Компетентності рівня junior для Кібербезпека	Компанії SoftServe
1. Базові знання з мереж	
1.1. Сучасні мережні технології Розуміє переваги сучасних мережних пристроїв. Розуміє вплив мереж на повсякденне життя. Може пояснити як використовуються вузли та мережні пристрої. Знає способи поєднання мереж та мережні топології. Може порівняти характеристики поширених типів мереж. Розуміє як локальні та глобальні мережі реалізують з'єднання з мережею Інтернет. Може описати чотири основні критерії надійної мережі. Може пояснити Пояснити як такі тенденції як BYOD, онлайнспівпраця, відео і хмарні обчислення змінюють спосіб взаємодії між людьми. Визначає деякі основні загрози мережній безпеці та знає рішення для запобігання ним.	2
1.2. Базові налаштування комутатора та кінцевого пристрою. Може пояснити як отримати доступ до пристрою під керуванням Cisco IOS з метою налаштування. Описує структуру команд програмного забезпечення Cisco IOS. Може налаштувати пристрій під керуванням Cisco IOS за допомогою CLI. Вміє використовувати команди IOS для зберігання поточних налаштувань. Може пояснити, як пристрої взаємодіють у мережному середовищі. Вміє налаштувати IP-адреси на кінцевому пристрої. Може провести перевірку з'єднання між двома кінцевими пристроями.	1
1.3. Протоколи та моделі. Знає як мережні протоколи дозволяють пристроям отримувати доступ до локальних і віддалених мережних ресурсів. Описує типи правил, яких необхідно дотримуватися для успішного спілкування. Розуміє чому для мережної взаємодії потрібні протоколи. Може пояснити мету дотримання вимог стеку протоколів та роль організацій зі стандартизації у створенні протоколів для забезпечення мережної сумісності. Знає як моделі TCP/IP і OSI використовуються для полегшення стандартизації процесу передавання даних. Може пояснити як інкапсуляція забезпечує передавання даних по мережі та як локальні хости одержують доступ до локальних ресурсів у мережі.	3
1.4. Фізичний рівень. Знає як протоколи, служби та мережні середовища фізичного рівня підтримують зв'язок між мережами передавання даних. Описує призначення і функції фізичного рівня у мережі. Знає характеристики фізичного рівня. Може визначити основні характеристики мідних кабелів. Може пояснити, як UTP-кабель використовується у мережах Ethernet. Може описати оптоволоконні кабелі та їх основні переваги перед іншими середовищами передавання. Вміє під'єднати пристрої за допомогою дротових і бездротових середовищ передавання даних.	1
1.5. Системи числення. Знає двійкову та шістнадцяткову систему числення. Вміє перетворювати числа між десятковою, двійковою та шістнадцятковою системами.	2
1.6. Канальний рівень. Знає характеристики і функції кадру Канального рівня. Розуміє особливості керування доступом до середовища передавання даних на Канальному рівні. Описує призначення та функції канального рівня при налаштуванні зв'язку для передавання даних через конкретне середовище. Може порівняти характеристики методів контролю доступу до середовища передавання даних для топологій WAN і LAN.	2
1.7. Комутація Ethernet. Знає зв'язок підрівнів Ethernet з полями кадру. Занє методи узгодження швидкості комутатора і методи пересилання Може описати MAC-адресу Ethernet. Пояснює, як комутатор створює таблицю MAC-адрес і пересилає кадри.	2
1.8. Мережний рівень. Знає як маршрутизатори використовують протоколи і служби мережного рівня для забезпечення наскрізного з'єднання. Знає призначення полів у таблиці маршрутизації на маршрутизаторі. Розуміє як мережний рівень використовує IP протоколи для надійного зв'язку. Може пояснити призначення основних полів заголовка в пакеті IPv4 та IPv6. Розуміє яким чином мережні пристрої використовують таблиці маршрутизації для спрямування пакетів до мережі призначення.	2
1.9. Визначення адрес. Знає призначення ARP та як ARP і ND дозволяють спілкуватися у мережі. Може порівняти ролі MAC- та IP-адрес. Описує процес виявлення сусіда в IPv6.	2
