ТЕХНІЧНИЙ ОПИС КОМПЕТЕНЦІЇ

Кібербезпека

\

1. ВСТУП

1.1. НАЗВА ТА ОПИС ПРОФЕСІЙНОЇ КОМПЕТЕНЦІЇ

1.1.1 Назва професійної компетенції:

Кібербезпека.

1.1.2 Опис професійної компетенції.

Спеціаліст з кібербезпеки - популярна в даний час та перспективна професія, сфера діяльності якої відноситься до інформаційної безпеки, що активно розвивається. Участь у профілактичних дослідженнях об'єктів захисту з метою пошуку вразливостей до атак на захищеність і цілісність даних, працездатність комп'ютерних систем та інформаційних сервісів, Налаштування системного програмного забезпечення та обладнання для забезпечення максимальної захищеності від зовнішніх загроз, розслідування інцидентів в області інформаційної безпеки, усунення їх наслідків і вироблення рекомендацій щодо їх недопущення в майбутньому складають основні завдання фахівця. Правила охорони праці та техніка безпеки при роботі з комп'ютерною технікою, враховуючи напружений робочий ритм фахівця, також відіграють важливу роль в професії. Щоденне вдосконалення навичок і тренування швидкого вирішення типових завдань з пошуку та усунення вразливостей серверів, комп'ютерних мереж, програмного забезпечення, в тому числі і методом прямого аналізу їх програмного коду – є запорукою зростання в професії. Робоча діяльність фахівця з інформаційної безпеки тісно пов'язана з іншими професіями в області інформаційних технологій, утворюючи єдиний технологічний ланцюжок з розробки та підтримки програмного і технічного забезпечення обчислювальних систем і комплексів. Використовуючи спеціальне програмне забезпечення, застосовуючи знання основних технологій забезпечення інформаційної безпеки, вміючи інсталювати, налаштовувати і адмініструвати комп'ютерні системи і програми, володіючи навичками щодо запобігання і розслідування інцидентів і аналізу вихідного коду, фахівець вирішує завдання в інтересах свого

роботодавця або замовника. У своїй роботі він використовує як внутрішнє законодавство, так і міжнародні правові юридичні норми і стандарти в області інформаційної безпеки, організації комп'ютерних мереж і обчислювальних систем. Аналізуючи інформаційні ресурси і сервіси, що не належать йому, фахівець з інформаційної безпеки виявляє притаманні йому високі морально-етичні принципи, що не дозволяють йому виконати свою роботу неякісно і несанкціоновано розпорядитися отриманим доступом до будь-яких даних, що не належать йому. Незалежно від того, працює він один або в команді, фахівець максимально орієнтований на максимальний результат, використовує системний підхід для аналізу поставлених перед ним завдань, планує і організовує свою діяльність, координуючи її з іншими співробітниками, або підкоряючись директивам керівництва і внутрішнім нормам організації.

1.2. ВАЖЛИВІСТЬ І ЗНАЧЕННЯ ЦЬОГО ДОКУМЕНТА

Технічний опис містить інформацію про обов'язкові стандарти і вимоги, що висуваються до учасників змагань, а також регламентують змагання з даної компетенції принципи, методи і процедури.

Кожен експерт і учасник, незалежно від свого статусу, повинен знати і розуміти даний Технічний опис.

2. СПЕЦИФІКАЦІЯ СТАНДАРТУ WORLDSKILLS (WSSS)

2.1. ЗАГАЛЬНІ ВІДОМОСТІ ПРО СПЕЦИФІКАЦІЇ СТАНДАРТІВ WORLDSKILLS (WSSS)

WSS визначає знання, розуміння і конкретні навички, які лежать в основі кращих міжнародних практик технічного і професійного рівня виконання роботи з точки зору демонстрації результатів технічної та додаткової освіти. Дані специфікації повинні відображати глобальне КОЛЕКТИВНЕ розуміння того, що

всі роботи, асоційовані з певними посадовими позиціями, повинні бути пов'язані з виробництвом або бізнесом.

Змагання з компетенції призначене для придбання та демонстрації кращої практики з навичок, описаних в WSSS в тій мірі, в якій вони можуть бути реалізовані. Стандартні специфікації — це керівництво, необхідне для навчання і підготовки до участі в змаганні.

Основна значущість специфікації визначена трьома складовими:

- основа завдань для конкурсу WorldSkills, які встановлюють базовий рівень навичок за професією, за результатами виконання яких можна визначити справжню роботу професіонала:
- дає можливість визначити розвиток національних і регіональних стандартів для членів руху WorldSkills і не тільки;
- в умовах глобалізації економіки і ринків специфікація дає можливість молодим людям і дорослим виживати і процвітати в сучасному світі.

