МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
Навчально-науковий інститут захисту інформації

На рецензію
Завідувач кафедри УІКБ
доктор економічних наук, професор
_____ С.В. Легомінова
«___»_____20__ р.

До захисту
Завідувач кафедри УІКБ
доктор економічних наук, професор
_____ С.В. Легомінова
«___»_____20__ р.

ДИПЛОМНА РОБОТА

на тему:

СЕРТИФІКАЦІЙНІ ПРОГРАМИ ДЛЯ ФАХІВЦІВ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ EC-COUNCIL ТА COMPTIA: ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА

СТУДЕНТ: Тищенко Віталій Сергійович _____
(підпис)

КЕРІВНИК: к.держ.упр., доц. Мужанова Тетяна Михайлівна _____
(підпис)

НОРМОКОНТРОЛЕР: к.т.н., доц. Дзюба Тарас Михайлович _____
(підпис)

Київ – 2022

«ЗАТВЕРДЖУЮ»
Завідувач кафедри УІКБ
_____ С.В. Легомінова
«_____»_____ 20__ р.

ЗАВДАННЯ
на дипломну роботу

студенту Тищенку Віталію Сергійовичу

Тема роботи: «СЕРТИФІКАЦІЙНІ ПРОГРАМИ ДЛЯ ФАХІВЦІВ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ EC-COUNCIL ТА COMPTIA: ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА», затверджена наказом по університету № 170 від «11» жовтня 2021 р.

1. **Термін здачі** студентом оформленої роботи «___» _____ 20___ р.
2. **Об'єкт дослідження:** професійна сертифікація у сфері інформаційної безпеки.
3. **Предмет дослідження:** порівняльна характеристика сертифікаційних програм для фахівців з інформаційної безпеки EC-Council та CompTIA.
4. **Мета дослідження** полягає у порівнянні сертифікаційних програм для фахівців з інформаційної безпеки EC-Council та CompTIA.
5. **Перелік питань, які мають бути розроблені:**

5.1 Вивчити основні засади професійної сертифікації у сфері IT та інформаційної безпеки.

5.2 Дослідити сертифікаційні програми для фахівців з інформаційної безпеки від EC-Council.

5.3 Проаналізувати професійні сертифікації CompTIA у сфері інформаційної безпеки, встановити спільні і відмінні риси сертифікацій EC-Council та CompTIA.

6. **Дата видачі завдання** «16» вересня 2021 р.

Науковий керівник _____ Т.М. Мужанова
підпис

Завдання прийнято до виконання _____ В.С. Тищенко
підпис

КАЛЕНДАРНИЙ ПЛАН

виконання дипломної роботи

студентом Тищенком Віталієм Сергійовичем

Дата видачі завдання: «16» вересня 2021 р.

№ з/п	Етапи дипломної роботи	Термін виконання етапів	Примітка
1.	Визначення об’єкта, предмета, мети та завдань дослідження.	16.09.2021	
2.	Збір та аналіз літератури.	28.09.2021	
3.	Вивчення основних засад професійної сертифікації у сфері IT та інформаційної безпеки.	12.10.2021	
4.	Дослідження сертифікаційних програм для фахівців з інформаційної безпеки від EC-Council.	26.10.2021	
5.	Аналіз професійних сертифікацій CompTIA у сфері інформаційної безпеки, порівняння сертифікацій EC-Council та CompTIA.	09.11.2021	
6.	Формулювання висновків до роботи.	23.11.2021	
7.	Оформлення роботи.	07.12.2021	
8.	Оформлення презентації.	14.12.2021	
9.	Отримання рецензії на роботу.	24.12.2021	
10.	Захист у ДЕК.	__.01.2022	

Студент: Тищенко Віталій Сергійович _____

(підпис)

Науковий керівник: Мужанова Тетяна Михайлівна _____

(підпис)

РЕФЕРАТ

Дипломна робота присвячена порівнянню сертифікаційних програм для фахівців з інформаційної безпеки EC-Council та CompTIA. Робота складається зі вступу, трьох розділів, що містять 14 рисунків, висновків та списку використаних джерел з 62 найменувань. Загальний обсяг роботи становить 80 аркушів, 5 з яких займає список використаних джерел.

Об'єктом дослідження є професійна сертифікація у сфері інформаційної безпеки.

Предметом дослідження є порівняльна характеристика сертифікаційних програм для фахівців з інформаційної безпеки EC-Council та CompTIA.

Метою роботи є порівняння сертифікаційних програм для фахівців з інформаційної безпеки EC-Council та CompTIA.

Для цього у роботі використані методи аналізу, класифікацій та порівняння, узагальнення.

Як результат у роботі розглянуто основні засади професійної сертифікації у сфері IT та інформаційної безпеки; досліджено сертифікаційні програми для фахівців з інформаційної безпеки від EC-Council; проаналізовано професійні сертифікації CompTIA у сфері інформаційної безпеки, встановлено спільні і відмінні риси сертифікацій EC-Council та CompTIA.

Галузь застосування. Результати дослідження можуть бути використані на підприємствах та організаціях у процесі формування професійних вимог до фахівців у сфері інформаційної безпеки, критеріїв відбору для кандидатів на зайняття вакантних посад, а також в ознайомчих цілях для студентів та фахівців, які хочуть підвищити рівень професійної кваліфікації.

Ключові слова: ПРОФЕСІЙНА СЕРТИФІКАЦІЯ У СФЕРІ IT ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, СЕРТИФІКАЦІЙНІ ПРОГРАМИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ EC-COUNCIL ТА COMPTIA.

ЗМІСТ

ВСТУП

Актуальність теми Внаслідок швидких темпів розвитку сучасних технологій та виникнення нових викликів для інформаційно-телекомунікаційних систем та інформаційних ресурсів підприємств перед фахівцями з питань інформаційної безпеки постає питання удосконалення власних професійних знань і навичок. Одним із перевірених і найбільш престижних способів підвищення кваліфікації у сфері інформаційної безпеки є незалежні від виробників сертифікаційні програми, зокрема таких авторитетних експертних організацій як EC-Council та CompTIA.

В умовах динамічного розвитку галузей IT та інформаційної безпеки перелік і зміст сертифікаційних програм у цих сферах постійно оновлюються відповідно до новітніх тенденцій. З огляду на це, професіонали з інформаційної безпеки, а також зацікавлені в них роботодавці потребують актуальної інформації про наявні можливості підвищення професійної кваліфікації.

Отже, дослідження й порівняння сертифікаційних програм від відомих експертних організацій EC-Council та CompTIA є актуальним, а використання його результатів сприятиме підвищенню рівня обізнаності роботодавців та фахівців у сфері інформаційної безпеки про актуальні сертифікаційні курси від незалежних галузевих організацій та умови їх проходження.

Мета і завдання дослідження. **Мета** роботи полягає у порівнянні сертифікаційних програм для фахівців з інформаційної безпеки EC-Council та CompTIA.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Вивчити основні засади професійної сертифікації у сфері IT та інформаційної безпеки.

2. Дослідити сертифікаційні програми для фахівців з інформаційної безпеки від EC-Council.

3. Проаналізувати професійні сертифікації CompTIA у сфері інформаційної безпеки, встановити спільні і відмінні риси сертифікацій EC-Council та CompTIA.

Об'єкт дослідження - професійна сертифікація у сфері інформаційної безпеки.

Предмет дослідження – порівняльна характеристика сертифікаційних програм для фахівців з інформаційної безпеки EC-Council та CompTIA.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та порівняння, класифікації, узагальнення.

Наукова новизна одержаних результатів. Представлена у результаті дослідження порівняльна характеристика сертифікаційних програм EC-Council та CompTIA базується на вивченні англомовних ресурсів від розробників зазначених програм і може бути основою при виборі сертифікаційної програми фахівцями з інформаційної безпеки та роботодавцями.

Практичне значення одержаних результатів. Застосування напрацювань дадуть змогу покращити підходи до формування професійних вимог до фахівців та критеріїв відбору для кандидатів на зайняття вакантних посад у сфері інформаційної безпеки на підприємства та в організаціях.

Розділ 1
ОСНОВНІ ЗАСАДИ ПРОФЕСІЙНОЇ СЕРТИФІКАЦІЇ У СФЕРІ ІТ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Організації - розробники сертифікаційних курсів у сфері ІТ та інформаційної безпеки

Професійна сертифікація сьогодні є широко поширеною практикою підтвердження професійних компетенцій фахівця у будь-якій сфері, а також ознакою конкурентної переваги при працевлаштуванні та просуванні кар'єрними сходами. Наявність спеціалізованого сертифікату сьогодні часто є обов'язковою вимогою при прийомі на роботу фахівця з ІТ та інформаційної безпеки.

У сфері інформаційної та кібербезпеки існує багато сертифікаційних програм від різних організацій-розробників, різноманітної спеціалізації та методики підготовки. Загалом програми сертифікації з кібербезпеки розділяють на дві основні категорії:

- професійні програми сертифікації з кібербезпеки;
- академічні програми сертифікації з кібербезпеки.

Професійні сертифікати з кібербезпеки призначені для людей, які вже працюють у сфері кібербезпеки (або тісно пов'язаних галузях ІТ та мереж) і мають намір пройти навчання щодо роботи з найновішими інструментами і програмним забезпеченням для виявлення, запобігання та боротьби з проблемами кібербезпеки. Ці сертифікати використовуються для того, щоб показати знання конкретних технологій. Одним із прикладів такого сертифікату є CompTIA Security Plus, який є професійним сертифікатом з кібербезпеки загального початкового рівня і вимагається для працевлаштування у Департаменті оборони США [1].

Академічні сертифікати з кібербезпеки розроблені, щоб надати здобувачам глибоке знання деяких з поточних проблем у сфері кібербезпеки. Приклади академічних програм сертифікації включають онлайн-сертифікацію з

кібербезпеки в Гарварді або онлайн-сертифікацію студентів з кібербезпеки в Університеті Меріленду. Ці курси зазвичай поєднуються з іншими курсовими та сертифікаційними програмами, щоб надати студентам необхідні навички та досвід для початку роботи в динамічній індустрії кібербезпеки [2].

Предметом нашого дослідження є професійні сертифікати з кібербезпеки. Серед великого різноманіття проесійних сертифікацйних програм є сертифікати, які мають вищий рейтинг визнання і довіри, більш затребувані на ринку інформаційної та кібербезпеки. Це не означає, що немає причин отримувати менш визнані сертифікати. Деякі організації вимагають від своїх співробітників отримати сертифікацію в чомусь, що може бути не таким відомим, як інші сертифікати.

Водночас для професіоналів, які є новачками в цій галузі або просто хочуть володіти статусом, який буде легко визнаний будь-якою компанією, краще отримати сертифікати, які пропонують авторитетні й потужні експертні організації. До таких насамперед відносять такі добре відомі та шановані в сфері кібербезпеки компанії: $(ISC)^2$, ISACA, GIAC, EC-Council, CompTIA. Розглянемо їхні сертифікаційні програми детальніше.

$(ISC)^2$

Міжнародний консорціум сертифікації безпеки інформаційних систем, більш відомий як $(ISC)^2$ є неприбутковою організацією з понад 140 000 сертифікованих членів [3]. $(ISC)^2$, є організацією-розробником дуже популярної у всьому світі сертифікаційної програми CISSP. Усі сертифікаційні курси $(ISC)^2$ показані на рисунку 1.1.

Рис. 1.1. Сертифікаційні програми $(ISC)^2$

Сертифікат CISSP – сертифікований спеціаліст із забезпечення безпеки інформаційних систем є одним із найбільш затребуваних і поважних сертифікатів у світі кібербезпеки. Такий сертифікат, на думку фахівців, має бути у списку тих, хто сподівається досягти успіху в галузі інформаційної та кібербезпеки. CISSP - це не сертифікація для початківців, а для тих, хто вже є досвідченими професіоналами з кібербезпеки. CISSP може допомогти фахівцям, які вже працюють у цій сфері, розвивати свою кар'єру. Як обов'язкова умова CISSP, кандидати повинні мати не менше п'яти років сукупного оплачуваного досвіду повної зайнятості. Цей досвід має охоплювати принаймні дві з восьми областей CISSP Common Body of Knowledge (CBK). Особам із вищою освітою може бути надано звільнення від стажу на один рік, зменшуючи необхідний стаж до чотирьох років [4].

Сертифікат SSCP – сертифікований практик із системної безпеки розрахований на фахівці, яким не вистачає п'ятирічного досвіду, але вони не хочуть відмовлятися від отримання сертифікату $(ISC)^2$. SSCP – це чудова сертифікація для професіоналів, які прагнуть розвивати свою кар'єру. На відміну від CISSP, SSCP вимагає лише мінімум одного року досвіду роботи в одній або кількох із семи областей SSCP CBK. Для фахівців зі ступенем бакалавра або магістра цей один рік досвіду може бути відмінений. Робота з отриманням сертифікації SSCP від $(ISC)^2$ ідеально підходить для професіоналів на будь-якій з таких посад: адміністратор мережевої безпеки, системний адміністратор, аналітик безпеки та адміністратор безпеки [5].

Ще однією сертифікацією $(ISC)^2$, яку варто згадати в першу чергу, є CCSP – сертифікований спеціаліст із хмарної безпеки. CCSP - це всесвітньо визнана сертифікація, яка дає професіоналам можливість продемонструвати свої навички проектування, керування та захисту даних, програм та інфраструктури, розміщених у хмарі. Оскільки все більше і більше організацій переносять всю свою інфраструктуру в хмару, потреба в кваліфікованих спеціалістах із хмарної безпеки продовжує зростати. Подібно до CISSP, CCSP не є сертифікацією для тих, хто тільки починає свою кар'єру, а скоріше для тих, хто вже створив міцний

фундамент у цій галузі. Передумови для CCSP включають п’ять або більше років оплачуваної повної зайнятості у сфері IT. Він також вимагає, щоб принаймні три з цих років проходили в інформаційній безпеці, а один рік - в одному або більше з шести доменів CCSP CBK. Отримання сертифікації CISSP можна замінити всіма іншими вимогами до досвіду [6].

Інші сертифікати $(ISC)^2$ включають: CAP (Сертифікований спеціаліст із авторизації), CSSLP (Сертифікований спеціаліст із безпеки життєвого циклу ПЗ), HCISPP (Спеціаліст з інформаційної безпеки та конфіденційності у сфері охорони здоров’я), CISSP-ISSAP (Професіонал з архітектури безпеки інформаційних систем), CISSP-ISSMP (Професіонал з управління безпекою інформаційних систем).

ISACA

Асоціація аудиту і контролю інформаційних систем (ISACA; англ. Information Systems Audit and Control Association) - міжнародна професійна асоціація, орієнтована на IT-управління. ISACA об'єднує фахівців в області IT-аудиту, IT-консалтингу, управління IT-ризиками та інформаційною безпекою. Основним завданням Асоціації є розробка і формалізація єдиних ефективних підходів до оцінки й управління IT-процесами та IT-системами. Місією асоціації є створювати цінність та довіру до інформаційних систем.

ISACA була зареєстрована в 1969 році невеликою групою людей, які визнали потребу в централізованому джерелі інформації та керівництва у зростаючій сфері контролю аудиту для комп’ютерних систем. Сьогодні Асоціація об'єднує більше 115 000 членів в 180-ти країнах, є співавтором поширеного у всьому світі стандарту з IT-управління CobiT, а також учасником багатьох інших методологічних проектів в галузі IT.

Відділення в Україні наразі об'єднує більше 50 IT-професіоналів, які представляють приватні та державні, місцеві та іноземні організації. Управління асоціацією провадиться незаангажовано по відношенню до будь-яких комерційних інтересів [7].

Найбільш відомими сертифікаційними програмами ISACA є CISA та CISM. Увесь перелік сертифікатів показано на рисунку 1.2.

Сертифікат CISA – сертифікований аудитор інформаційних систем є широко визнаною сертифікацією, яка охоплює контроль, гарантію та безпеку аудиту інформаційної безпеки. Наявність сертифікації CISA доводить, що професіонал здатний і достатньо обізнаний, щоб оцінити вразливі місця, звітувати про проблеми з дотриманням вимог і запровадити контроль безпеки в організації [8].

Рис. 1.2. Сертифікаційні курси ISACA

На сходинку вище CISA є статус CISM - сертифікований менеджер інформаційної безпеки. Ця сертифікація призначена для тих, хто хоче продемонструвати свої знання з управління інформаційною безпекою. Незалежні дослідження визначили CISM як одну з найбільш високооплачуваних і затребуваних IT-сертифікацій. Оскільки це сертифікація, орієнтована на управління, ті, хто хоче її отримати, повинні мати практичний досвід управління, проектування та нагляду за програмою інформаційної безпеки підприємства [9].

Інші сертифікати ISACA у сфері інформаційної безпеки включають: CGEIT (Сертифікат з управління IT підприємства), CRISC (Сертифікат у сфері

управління ризиками та інформаційними системами), CDPSE (Сертифікат інженера із забезпечення конфіденційності даних).

