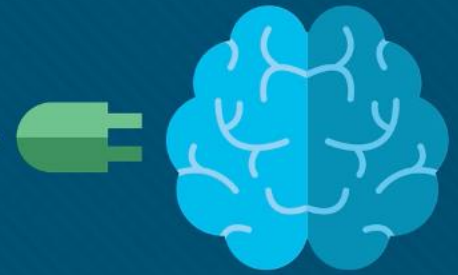


Розділ 5. Чи готові Ви пов’язати своє майбутнє з кібербезпекою?

Вступ до кібербезпеки (I2CS)

Мета розділу

Розділ 5. Чи готові Ви пов’язати своє майбутнє з кібербезпекою?

Мета розділу: Отримати доступ до різноманітної інформації та ресурсів, щоб вивчити різні варіанти кар’єри в галузі кібербезпеки.

Назва теми	Мета вивчення теми
Правові та етичні питання	Визначити деякі особисті та корпоративні юридичні питання, які можуть виникнути під час роботи в сфері кібербезпеки.
Освіта та кар'єра	Визначити, які професійні сертифікати та наступні кроки потрібно зробити, щоб продовжити кар'єру в галузі кібербезпеки.

5.1 Правові та етичні питання

Правові питання кібербезпеки

Для захисту від атак фахівці з кібербезпеки повинні володіти тими ж навичками, що й зловмисники. Проте фахівці з кібербезпеки використовують свої навички в межах закону.

Персональні правові питання

- На роботі чи вдома у вас може бути можливість та навички зламати комп'ютер або мережу інших. Але є стара приказка: «Те, що ти можеш, не означає, що ти повинен». Більшість зломів залишають сліди, які можна відстежити і вони приведуть до вас.
- Фахівці з кібербезпеки розвивають багато навичок, які можна використовувати як позитивно, так і незаконно. Завжди існує величезний попит на тих, хто вирішує використати свої кібер-навички у законних межах.

Правові питання кібербезпеки (прод.)

Корпоративні правові питання

- У більшості країн діють закони про кібербезпеку, яких підприємства та організації повинні дотримуватися.
- У деяких випадках, якщо ви порушуєте закони про кібербезпеку під час виконання своєї роботи, організація може бути покарана, і ви можете втратити роботу. В інших випадках можливе кримінальне переслідування, штрафи та ув'язнення.
- Загалом, якщо ви не впевнені в тому, що певна дія або поведінка є законною, то припускайте, що вона незаконна і не робіть цього. Завжди звертайтеся до юридичного або кадрового відділу організації.

Правові питання кібербезпеки (прод.)

Міжнародне право та кібербезпека

- Міжнародне право з кібербезпеки – сфера, яка постійно розвивається. Кібератаки відбуваються у кіберпросторі, електронному просторі, створеному, обслуговуваному та що належить як державним, так і приватним організаціям. У кіберпросторі немає традиційних географічних кордонів. Щоб ще більше ускладнити проблеми, набагато легше замаскувати джерело атаки в кібервійні, ніж у звичайній війні.

- Світове суспільство все ще дискутує, як краще боротися з кіберпростором. Практика країни, opinio juris (відчуття в країни, що вона прив'язана до відповідного закону) та будь-які розроблені договори будуть формувати міжнародне право з кібербезпеки.

Етичні проблеми кібербезпеки

- Згадайте тест на проникнення, який ви проводили для @Apollo. Цей тест показав, що один із ваших колег, який розпочав роботу одночасно з вами, несе відповідальність за витік даних. Ви думаєте не включати це у свій звіт, оскільки вони можуть зіткнутися з проблемами.

- **Поставте собі наведені нижче запитання, щоб допомогти вам визначити як діяти найкраще.**

  - Це законно?
  - Чи відповідають ваші дії політиці @Apollo?
  - Чи будуть ваші дії сприятливими для @Apollo та зацікавлених сторін?
  - Чи було б добре, якби всі в @Apollo зробили цю дію?
  - Чи буде результат вашої дії відображати @Apollo у позитивному світлі в заголовках новин?