Під час змагань оцінка знань і навичок буде проводитися через оцінку виконання конкурсних завдань. Окремих теоретичних тестів для оцінки знань і навичок не проводиться.

Стандартні специфікації поділяються на чіткі розділи з номерами і заголовками. Кожному розділу призначено відсоток відносної важливості в рамках WSSS. Сума всіх відсотків відносної важливості становить 100.

Конкурсне завдання повинно оцінювати тільки ті навички, які вказані в WSSS. Схема оцінки і конкурсне завдання повинні слідувати розподілу оцінок в межах процентних норм WSSS і відображати WSSS настільки всебічно і в максимально можливій мірі, наскільки допускають обмеження змагання по компетенції. Допускається варіативність такого розподілу не більше ніж в 5% за умови, що це не спотворює пропорції, присвоєні WSSS.

Єдина система WSSS "WORLDSKILLS STANDARDS SPECIFICATION" дозволяє провести наскрізний аналіз ступеня оволодіння учасниками даної професії. Це можливо тільки в тому випадку, якщо будь-яке конкурсне завдання

складається, а оцінка результатів його виконання проводиться відповідно до вимог WSSS. Кожен розділ WSSS має вагову характеристику і в сумі дає 100 балів.

2.2. WSS КОМПЕТЕНЦІЇ

РОЗДІЛ		ВАЖЛИВІСТЬ
1	**ОРГАНІЗАЦІЯ РОБОТИ**	**3%**
	Спеціаліст повинен знати і розуміти • Документацію та правила з охорони праці та техніки безпеки. • Важливість підтримки робочого місця в належному стані. • Значимість планування всього робочого процесу, способи організації ефективної роботи і розподілу робочого часу. • Принципи і практики, які дозволяють продуктивно працювати в команді. • Аспекти систем, які дозволяють підвищити продуктивність і виробити оптимальну стратегію роботи. • Вплив нових технологій на організацію роботи.	
	Спеціаліст повинен вміти • Виконувати вимоги з охорони праці та техніки безпеки. • Організовувати робоче середовище для максимально ефективної роботи. • Швидко вирішувати поширені типові завдання в області інформаційної безпеки. • Враховувати тимчасові обмеження і терміни при організації своєї діяльності і планувати графік робочого дня. • Ефективно використовувати відведений для роботи час і обчислювальні ресурси в рамках обмежень. • Використовувати сучасні інструментальні та програмні засоби для здійснення своєї діяльності. • Відстежувати сучасні тенденції індустрії і враховувати їх у своїй діяльності. • Аналізувати вимоги до результату і особливі умови здійснення діяльності. • Працювати в умовах постійно змінної ситуації. • Представляти результат своєї роботи в необхідному вигляді.	
2	**КОМУНІКАЦІЙНІ ТА ОСОБИСТІ НАВИЧКИ**	**4%**
	Спеціаліст повинен знати і розуміти • Принципи, що лежать на основі збору та подання інформації. • Способи аналізу та оцінки інформації з різних джерел. • Способи і технології роботи з інформацією в умовах її неповноти або обмеженості часу.	

	• Термінологію у сфері інформаційної безпеки. • Основні вимоги до письмової та усної ділової комунікації. • Важливість підтримки знань на високому рівні і вміння їх використовувати для аналізу завдань і представлення результату. • Важливість вміння вирішувати конфліктні ситуації і непорозуміння. • Основні вимоги до суміжних професій і специфіку діяльності їх представників. • Способи подання інформації в наочному графічному вигляді..	
	Спеціаліст повинен вміти • Збирати, аналізувати і оцінювати інформацію. • Коректно тлумачити і вживати професійну термінологію в залежності від ситуації. • Розуміти і виконувати пред'являються вимоги як до результату, так і до процесу трудової діяльності. • Доносити результат своєї професійної діяльності до інших людей, в тому числі неспеціалістів в області інформаційної безпеки. • Планувати спілкування з іншими людьми і презентувати результати своєї роботи. • Враховувати вимоги і завдання до результату своєї діяльності. • Користуватися сучасними текстовими і графічними редакторами з метою письмової комунікації. • Критикувати свої ідеї і результат своєї професійної діяльності. • Складати звіти за результатами своєї професійної діяльності. • Консультувати фахівців і неспеціалістів в області інформаційної безпеки з професійних питань. • Реагувати на заявки систем масового обслуговування.	
3	**ПРОФЕСІЙНА ЕТИКА**	**6%**
	Спеціаліст повинен знати і розуміти • Юридичні аспекти професійної діяльності. • Основні професійні норми і стандарти. • Професійну етику. • Важливість зберігання конфіденційної інформації в таємниці. • Соціальну та юридичну відповідальність за свої дії та бездіяльності.	
	Спеціаліст повинен вміти • Працювати з юридичною літературою і знаходити необхідні норми. • Застосовувати юридичні норми у своїй професійній діяльності.. • Забезпечувати конфіденційність даних. • Домагатися максимально якісного результату роботи незалежно від будь-яких умов.	
4	**ТЕХНОЛОГІЇ**	**6%**
	Спеціаліст повинен знати і розуміти • Архітектуру і принципи функціонування ЕОМ. • Принципи організації роботи операційних систем. • Принципи роботи СУБД та основи забезпечення їх безпеки. • Принципи віртуалізації.	

