIDCON INTERNATIONAL CONSULTING COMPANY

ПРО КОМПАНІЮ “СІДКОН”
Книги та практичні видання для бізнесу:





SIDCON INTERNATIONAL CONSULTING COMPANY

ДЯКУЮ ЗА УВАГУ!

Олена Ткаченко
tkachenko@sidcon.com.ua