GIAC

GIAC - Global Information Assurance Certification - це організація, заснована в 1999 році для підтвердження навичок фахівців із інформаційної безпеки. Сертифікату GIAC довіряють тисячі компаній і державних установ, включаючи Агентство національної безпеки США. Сертифікати GIAC засновані на освітніх методиках відомого у сфері навчання з інформаційної та кібербезпеки американського інституту SANS [10]. GIAC пропонує багато різних сертифікатів у таких категоріях як кіберзахист, тестування на проникнення, реагування на інциденти, криміналістична експертиза та інших (Рис. 1.3).

Рис. 1.3. Сертифікаційні курси GIAC

Розглянемо детальніше найбільш популярні із сертифікацій GIAC.

GSEC – основи безпеки GIAC, є одним із найбільших сертифікатів початкового рівня, які пропонує GIAC. Цей сертифікат підтверджує, що знання спеціаліста з інформаційної безпеки виходять за рамки простого знання термінології та концепцій. Метою GSEC є підтвердження практичних знань фахівця. Немає перерахованих передумов для GSEC, але ті, хто бажає скласти іспит, повинні мати робочі знання з безпеки IT та мереж [11].

GMOB – аналітик безпеки мобільних пристроїв GIAC, є одним із найцікавіших сертифікатів, які пропонує GIAC, оскільки він дозволяє професіоналам проявити свої здібності у сфері безпеки мобільних пристроїв. Мобільні пристрої є основною частиною особистого та професійного життя кожного. Важливо мати кваліфікованих людей для захисту цих пристроїв, які з'єднують нас разом. Сертифікація GMOB підтверджує, що власники сертифікату продемонстрували знання щодо оцінки та керування безпекою мобільних пристроїв і програм [12].

GCFA – GIAC Certified Forensic Analyst Professionals, для фахівців які зацікавлені в кар'єрі судового аналітика, безумовно, виграють від отримання сертифікації GCFA. GCFA — це широко визнана сертифікація судового аналітика, яка охоплює широкий спектр криміналістичних тем, таких як розширене реагування на інциденти та цифрова криміналістична експертиза, криміналістична експертиза пам'яті, аналіз хронології, виявлення антикриміналістів, пошук загроз та реагування на інциденти вторгнення APT (пакетних менеджерів) [13].

Інші відомі сертифікати GIAC у сфері інформаційної безпеки включають (але не обмежуються): GCIH (Сертифікований оператор інцидентів), GPEN (Сертифікований тестувальник на проникнення), GCIA (Сертифікований аналітик взлому), GCFE (Сертифікований комп'ютерний криміналіст), GNFA (Сертифікований мережевий криміналіст-аналітик).

Сертифікаційні програми від EC-Council, CompTIA є предметом нашого подальшого дослідження.

1.2 Типові етапи процесу професійної сертифікації на прикладі EC-Council та CompTIA

Огляд послідовності й змісту дій для проходження сертифікаційних програм від провідних організацій-надавачів послуг професійної сертифікації показав, що процес сертифікації відбувається у відповідності до переліку типових кроків, яким має слідувати здобувач для отримання бажаного сертифікату. Розглянемо їх детальніше на прикладі EC-Council та CompTIA.

EC-Council

EC-Council пропонує здобувачу здійснити такі кроки для отримання сертифікату:

1. Вибір шляху до іспиту.
2. Навчання для сертифікаційного іспиту
3. Реєстрація на сертифікаційний іспит
4. Складання іспиту
5. Підтримка актуальності сертифікату та його поновлення

Крок 1

Перший крок передбачає, що учасник має визначити для себе метод, який буде використовувати для отримання сертифікату. EC-Council пропонує два шляхи відповідно до кожної сертифікації, а саме: пройти офіційний тренінг або подати і отримати схвалення заявки на іспит без нього. Перший варіант підходить для всіх кандидатів, як нових, так і тих, хто поновлює свою сертифікацію, оскільки курс сертифікації оновлюється раз в декілька років. У разі, якщо кандидат обирає другий варіант, тоді потрібно мати сертифікат версії від першої до останньої або досвід роботи мінімум два роки в сфері інформаційної безпеки.

Крок 2

Другий крок передбачає, що незалежно від наявності знань кандидат має ознайомитись зі змістом навчальної програми для того, щоб розібратися, з якими модулями виникають питання або невпевненість щодо їх 100% знання. Для цього

учасник має завантажити план іспиту за обраним курсом, ознайомитися з його цілями, зосередити своє навчання на розділах, в яких виникають питання, потренуватися на практичних іспитах, щоб імітувати середовище тестування.

Крок 3

Проходячи третій крок, кандидат реєструється на іспит для його подальшого складання. Кандидату потрібно зареєструватися не менш ніж за 3 дні до бажаної дати іспиту. Існує два варіанти реєстрації для складання іспиту:

1. Реєстрація для складання іспиту в центрі офлайн тестування через Pearson VUE.

2. Реєстрація на іспит дистанційно через платформу ProctorU, яка забезпечує віддалений нагляд і захист цілісності для тестування й оцінювання онлайн.

Незалежно від того, який варіант буде обрано, учасник проходить іспит за особистої присутності або дистанційно. Важливим при виборі дистанційного проходження іспиту є пам’ятати, що для цього потрібно скласти тест на знання засад роботи на обладнанні.

Крок 4

Четвертий крок передбачає складання іспиту. На цьому етапі все залежить від учасника та його підготовки до іспиту. Важливими рекомендаціями, які дають EC-Council є такі: мати гарний настрій, бути зосередженим, розпланувати свій графік так, щоб нічого не відволікало від іспиту, налаштуватися на позитивний результат випробування.

Крок 5

Останній крок встановлює план дій для поновлення наявного сертифікату. Для цього необхідно здійснити такі кроки:

- створити обліковий запис на сайті EC-Council;
- перейти на сторінку безперервної освіти;
- сплатити річну плату (за потреби);
- подати інформацію про зароблені кредити через сайт.

Кредити безперервної освіти.

Отримавши сертифікацію EC-Council, фахівець повинен почати процес збереження своїх облікових даних, для того щоб не довелося знову складати іспит. Програма безперервної освіти (ECE) вимагає від кандидатів подавати 120 кредитів кожні три роки, щоб зберегти свою сертифікацію, усі подані заходи мають бути пов'язані з IT-безпекою [14].

У таблиці показано види діяльності та їх цінність в кредитних балах програми ECE:

Таблиця 1.1.

Види діяльності для отримання кредитів безперервної освіти

Діяльність	Кількість зароблених кредитів
Волонтерство в державному секторі	1 кредит на годину
Засідання глав асоціації/організації (за кожну зустріч)	1 кредит на годину
Авторство статті/розділу книги	20 кредитів
Авторський курс/модуль	40 кредитів
Авторський інструмент	40 кредитів
Авторська книга	100 кредитів
Внесок у розвиток іспиту	від 40 – 100 кредитів
Сертифікація/Іспит	40 кредитів
Іспит EC-Council	120 кредитів
Опитування EC-Council	20 кредитів
Освітній курс	1 кредит на годину
Освітній семінар/конференція/захід	1 кредит на годину
Вища освіта	15 кредитів за годину семестру
Визначити нову вразливість	10 кредитів
Презентація	3 кредити на годину
Читання книги з ІБ, огляд статей або книги, вивчення прикладу	5 кредитів
Вивчати нове	21 кредит на день
Вдосконалення навчання	11 кредитів на день
Приймати участь в наглядовій раді	80 кредитів

CompTIA

На відміну від EC-Council CompTIA пропонує чотири кроки проходження сертифікації:

1. Вибір сертифікаційної програми
2. Ознайомлення з обраною сертифікацією
3. Навчання і підготовка до іспиту
4. Реєстрація та складання іспиту

Крок 1

На цьому етапі учаснику пропонується дослідити наявні IT-сертифікати, які відповідають інтересам і допоможуть досягти кар'єрних цілей. Для того, щоб дізнатися про різні варіанти розвитку кар'єри в IT та обсяги оплати праці у сфері IT і таким чином вирішити, яка IT-сертифікація найкраща учасникам рекомендовано використовувати CompTIA Career Pathway та CompTIA Career Roadmap.

Так, кар'єрний шлях у сфері кібербезпеки передбачає проходження такої послідовності сертифікаційних програм CompTIA: 1. Основи IT - IT Fundamentals (ITF+); 2. IT для початківців - CompTIA A+; 3. Мережі - CompTIA Network+; 4. IT-безпека - CompTIA Security+; 5. Тестування вразливостей - CompTIA PenTest+; 6. Аналітика кібербезпеки - CySA+; 7. Просунутий професіонал з кібербезпеки - CompTIA CASP+ (Рис. 1.4).

Рис. 1.4. Послідовність сертифікацій для розвитку кар'єри у сфері кібербезпеки

IT-сертифікації CompTIA охоплюють від початкових знань комп'ютерного обладнання та комп'ютерного програмного забезпечення до передових навичок в галузі IT-безпеки, кібербезпеки, IT-мереж і хмарних обчислень.

Крок 2

Перш ніж почати підготовку до отримання IT-сертифікації, учасник має переконатися, що розуміє загальну картину того, що є на іспиті. Для цього необхідно завантажити й ознайомитися із цілями іспиту, практикуватися з тестовими запитаннями, щоб побачити обсяг очікуваних знань і навичок, типи запитань тощо. Вивчення запитань для практичних тестів дадуть кандидату гарне уявлення про те, чого очікувати на сертифікаційного іспиту.

Здобувачу своїх сертифікатів CompTIA настійливо рекомендує переглянути онлайн-спільноти на Facebook, LinkedIn та Reddit, щоб дізнатися, що інші говорять про іспити CompTIA.

Крок 3

CompTIA пропонує безліч варіантів сертифікаційного навчання, які розроблені для підготовки здобувача до сертифікаційного іспиту CompTIA. Так, кандидат може обрати традиційні навчальні посібники та книги, онлайн-навчання, інтерактивні лабораторії, онлайн-підготовку до іспиту та відео-навчання, щоб створити необхідний індивідуальний навчальний досвід.

Якщо кандидат надає перевагу навчальній програмі під керівництвом інструктора, а не самостійному навчанню, також є можливість знайти варіанти навчання в аудиторії.

Крок 4

Коли учасник впевнений в своїх знаннях, необхідних для сертифікації, настає час скласти іспит. Спочатку потрібно придбати ваучер на іспит, потім знайти центр тестування Pearson VUE поблизу і зареєструватися на іспит.

Учасник може пройти іспит онлайн або за особистої присутності у центрі тестування.

Онлайн-тестування дає учаснику можливість пройти сертифікаційний іспит з такими перевагами:

- безпечний і простий спосіб тестування з дому, в закритому офісі або будь-якому місці, де є доступна приватна зона;
- гнучкість планування іспиту на будь-який зручний час;
- технічна підтримка, якщо під час екзаменаційної сесії виникнуть проблеми.

Для проходження онлайн-тестування учаснику необїхідно забезпечити наявність тихого, закритого, приватного місця, використання надійного пристрою, що відповідає системним вимогам і має веб-камеру; надійне стабільне інтернет-з'єднання з мінімальною швидкістю 1 Мбіт/с.

Персональне тестування CompTIA за умови особистої присутності надає кандидату варіанти тестування в будь-якому з тисяч тестових центрів Pearson VUE, розташованих по всьому світу.

Учаснику рекомендують обрати тестування у тестовому центрі за умови відсутності тихого приватного місця для проходження спиту, надійного доступу до Інтернету, а також, якщо учасник має обмежене розуміння письмової та усної англійської мови чи наявні інші мовні бар'єри [15].

Як і в розглянутому вище порядку отримання професійних сертифікатів від EC-Council CompTIA вимагає від власників сертифікатів брати участь у програмі безперервної освіти, щоб поновити наявну сертифікацію. Наприклад, сертифікованому фахівцю Security+ необхідно зібрати принаймні 50 одиниць безперервної освіти протягом 3-х років, після чого сертифікат автоматично поновлюється. Способи отримання таких одиниць є подібними до тих, які встановлені в EC-Council.

Таким чином, за результатами дослідження порядку отримання сертифікату від EC-Council та CompTIA, а також огляду послідовності й змісту дій для проходження сертифікаційних програм від інших провідних організацій-надавачів послуг професійної сертифікації виділено такі типові етапи сертифікації (Рис. 1.5).

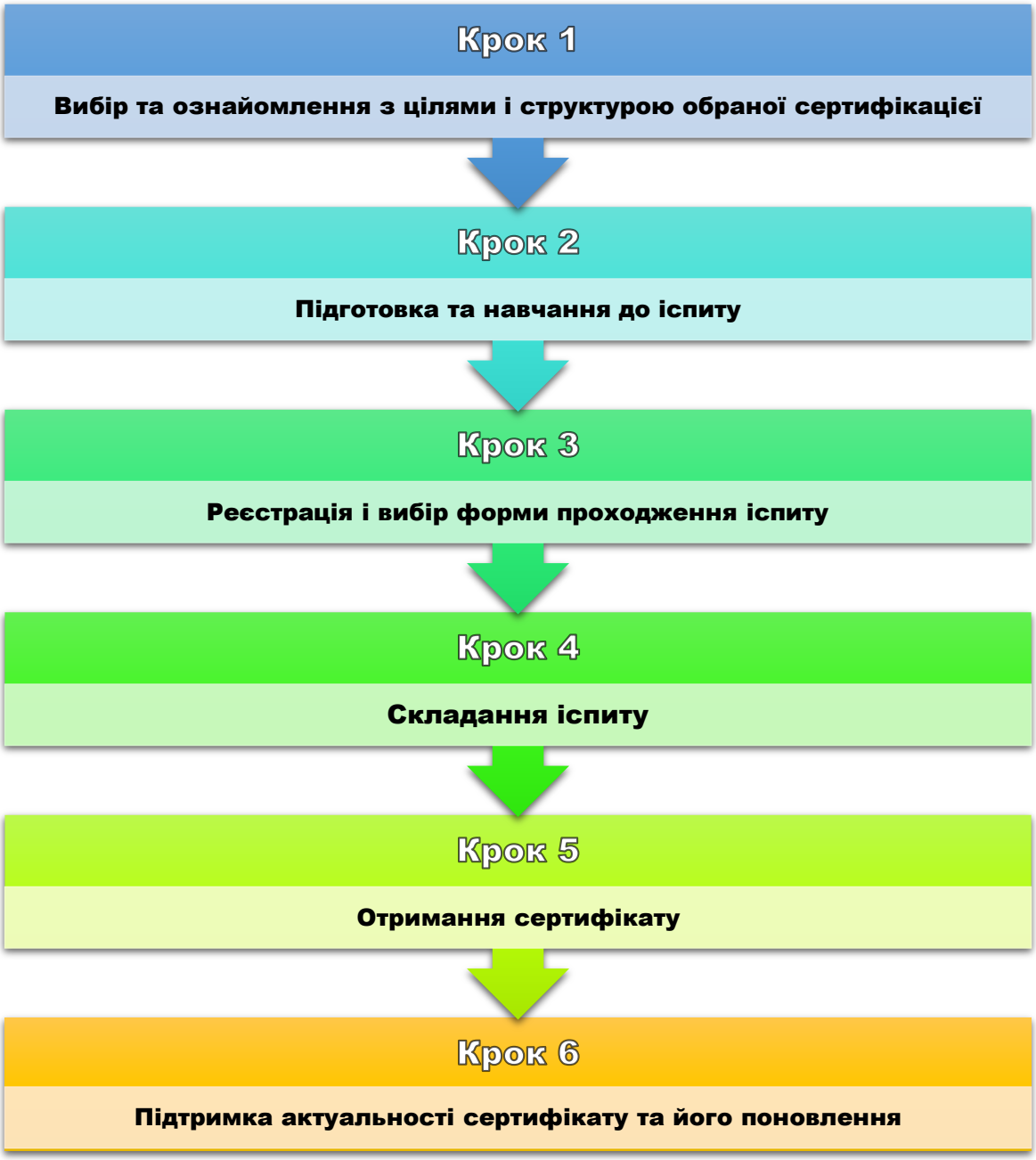

Рис. 1.5. Типові етапи проходження сертифікаційних програм

Підсумовуючи, варто відзначити, що зазначена послідовність етапів з невеликими відхиленнями є характерною для більшості сертифікаційних програм від різних розробників. Деякі експертні організації, що проводять професійну сертифікацію фахівців у сфері інформаційної безпеки, наприклад, ISACA, одним з етапів отримання сертифікату визначають етап отримання членства в організації. Однак такий крок не є обов'язковим, а скоріше є чинником зменшення витрат на сертифікацію, оскільки для членів організації нижчою є вартість іспитів, навчальних матеріалів тощо.