	• Принципи організації локальних і глобальних обчислювальних мереж. • Основні протоколи передачі даних і мережеві технології. • Основні мови програмування. • Можливості антивірусного програмного забезпечення.	
	Спеціаліст повинен вміти • Адмініструвати операційні системи, СУБД, веб-сервера, поштові сервера, проксі. • Налаштовувати міжмережеві екрани, маршрутизатори, мережеве обладнання та програмне забезпечення. • Створювати і використовувати віртуальні машини. • Налаштовувати продуктивність файлових систем, працювати з кластерними файловими системами, організовувати RAID-масиви. • Налаштовувати віртуальні приватні мережі. • Організовувати віддалений доступ до ресурсів. • Відновлювати дані з резервних копій. • Аналізувати програмний код на мовах веб-розробки і розробляти програмне забезпечення на них. • Інсталювати і налаштовувати операційні системи і програмне забезпечення. • Автоматизувати завдання.	
5	**ПОШУК ВРАЗЛИВОСТЕЙ**	**26%**
	Спеціаліст повинен знати і розуміти • Різні методології пошуку вразливостей інформаційних ресурсів, комп'ютерних мереж і додатків. • Популярні методи атак з боку зловмисників. • Знайдені і опубліковані критичні уразливості в операційних системах і серверах. • Особливості використання різних сканерів безпеки. • Методологію складання звіту про проведений пошук вразливостей. • Основні способи захисту вид атак на типові уразливості додатків.	
	Спеціаліст повинен вміти • Працювати зі сканерами вразливостей. • Самостійно перевіряти технічні засоби і налаштування мережевого і серверного програмного забезпечення на наявність вразливостей. • Тестувати інформаційні системи і сервера на наявність відомих і широко поширених вразливостей. • Аналізувати програмний код веб-сервісів на наявність вразливостей. • Тестувати програмне забезпечення, в тому числі і веб-додатки, на наявність потенційних і прихованих вразливостей. • Ідентифікувати загрози і уразливості інформаційних систем і додатків. • Аналізувати цілісність даних СУБД.	
6	**АНАЛІЗ ЗАХИЩЕНОСТІ**	**22%**
	Спеціаліст повинен знати і розуміти	

	• Способи та рекомендації щодо обстеження об'єктів захисту та узагальнення даних про їх стан. • Галузеві та міжгалузеві індустріальні стандарти, а також інші внутрішні та міжнародні нормативні документи в галузі інформаційної безпеки. • Загальноприйняті класифікації загроз інформаційній безпеці. • Типові причини атак на інформаційні ресурси і системи, їх наслідки. • Основні способи захисту інформаційних систем, в тому числі і веб-додатків, забезпечення безпеки і цілісності даних від атак зловмисників. • Склад і актуальність останніх оновлень операційних систем і програмного забезпечення для забезпечення інформаційної безпеки.	
	Спеціаліст повинен вміти • Аналізувати існуючі методи та засоби забезпечення інформаційної безпеки та пропонувати заходи щодо їх вдосконалення та розвитку. • Збирати інформацію по IT-інфраструктурі об'єкта захисту з метою вироблення і прийняття рішень і заходів щодо захисту інформації. • Застосовувати аналізатори захищеності веб-додатки, включаючи онлайн-сервіси оцінки захищеності. • Контролювати стан об'єкта захисту, в тому числі і в частині дотримання загальноприйнятих або задокументованих в стандартах правил і норм. • Оцінювати ризики інформаційної безпеки використовуючи класифікації веб-загроз. • Розробляти моделі загроз і порушника. • Складати звіти та організаційно-розпорядчу документацію за результатами обстеження. • Розробляти рекомендації щодо підвищення рівня захищеності.	
7	**АДМІНІСТРУВАННЯ**	**10%**
	Спеціаліст повинен знати і розуміти • Принципи функціонування, способи налаштування і управління різними операційними системами і серверами. • Правила монтажу, способи налагодження та налаштування мережевого обладнання та програмного забезпечення. • Правила організації моніторингу безпеки, зберігання журналів подій. • Основні причини компрометації безпеки операційних систем, серверів і програмного забезпечення, а також способи їх запобігання. • Способи організації доступу до віддалених ресурсів. • Важливість своєчасного оновлення версій і захисту від знайдених вразливостей. • Методи підвищення захищеності операційних систем і серверів.	
	Спеціаліст повинен вміти • Супроводжувати розробку інформаційних систем в частині питань інформаційної безпеки на всіх стадіях.	