Корпоративні етичні питання

- Багато професійних IT-організацій, таких як Асоціація безпеки інформаційних систем (ISSA), опублікували кодекси етики, щоб допомогти керувати діями та поведінкою співробітників.
- У Cisco також є команда, яка займається виключно етичною діловою поведінкою, і Кодекс ділової поведінки, який допомагає співробітникам приймати ділові рішення та вирішувати будь-які проблеми, з якими вони можуть зіткнутися.

5.2 Освіта та кар'єра

Станьте гуру з кібербезпеки

- Ви досягли успіху у своїй ролі аналітика з безпеки початкового рівня в @Apollo, але є багато вакансій з кібербезпеки, які варто розглянути.
- Навіть якщо ви тільки починаєте свою кар’єру в галузі кібербезпеки, варто почати переглядати пошукові системи, такі як Indeed, ITJobMatch, Monster і CareerBuilder, щоб зрозуміти, які вакансії доступні в цій сфері!

Професійні сертифікації

Сертифікати з кібербезпеки – це чудовий спосіб перевірити свої навички та знання, а також підвищити свій кар’єрний ріст.

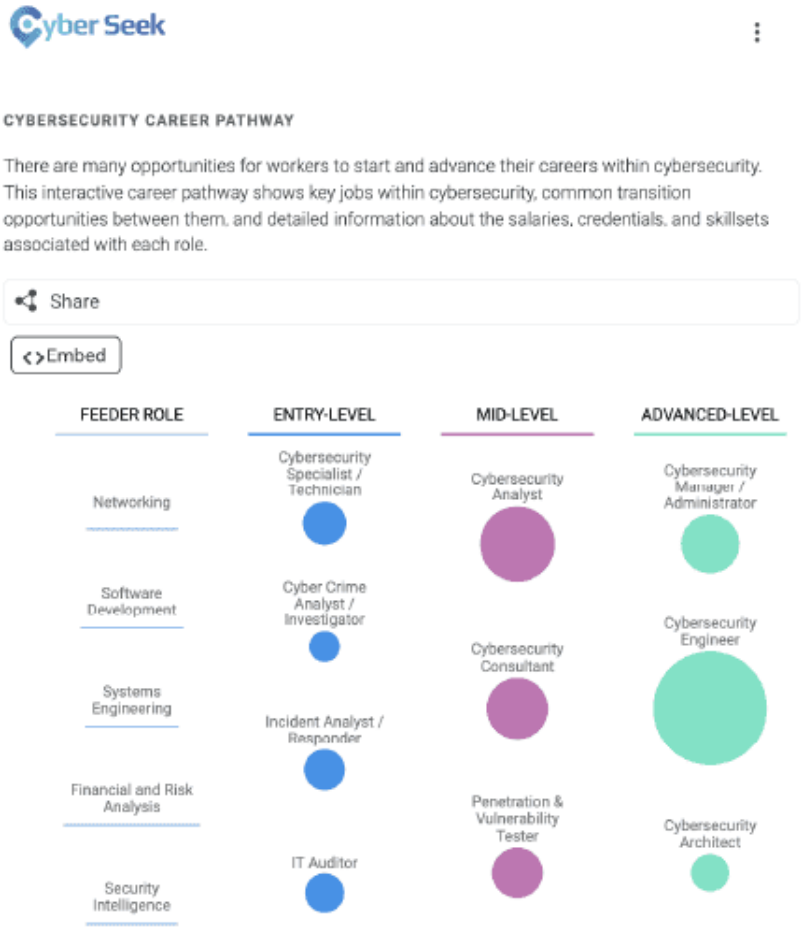
- **Microsoft Technology Associate (MTA) Основи безпеки:** Ця сертифікація орієнтована на учнів старших класів, студентів та тих, хто зацікавлений у зміні професії.
- **Palo Alto Networks Certified Cybersecurity Associate:** Це сертифікація початкового рівня для новачків, які готуються розпочати свою кар’єру у сфері кібербезпеки.
- **ISACA CSX Cybersecurity Fundamentals Certificate:** Ця сертифікація призначена для нещодавніх випускників середньої освіти та тих, хто зацікавлений у зміні професії. Термін дії цього сертифіката не закінчується і не вимагає періодичної повторної сертифікації.

Професійні сертифікації (прод.)