1.3 Центр тестування Pearson VUE як база професійної сертифікації з інформаційної безпеки

Як відзначалося вище, типовими способами проходження кваліфікаційного іспиту для отримання сертифікату у сфері IT та інформаційної безпеки є тестування онлайн або в авторизованих організаціями-розробниками сертифікаційних курсів навчальних центрах.

Одним із найбільш потужним з них є Pearson VUE (Virtual University Enterprises), який є світовим лідером у проведенні сертифікованого електронного тестування з представництвом в більш ніж 175 країнах. Щорічно у його авторизованих центрах близько 14 млн людей перевіряють рівень своїх знань.

Pearson VUE розробляє систему електронного тестування та проводить сертифікацію спеціалістів за допомогою найбільшої, ультрасучасної, забезпеченої багаторівневою системою захисту, мережі в більш ніж п’яти тисячах тестових центрів по всьому світу. Pearson VUE працює з державними підприємствами та навчальними організаціями, IT-компаніями та спільнотами, серед яких: Cisco, Oracle, Microsoft, Apple, Symantec, Novell, Intel, Citrix, IBM [16].

Авторизований центр тестування VUE, відкритий на базі IT Education Academy з 2014 року, пропонує послуги з організації тестування на знання програмних продуктів і устаткування світових лідерів у сфері IT-технологій [17].

Центр тестування Pearson Vue - автоматизоване складання іспитів і сертифікація від компаній, які розробляють і передають свої тести в міжнародну мережу тестових центрів. Центр забезпечує необхідні умови для проведення надійного, якісного та справедливого для всіх електронного тестування.

Переваги сертифікації для фахівця:

- сертифікат визнається майже у всіх країнах світу;
- роботодавці прагнуть наймати сертифікованих фахівців;
- можливість претендувати на вищий рівень заробітної плати;
- сертифікація – система незалежної оцінки кваліфікації IT-спеціаліста.

Переваги сертифікації для компанії:

- висока кваліфікація працівника – основа успішного розвитку компанії;
- основа репутації бізнесу – якість послуг, що надаються;
- сертифікація фахівців зміцнює позиції компанії на ринку;
- сприяє збільшенню прибутку.

Які вендори дають можливість отримати сертифікат?

Центр тестування Pearson Vue має можливість проводити тестування і сертифікацію студентів з будь-якого продукту провідних вендорів IT-ринку, а це близько 100 компаній, серед яких: Microsoft, Cisco Systems, Adobe Systems, Oracle, Zend Technologies, Citrix, Hewlett Packard, IBM.

Реєстрація в Pearson VUE

Щоб зареєструватися в системі Pearson VUE, необхідно:

1. Зайти на офіційний сайт www.pearsonvue.com.
2. Вибрати вкладку «For Test Takers» https://home.pearsonvue.com/test-taker.aspx.
3. Обрати необхідного вендора.
4. Перейти за посиланням «Create Account», ввести необхідні дані.

Інструкція внесення даних:

1. Поля First Name/Given Name і Last Name/Surname/Family Name необхідно заповнювати латинськими літерами відповідно до правильної транслітерації імені та прізвища.
2. Ввести адресу і телефон. Відповісти на додаткові питання.
3. Після успішного закінчення реєстрації на вказану поштову скриньку прийде повідомлення з тимчасовим паролем. При першій реєстрації в системі буде затребувана зміна пароля.
4. Після реєстрації на сайті Pearson VUE вибрати необхідний іспит і зробити його оплату. Аби призначити екзамен в персональному розділі, оберіть пункт меню «Schedule Exams».
5. Вибрати мову іспиту, натиснути «Next».

6. Обрати зі списку найближчий сертифікаційний центр. Натиснути «Next». Далі календарі вибрати дату і час іспиту, підтверджуючи по черзі спочатку дату, потім час, кнопкою «Select Appointment».

7. Прийняти умови угоди про «Сертифікації та конфіденційності». Перевірити отриману інформацію про вибраний іспит (*код іспиту, сертифікаційний центр, дата і час*), ввести код ваучера на знижку (якщо такий є) і перейти до оплати іспиту.

8. Оплачувати іспит можна міжнародними пластиковими картами American Express, JCB, MasterCard і VISA.

9. У підтвердження реєстрації на ваш email прийде лист «Order Confirmation».

Загалом, в Україні працює 19 авторизованих центрів тестування, що знаходяться в найбільших містах країни:

- Київ: CyberBionic Systematics; Ukraine Supreme Legal Council; Фаст Лейн; IT Distribution LLC; IT Education Academy; S&T Ukraine; SI BIS LLC; Sitronics Telecom Solutions Ukraine; Smart Business; Державний університет телекомунікацій; Віадук-Телеком; БМС Консалтинг;
- Харків: Квантор V; Комп'ютерна академія «Шаг»; Харківський національний університет радіоелектроніки;
- Дніпро: Комп'ютерна академія «Шаг»; SoftServe University;
- Львів: SoftServe University;
- Миколаїв: Комп'ютерна академія «Шаг»;
- Тернопіль: Тернопільський національний технічний університет ім. Івана Пулюя.

Таким чином, фахівці з інформаційної безпеки мають можливість скласти іспити для отримання професійного сертифіката як віддалено, так і очно на базі близько 20-ти авторизованих центрів тестування у найбільших містах України.

Висновки до розділу 1

Основними організаціями які займаються сертифікацією фахівців з інформаційної безпеки є такі як: ISACA, GIAC, EC-Council, (ISC)², CompTIA. Важливими є сертифікати з тесту на проникнення, аналітика безпеки, цифрового криміналіста, менеджер інформаційної безпеки, аудитор інформаційних систем.

Процес сертифікації в організаціях Comptia та EC-Council мають незначні відмінності, в EC-Council безперервна освіта є обов'язковим кроком (пунктом) для отримання сертифікації, comptia в свою чергу не приділяє цьому питанню такої великої уваги та потреби, але це не означає що повторне підтвердження сертифікату не є обов'язковим. Фахівці або кандидати можуть складати іспит як на офіційному сайті обраної сертифікації, або ж через спеціалізовані центри освіти.

Встановлено що у провідних організаціях CompTIA, EC-Council, ISACA, GIAC, (ISC)² проходить за такими типовими етапами: Вибір та ознайомлення з цілями та структурою обраної сертифікаціЄї, Підготовка та навчання до іспиту, Реєстрація і вибір форми проходження іспиту, Складання іспиту, Отримання сертифікату, Підтримка актуальності сертифікату та його поновлення.

Pearson VUE займає велику частку цього процесу, адже центр забезпечує необхідні умови для проведення надійного, якісного та справедливого для всіх електронного тестування. Описано переваги сертифікації для фахівців та компаній. В Україні працює 19 авторизованих центрів.

Розділ 2.
СЕРТИФІКАЦІЙНІ ПРОГРАМИ ДЛЯ ФАХІВЦІВ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ВІД EC-COUNCIL

2.1 Напрями діяльності й категорії професійної сертифікації EC-Council

Міжнародна рада консультантів з питань електронної комерції (International Council of Electronic Commerce Consultants - EC-Council) - це американська неурядова організація, яка була створена у 2001 році після сумнозвісних атак 11 вересня для того, щоб надавати послуги із сертифікації та навчання в галузі електронного бізнесу та кібербезпеки [18].

EC-Council, офіційно зареєстрована як Міжнародна рада консультантів з електронної комерції, була утворена для створення навчальних та сертифікаційних програм з інформаційної безпеки, щоб допомогти тій спільноті, на яку покладається наша пов'язана економіка, щоб врятувати їх від руйнівної кібератаки. EC-Council швидко заручилася підтримкою провідних дослідників та експертів з усього світу та розпочала свою першу програму інформаційної безпеки, сертифікованого етичного хакера.

Разом з цією постійно зростаючою командою експертів з питань тематики та дослідників InfoSec EC-Council продовжувала створювати різні стандарти, сертифікати та навчальні програми в галузі електронної комерції та інформаційної безпеки.

Міжнародна рада консультантів з електронної комерції, також відома як EC-Council, є найбільшим у світі органом з технічної сертифікації кібербезпеки. Працює у 145 країнах по всьому світу, і є власником та розробником всесвітньо відомого сертифікованого етичного хакера (CEH), експерта з кримінальної експертизи комп'ютерного злому (CHFI), сертифікованого аналітика безпеки (ECSA), ліцензованого тестування на проникнення, серед інших.

EC-Council навчила та сертифікувала понад 200 тисяч фахівців з інформаційної безпеки у всьому світі, які вплинули на мислення кібербезпеки незліченних організацій у всьому світі.

Програми сертифікації визнані у всьому світі та отримали схвалення від різних урядових установ, включаючи Федеральний уряд США через законопроект Post-9/11 GI Bill «Про пільги для Ветеранів після 11 вересня», а також Агентство національної безпеки США (АНБ) та Комітет з систем національної безпеки (CNSS), що засвідчує сертифіковану етичну етику EC-Council [19].

Міжнародна рада консультантів з питань електронної комерції (EC-Council) - це організація, що базується на її членстві, яка сертифікує окремих людей у різних галузях електронного бізнесу та інформаційної безпеки.

Організація є власником і розробником всесвітньо відомої програми сертифікованого етичного хакера (Certified Ethical Hacker - CEH) і ще 19-ти курсів за 6-ма категоріями:

1. Базовий рівень, в т.ч. сертифікований спеціаліст з безпеки – ECSS, сертифікований спеціаліст з криптографії – ECES;

2. Основи, серед яких CEH, CEH (Master), сертифікований фахівець із безпеки мереж - CND;

3. Просунутий рівень, зокрема сертифікований тестувальник на проникнення – CPENT, сертифікований аналітик операційного центру безпеки – CSA;

4. Спеціаліст: сертифікований спеціаліст з обробки інцидентів – ECIH, сертифікований спеціаліст із розслідувань інцидентів комп’ютерної безпеки - CHFI;

5. Управління - сертифікований директор з інформаційної безпеки – CCISO; Обізнаність з безпеки - сертифікований безпечний користувач ПК – CSCU.

На рисунку 2.1 структуровано курси програм EC-Council за рівнем їх складності та відповідністю категоріям інформаційної безпеки.

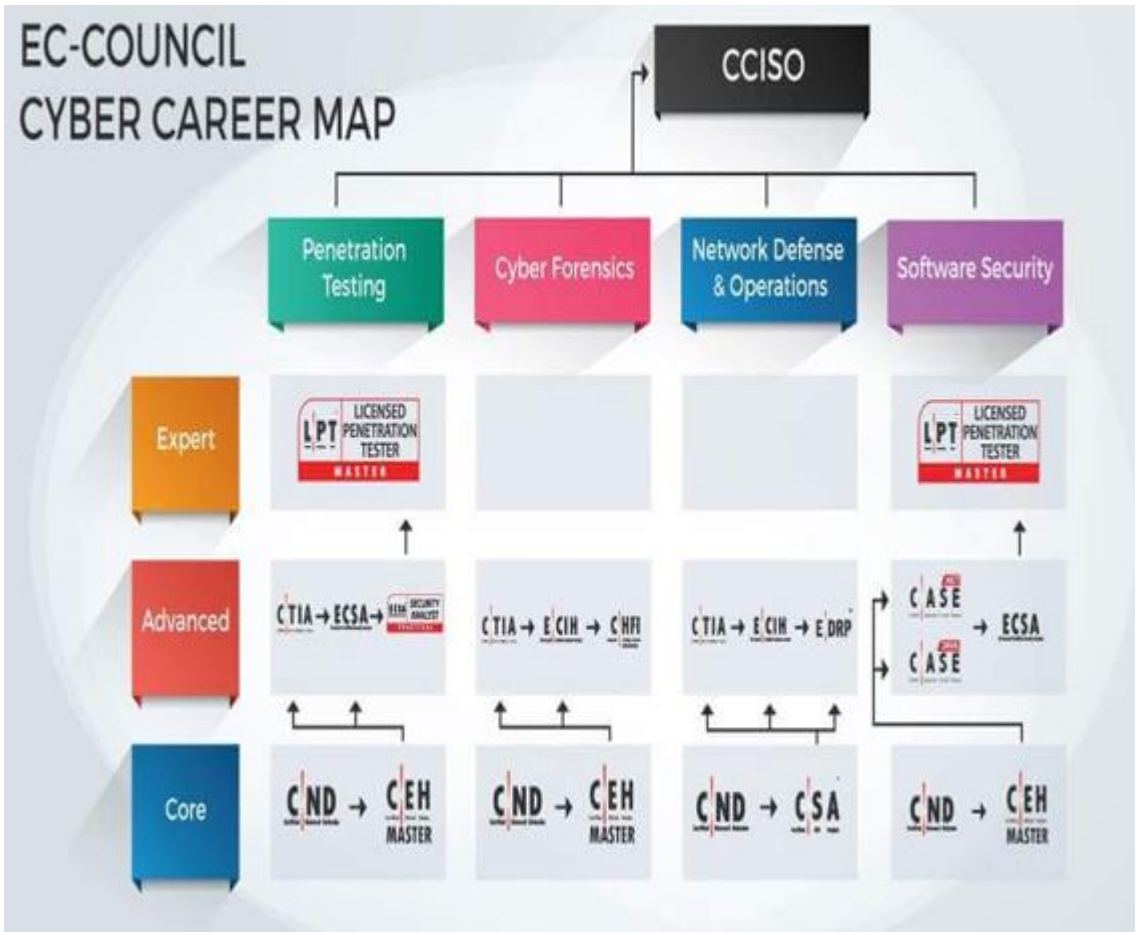

Рис. 2.1. Перелік сертифікаційних програм EC-Council

Усі іспити EC-Council доступні в Центрі іспитів ECC за посиланням www.eccexam.com (крім всіх тестів на основі ефективності). Кандидати можуть знайти авторизовані центри тестування EC-council, щоб запланувати свої іспити або вибрати, щоб скласти іспити віртуально за допомогою служб дистанційного контролю (RPS) EC-Council. Іспит CEH (312-50) також доступний у центрах тестування Pearson Vue. Іспити CEH (Практичний), ECSA (практичний) та CPENT доступні лише через портал Аспен Ec-Council.

Варто зазначити, що EC-Council складається з кількох організацій, які допомагають досягти тієї ж мети, яка полягає у створенні кращого та безпечнішого кіберсвіту за допомогою інформування та освіти, серед яких:

- власне Міжнародна рада консультантів з електронної комерції (EC-Council);
- підрозділ, відповідальний за навчання і сертифікацію (EC-Council Training & Certification);

- підрозділ корпоративного консультування й дорадчих послуг (EC-Council Global Services);
- підрозділ з організації академічної освіти (EC-Council University);
- підрозділ з організації глобальних заходів (EC-Council Global Services);
- неприбуткова організація EC-Council Foundation) (Рис. 2.2).

Рис. 2.2. Структура EC-Council

EC-Council створює контент (матеріали курсів та іспитів) та проводить сертифікацію через власний канал авторизованих навчальних центрів, який складається з понад 700 партнерів, які представляють понад 2000 фізичних місць у більш ніж 145 країнах по всьому світу [20].

Програми сертифікації EC-Council визнані в усьому світі і отримали схвалення від різних державних установ, включаючи Федеральний уряд США, Агентство національної безпеки (АНБ) і Комітет систем національної безпеки (CNSS). EC-Council отримала акредитацію від Американського національного інституту стандартів (ANSI) для сертифікаційних програм CEH, CCISO, CHFI та CND.

Підрозділ навчання і сертифікації ECC забезпечує функціонування iClass, який є прямою навчальною програмою для сертифікації EC-Council. iClass надає курси сертифікації за допомогою різних методологій навчання: під керівництвом інструктора в клієнтських закладах, синхронної доставки в прямому ефірі, під керівництвом інструктора онлайн та асинхронно через нашу платформу

потокового відео. Відео курсів iClass також можна завантажити на мобільний пристрій, наприклад iPad, і відправити на місце розташування клієнта.

Університет EC-Council, який акредитований Комісією з акредитації дистанційної освіти США, пропонує такі програми як бакалавр із кібербезпеки, магістр із кібербезпеки та програму випуску сертифікатів.

Робота підрозділу EGS спрямована на те, щоб допомогти організаціям зрозуміти та ефективно керувати своєю позицією щодо ризиків у сфері кібербезпеки. EGS спеціалізується на допомозі клієнтам приймати зважені бізнес-рішення для захисту своїх організацій. EGS має понад 20 спеціалізованих сфер кібербезпеки, про які інформують найкращі фахівці з кібербезпеки, кожен з яких присвятив своє життя захисту організацій від кібератак.