	• Інсталювати операційні системи, сервера та інше програмне забезпечення на технічні засоби. • Встановлювати і налаштовувати безпечну конфігурацію операційної системи, серверів і програмного забезпечення з урахуванням пропонованих вимог. • Адмініструвати IT-інфраструктуру, в тому числі і віддалено. • Конфігурувати і контролювати стан технічних систем, усувати виникаючі проблем. • Розмежовувати права користувачів і налаштовувати безпечний доступ до операційних систем, серверів і програмного забезпечення. • Використовувати штатні та спеціальні засоби моніторингу безпеки операційних систем. • Застосовувати засоби безпечного віддаленого моніторингу та конфігурування операційних систем, серверів і програмного забезпечення. • Отримувати, інсталювати і відстежувати роботу з SSL-сертифікатами. • Налаштовувати і контролювати Засоби захисту інформації відповідно до вимог політик інформаційної безпеки.	
8	**КРИПТОГРАФІЯ**	**8%**
	Спеціаліст повинен знати і розуміти • Основні категорії безпеки інформації та роль криптографії в них. • Принципи криптографії з закритим і відкритим ключем. • Роль шифрування і основні області його застосування в додатках. • Основні властивості криптографічних протоколів, що використовуються в інтернеті. • Методи оцінки стійкості криптографічних алгоритмів і протоколів. • Галузеві стандарти і законодавство, що регулює використання криптографії, в тому числі шифрування і електронних підписів.	
	Спеціаліст повинен вміти • Вибирати і конфігурувати використовувані протоколи відповідно до їх призначення та вимог законодавства. • Працювати з системними утилітами операційних систем, що реалізують криптографічні протоколи. • Створювати відкриті, закриті ключі, сертифікати і налаштовувати на коректну роботу використовують їх протоколи і утиліти. • Взаємодіяти з іншими фахівцями з питань криптографічного захисту інформації. • Використовувати спеціальні засоби криптографічного захисту інформації та застосування електронного підпису. • Захищати канали зв'язку за допомогою криптографічних методів на базі різних програмних продуктів в області безпеки..	
9	**РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ**	**15%**
	Спеціаліст повинен знати і розуміти • Основні методи збору інформації для розслідування інциденту.	

	• Юридичні аспекти розслідування інцидентів, збору та подання доказової бази. • Типову мотивацію порушників.	
	Спеціаліст повинен вміти • Використовувати основні методи та інструменти розслідування інцидентів. • Визначити склад юридично значущої законодавчої бази. • Здійснювати моніторинг та аналіз інцидентів інформаційної безпеки, в тому числі і аналіз системних журналів і логів. • Контролювати витоку інформації обмеженого доступу. • Формувати рекомендації щодо усунення загрози на підставі розслідування інциденту. • Створювати звіт про розслідування.	

3. ОЦІНОЧНА СТРАТЕГІЯ І ТЕХНІЧНІ ОСОБЛИВОСТІ ОЦІНКИ

3.1. ОСНОВНІ ВИМОГИ

Стратегія встановлює принципи і методи, яким повинні відповідати оцінка і нарахування балів.

Експертна оцінка лежить в основі змагань. З цієї причини вона є предметом постійного професійного вдосконалення і ретельного дослідження. Накопичений досвід в оцінці визначатиме майбутнє використання і напрямок розвитку основних інструментів оцінки, що застосовуються на змаганнях: схема виставлення оцінки та конкурсне завдання.

Схема виставлення оцінки повинна відповідати відсотковим показникам в WSSS. Конкурсне завдання є засобом оцінки для змагання за компетенцією, воно також має відповідати WSSS.

Схема виставлення оцінки в загальних рисах є визначальним фактором для процесу розробки Конкурсного завдання. У процесі подальшої розробки Схема виставлення оцінки і конкурсне завдання будуть розроблятися і розвиватися за допомогою ітеративного процесу для того, щоб спільно оптимізувати взаємозв'язки в рамках WSSS і стратегії оцінки.

3.2. ВИМОГИ ДО КВАЛІФІКАЦІЇ

На змаганнях учасники демонструють, а експерти оцінюють компетенції у вищевказаній предметній галузі. Конкурсне завдання складається виключно з практичної роботи. Конкурс проводиться для демонстрації та оцінки кваліфікації в даному виді майстерності. Конкурсне завдання складається тільки з практичних завдань.