- **CompTIA Security+:** Це сертифікат безпеки початкового рівня, який відповідає вимогам Директиви Міністерства оборони США 8570.01-M, що є важливим пунктом для тих, хто хоче працювати в галузі IT-безпеки для федерального уряду.
- **EC Council Certified Ethical Hacker (CEH):** Ця сертифікація перевіряє ваше розуміння та знання того, як шукати слабкі місця та вразливості в цільових системах, використовуючи ті ж знання та інструменти, що й зловмисний хакер, але законним і легітимним способом.
- **ISC2 Certified Information Systems Security Professional (CISSP):** Це найбільш впізнаваний і популярний сертифікат безпеки Щоб скласти іспит, необхідно мати принаймні п’ять років досвіду роботи у відповідній галузі.
- **Cisco Certified CyberOps Associate:** Ця сертифікація підтверджує навички, необхідні для аналітиків з кібербезпеки в операційних центрах безпеки.

Кар'єрні шляхи в галузі кібербезпеки

- CyberSeek – це інструмент, який надає детальні дані про попит і пропозицію на ринку праці в галузі кібербезпеки, щоб допомогти закрити розрив у навичках із кібербезпеки.



5.3 Контрольна робота

Що ми вивчили у цьому розділі?

- Для захисту від атак фахівці з кібербезпеки повинні володіти тими ж навичками, що й зловмисники. Проте фахівці з кібербезпеки використовують свої навички в межах закону.

- **Особисті правові питання:** На роботі чи вдома у вас може бути можливість та навички зламати комп’ютер або мережу інших. Але є стара приказка: «Те, що ти можеш, не означає, що ти повинен». Більшість зломів залишають сліди, які можна відстежити і вони приведуть до вас.

- **Корпоративні правові питання:** У більшості країн діють закони про кібербезпеку, яких підприємства та організації повинні дотримуватися.

- Міжнародне право з кібербезпеки – сфера, яка постійно розвивається. Кібератаки відбуваються у кіберпросторі, електронному просторі, створеному, обслуговуваному та що належить як державним, так і приватним організаціям. У кіберпросторі немає традиційних географічних кордонів. Щоб ще більше ускладнити проблеми, набагато легше замаскувати джерело атаки в кібервійні, ніж у звичайній війні.

Що ми вивчили у цьому розділі? (прод.)

- Багато професійних IT-організацій, таких як Асоціація безпеки інформаційних систем (ISSA), опублікували кодекси етики, щоб допомогти керувати діями та поведінкою співробітників.
- **Microsoft Technology Associate (MTA) Основи безпеки: ця сертифікація призначена для студентів старших класів і коледжів, а також для тих, хто хоче змінити кар’єру.**
- **Palo Alto Networks Certified Cybersecurity Associate:** Це сертифікація початкового рівня для новачків, які готуються розпочати свою кар’єру у сфері кібербезпеки.
- **ISACA CSX Cybersecurity Fundamentals Certificate:** Ця сертифікація призначена для нещодавніх випускників середньої освіти та тих, хто зацікавлений у зміні професії. Термін дії цього сертифіката не закінчується і не вимагає періодичної повторної сертифікації.

Що ми вивчили у цьому розділі? (прод.)

- **CompTIA Security+:** Це сертифікат безпеки початкового рівня, який відповідає вимогам Директиви Міністерства оборони США 8570.01-M, що є важливим пунктом для тих, хто хоче працювати в галузі IT-безпеки для федерального уряду.

- **EC Council Certified Ethical Hacker (CEH):** Ця сертифікація перевіряє ваше розуміння та знання того, як шукати слабкі місця та вразливості в цільових системах, використовуючи ті ж знання та інструменти, що й зловмисний хакер, але законним і легітимним способом.

- **ISC2 Certified Information Systems Security Professional (CISSP):** Це найбільш впізнаваний і популярний сертифікат безпеки Щоб скласти іспит, необхідно мати принаймні п’ять років досвіду роботи у відповідній галузі.

- **Cisco Certified CyberOps Associate:** Ця сертифікація підтверджує навички, необхідні для аналітиків з кібербезпеки в операційних центрах безпеки.

Що ми вивчили у цьому розділі? (прод.)

- CyberSeek – це інструмент, який надає детальні дані про попит і пропозицію на ринку праці в галузі кібербезпеки, щоб допомогти закрити розрив у навичках із кібербезпеки.