Група конференцій та заходів EC-Council відповідає за планування, організацію та проведення конференцій по всьому світу. TakeDownCon і Hacker Halted — це конференції з IT-безпеки, які збирають всесвітньо відомих доповідачів для виступів, панелей, дебатів і секційних сесій. Конференції проводилися в Далласі, Лас-Вегасі, Сент-Луїсі, Хантсвіллі, Меріленді, Коннектикуті, Міртл-Біч, Маямі, Атланті, Ісландії, Гонконгу, Єгипті, Сінгапурі, Мумбаї, Дубаї, Бахрейні, Лондоні, Абу-Дабі та Куала-Лумпурі. Інші заходи включають саміти CISO, глобальні форуми CISO та коктейльні прийоми для керівників, на яких EC-Council залучає доповідачів та контент до професіоналів з IT-безпеки керівного рівня.

Змагання Global Cyberlympics – це змагання типу «захоплення прапора», в яких беруть участь приблизно 1000 учасників з усього світу. EC-Council об’єднує хакерів онлайн для попередніх раундів на вибування, а потім збирає дві найкращі команди (6-8 гравців на команду) з кожного регіону для участі в остаточному змаганні один до одного [21].

2.2 Сертифікований етичний хакер (CEH)

Опис сертифікаційної програми

Сертифікований етичний хакер (CEH) – це кваліфікація, отримана шляхом демонстрації знань щодо оцінки безпеки комп'ютерних систем шляхом пошуку слабких місць та вразливих місць у цільових системах, з використанням тих самих знань та інструментів, що і зловмисний хакер, але законним та законним чином для оцінки положення безпеки цільова система.

Ці знання оцінюються, відповідаючи на запитання з кількома варіантами вибору щодо різних технік та інструментів етичного злому. Код іспиту CEH-312-50. Ця сертифікація тепер стала базовою з переходом до CEH (Практична), запущеної у березні 2018 р. Перевірка навичок тестування на проникнення у лабораторному середовищі, де кандидат повинен продемонструвати вміння застосовувати методи та використовувати інструменти тестування на проникнення для досягнення мети різними методами модельованої системи у віртуальному середовищі [22].

Етичні хакери використовуються організаціями для проникнення в мережі та комп'ютерні системи з метою виявлення та усунення вразливостей безпеки.

CEH зосереджується на останніх атаках шкідливого програмного забезпечення, новітніх інструментах злому та нових векторах атак у кіберпросторі. Включає в себе хакерські проблеми в кінці кожного модуля і будується на 100% відповідності до NICE 2.0 Framework, щоб забезпечити систематичне зіставлення ролей вакансій.

EC-council критикували за випадки неетичної поведінки, і багато фахівців з кібербезпеки описували її як паперову фабрику. В основному це пов'язано з відсутністю спеціалізованих знань або навичок у сертифікатах.

Вимоги до здобувача сертифікату

Сертифікація досягається шляхом складання іспиту CEH після проходження навчання в Акредитованому навчальному центрі (ATC) або проходження через навчальний портал EC-Council iClass. Якщо кандидат вибирає самостійне

навчання, необхідно заповнити заявку та подати підтвердження двох років відповідного досвіду роботи в сфері інформаційної безпеки. Ті, хто не має необхідних двох років досвіду роботи, пов'язаної з інформаційною безпекою, можуть подати запит про освіту [23].

Цільова аудиторія курсу

Ця сертифікаційна програма підходить для таких спеціальностей та для тих, хто хоче отримати бажану посаду:

- Аналітик / адміністратор інформаційної безпеки
- Офіцер безпеки з питань забезпечення інформації (ІА)
- Менеджер з інформаційної безпеки / спеціаліст
- Інженер з безпеки інформаційних систем / менеджер
- Фахівець / офіцер з питань інформаційної безпеки
- Аудитор з інформаційної безпеки / ІТ
- Аналітик ризиків / загроз / вразливостей
- Системний адміністратор
- Адміністратор та інженер мережі
- Аудитор безпеки середнього рівня
- Молодший тестувальник на проникнення
- Архітектор рішень
- Адміністратор безпеки ІТ
- Аналітик з кіберзахисту
- Аналітик з оцінки вразливостей
- Аналітик запобігання
- Адміністратор безпеки InfoSec

Структура курсу

Курс складається з 20 модулів серед яких: вступ до етичного хакерства; методи пошуку та спостереження; сканування мереж; реєстрація; аналіз вразливостей; злом системи; загрози зловмисного програмного забезпечення; моніторинг трафіку (сніффінг); соціальна інженерія; відмова в обслуговуванні; викрадення сеансу; обхід брандмауерів; злом веб-серверів; злом веб-додатків;

SQL ін’єкція; злом бездротових мереж; злом мобільних платформ; злом IoT (інтернет речей); хмарні обчислення; криптографія (Рис. 2.1).

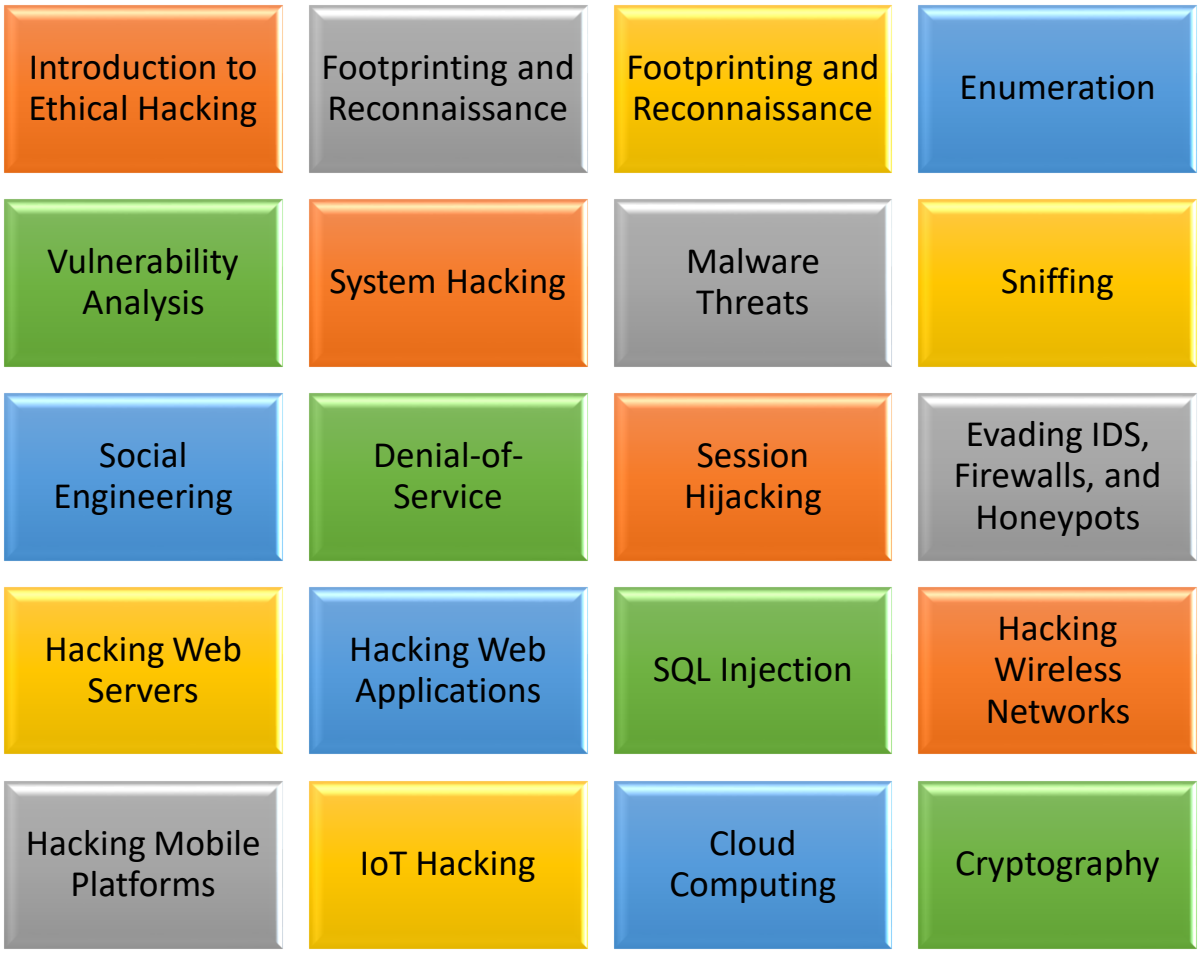

Рис. 2.3. Структура курсу CEH

Останнє оновлення курсу

CEH v11 продовжує впроваджувати новітні методи злому та найсучасніші інструменти та експлойти, які використовуються хакерами та фахівцями з інформаційної безпеки сьогодні

У своїй 11-й версії CEH продовжує розвиватися з використанням найновіших операційних систем, інструментів, тактики, експлойтів та технологій. Нижче наведено кілька критичних оновлень CEH v11: Включення ОС Parrot Security. У порівнянні з Kali Linux, ОС Parrot Security пропонує кращу продуктивність на ноутбуках та машинах з меншою потужністю, одночасно пропонуючи інтуїтивно зрозумілий вигляд із більшим сховищем загальних інструментів. Повторно відображений у NIST/NICE Framework CEH v11

ретельно відображається на важливі спеціальні сфери в рамках категорії ролей вакансій «Захист та охорона» (PR) у рамках NIST/NICE, що перекривається з іншими ролями, включаючи Аналіз (AN) та Безпечне забезпечення (SP). Покращена хмарна безпека, модулі IoT та OT CEH v11 охоплює оновлені модулі Cloud та IoT для включення контейнерних технологій CSP (наприклад, Docker, Kubernetes), загроз хмарних обчислень та низки інструментів злому IoT (наприклад, Shikra, Bus Pirate, Facedancer 21, і більше). [24].

Сучасний аналіз шкідливих програм CEH v11 тепер містить найновіші тактики аналізу шкідливих програм для вимагачів, банківських та фінансових шкідливих програм, ботнетів IoT, аналізу шкідливих програм OT, шкідливих програм для Android.

Збільшення лабораторного часу та зосередження уваги Більше 50% курсу CEH V11 присвячено практичним навичкам у діапазонах у реальному часі за допомогою лабораторій EC-Council.

Поточна версія CEH-V11, яка використовує код іспиту EC-Council 312-50, як це робили попередні версії. Вартість CEH V11 становить 1199 доларів. Хоча нещодавно вийшла нова версія V11, цей іспит містить 125 запитань із кількома варіантами вибору з обмеженням у 4 години.

Умови проходження іспиту

Для того, щоб зберегти високу цілісність сертифікаційних іспитів, іспити EC-council надаються у кількох формах (тобто різні бази даних запитань). Кожна форма ретельно аналізується шляхом бета -тестування відповідною групою зразків під компетенцією комітету експертів з предметів, які гарантують, що кожен з іспитів не тільки володіє академічною суворістю, але й має можливість застосування у реальному світі. Також є процес визначення рейтингу складності кожного питання. Індивідуальний рейтинг потім вносить загальний бал за кожну форму іспиту. Щоб гарантувати, що кожна форма має рівні стандарти оцінювання, бали встановлюються на основі "за форму іспиту". Залежно від того, яка форма іспиту проводиться, результати балів можуть становити від 60% до 85%.

EC-Council та різні Акредитовані навчальні центри проводять іспит в таких як PearsonVUE та власні центри сертифікації EC-Council. В таблиці нижче позначено загальну інформацію про іспит.

Таблиця 2.1.

Загальна інформація про іспит CEH

Вартість	1199 $(USD)
Кількість питань	125
Тривалість випробування	4 години
Формат тесту	Широкий вибір
Кількість модулів	20
Тестова доставка	ECC EXAM, VUE
Префікс іспиту	312-50 (ECC EXAM), 312-50 (VUE)
Прохідний бал	Від 60%до 85%

Термін дії сертифікату

Як тільки кандидат отримує сертифікацію EC-Council, відносини між EC-Council і кандидатом завжди регулюватимуться угодою про сертифікацію кандидатів у EC-Council, з якою кандидат повинен погодитися, перш ніж отримати сертифікацію [25].

Якщо сертифікований учасник не відповідає вимогам сертифікації протягом 3 років, EC-Council призупиняє його/її сертифікацію. Призупиненим членам не буде дозволено використовувати логотипи сертифікації та відповідні переваги членства в EC-Council. Відсторонені учасники повинні виправити своє призупинення протягом максимум 12 місяців з дати закінчення 3-річного періоду.

Якщо цього не зробити, сертифікація та статус учасника буде скасовано, а для отримання сертифікації учаснику доведеться знову оскаржити й скласти сертифікаційний іспит. Якщо учасник не відповідає вимогам щодо сертифікації протягом періоду призупинення, його буде скасовано, і він більше не зможе продовжувати використання логотипу сертифікації та пов’язаних переваг.

Учасники, чия сертифікація анульована, повинні будуть повторно здати відповідний новий іспит, щоб відновити свою сертифікацію.

Кредити безперервної освіти

Учасники, які мають призначення CEH (а також інші сертифікати EC-Council), повинні проходити повторну сертифікацію за цією програмою кожні три роки, щонайменше на 120 кредитів. Якщо сертифікований фахівець отримав сертифікат/и, які включені в схему ECE (EC-Council Continuing Education - безперервна освіта EC-Council), він/вона повинен буде отримати 120 кредитів (за сертифікацію) протягом трьох років.

Якщо учасник має кілька сертифікатів, отримані кредити будуть застосовані до всіх сертифікатів. Кредити можна отримати багатьма способами, включаючи відвідування конференцій, написання наукових робіт, підготовку до навчальних занять у суміжній області (для викладачів), читання матеріалів із суміжних предметів, складання іспиту новішої версії сертифікації, відвідування вебінарів, та багато інших.

Кваліфіковані заходи ECE повинні бути завершені протягом 3-річного вікна програми ECE і повинні бути подані лише за один 3-річний період. Кредити ECE нараховуються на річній основі з 1 січня по 31 грудня кожного календарного року. Сертифіковані члени повинні зареєструвати свої кредити ECE, отримані до 1 лютого наступного року, щоб зберегти свій статус сертифікації.

2.3 Сертифікований захисник мережі (CND)

Опис сертифікаційної програми

Certified Network Defender (CND) — це практична навчальна програма, яку ведуть інструктори, яка не залежить від виробника. Це програма з інтенсивним лабораторним використанням навичок, що базується на освітній системі безпеки та аналізі робочих ролей, представлених Національною структурою компетенцій Infocomm (NICF), а також на основі аналізу завдань та освітньої системи з питань кібербезпеки від Національної ініціативи освіти з кібербезпеки. (NICE). Курс

також був зіставлений з глобальними посадовими ролями та посадовими ролями Міністерства оборони (DoD) для системних/мережевих адміністраторів.

Програма готує мережевих адміністраторів, як визначити, які частини організації мають бути перевірені та перевірені на наявність уразливостей безпеки, а також як зменшити, запобігти та пом'якшити ризики в мережі. CND охоплює підхід до захисту, виявлення, реагування та прогнозування безпеки мережі.

Більше 50% курсу CND містить практичні лабораторії, присвячені тому, щоб допомогти студентам навчитися практичним навичкам у реальному часі, призначених для охоплення таких областей, як керування мережевим захистом, захист периметра мережі, захист кінцевих точок, захист додатків і даних, віртуальний бізнес, хмарні технології, і захист бездротової мережі, виявлення інцидентів і реагування на них, а також передбачення загроз, які нададуть мережевим адміністраторам реальний досвід, який можна застосувати до сучасних технологій і операцій мережевої безпеки [26].

Вимоги до здобувача сертифікату

CND має 2 варіанти допуску до іспиту, але самі вимоги більш серйозні:

• Пройти офіційний курс, отримати за нього ваучер до іспиту;

• Чи підтвердити 2 роки досвіду, заплатити внесок і купити ваучер.

Наявність більш вищої сертифікації не дає можливості придбати ваучер без доведення навичок.

Цільова аудиторія курсу

Наступні особи можуть розглядати сертифікати мережевої безпеки від EC-Council як наступний крок у своїй кар'єрі:

- Сертифікований мережевий адміністратор/інженер Cisco або Microsoft
- Сертифікований мережевий аналітик Wireshark
- Сертифікований спеціаліст SolarWinds
- Сертифікований професіонал мережі Juniper
- Професіонали із сертифікатом Comptia Network+/Security+
- Викладачі університетів, які викладають курси з кібербезпеки

- IT-спеціалісти, які планують кар’єрний перехід
- Студенти, які хочуть почати кар'єру в галузі кібербезпеки

Особи, які пройшли курс кібербезпеки CND v2, мають право на такі посади початкового рівня:

- Адміністратори мережі початкового рівня
- Адміністратори мережевої безпеки початкового рівня
- Аналітик безпеки даних
- Молодший інженер мережевої безпеки
- Молодший технік із захисту мережі
- Аналітик безпеки
- Оператор охорони

Структура курсу

Курс складається з 14 модулів: основи комп'ютерних мереж і підходи до їх захисту; загрози мережевої безпеки, уразливості і атаки; управління мережевою безпекою, протоколи та пристрої; проектування і впровадження політики мережевої безпеки; фізична безпека; безпека хостів; проектування і конфігурація міжмережевих екранів; IDS: проектування і конфігурація систем виявлення вторгнень; VPN: проектування і конфігурація віртуальних приватних мереж; Wi-Fi: захист бездротових мереж; моніторинг та аналіз мережевого трафіку; ризики і управління уразливостями; створення резервних копій та відновлення даних; управління реагуванням на інциденти.