3.3. ТЕОРЕТИЧНІ ЗНАННЯ

Теоретичні знання необхідні, але вони не піддаються явній перевірці. Знання стандартів, правил і юридичних норм в явному вигляді не перевіряється. Знання правил і норм WSR мається на увазі і є необхідним для участі в змаганнях, але ніяк не оцінюється.

3.4. ПРАКТИЧНА РОБОТА

Практична робота може становити як вирішення кількох окремих завдань, так і виконання одного комплексного завдання. В ході виконання практичної роботи Конкурсант повинен показати вміння та навички пошуку вразливостей, безпечного конфігурування, розслідування інцидентів, а також інші професійні вміння, які оцінюються відповідно до WSSS.

4. СХЕМА ВИСТАВЛЕННЯ ОЦІНКИ

4.1. ЗАГАЛЬНІ ОЦІНКИ

Схема виставлення оцінки є основним інструментом змагань WSR, визначаючи відповідність оцінки Конкурсного завдання та WSSS. Вона призначена для розподілу балів по кожному оцінюваному аспекту, який може відноситися тільки до одного модулю WSSS.

У розділі 2.1 вказано максимально допустимий відсоток відхилення, схеми виставлення оцінки Конкурсного завдання від пайових співвідношень, наведених у специфікації стандартів.

Схема виставлення оцінки та конкурсне завдання можуть розроблятися однією людиною, групою експертів або Стороннім розробником. Детальна і остаточна Схема виставлення оцінки та конкурсне завдання, повинні бути затверджені Менеджером компетенції.

Крім того, всім експертам пропонується представляти свої пропозиції щодо розробки Схем виставлення оцінки та конкурсних завдань на форум експертів для подальшого їх розгляду Менеджером компетенції.

У всіх випадках повна і затверджена Менеджером компетенції Схема виставлення оцінки повинна бути введена в інформаційну систему змагань (CIS) не менше ніж за два дні до початку змагань, з використанням стандартної електронної таблиці CIS або інших узгоджених способів. Головний експерт є відповідальним за даний процес.

4.2. КРИТЕРІЇ ОЦІНКИ

Критерії оцінки збігаються з відповідними розділами специфікації WSS. Нижче наведено приклад призначення критеріїв оцінки та кількості виставлених балів (об'єктивні та суддівські). Загальна кількість балів за всіма критеріями оцінки становить 100, якщо в ході чемпіонату виконуються не всі модулі Конкурсного завдання-максимально можливий бал оцінки всього завдання повинен бути зменшений на відповідне відсутньому модулю значення.

Критерії			Завдання		
	Назва	Важливість	Модуль 1	Модуль 2	Модуль 3
A	ОРГАНІЗАЦІЯ РОБОТИ	**3**	1	1	1
B	КОМУНІКАЦІЙНІ ТА ОСОБИСТІСНІ НАВИЧКИ	**4**	2		2
C	ПРОФЕСІЙНА ЕТИКА	**6**	2	2	2
D	ТЕХНОЛОГІЯ	**6**	2	4	
E	ПОШУК ВРАЗЛИВОСТЕЙ	**26**	16	7	3
F	АНАЛІЗ ЗАХИЩЕНОСТІ	**22**	15	4	3
G	АДМІНІСТРУВАННЯ	**10**		10	

H	КРИПТОГРАФІЯ	**8**		8	
I	РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ	**15**			15
ПІДСУМОК		**100**	**38**	**36**	**26**

У разі меншої тривалості виконання Конкурсного задавання в який-небудь з модулів, на відповідний модуль відводиться менша кількість балів.

Кожен аспект оцінюють три експерта, кожен експерт повинен провести оцінку, після чого відбувається порівняння виставлених оцінок. У разі розбіжності оцінок експертів більш ніж на 1 бал, експертам необхідно винести оцінку даного аспекту на обговорення і усунути розбіжність.

4.3. СПЕЦИФІКАЦІЯ ОЦІНКИ КОМПЕТЕНЦІЇ

Оцінка Конкурсного завдання ґрунтуватиметься на зазначених у розділі 4.2. критеріїв. Оцінка кожного модуля може здійснюватися як за всіма, так і за частиною критеріїв.

4.4 СИСТЕМА ШТРАФІВ

У разі порушення учасниками та / або експертами вимог Кодексу етики, регламенту змагань, умов даного технічного опису, вимог Конкурсного завдання, до них можуть бути застосовані штрафні санкції, включаючи видалення з майданчика і анулювання результатів за модуль, за день, за всі дні.

5. КОНКУРСНЕ ЗАВДАННЯ

5.1. ОСНОВНІ ВИМОГИ

Віковий ценз учасників для виконання Конкурсного завдання визначається діючими на змагальному майданчику нормами і правилами техніки безпеки, Режимом охорони праці. Оцінка знань учасника повинна проводитися виключно через практичне виконання Конкурсного завдання.