Останне оновлення курсу

У вересні 2020 року було анонсоване оновлення курсу - Certified Network Defender CNDv2, перше за довгі роки. EC-Council в своїй програмі обіцяє в новій версії зробити акцент на віддалену роботу і хмарні технології. У порівнянні з CNDv1, CNDv2 складається вже з 20-ти модулів, які поєднують кілька старих і 10 нових модулів.

На даний момент список приблизно такий: сучасні мережеві атаки і стратегії захисту; адміністративна безпека мережі; технічна безпека мережі; безпека периметра; захист кінцевих точок Windows; захист кінцевих точок Linux; захист

кінцевих точок мобільних пристроїв; захист кінцевих точок Інтернету речей (IoT); захист додатків; безпека даних; безпека корпоративної віртуальної мережі; безпека корпоративної хмарної мережі; безпека корпоративних бездротових мереж; моніторинг та аналіз мережевого трафіку; моніторинг та аналіз мережевих журналів; реагування на інциденти і розслідування інцидентів; безперервність бізнесу та відновлення після збоїв; прогнозування й управління ризиками; оцінка загроз з аналізом поверхні атаки; прогнозування за допомогою розвідки в області кіберзагроз (Рис. 2.4).

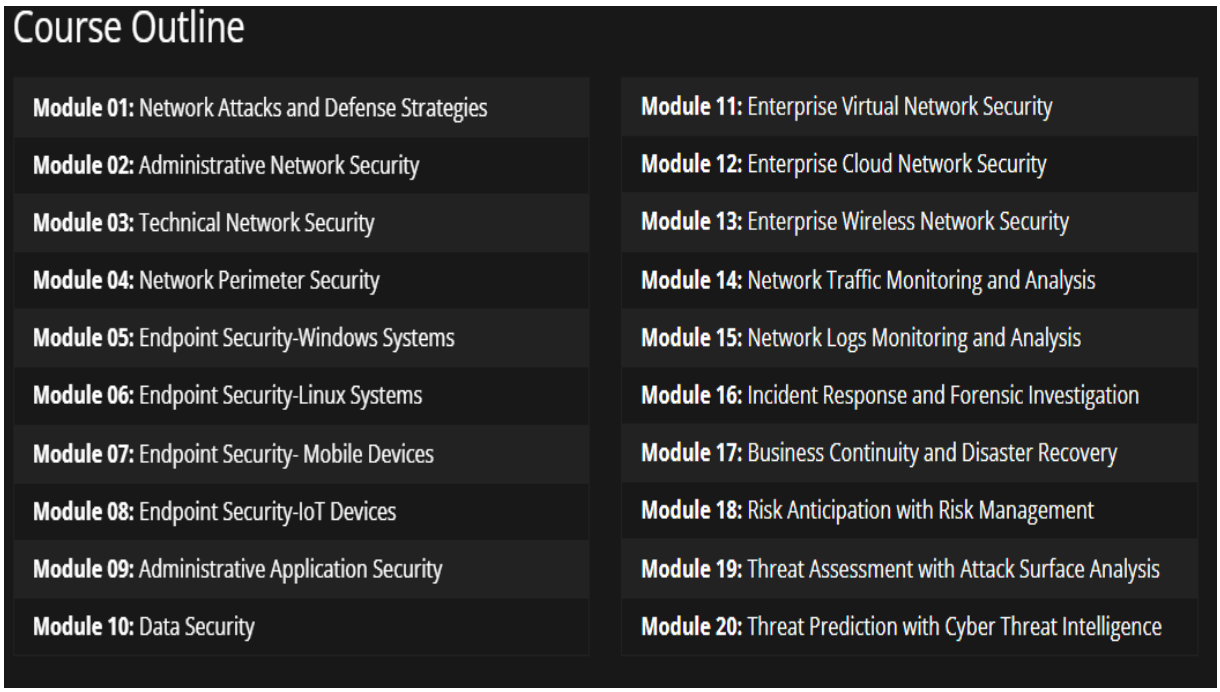

Рис. 2.4. Структура курсу CND

У новій версії курсу зросла кількість лабораторних робіт, і тепер велика частина часу відводиться на практичну роботу, а не на прослуховування лекцій. Змін в іспиті не помічено - критерії допуску, прохідний бал, кількість питань і час залишилися без змін, але, ймовірно, пул питань буде повністю оновлений.

Умови проходження іспиту

Варіантів проходження курсу в EC-Council кілька:

• Самостійно з використанням готових відео- і матеріалами iLearn, але такий спосіб не дає права здавати іспит тому, ймовірно, призначений тільки для тих, хто підтвердив свій досвід або просто не збирається здавати іспит;

• Навчання в форматі iClass - iclass.eccouncil.org, яке підходить, якщо немає можливості навчатися в акредитованому центрі з інструктором або найближчий центр не проводить потрібні програми. Цей варіант і всі наступні дають право здавати іспит;

• Навчання в акредитованому центрі.

Це не повний список варіантів навчання, оскільки є ще майстер-класи, які не входять до складу формату iClass, і культурно-масові заходи (чимось схоже на майстер-класи, тільки під іншою обгорткою), після участі в яких тим, хто навчається, надають весь доступ iLearn + ключ.

Всі матеріали для занять будуть доступні в кабінеті Aspen. А доступ до лабораторій буде організований у залежності від формату навчання.

Для підготовки до іспиту EC-Council надає доступ до CND Assessment - 50 тренувальних питань, які схожі на ті, які будуть на реальному іспиті.

Таблиця 2.2.

Загальна інформація про іспит CND

Кількість питань	100
Тривалість випробування	4 години
Формат тесту	Мультивибір(тести/практичні)
Доставка тесту	ECC EXAM
Префікс іспиту	312-38(ECC EXAM)
Вартість іспиту	450$(USD)
Прохідний бал	Від 60% до 85%

Термін дії сертифікату

Як і всі інші сертифікати EC-Council, дійсний 3 роки впродовж яких потрібно пройти контроль знань для отримання кредиту освіти та продовження терміну дії.

Кредити безперервної освіти

Як і в сертифікаційній програмі CEH учасники повинні заробити 120 кредитів ECE кожні три роки, щоб поновити свою сертифікацію CND. Існують певні вимоги до програми ECE для виконання цієї вимоги щодо поновлення

CND. Фахівці мають заробити 40 кредитів ECE за кожен рік, а також сплатити 80 доларів США щорічного членського внеску в EC-Council.

2.4 Сертифікований фахівець з інцидентів безпеки (E|CIH)

Опис сертифікаційної програми

EC-Council Certified Incident Handler - це остання ітерація сертифікованої програми EC-Council (E|CIH) була розроблена та розроблена у співпраці з кібербезпекою та практиками реагування на інциденти та реагування на них у всьому світі.

Це всебічна програма на рівні спеціалістів, яка передає знання та навички, необхідні організаціям для ефективного подолання наслідків після порушення, шляхом зменшення впливу інциденту, як з фінансової, так і з репутаційної точки зору.

Слідом за ретельним розвитком, який включав ретельний аналіз завдань (JTA), пов'язаний з обробкою інцидентів та роботами, які надають першу допомогу інцидентам, EC-Council розробила високо інтерактивну, всеосяжну, на основі стандартів інтенсивну триденну програму навчання та сертифікацію, яка забезпечує структуровану підхід до вивчення вимог поводження з реальними ситуаціями та реагування на них.

Професіонали, зацікавлені у вирішенні інцидентів та реагуванні на них як кар’єру, потребують всебічного навчання, яке не лише передає концепції, але й дозволяє їм випробувати реальні сценарії. Програма E|CIH включає практичне навчання, яке проводиться в лабораторіях у рамках навчальної програми.

Справжнє працевлаштування після отримання сертифікату може бути досягнуто лише тоді, коли мета навчальних програм відповідає стандартам, опублікованим урядом та галузями, та рамкам реагування на них

E | CIH-це програма, керована методами, яка використовує цілісний підхід для охоплення широких концепцій, що стосуються обробки організаційних інцидентів та реагування від підготовки та планування процесу реагування на

інцидент до відновлення активів організації після інциденту безпеки. Ці концепції є важливими для обробки та реагування на інциденти безпеки, щоб захистити організації від майбутніх загроз або атак/

Вимоги до здобувачів сертифікату

Щоб мати право складати іспит E|CIH, кандидат повинен відвідати офіційний тренінг E|CIH через будь-який з уповноважених навчальних центрів EC-Council або зайти на онлайн-тренінги EC-Council через iWeek або приєднатись до програми самонавчання через iLearn [27].

Кандидати, які мають не менше 1 року досвіду роботи в тій галузі, які хотіли б подати заявку, щоб скласти іспит безпосередньо без відвідування навчання, повинні сплатити 100 доларів США. Ця оплата включена до плати за навчання, якщо учасник вирішить відвідати тренінг.

Цільова аудиторія курсу

Навички поводження з інцидентами, які викладаються в E|CIH, доповнюють наведені нижче посади, а також багато інших завдань з кібербезпеки:

• Тестери проникнення

• Аудитори з оцінки вразливості

• Адміністратори з оцінки ризиків

• Адміністратори мережі

• Інженери з безпеки додатків

• Слідчі/ аналітики та аналітики SOC

• Системні адміністратори/інженери

• Адміністратори брандмауера та мережеві менеджери/IT менеджери

Структура курсу

Курс E|CIN складається з дев’яти модулів: вступ; обробка інцидентів та реагування на них; готовність до криміналістики та перша реакція; поводження та реагування на випадки шкідливого програмного забезпечення; обробка та реагування на випадки безпеки електронної пошти; обробка та реагування на інциденти з мережевою безпекою; обробка та реагування на інциденти безпеки

веб додатків; обробка та реагування на інциденти хмарної безпеки; поводження та реагування на загрози з боку інсайдерів (Рис. 2.5).

Рис. 2.5. Структура курсу E|CIN

Останнє оновлення курсу

Останнє оновлення сертифікаційного курсу E|CIN вийшло в 2019 році. Оновлена сертифікація включає в себе абсолютно нову навчальну програму з більшим акцентом на першочергове реагування та підготовку до судово-криміналістичної експертизи. Також додано нові лабораторії та перероблено з нуля практичні завдання та тести [28].

Умови проходження курсу

E|CIH дозволяє фахівцям із кібербезпеки продемонструвати своє володіння знаннями та навичками, необхідними для вирішення інцидентів

Таблиця 2.3.

Загальна інформація про іспит E|CIH

Назва іспиту	EC-Council Certified Incident Handler
Код іспиту	212-89
Кількість запитань	100
Тривалість	3 години
Наявність екзаменаційного порталу	EC-Council
Формат тестування	Мультивибір
Ціна (USD)	100$(USD)

Термін дії

Сертифікат ECIH дійсний протягом 3 років. Щоб поновити свої облікові дані на наступний 3-річний період, вам потрібно оновити свій кредитний рахунок EC-Council Continuing Education (ECE) на порталі EC-Council Aspen та надати підтвердження отриманих кредитів.

Кредити безперервної освіти

Учасники, які мають призначення ECIH (а також інші сертифікати EC-Council), повинні проходити повторну сертифікацію за цією програмою кожні три роки, щонайменше на 120 кредитів. Якщо сертифікований фахівець отримав сертифікат/и, які включені в схему ECE, він/вона повинен буде отримати 120 кредитів (за сертифікацію) протягом трьох років [29].

Якщо учасник має кілька сертифікатів, отримані кредити будуть застосовані до всіх сертифікатів. Кредити можна отримати багатьма способами, включаючи відвідування конференцій, написання наукових робіт, підготовку до навчальних занять у суміжній області (для викладачів), читання матеріалів із суміжних предметів, складання іспиту новішої версії сертифікації, відвідування вебінарів, та багато інших.

Кваліфіковані заходи ECE повинні бути завершені протягом 3-річного вікна програми ECE і повинні бути подані лише за один 3-річний період. Кредити ECE

нараховуються на річній основі з 1 січня по 31 грудня кожного календарного року. Сертифіковані члени повинні зареєструвати свої кредити ECE, отримані до 1 лютого наступного року, щоб зберегти свій статус сертифікації.

Висновки до розділу 2

Міжнародна рада консультантів з питань електронної комерції (EC-Council) - це американська неурядова організація, яка надає послуги із сертифікації та навчання в галузі електронного бізнесу та кібербезпеки. EC-Council працює у 145 країнах по всьому світу, і є власником та розробником багатьох всесвітньо відомих сертифікаційних програм, серед яких CEH, CHFI, ECSA, CND та інші. За час свого існування організація навчила й сертифікувала понад 200 тисяч фахівців із інформаційної безпеки у всьому світі.

Сертифікований етичний хакер (CEH) – це кваліфікація, отримана шляхом демонстрації знань щодо оцінки безпеки комп'ютерних систем шляхом пошуку слабких місць та вразливих місць у цільових системах, з використанням тих самих знань та інструментів, що і зловмисний хакер, але законним шляхом та законним чином для оцінки положення безпеки цільової системи. Курс складається з 20 модулів, іспит триває 4 години і складається з 125 запитанн, прохідний бал від 60% до 85%. Термін дії сертифікату 3 роки, впродовж яких потрібно підвердити його актуальність.

Certified Network Defender (CND) - це програма з інтенсивним лабораторним використанням навичок, що базується на освітній системі безпеки та аналізі робочих ролей, представлених Національною структурою компетенцій Infocomm (NICF). Програма готує мережевих адміністраторів, як визначити, які частини організації мають бути перевірені та перевірені на наявність уразливостей безпеки, а також як зменшити, запобігти та пом'якшити ризики в мережі. Курс складається з 20 модулів, іспит триває 4 години, складається з 100 питанн, прохідний бал від 60% до 85%. Термін дії 3 роки.

E|CIH -це всебічна програма на рівні спеціалістів, яка передає знання та навички, необхідні організаціям для ефективного подолання наслідків після порушення, шляхом зменшення впливу інциденту, як з фінансової, так і з репутаційної точки зору. Курс складається з 9 модулів, іспит тприває 3 години, складається 100 питанньь, термін дії 3 роки.

Розділ 3

ПРОФЕСІЙНІ СЕРТИФІКАЦІЇ COMPTIA У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1 Напрями незалежної сертифікації фахівців CompTIA

Відомою професійною організацією, яка займається незалежною сертифікацією в галузі IT та інформаційної безпеки, є Асоціація галузі інформаційних технологій (Computing Technology Industry Association – CompTIA), США [30].

CompTIA була створена в 1982 році як Асоціація кращих дилерів комп'ютерів (ABCD). Пізніше ABCD змінила назву на Асоціацію індустрії обчислювальних технологій [31].

У 2010 році CompTIA переїхала до своєї всесвітньої штаб-квартири в Даунерс-Гроув, штат Іллінойс. Портал CompTIA перейшов до гібридної версії моделі з відкритим доступом у квітні 2014 року з ексклюзивним вмістом для членів, які платять внески [32].

Цей крок розширив охоплення організації, щоб залучити ширшу, більш різноманітну групу членів, і протягом року членство CompTIA зросло з 2050 членів до понад 50 000 у 2015 році. До кінця 2016 року організація налічувала понад 100 000 членів у всьому світі.

CompTIA запустила програму Dream IT у 2014 році, щоб надати ресурси для дівчат і жінок у Сполучених Штатах, зацікавлених в IT-індустрії. У жовтні 2015 року програму було розширено на Великобританію [33].

Skillsboost, онлайн-ресурс CompTIA для шкіл, був запущений у червні 2015 року. Він містив ресурси для учнів, батьків і вчителів, які пропагують важливість володіння комп’ютером. CompTIA провела свій перший щорічний саміт постачальників ChannelCon у 2015 році. Самміт постачальників призначений

виключно для людей, які відвідують ChannelCon, головну конференцію галузі для співпраці, освіти та спілкування. Яка вирішує проблеми в IT-індустрії [34].

У січні 2017 року CompTIA заснувала професійну асоціацію IT, засновану на придбанні Асоціації професіоналів інформаційних технологій [35].

Асоціація галузі інформаційних технологій (CompTIA) є провідним голосом та захисником глобальної екосистеми інформаційних технологій вартістю 5 трильйонів доларів США. Завдяки освіті, навчанню, сертифікації, благодійності та дослідженню ринку CompTIA сприяє зростанню промисловості, розвитку висококваліфікованої робочої сили та бере на себе зобов'язання створити інноваційного середовище, в якому можливості та переваги технологій доступні для всіх.

Учасники та власники сертифікатів охоплюють увесь спектр спеціалістів технологічних компаній від відомих лідерів Fortune 500 до малого та середнього технічного бізнесу, які допомагають клієнтам вирішувати реальні бізнес-проблеми у всьому світі, та інноваторів у сфері технічних послуг, які підтримують впровадження й управління новітніми технологічними рішеннями.

Організація співпрацює з окремими спеціалістами в галузі технологій як найбільшою програмою акредитації, нейтральною для постачальників, для технологічних працівників. Компанія CompTIA надала більш ніж 2,5 мільйона сертифікатів у таких сферах, як кібербезпека, мережа, хмарні обчислення та технічна підтримка.

CompTIA також підтримує потужну партнерську програму по всьому світу з тисячами академічних установ, некомерційних організацій, центрів вакансій та інших організацій.

В епоху, коли кожна особа займається технікою і кожна організація має технологічні можливості, CompTIA є провідним місцем для обох. Як асоціація, присвячена інноваціям, CompTIA об'єднує навчання та можливості у затишному, перспективному місці.

На сьогодні CompTIA реалізує професійні сертифікаційні курси за такими 4-ма напрямами в галузі IT (Рис. 3.1):

Основи IT: Основи IT - IT Fundamentals (ITF+); IT для початківців - CompTIA A+, Мережі - CompTIA Network+; IT-безпека - CompTIA Security+;

Інфраструктура: Хмарні технології - CompTIA Cloud+; ОС Linux - CompTIA Linux+; Серверні платформи - CompTIA Server+;

Кібербезпека: Аналітик кібербезпеки - CySA+; Фахівець з тестування вразливостей - CompTIA PenTest+; Просунутий професіонал з кібербезпеки - CompTIA CASP+;

Додаткові професійні сертифікати: IT-проекти - CompTIA Project+; Технічний тренер з IT - CompTIA CTT+; Основи хмарних технологій для нетехнічних фахівців - CompTIA Cloud Essentials+.

З 1 січня 2011 року було складено понад 2,3 мільйона іспитів, акредитованих ISO/ANSI CompTIA [36].

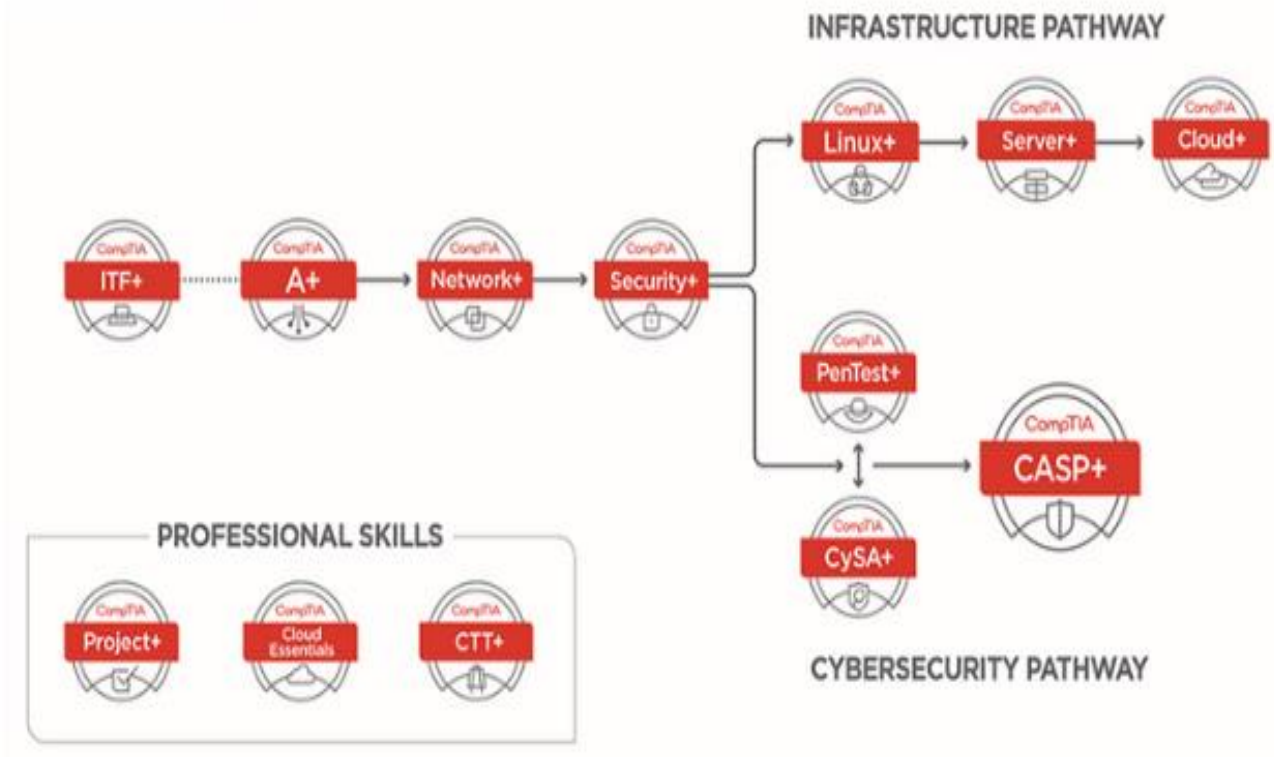

Рис. 3.1. Сертифікаційні курси CompTIA

Коротка інформація про зазначені сертифікаційні програми CompTIA представлена у таблиці 3.1.

Таблиця 3.1.

Коротка інформація про сертифікаційні програми CompTIA

Назва програми	Короткий опис
CompTIA IT Fundamentals	початковий сертифікат для отримання базових знань та навичок в сфері IT.
CompTIA A+	підтверджує наявність основних навичок роботи з IT на різних пристроях та операційних системах.
CompTIA Network+	підтверджує основні навички, необхідні для впевненого проектування, налаштування, управління та усунення несправностей будь -яких дротових та бездротових пристроїв.
CompTIA Security+	забезпечує глобальний орієнтир найкращого досвіду роботи в IT-мережі та оперативної безпеки, однієї з найшвидше зростаючих галузей IT.
CompTIA Cloud +	підтверджує навички, необхідні для розгортання та автоматизації безпечних хмарних середовищ, які підтримують високу доступність бізнес-систем і даних.
CompTIA Linux+	підтверджує навички IT-фахівців з практичним досвідом налаштування, моніторингу та підтримки серверів під керуванням операційної системи Linux.
CompTIA Server+	охоплює архітектуру сервера, адміністрування, зберігання, безпеку, роботу в мережі, усунення несправностей, а також відновлення після аварій.
CompTIA CySA+	підтверджує, що кандидати володіють знаннями та навичками, необхідними для використання методів розвідки та виявлення загроз, аналізу та інтерпретації даних, виявлення та усунення вразливих місць, розробки запобіжних заходів, ефективного реагування на інциденти та їх відновлення.

Продовження таблиці 3.1.

CompTIA CASP+	охоплює технічні навички в архітектурі безпеки та вищій інженерії безпеки в традиційних, хмарних і гібридних середовищах, управлінні, обробці ризиків і забезпеченні нормативної відповідності, оцінки готовності підприємства у сфері кібербезпеки та впровадження відповідних рішень.
CompTIA PenTest+	підтверджує наявність знань та навичок, необхідних для планування та оцінки, розуміння законодавчих та нормативних вимог відповідності, виконання сканування вразливостей і тестування на проникнення, аналізу даних та ефективного звітування та передачі результатів.
CompTIA Project+	підтверджує наявність знань та навичок, необхідних для керування життєвим циклом проекту та ресурсами, забезпечення відповідного спілкування, ведення проектної документації.
CompTIA CTT+	Підтверджує наявність необхідних навичок та знань для підготовки, презентації, проведення та оцінки навчального заняття, планування лекцій, комунікативності
CompTIA Cloud Essentials+	Забезпечує знаннями з підвищення ефективності, керування витратами, зменшення ризиків безпеки для організацій, розуміння основних бізнес та технічних компонентів, розуміння конкретних проблем та заходів безпеки, а також нових технологічних концепцій, рішень та переваг для організацій

Пов'язані посади та кар'єри

На додаток до рівнів сертифікації, CompTIA групує свої сертифікати в кілька кар’єрних шляхів:

- інформаційна безпека;

- мережні та хмарні технології;
- обладнання, послуги та інфраструктура;
- IT-менеджмент і стратегія;
- Інтернет та мобільний зв’язок;
- розробка програмного забезпечення;
- навчання;
- продуктивність офісу.

Сторінка CompTIA, присвячена питанням сертифікації, дозволяє вибрати рівень сертифікації та/або кар’єрний шлях, а потім повертає список сертифікатів, на яких потрібно зосередитися. Наприклад, одним із найпопулярніших напрямків кар’єри в IT є адміністрування мережі. Кар'єрний шлях CompTIA Network and Cloud Technologies пропонує численні сертифікати, які можуть допомогти просунути вашу кар'єру адміністрування мережі, наприклад IT Fundamentals+, A+ і Network+ (основні сертифікати), а також Cloud+ і Linux+ (сертифікація інфраструктури) і Cloud Essentials.

Тим, хто цікавиться мережевою безпекою (одна з найбільш швидкозростаючих галузей IT), варто розглянути сертифікації в кар’єрному шляху CompTIA щодо інформаційної безпеки. Сюди входять усі чотири основні сертифікації (Основи IT, A+, Network+ і Security+), а також усі сертифікати кібербезпеки (CySA+, PenTest+ і CASP+).

CompTIA надає комплексну дорожню карту IT-сертифікації, яка охоплює сертифікати від CompTIA, а також від ряду інших організацій, включаючи Cisco, EC-Council, Microsoft, $(ISC)^2$, ISACA, Mile2 тощо.

Оскільки сертифікаційні програми CompTIA не зосереджені на одній навичці (наприклад, створення мережі або віртуалізація), власники сертифікатів CompTIA можуть опинитися на різних посадах залежно від свого досвіду, рівня кваліфікації та сфер інтересів. Ось лише деякі з можливих варіантів кар’єри, які можуть реалізувати власники сертифікатів CompTIA:

A+ : як правило, власники сертифікату A+ знаходять роботу на посадах підтримки, таких як адміністратори підтримки, технічні спеціалісти або спеціалісти з підтримки.

Network+ : професіонали Network+ в основному працюють на посадах, пов'язаних з мережею, наприклад, мережеві аналітики, адміністратори або спеціалісти з підтримки. Власники сертифікатів також можуть працювати мережевими інженерами, польовими техніками або техніками служби підтримки мережі.

Аналітик безпеки CySA+ : загальні ролі для професіоналів, які цікавляться кібербезпекою, інформаційною безпекою та аналізом ризиків, можуть виконувати роль інженерів з безпеки, аналітиків або спеціалістів з кібербезпеки, аналітиків загроз чи вразливостей або аналітиків операційних центрів безпеки (SOC).

Security+ : фахівці за цим напрямом займають різноманітні посади, наприклад адміністратори мережі, системи чи безпеки, менеджери безпеки, спеціалісти чи адміністратори та консультанти з безпеки.

Server+ : ролі для професіоналів серверів включають адміністраторів сховищ та серверів, а також службу підтримки серверів або спеціалістів із IT/сервера.

Linux+ : професіонали Linux часто працюють на таких посадах як адміністратори баз даних Linux, адміністратори мережі або веб-адміністратори.

Cloud+/Cloud Essentials: власники сертифікації Cloud+ зазвичай працюють як спеціалісти з хмари, розробники або адміністратори системи та мережі. Фахівці Cloud Essentials, як правило, працюють у сферах, пов’язаних із хмарними технічними продажами або розвитком бізнесу.

CASP+ : загальні ролі для власників сертифікату CASP+ включають спеціалістів з кібербезпеки, спеціалістів InfoSec, спеціалістів із інформаційної безпеки та архітекторів безпеки.

Project+ : власники повноважень Project+ зазвичай виконують роль керівництва проекту, наприклад, керівники проектів, координатори та директори або керівники команд [37].

CompTIA пропонує декілька способів проходження сертифікаційних тренінгів, призначених для успішного складання іспитів:

- електронне (інтернет)-навчання;
- віртуальні лабораторії;
- підготовка до іспиту;
- навчальні посібники;
- навчання під керівництвом інструкторів.

Сертифікати CompTIA діють упродовж 3-річного терміну, а їхні власники зобов'язуються брати участь у програмі безперервної освіти, щоб поновити наявну сертифікацію.

Для самостійної підготовки до іспитів на отримання сертифікатів CompTIA пропонує власні комплексні рішення для інтерактивного електронного навчання CertMaster Learn (вивчення теоретичних питань), CertMaster Labs (практична підготовка) і CertMaster Practice (оцінювання рівня знань і готовності до іспиту). Для бажаючих проводяться підготовчі тренінги у класі або онлайн.

Навчання та ресурси CompTIA

CompTIA надає різноманітні та широкі можливості навчання, включаючи навчання в класі, навчальні матеріали та електронне навчання. Широкий спектр авторизованих партнерів постачальників навчання CompTIA (CAPPs), таких як Global Knowledge, Learning Tree International та інші, працюють у всьому світі. Вартість пропозицій для класу та онлайн/електронного навчання варіюється від 2000 до 4000 доларів США, залежно від деталей.

CompTIA співпрацює з третіми сторонами, щоб пропонувати матеріали для самостійного навчання. Вміст, який пройшов процес перевірки, позначається логотипом CompTIA Approved Quality Content (CAQC). Інші матеріали, які

дозволяють навчатися у власному темпі, наприклад аудіосегменти, уроки та додаткові ресурси, доступні через CompTIA Marketplace.

Нарешті, усі кандидати на сертифікацію CompTIA A+, Linux+, Network+, Server+, Security+ і IT Fundamentals+ повинні перевірити CertMaster, онлайн-інструмент підготовки до тестування CompTIA. CertMaster допоможе визначити, які теми добре відомі, а які потрібно оновити, а також пропонує навчання, яке допоможе заповнити прогалини.

Тестування здобувачів сертифікатів CompTIA здійснюється онлайн або в авторизованих пунктах Асоціації.

3.2 Сертифікація CompTIA Security+

Опис сертифікаційної програми

Однією з найбільш відомих і популярних сертифікацій Асоціації CompTIA є програма, присвячена питанням інформаційної безпеки - Security+.

Security+ - це міжнародна сертифікація, яка підтверджує наявність у здобувача базових навичок, необхідних для виконання основних функцій у галузі безпеки IT і створює основу для зайняття ним позицій середнього рівня та побудови кар'єри в галузі інформаційної безпеки.

Security+ постійно оновлюється згідно з останніми тенденціями безпеки IT, охоплюючи найважливіші технічні навички з оцінки й управління ризиками, реагування на інциденти, цифрової криміналістики, безпеки корпоративних мереж, мобільних, гібридних та хмарних операцій, впровадження заходів IT-безпеки тощо.

CompTIA пропонує цілий ряд інструментів для підготовки, що включає навчальні посібники, електронне навчання та онлайн-курси. Наприклад, вони пропонують офіційний навчальний посібник CompTIA Security+, електронне навчання CertMaster та підготовку до тестів, онлайн-тренінги в прямому ефірі та CompTIA Labs – віртуальне лабораторне середовище.

Вимоги до здобувача сертифікату

CompTIA не встановлює передумов для сертифікації Security+. Немає жодних вимог щодо віку чи освіти, але CompTIA рекомендує, щоб кандидат мав принаймні два роки досвіду роботи з IT-адміністрування з акцентом на безпеку.

Цільова аудиторія курсу

CompTIA рекламує сертифікацію, називаючи її «трампліном у вакансіях з кібербезпеки середнього рівня». Посади, які обіймають власники CompTIA Security+, можуть включати такі посади у сфері IT та безпеки, як:

- адміністратор безпеки;
- системний адміністратор;
- менеджер/аналітик служби підтримки;
- мережевий/хмарний інженер;
- інженер з безпеки/аналітик;
- розробник програмного забезпечення;
- IT-аудитор;
- менеджер IT-проектів;
- менеджер з інформаційної безпеки;
- архітектор безпеки.

Структура курсу

Курс складається з 4 модулів: атаки, загрози та вразливості; архітектура та дизайн; впровадження; операції та реагування на інциденти; управління, ризики та відповідність (Рис. 3.2).

Рис. 3.2. Структура курсу Security+

Останнє оновлення курсу

Сертифікаційний іспит CompTIA Security+ відповідно до оновленої в листопаді 2020 року версії SY0-601, включає 5 доменів: атаки, загрози і вразливості; архітектура і проектування корпоративних середовищ безпеки; реалізація (управління ідентичністю, контроль доступу, криптографія, безпека бездротових мереж і наскрізна безпека); операції та реагування на інциденти; управління ризиками і забезпечення відповідності нормативним документам (PCI-DSS, SOX, HIPAA, GDPR, FISMA, NIST, CCPA).