Конкурсне завдання є закритим для учасників чемпіонатів, зразкове завдання по кожному модулю, включаючи використовувані технології і

одержуваний результат, публікується за два місяці до чемпіонату. Остаточне завдання, що відповідає чинному технічному опису компетенції, надається учасникам в день змагань. Виняток можуть становити закриті модулі, знання змісту яких навіть за кілька днів до початку їх виконання, може критично вплинути на валідність оцінки результату. У цьому випадку завдання надається учасникам для ознайомлення безпосередньо перед виконанням модуля – при цьому час на ознайомлення Конкурсанта із завданням не повинно бути менше 15 хвилин.

5.2. СТРУКТУРА КОНКУРСНОГО ЗАВДАННЯ

Конкурсне завдання являє собою серію з трьох незалежних між собою модулів з сумарною тривалістю робочого часу 12 годин, для виконання яких відводиться три дні. Кожен модуль повинен виконуватися:

- до обіду без перерви і подальших доопрацювань;
- після обіду без перерви і наступних доопрацювань;
- один день (до і після обіду) з перервою на обід, без подальших доопрацювань.

Кожен день виконується не більше двох модулів. Кожен модуль оцінюється окремо, за підсумками його завершення. Метою кожного модуля є перевірка всіх умінь і навичок WSSS з розділу 2.2. - таким чином конкурсне завдання має включати оцінку по кожному з розділів WSSS, але не виходити за його межі.

Нижче наведено приклад Конкурсного завдання, що складається з трьох модулів.

МОДУЛЬ	ЧАС РОБОТИ	ОПИС
АУДИТ БЕЗПЕКИ	до і після обіду: 4 години, без	Для наданих одного або декількох інформаційних ресурсів (наприклад, веб-сайтів) проводиться пошук вразливостей, аналіз захищеності та пропонуються заходи щодо її підвищення. Результатом виконання є звіт із зазначенням типом

	урахування часу на обід і брифінг	знайдених вразливостей, можливих загроз і сформованих рекомендацій.
БЕЗПЕЧНА КОНФІГУРАЦІЯ	до і після обіду: 4 години, без урахування часу на обід і брифінг	Здійснюються налаштування операційної системи, веб-сервера, сервера баз даних, іншого програмного забезпечення, в тому числі і для підвищення захищеності і стійкості до відмов системи. Встановлення і конфігурування безпечної роботи інформаційної системи (наприклад, веб сайту з базою даних) з аналізом його програмного коду, пошуку вразливостей і загроз, доопрацювання і усунення знайдених недоліків і програмуванням (рефакторінгом програмного коду з точки зору підвищення безпеки) окремих його функцій. Результатом виконання є штатно функціонуючий інформаційний ресурс (наприклад, веб-сайт) в максимально безпечному оточенні.
РОЗСЛІДУВАННЯ ІНЦИДЕНТУ	до і після обіду: 4 години, без урахування часу на брифінг	Пошук причин порушення функціонування інформаційної системи з документуванням ходу дій зловмисника, відновленням цілісності даних, рекомендаціями до запобігання подібних дій в майбутньому. Результатом виконання є штатно функціонуюча інформаційна система та звіт із зазначеним вище вмістом.

У разі, якщо чемпіонат проводиться менше трьох днів, можливе виконання окремих модулів Конкурсного завдання з відповідним зменшенням максимально можливих набраних балів. Формат змагання, залежно від складу Конкурсного завдання, є індивідуальним або командним (2 людини в команді). Кожен учасник повинен оптимально розподілити свій час по виконанню конкурсного завдання в кожен конкурсний день.

Кожна частина завдання повинна супроводжуватися критеріями виставлення оцінок. Ці критерії затверджуються безпосередньо перед початком змагань, згідно з даним технічним описом. Допускається використання україномовних і англомовних версій операційних систем і програмного

забезпечення, однак офіційною мовою при роботі з Конкурсним завданням є українська мова.

5.3. ВИМОГИ ДО РОЗРОБКИ КОНКУРСНОГО ЗАВДАННЯ

У разі індивідуального Конкурсного завдання кожен модуль Конкурсного завдання виконується Конкурсантом строго індивідуально на одному робочому місці, що представляє собою персональний комп'ютер з доступом через локальну обчислювальну мережу до одного або декількох серверів. У разі командної роботи допускається спілкування між учасниками однієї команди.