Умови проходження іспиту

Сертифікаційний іспит CompTIA Security+ підтвердить наявність у кандидата знань і навичок, необхідних для оцінки стану безпеки корпоративного середовища, а також рекомендації та впровадження відповідних рішень безпеки; відстежувати та захищати гібридні середовища, зокрема хмарні, мобільні та інтернету речей; працювати, усвідомлюючи застосовні закони та політику,

включаючи принципи управління, ризиків та відповідності; виявляти, аналізувати та реагувати на події та інциденти безпеки.

Таблиця 3.2.

Загальна інформація про іспит Security+

Код іспиту	SY0-601
Дата випуску	12 листопада, 2020р.
Кількість питань	90
Тип питань	Різноманітний вибір і на основі продуктивності
Тривалість іспиту	90 хвилин
Прохідний бал	700 балів (шкала від 100-900)
Мова іспиту	англійська, японська
Закінчення терміну дії	3 роки після випуску
Постачальник тестування	Pearson VUE Тестовий центр або онлайн тестування
Вартість	370$ USD

Термін дії сертифікату

Сертифікати CompTIA діють упродовж 3-річного терміну, а їхні власники зобов'язуються брати участь у програмі безперервної освіти, щоб поновити наявну сертифікацію.

Кредити безперервної освіти

Для сертифікату Security+ потрібно набрати 50 балів активності впродовж 3 років дії сертифікату. Для отримання балів потрібно виконати певні дії: Отримати сертифікат який не відноситься до CompTIA; брати учать у заходах IT-індустрії; Опублікувати статтю, технічний документ або допис у блозі або книзі; Отримати відповідний досвід роботи [38].

3.3 Сертифікований аналітик кібербезпеки (CySA+)

Опис сертифікаційної програми

CompTIA Cybersecurity Analyst (CySA+) - це сертифікація IT-спеціалістів, які застосовує поведінкову аналітику до мереж і пристроїв для запобігання, виявлення та боротьби з загрозами кібербезпеки шляхом постійного моніторингу безпеки.

Здобувач сертифікату CySA+ повинен не тільки активно фіксувати, контролювати, аналізувати й реагувати на дані щодо мережевого трафіку, але також мати знання й навички з безпеки програмного забезпечення й додатків, виявлення загроз, реагування на інциденти і дотримання нормативних вимог у галузі IT та інформаційної безпеки.

Оскільки зловмисники навчилися уникати традиційних рішень на основі сигнатур, таких як брандмауери та антивірусне програмне забезпечення, підхід на основі аналітики в галузі IT-безпеки стає все більш важливим для організацій. CompTIA CySA+ застосовує поведінкову аналітику до мереж, щоб покращити загальний стан безпеки шляхом виявлення та боротьби зі зловмисним програмним забезпеченням і розширеними постійними загрозами, що призводить до покращення видимості загроз на широкій поверхні атаки. Це підтвердить здатність IT-фахівця активно захищати та постійно покращувати безпеку організації.

Вимоги до здобувача сертифікату

CySA+ - це єдиний сертифікат для аналітиків безпеки середнього рівня, які мають володіти мінімум 4-річним досвідом роботи в галузі інформаційної безпеки або пов’язаних сферах, а також мають мати сертифікати основного рівня CompTIA (Network+, Security+) або рівнозначні знання.

Цільова аудиторія курсу

Посади, які використовують CompTIA CySA+:

- аналітик безпеки;
- аналітик SOC (операційного центру безпеки) II рівня;

- фахівець з моніторингу безпеки;
- аналітик розвідки загроз;
- інженер безпеки;
- аналітик безпеки додатків;
- фахівець або куратор з реагування на інциденти;
- спеціаліст з аналізу дотримання вимог;
- спеціаліст з полювання на загрози.

Структура курсу

Курс CompTIA CySA+ складається з 5 модулів: управління загрозами та вразливостями; безпека програмного забезпечення та систем; операції та моніторинг безпеки; реакція на інциденти; відповідність та оцінка (Рис. 3.3).

Рис. 3.3. Структура сертифікаційного курсу CySA+

Останнє оновлення курсу

Програма CySA+ була оновлена у квітні 2020 року і зараз містить 5 доменів, які охоплюють такі питання: управління загрозами і вразливостями; безпека систем і ПЗ; забезпечення відповідності нормативним вимогам і її оцінювання;

операції безпеки, насамперед запобіжного характеру, їх моніторинг та коригування; реагування та відновлення після інцидентів [39].

Незважаючи на те, що формат сертифікаційного іспиту не змінився, частина змісту іспиту є - після реструктуризації областей знань CS0-002 представляє кандидатів на сертифікацію з п’ятьма доменами на відміну від чотирьох у CS0-001. Слід також зазначити, що рекомендований практичний досвід дещо збільшився з трьох-чотирьох років до мінімум чотирьох.

Умови проходження іспиту

Сертифікація CompTIA Cybersecurity Analyst (CySA+) підтверджує, що кандидати мають знання та навички, необхідні для використання методів розвідки та виявлення загроз, аналізу та інтерпретації даних, виявлення та усунення вразливостей, пропонування запобіжних заходів, а також ефективного реагування та відновлення після інцидентів.

Таблиця 3.3.

Загальна інформація про іспит CySA+

Код іспиту	CS0-002
Дата випуску	21 квітня, 2020 р.
Кількість питань	85
Тип питань	Різноманітний вибір і на основі продуктивності
Тривалість іспиту	165 хвилин
Прохідний бал	700 балів(шкала від 100-900)
Мова іспиту	англійська, японська
Закінчення терміну дії	3 роки після випуску
Постачальник тестування	Pearson VUE Тестовий центр або онлайн тестування
Вартість	370$ USD

Термін дії сертифікату

Сертифікат CompTIA CySA+ діє упродовж 3-річного терміну, а його власники зобов'язуються брати участь у програмі безперервної освіти, щоб поновити наявну сертифікацію.

Кредити безперервної освіти

Для сертифікату CySA+ потрібно набрати 60 балів активності впродовж 3 років дії сертифікату. Для отримання балів потрібно: отримати сертифікат, який не відноситься до CompTIA; брати учать у заходах IT-індустрії; опублікувати статтю, технічний документ або допис у блозі або книзі; отримати відповідний досвід роботи; завершити курс Американської ради освіти.

3.4 Сертифікований тестувальник на проникнення (Pentest+)

Опис сертифікаційної програми

PenTest+ - сертифікація середнього рівня, зосереджена на тестуванні на проникнення. PenTest+ - це сертифікат для професіоналів з кібербезпеки, яким доручено тестування на проникнення та оцінка вразливостей та керування ними. CompTIA PenTest+ є сертифікацією кібербезпеки середнього рівня, яка зосереджується на наступальних навичках за допомогою ручного тестування й оцінювання вразливості.

Випущений 31 липня 2018 року, PenTest+ охоплює аналіз ризиків, виявлення загроз і тестування на проникнення, а також інструменти та методи етичного злому. PenTest+ акредитований за стандартами ANSI та ISO 17024 і наразі відповідає стандарту DOD 8570.

Вимоги до здобувача сертифікату

Для отримання статусу PenTest+ рекомендовано мати мінімум 3-4 роки практичного досвіду в галузі інформаційної безпеки або пов'язаного з цим. Хоча для цього немає жодних обов'язкових умов, PenTest+ призначений для роботи з CompTIA Security+ або еквівалентним досвідом і має практичну технічну

спрямованість. Здобувачам також бажано мати сертифікати Network+, Security+ або еквівалентні знання.

Цільова аудиторія курсу

Посади, які використовують CompTIA PenTest+:

- тестувальник на проникнення;
- консультант з безпеки;
- тестувальник проникнення хмар;
- тестувальник проникнення веб-додатків;
- фахівець із хмарної безпеки;
- спеціаліст з мережі та безпеки.

Структура курсу

Сертифікаційний курс PenTest+ складається з 5 модулів: планування та визначення обсягу; збір інформації та сканування вразливостей; атаки та експлойти; звітність та комунікації; інструменти та аналіз коду; планування та визначення обсягу (Рис. 3.4) [40].

Рис. 3.4. Структура сертифікаційного курсу PenTest+

Останнє оновлення курсу

Домени іспитів, охоплені CompTIA PenTest+ PT0-001 і PT0-002, не суттєво відрізняються, оскільки вони все ще мають відношення до посадових ролей, але деякі незначні зміни є. Зокрема, було змінено назву іспитового домену 2.0 із «Збір інформації та ідентифікація вразливостей» на «Збір інформації та сканування вразливостей». Також змінено порядок двох доменів – те, що раніше було 5.0 Reporting and Communication, тепер 4.0 (з такою ж назвою), а те, що раніше було інструментами тестування на проникнення 4.0, тепер 5.0 Tools and Code Analysis [41].

Умови проходження іспиту

CompTIA PenTest+ підтверджує, що кандидат володіє знаннями та навичками, необхідними для планування та масштабів тестування на проникнення, включаючи сканування вразливостей, розуміння юридичних вимог та вимог відповідності, аналізу результатів та створення письмового звіту з методами усунення.

Таблиця 3.4.

Загальна інформація про іспит PenTest+

Код іспиту	PT0-002
Дата випуску	28 жовтня, 2021р.
Кількість питань	85
Тип питань	Різноманітний вибір і на основі продуктивності
Тривалість іспиту	165 хвилин
Прохідний бал	700 балів(шкала від 100-900)
Мова іспиту	Англійська, Японська
Закінчення терміну дії	3 роки після випуску
Постачальник тестування	Pearson VUE Тестовий центр або онлайн тестування
Вартість	370$ USD

Термін дії сертифікату

Сертифікат CompTIA PenTest+ діє упродовж 3-річного терміну, а його власники зобов'язуються брати участь у програмі безперервної освіти, щоб поновити наявну сертифікацію.

Кредити безперервної освіти

Для сертифікату PenTest+ потрібно набрати 60 балів активності впродовж 3 років дії сертифікату. Для отримання балів потрібно виконати певні дії: Отримати сертифікат який не відноситься до CompTIA; брати учать у заходах, конференціях IT-індустрії; Опублікувати статтю, технічний документ або допис у блозі або книзі; Отримати відповідний досвід роботи; завершити курс Американської ради освіти [42].

3.5 Спільні й відмінні риси сертифікацій для фахівців з інформаційної безпеки від EC-Council та CompTIA

У підсумку порівняльної характеристики сертифікаційних програм з інформаційної безпеки EC-Council та CompTIA виділено такі їх *спільні риси*:

- схожі місії обох організацій;
- аналогічний порядок сертифікації;
- однакова кількість сертифікаційних програм з інформаційної безпеки;
- практична спрямованість підготовки в обох організаціях;
- ідентичні форми проходження сертифікаційного іспиту;
- однакові умови підтвердження актуальності сертифікату.

До *відмінних рис* віднесено такі:

- різна структура (рівні) сертифікаційних програм;
- вимоги щодо досвіду здобувача сертифікату;
- відмінні умови проходження, структура та мови сертифікаційного іспиту;
- разюча різниця у кількості сертифікованих фахівців з кібербезпеки;
- вартість сертифікаційного іспиту.

Детальна інформація подана у таблиці 3.5.

Таблиця 3.5

Порівняльна характеристика сертифікаційних програм для фахівців з інформаційної безпеки EC-Council та CompTIA

Критерій	EC-Council	CompTIA
Місія організації (сертифікації)	Підтвердження навичок та знань, необхідних фахівцям із інформаційної безпеки, які допоможуть запобігти кіберконфлікту, якщо виникне така потреба	Підтвердження наявності у здобувачів базових навичок, необхідних для виконання основних функцій у галузі безпеки IT, створення основи для зайняття ними позицій середнього рівня та побудови кар'єри у сфері ІБ.
Порядок сертифікації (етапи)	1. Вибір шляху до іспиту. 2. Навчання для сертифікаційного іспиту. 3. Реєстрація на сертифікаційний іспит. 4. Складання іспиту. 5. Підтримка актуальності сертифікату та його поновлення.	1. Вибір сертифікації. 2. Ознайомлення з обраною сертифікацією. 3. Навчання і підготовка до іспиту. 4. Реєстрація і складання іспиту. 5. Підтримка актуальності сертифікату
Структура (рівні) сертифікаційних програм	Базовий Просунутий Експертний	Початковий Середній Просунутий Експертний
Теоретична/ практична спрямованість підготовки	Практична спрямованість підготовки	Практична спрямованість підготовки
Основні сертифікації з ІБ	CEH, CND, ECIN	Security+, CySA+, PenTest+
Вимоги щодо досвіду здобувача	CEH, CND – 2 роки ECIN – 1 рік	Security+ - 2 роки CySA+, PenTest+ - 3-4 роки

Продовження табл. 3.5.

Умови здачі сертифікаційного іспиту	Пройти офіційний курс, отримати за нього ваучер до іспиту або Підтвердити 2 роки досвіду, заплатити внесок і купити ваучер.	Рекомендовано (необов'язково) пройти офіційний курс, отримати за нього ваучер до іспиту. Мати від 2 до 4-х років досвіду.
Структура іспиту (год, пит)	CEH - Курс складається з 20 модулів, іспит триває 4 години і складається з 125 запитань, прохідний бал від 60% до 85%. CND - Курс складається з 20 модулів, іспит триває 4 години, складається з 100 питань, прохідний бал - від 60% до 85%. ECIN - Курс складається з 9 модулів, іспит триває 3 години, складається зі 100 питань	Security+ - Курс складається з 4 модулів, іспит триває 90 хвилин і містить 90 питань, прохідний бал становить 700 (шкала від 100 до 900 балів). CySA+ - Курс складається з 5 модулів, іспит триває 165 хвилин і містить 85 питань, прохідний бал - 700 (шкала від 100 до 900 балів). PenTest+ - Курс складається з 5 модулів, іспит триває 165 хвилин і містить 85 питань, прохідний бал - 700 (шкала від 100 до 900 балів).
Форми проходження іспиту	Тестування офлайн в PearsonVUE або онлайн в особистому кабінеті EC-Council	Тестування офлайн в PearsonVUE або онлайн в особистому кабінеті CompTIA
Підтвердження актуальності сертифікату	Отримати120 кредитів упродовж 3-х років	Отримати 60 балів упродовж 3-х років
Кількість сертифікованих	220 тисяч фахівців з кібербезпеки	2,5 мільйони фахівців з кібербезпеки
Мова іспиту	Англійська	Англійська, японська
Вартість іспиту	CEH – 1199$ CND – 450$ ECIN – 100$	Security+ - 370$ CySA+ - 370$ PenTest+ - 370$

Висновки до розділу 3

Встановлено, що Асоціація галузі інформаційних технологій (Computing Technology Industry Association – CompTIA) - відома професійна організація, яка займається незалежною сертифікацією в галузі IT та інформаційної безпеки. CompTIA є нейтральною неурядовою організацією, яка працює в понад 120 країнах світу, є власником відомих сертифікаційних програм, серед яких Security+, CySA+, PenTest+ та інші. З часу створення організація сертифікувала 2,5 мільйонів фахівців з інформаційної безпеки у всьому світі.

Однією із найбільш популярних програм Асоціації CompTIA є міжнародна сертифікація Security+, яка підтверджує наявність у здобувача базових навичок, необхідних для виконання основних функцій у галузі безпеки IT і створює основу для зайняття ним позицій середнього рівня та побудови кар'єри в галузі інформаційної безпеки. Курс складається з 4 модулів, іспит триває 90 хвилин і містить 90 питань, прохідний бал становить 700 (шкала від 100 до 900 балів). Сертифікат Security+ дійсний 3 роки з моменту отримання.

CySA+ - це сертифікація IT-спеціалістів, які застосовують поведінкову аналітику до мереж і пристроїв для запобігання, виявлення та боротьби з загрозами кібербезпеки шляхом постійного моніторингу безпеки. Курс складається з 5 модулів, іспит триває 165 хвилин і містить 85 питань, прохідний бал становить 700 (шкала від 100 до 900 балів). Сертифікат CySA+ дійсний 3 роки з моменту отримання.

Затребуваним серед фахівців у сфері інформаційної безпеки є сертифікат PenTest+, який призначений для професіоналів з кібербезпеки середнього рівня і зосереджується на формуванні наступальних навичок за допомогою ручного тестування й оцінки вразливості. Курс складається з 5 модулів, іспит триває 165 хвилин і містить 85 питань, прохідний бал становить 700 (шкала від 100 до 900 балів). Сертифікат PenTest+ дійсний 3 роки з моменту отримання.

У підсумку порівняльної характеристики сертифікаційних програм з інформаційної безпеки EC-Council та CompTIA виділимо такі їх *спільні риси*:

схожі місії обох організацій; аналогічний порядок сертифікації; однакова кількість сертифікаційних програм з інформаційної безпеки; практична спрямованість підготовки в обох організаціях; ідентичні форми проходження сертифікаційного іспиту; однакові умови підтвердження актуальності сертифікату.