Конфігурація і склад програмного забезпечення робочих місць повинні бути ідентичні у всіх учасників і достатні для виконання всіх модулів Конкурсного завдання. Електроживлення і пропускна здатність ЛВС повинні бути достатні для одночасної безперебійної інтенсивної роботи всіх конкурсантів та експертів. План забудови майданчика повинен відповідати зазначеному в даному документі настільки, наскільки це дозволяють умови проведення і можливості приймаючої сторони: в будь-якому випадку він затверджується експертами перед початком змагань.

При розробці Конкурсного завдання повинні бути розроблені і затверджені всі його модулі (за винятком ситуації, коли змагання тривають менше трьох днів – в цьому випадку один або кілька модулів можуть бути виключені із завдання відповідно до часу роботи, а максимальна оцінка за виконання конкурсного завдання знижена відповідним чином).

5.4. РОЗРОБКА КОНКУРСНОГО ЗАВДАННЯ

Для представлення конкурсного завдання використовується формат MS Office, спеціальні файли (наприклад, файли конфігурації) надаються у форматах, доступних для роботи за допомогою програмного забезпечення, що входить в інфраструктурний лист. Представлені зразки Конкурсного завдання повинні

актуалізуватися один раз на рік. Розробка Конкурсного завдання здійснюється за наступним планом.

ЧАС ДО ЗМАГАНЬ	ДІЇ
6 місяців	Формування робочої групи розробників завдання з експертів компетенції або сторонніх розробників (професіоналів індустрії). Завдання може складатися, як тільки з текстового опису (в цьому випадку Вступні файли готує головний експерт) або з текстового опису і всіх вступних даних.
2 місяці	Публікація зразкового завдання по кожному модулю, включаючи використовувані технології і очікувані вимоги до результату. При публікації завдання слід врахувати, що: • завдання відповідає технічному опису; • завдання по кожному модулю можливо виконати; • час на виконання завдання по кожному модулю адекватно складності та обсягу завдання; • інфраструктурний лист точно сформульований і достатній для виконання всіх завдань; • завдання та інфраструктурний лист узгоджені з технічним експертом; • інструкції для учасника зрозумілі, точні і не допускають різночитань і протиріч; • конкурсне завдання є повним у всіх аспектах; • розроблена відповідна схема нарахування балів, що містить точні і справедливі критерії оцінки кожного модуля.
Два дні до початку змагань	Затвердження остаточного конкурсного завдання експертною групою і, при необхідності, внесення до нього змін. Зміни не повинні впливати на складність завдання, не повинні ставитися до інших професійних областей, не описаних в WSSS, а також виключати будь-які блоки WSSS. Також внесені зміни повинні бути виконані за допомогою затвердженого для змагань інфраструктурного листа. Остаточний варіант конкурсного завдання, разом з усією документацією повинен перебувати у вільному доступі в зоні перебування експертів на змаганнях.

6. ВИМОГИ ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ

6.1 ВИМОГИ ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ НА ЗМАГАННЯХ

Професійна діяльність регламентується поточним законодавством і нормативними актами. Перелік вимог та відповідні їм інструкції публікує Організатори змагань. Вся документація з техніки безпеки та охорони праці надається оргкомітетом змагань.

7. МАТЕРІАЛИ ТА ОБЛАДНАННЯ

7.1. ІНФРАСТРУКТУРНИЙ ЛИСТ

В інфраструктурному листі перераховано все обладнання, матеріали та програмне забезпечення, які надає Організатор змагань. З інфраструктурним листом можна ознайомитися на веб-сайті змагань; при розробці інфраструктурного листа для регіональних змагань необхідно керуватися ним.

В інфраструктурному листі вказані найменування і кількість матеріалів і одиниць обладнання, що визначені експертами для змагань.

7.2. МАТЕРІАЛИ, ОБЛАДНАННЯ ТА ІНСТРУМЕНТИ В ІНСТРУМЕНТАЛЬНОМУ ЯЩИКУ (ТУЛБОКС, TOOLBOX)

Конкурсанту дозволяється використовувати власні:

- клавіатуру на будь-якій мові (якщо конкурсант користується своєю клавіатурою, і вона виходить з ладу, організатор надає йому заміну);
- мовні файли для клавіатури;
- миша.

Всі матеріали, принесені конкурсантами, можуть бути перевірені експертами на наявність внутрішніх запам'ятовуючих пристроїв. У разі виявлення матеріали будуть вилучатися, а до учасників/команд, які порушили

правила, застосовуються штрафні санкції, аж до анулювання всіх результатів і видалення з майданчика.

7.3. МАТЕРІАЛИ, ОБЛАДНАННЯ ТА ІНСТРУМЕНТИ, ЩО НАЛЕЖАТЬ ЕКСПЕРТАМ

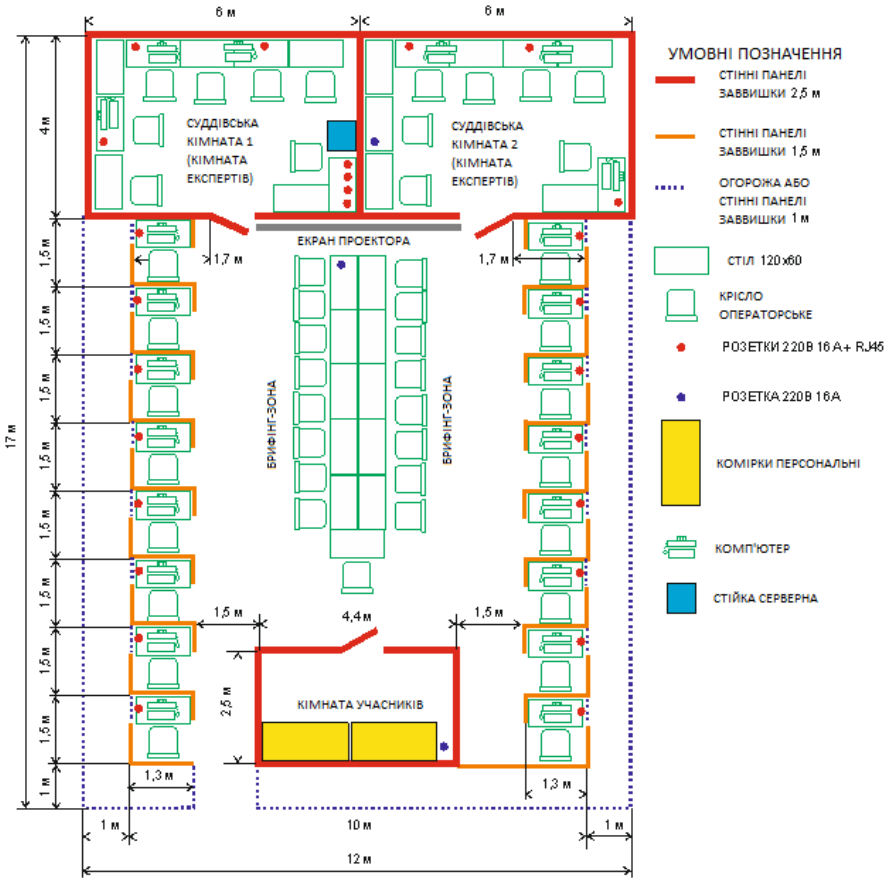
Допускається використовувати персональні комп'ютери, але в спеціальній зоні. У приміщеннях для проведення оцінювання використання будь-яких електронних пристроїв заборонено, крім спеціально організованих для оцінювання.

7.4. МАТЕРІАЛИ ТА ОБЛАДНАННЯ, ЗАБОРОНЕНІ НА МАЙДАНЧИКУ

Наступні матеріали та обладнання можуть бути пронесені і використані на майданчику тільки за окремим дозволом експертів:

- додаткові програми та бібліотеки, не передбачені інфраструктурним листом;
- мобільні телефони;
- Фото / відео пристрої;
- карти пам'яті та інші носії інформації;
- внутрішні пристрої пам'яті у власному обладнанні;
- книги, довідники та інші джерела інформації.

7.5. ЗАПРОПОНОВАНА СХЕМА КОНКУРСНОГО МАЙДАНЧИКА



8. ОСОБЛИВІ ПРАВИЛА ВІКОВОЇ ГРУПИ 14-16 РОКІВ

Час на виконання завдання не повинні перевищувати 4 годин на день. При розробці Конкурсного завдання і схеми оцінки необхідно враховувати специфіку і обмеження техніки безпеки і охорони праці для даної вікової групи. Так само необхідно враховувати антропометричні, психофізіологічні та психологічні особливості даної вікової групи. Тим самим конкурсне завдання і Схема оцінки може стосуватися не всіх блоків і полів WSSS в залежності від специфіки компетенції.

9. ПРЕДСТАВЛЕННЯ КОМПЕТЕНЦІЇ ВІДВІДУВАЧАМ

9.1. МАКСИМАЛЬНЕ ЗАЛУЧЕННЯ ВІДВІДУВАЧІВ

Майданчик проведення конкурсу має максимізувати залучення відвідувачів до процесу.

- Демонстраційні екрани, що показують хід робіт та інформацію про Учасника, що рекламують кар'єрні перспективи.
- Текстові описи конкурсних завдань: розміщення конкурсного завдання на загальний огляд.
- Демонстрація закінчених модулів: результат виконання кожного з модулів може бути опублікований по завершенні оцінки.

9.2. ДОСТУП ВІДВІДУВАЧІВ НА МАЙДАНЧИК

Доступ будь-яких відвідувачів на майданчик, крім учасників Чемпіонату, допускається тільки з дозволу експертів.