До *відмінних рис* віднесемо такі: різна структура (рівні) сертифікаційних програм; вимоги щодо досвіду здобувача сертифікату; відмінні умови проходження, структура та мови сертифікаційного іспиту; разюча різниця у кількості сертифікованих фахівців з кібербезпеки; вартість сертифікаційного іспиту.

ВИСНОВКИ

Основними організаціями які займаються сертифікацією фахівців з інформаційної безпеки є такі як: ISACA, GIAC, EC-Council, (ISC)², CompTIA. Важливими є сертифікати з тесту на проникнення, аналітика безпеки, цифрового криміналіста, менеджер інформаційної безпеки, аудитор інформаційних систем.

Процес сертифікації в організаціях Comptia та EC-Council мають незначні відмінності, в EC-Council безперервна освіта є обов'язковим кроком (пунктом) для отримання сертифікації, comptia в свою чергу не приділяє цьому питанню такої великої уваги та потреби, але це не означає що повторне підтвердження сертифікату не є обов'язковим. Фахівці або кандидати можуть здавати іспит як на офіційному сайті обраної сертифікації, або через спеціалізовані центри освіти.

Встановлено що у провідних організаціях CompTIA, EC-Council, ISACA, GIAC, (ISC)² проходить за такими типовими етапами: Вибір та ознайомлення з цілями і структурою обраної сертифікації, Підготовка та навчання до іспиту, Реєстрація і вибір форми проходження іспиту, Складання іспиту, Отримання сертифікату, Підтримка актуальності сертифікату та його поновлення.

Pearson VUE займає велику частку цього процесу, адже центр забезпечує необхідні умови для проведення надійного, якісного та справедливого для всіх електронного тестування. Описано переваги сертифікації для фахівців та компаній. В Україні працює 19 авторизованих центрів.

Міжнародна рада консультантів з питань електронної комерції (EC-Council) - це американська неурядова організація, яка надає послуги із сертифікації та навчання в галузі електронного бізнесу та кібербезпеки. EC-Council працює у 145 країнах по всьому світу, і є власником та розробником багатьох всесвітньо відомих сертифікаційних програм, серед яких CEH, CHFI, ECSA, CND та інші. За час свого існування організація навчила й сертифікувала понад 200 тисяч фахівців із інформаційної безпеки у всьому світі.

Сертифікований етичний хакер (CEH) – це кваліфікація, отримана шляхом демонстрації знань щодо оцінки безпеки комп'ютерних систем шляхом пошуку

слабких місць та вразливих місць у цільових системах, з використанням тих самих знань та інструментів, що і зловмисний хакер, але законним шляхом та законним чином для оцінки положення безпеки цільової системи. Курс складається з 20 модулів, іспит триває 4 години і складається з 125 запитань, прохідний бал від 60% до 85%. Термін дії сертифікату 3 роки, впродовж яких потрібно підтвердити його актуальність.

Сертифікований захисник мереж (CND) - це програма з інтенсивним лабораторним використанням навичок, що базується на освітній системі безпеки та аналізі робочих ролей, представлених Національною структурою компетенцій Infocomm (NICF). Програма готує мережевих адміністраторів, як визначити, які частини організації мають бути перевірені та перевірені на наявність уразливостей безпеки, а також як зменшити, запобігти та пом'якшити ризики в мережі. Курс складається з 20 модулів, іспит триває 4 години, складається з 100 питань, прохідний бал від 60% до 85%. Термін дії 3 роки.

E|CIH -це всебічна програма на рівні спеціалістів, яка передає знання та навички, необхідні організаціям для ефективного подолання наслідків після порушення, шляхом зменшення впливу інциденту, як з фінансової, так і з репутаційної точки зору. Курс складається з 9 модулів, іспит триває 3 години, складається 100 питанньь, термін дії 3 роки.

Встановлено, що Асоціація галузі інформаційних технологій (Computing Technology Industry Association – CompTIA) - відома професійна організація, яка займається незалежною сертифікацією в галузі IT та інформаційної безпеки. CompTIA є нейтральною неурядовою організацією, яка працює в понад 120 країнах світу, є власником відомих сертифікаційних програм, серед яких Security+, CySA+, PenTest+ та інші. З часу створення організація сертифікувала 2,5 мільйонів фахівців з інформаційної безпеки у всьому світі.

Однією із найбільш популярних програм Асоціації CompTIA є міжнародна сертифікація Security+, яка підтверджує наявність у здобувача базових навичок, необхідних для виконання основних функцій у галузі безпеки IT і створює основу для зайняття ним позицій середнього рівня та побудови кар'єри в галузі

інформаційної безпеки. Курс складається з 4 модулів, іспит триває 90 хвилин і містить 90 питань, прохідний бал становить 700 (шкала від 100 до 900 балів). Сертифікат Security+ дійсний 3 роки з моменту отримання.

CySA+ - це сертифікація IT-спеціалістів, які застосовують поведінкову аналітику до мереж і пристроїв для запобігання, виявлення та боротьби з загрозами кібербезпеки шляхом постійного моніторингу безпеки. Курс складається з 5 модулів, іспит триває 165 хвилин і містить 85 питань, прохідний бал становить 700 (шкала від 100 до 900 балів). Сертифікат CySA+ дійсний 3 роки з моменту отримання.

Затребуваним серед фахівців у сфері інформаційної безпеки є сертифікат PenTest+, який призначений для професіоналів з кібербезпеки середнього рівня і зосереджується на формуванні наступальних навичок за допомогою ручного тестування й оцінки вразливості. Курс складається з 5 модулів, іспит триває 165 хвилин і містить 85 питань, прохідний бал становить 700 (шкала від 100 до 900 балів). Сертифікат PenTest+ дійсний 3 роки з моменту отримання.

За результатами порівняльної характеристики сертифікаційних програм з інформаційної безпеки EC-Council та CompTIA виділимо такі їх *спільні риси*: схожі місії обох організацій; аналогічний порядок сертифікації; однакова кількість сертифікаційних програм з інформаційної безпеки; практична спрямованість підготовки в обох організаціях; ідентичні форми проходження сертифікаційного іспиту; однакові умови підтвердження актуальності сертифікату.

До *відмінних рис* сертифікаційних програм з інформаційної безпеки EC-Council та CompTIA віднесемо такі: різна структура (рівні) сертифікаційних програм; вимоги щодо досвіду здобувача сертифікату; відмінні умови проходження, структура та мови сертифікаційного іспиту; разюча різниця у кількості сертифікованих фахівців з кібербезпеки; вартість сертифікаційного іспиту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cybersecurity certifications for professionals. URL: https://cybersecurityguide.org/programs/cybersecurity-certifications/#Professional (дата звернення: 12.10.2021).

2. Cybersecurity certification programs for students. URL: https://cybersecurityguide.org/programs/cybersecurity-certifications/#Academic (дата звернення: 12.10.2021).

3. Abou us ISC^2. URL: https://www.isc2.org/about (дата звернення: 12.10.2021).

4. ISC^2 CISSP Certification. URL: https://www.isc2.org/Certifications/CISSP (дата звернення: 12.10.2021).

5. ISC^2 SSCP Certification. URL: https://www.isc2.org/Certifications/SSCP (дата звернення: 12.10.2021).

6. ISC^2 CCSP Certification. URL: https://www.isc2.org/Certifications/CCSP (дата звернення: 12.10.2021).

7. ISACA. About us. URL: https://www.isaca.org/why-isaca/about-us (дата звернення: 12.10.2021).

8. CiSA Certification. URL: https://www.isaca.org/credentialing/cisa (дата звернення: 12.10.2021).

9. ISACA Homepage. URL: https://www.isaca.org/ (дата звернення: 12.10.2021).

10. Cyber Security Training, Certifications, Degrees and Resources. URL: https://www.sans.org/ (дата звернення: 12.10.2021).

11. GIAC Security Essentials (GSEC). URL: https://www.giac.org/certification/security-essentials-gsec (дата звернення: 12.10.2021).

12. GIAC Mobile Device Security Analyst (GMOB). URL: https://www.giac.org/certification/mobile-device-security-analyst-gmob (дата звернення: 12.10.2021).

13. GIAC Certified Forensic Analyst (GCFA). URL: https://www.giac.org/certification/certified-forensic-analyst-gcfa (дата звернення: 12.10.2021).

14. How to get a CEH certification? URL: https://www.umbctraining.com/how-to-get-a-ceh-certification/ (дата звернення: 12.10.2021).

15. 4 Steps to Certification by CompTIA. URL: https://www.comptia.org/certifications/4-steps-to-certification (дата звернення: 12.10.2021).

16. Pearson VUE. About. URL: https://home.pearsonvue.com/About.aspx (дата звернення: 12.10.2021).

17. Авторизований центр тестування VUE. URL: https://itea.ua/uk/testing_and_certification/ (дата звернення: 12.10.2021).

18. EC-Council. About us. URL: https://www.eccouncil.org/about/ (дата звернення: 12.10.2021).

19. Post-9/11 GI Bill (Chapter 33). URL: https://www.va.gov/education/about-gi-bill-benefits/post-9-11/ (дата звернення: 26.10.2021).

20. Cyber-Handbook-Enterprise 2017. URL: https://www.eccouncil.org/wp-content/uploads/2017/05/Cyber-Handbook-Enterprise.pdf. (дата звернення: 26.10.2021).

21. Cyber-Handbook-Enterprise 2018. URL: https://www.eccouncil.org/wp-content/uploads/2017/05/Cyber-Handbook-Enterprise.pdf (дата звернення: 26.10.2021).

22. EC-Council CEH Certification. URL: https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/ (дата звернення: 26.10.2021).

23. Global training partners EC-Council. URL: http://www.eccouncil.org/Support/global-sites/global-training-partners (дата звернення: 26.10.2021).

24. CEH v11 Brochure. URL: https://www.eccouncil.org/wp-content/uploads/2020/09/CEHv11-Brochure.pdf (дата звернення: 26.10.2021).

25. Certification agreement for members. URL: https://www.eccouncil.org/members/Certification/agreement.pdf (дата звернення: 26.10.2021).

26. EC-Council Certified Network Defender (CND). URL: https://www.cedsolutions.com/1325/certification/ec-council-cnd-cyber-security-training (дата звернення: 26.10.2021).

27. EC-Council iclass! URL: https://iclass.eccouncil.org (дата звернення: 26.10.2021).

28. ECIH v2 released by EC-Council (Certified Incident Handler). URL: https://blog.firebrand.training/2019/02/ec-council-releases-ecih-v2-certified.html (дата звернення: 26.10.2021).

29. What are continuing education units (CEUS) and why do you need them? URL: https://intellectualpoint.com/what-are-continuing-education-units/ (дата звернення: 26.10.2021).

30. CompTIA's Update Ready to Install. URL: https://sync-magazine.com/2015/comptia/ (дата звернення: 09.11.2021).

31. ABCD-to-CompTIA-explaining-the-history-of-comptia-security-training. URL: http://theartofservice.com/abcd-to-comptia-explaining-the-history-of-comptia-security-training.html (дата звернення: 09.11.2021).

32. CompTIA Opts for New Open-Access Membership Model. URL: https://associationsnow.com/2014/04/comptia-opts-new-open-access-membership-model/ (дата звернення: 09.11.2021).

33. Advancing Women in Technology. AWIT Career Resource Center. URL: https://associationsnow.com/2014/04/comptia-opts-new-open-access-membership-model/ (дата звернення: 09.11.2021).

34. CompTIA ChannelCon 2016 Vendor Summit Examines How To Thrive In The IT Channel. URL: https://www.varinsights.com/doc/comptia-channelcon-vendor-summit-examines-channel-0001 (дата звернення: 09.11.2021).

35. CompTIA launches professional association to help fill skills gap in IT. URL: https://www.techrepublic.com/article/comptia-launches-professional-association-to-help-fill-skills-gap-in-it/ (дата звернення: 09.11.2021).

36. CompTIA Security+ URL: CompTIA Security+. URL: https://www.comptia.org/certifications/ security (дата звернення: 09.11.2021).

37. CompTIA Certification Guide: Overview and Career Paths. URL: https://www.businessnewsdaily.com/10718-comptia-certification-guide.html (дата звернення: 09.11.2021).

38. CompTIA countinuing education. URL: https://www.comptia.org/continuing-education/choose/renewing-with-multiple-activities/training-and-higher-education (дата звернення: 09.11.2021).

39. The CySA+ knowledge domains. URL: https://resources.infosecinstitute.com/ certification/the-cysa-plus-knowledge-domains/ (дата звернення: 09.11.2021).

40. CompTIA PenTest+ Certification Exam Objectives. URL: https://partners.comptia.org/docs/default-source/resources/comptia-pentest-pt0-002-exam-objectives-(4-0) (дата звернення: 09.11.2021).

41. CompTIA PenTest+ PT0-001 vs. PT0-002: What's the Difference? URL: https://www.comptia.org/blog/comptia-pentest-001-vs-002 (дата звернення: 09.11.2021).

42. Training and Higher Education CompTIA. URL: https://www.comptia.org/continuing-education/choose/renewing-with-multiple-activities/training-and-higher-education (дата звернення: 09.11.2021).

43. Балабанова Л.В., Сардак О.В. Управління персоналом: навч. посіб. К.: Центр учбової літератури, 2011. 468 с.

44. Богданович В.Ю., Романченко І.С., Свида І.Ю. Теоретичні основи забезпечення національної безпеки України в умовах позаблоковості: монографія. Львів.: АСВ. 2011. 414 с.

45. Информационная безопасность: Учебное пособие. Ясенев В.Н., Дорожкин А.В., Сочков А.Л., Ясенев О.В. Под общей редакцией проф. Ясенева В.Н. Нижний Новгород: Нижегородский госуниверситет им. Н.И. Лобачевского, 2017. 198 с.

46. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2005, MOD). ГСТУ СУІБ 1.0/ISO/IEC 27001:2010. К.: Національний банк України. 2010. 49 с.

47. Нехай В.А., Нехай В.В. Інформаційна безпека як складова економічної безпеки підприємств. Науковий вісник Міжнародного гуманітарного університету. 2017. №1. С.137-140. URL: http://www.vestnik-econom.mgu.od.ua/journal/2017/24-2-2017/30.pdf (дата звернення: 09.11.2021).

48. Обеспечение информационной безопасности бизнеса / В. В. Андрианов, С. Л. Зефиров, В. Б. Голованов и др. 2-е, перераб. и доп. М. : ЦИПСиР, 2011. 373 с.

49. Северина С.В. Інформаційна безпека та методи захисту інформації. Вісник Запорізького національного університету. 2016. № 1 (29). С.155-161.

50. Сороковская А. А. Информационная безопасность предприятия : новые угрозы и перспективы. URL: http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon /2010_2_2/032-035.pdf (дата звернення: 09.11.2021).

51. Бурячок В.Л., Киричок Р.В., Складанний П. М. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. К. 2018. 320 с.

52. Васильєв Ю. Класифікація та аналіз загроз інформаційній безпеці в ключових системах інформаційної інфраструктури Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2015. Вип. 1 (29). С.56-61.

53. Герасименко О. В. Інформаційна безпека підприємства: поняття та методи її забезпечення. URL: http://intkonf.org/ken-gerasimenko-ov-kozak-avinformatsiyna-bezpeka-pidpriemstva-ponyattyata-metodi-yiyi-zabezpechennya (дата звернення: 28.05.2020)

54. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. К., 2009. 608 с.

55. ДСТУ ISO 19011:2012 Настанови щодо здійснення аудитів систем управління (ISO 19011:2011, IDT). К.: Мінекономрозвитку України, 2013. 34 с.

56. Єжова Л.Ф., Корченко А.О., Мачалін І.О., Скачек Л.М., Хорошко В.О. Управління інформаційною безпекою. В 2-х томах. Видання друге, доповнене та перероблене. Том 2. К. 2012. 347 с.

57. Желіховський В.М., Ліпкан В.А., Максименко Ю.Є. Інформаційна безпека України в умовах євроінтеграції: Навчальний посібник. К.: КНТ. 2006. 280 с.

58. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. М.: Логос; ПБОЮЛ Н.А. Егоров. 2001. 264 с.

59. Захарченко М.В., Кононович В.Г., Кільдішев В.Й., Голев Д.В. Інформаційна безпека інформаційно-комунікаційних систем. Лабораторний практикум. Частина 1. Комплекси засобів захисту інформації від НСД: навч. посіб. За ред. ак. МАІ М.В. Захарченка. Одеса: ОНАЗ ім. О.С. Попова, 2011. 168 с.

60. Інформаційна безпека підприємства. Основні положення та ввідні поняття URL: http://stud.com.ua/21678/ekonomika/informatsiyna_bezpeka_pidpriyemstva (дата звернення: 09.11.2021)

61. Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD). ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. К.: Національний банк України. 2010. 163 с.

62. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2005, MOD). ГСТУ СУІБ 1.0/ISO/IEC 27001:2010. К.: Національний банк України. 2010. 49 с.