1.10. Базові налаштування маршрутизатора. Може налаштувати початкові параметри на маршрутизаторі Cisco під керуванням IOS. Вміє налаштовувати два активні інтерфейси на маршрутизаторі Cisco під керуванням Cisco IOS. Вміє налаштовувати пристрої на використання шлюзу за замовчуванням.	1
1.11. Адресація IPv4. Знає структуру адреси IPv4, включаючи мережну частину, вузлову частину і маску підмережі. Може порівняти характеристики та способи використання одноадресних, широкомовних і групових адрес IPv4. Знає публічні, приватні та зарезервовані IPv4- адреси. Розуміє як підмережі сегментують мережу для забезпечення кращої комунікації. Може обчислити підмережі IPv4 для префікса /24 та для префікса /16 і /8. Враховуючи набір вимог до підмережі, вміє реалізувати схему адресації IPv4. Розуміє як створити гнучку схему адресації за допомогою маски підмережі змінної довжини (VLSM). Вміє реалізовувати схему адресації VLSM.	3

1.12. Адресація IPv6. Знає необхідність адресації IPv6. Розуміє який вигляд мають адреси IPv6. Може порівняти типи мережних адрес IPv6. Знає як налаштовувати статичні глобальні індивідуальні адреси та локальні адреси каналу мережі IPv6. Вміє динамічно налаштовувати глобальні індивідуальні адреси. Вміє визначати адреси IPv6. Вміє реалізовувати схему адресації розподілу мережі IPv6 на підмережі.	1
1.13. Протокол ICMP. Знає принцип використання потоколу ICMP для перевірки мережного з'єднання. Вміє використовувати утиліти ping і traceroute для тестування мережного з'єднання. Вміє використовувати різні засоби для перевірки мережного з'єднання.	3
1.14. Транспортний рівень Знає операцій протоколів транспортного рівня з точки зору підтримки наскрізного з'єднання. Розуміє призначення транспортного рівня при керуванні наскрізним з'єднанням. Знає характеристики TCP та UDP. Розуміє яким чином TCP і UDP використовують номери портів. Розуміє як процес створення і завершення сеансів TCP сприяють надійному передаванню даних. Знає як процес передавання блоків даних протоколу TCP і забезпечується їх гарантована доставка. Може порівняти особливості роботи протоколів транспортного рівня з точки зору підтримки наскрізного з'єднання.	3
1.15. Прикладний рівень Знає як рівні прикладних програм, подання даних і сеансів спільно працюють для забезпечення мережних сервісів застосункам кінцевого користувача. Розуміє процес функціонування застосунків кінцевих користувачів у одноранговій мережі. Знає принцип роботи протоколів Інтернету й електронної пошти та принципи роботи протоколів DNS і DHCP.	3
1.16. Основи мережної безпеки Розуміє чому на мережних пристроях слід запроваджувати основні заходи безпеки. Визначити вразливості систем безпеки. Може визначити загальні методи пом'якшення наслідків атак. Вміє налаштовувати на мережних пристроях захисні функції з метою пом'якшення загроз безпеці.	2
1.17. Створення невеликої мережі Вміє доцільно обирати пристрої, протоколи і застосунки, які використовуються у невеликій мережі. Вміє використовувати результати команд ping і tracert для перевірки з'єднання та підтримки відповідної працездатності мережі. Може використати команди вузла та IOS для отримання інформації про пристрої у мережі. Вміє описати традиційні методи виявлення і усунення несправностей у мережі. Вміє усунути несправностей пристроїв у мережі.	2
2. Основи комутації, маршрутизації та бездротових мереж	
2.1. Базові налаштування пристрою Вміє налаштувати порти комутатора відповідно до вимог мережі. Вміє налаштувати захищений доступ для керування комутатором. Вміє налаштувати основні параметри на маршрутизаторі, використовуючи CLI, для маршруту між двома безпосередньо під'єднаними мережами. Може перевірити з'єднання між двома мережами, які безпосередньо під'єднані до маршрутизатора.	2
2.2. Принципи комутації. Знає принцип виконання пересилання кадрів у комутованій мережі. Може порівняти домени колізій і широкомовні домени.	1
2.3. Віртуальні локальні мережі Розуміє мету застосування VLAN у комутованій мережі. Розуміє як комутатор пересилає кадри на основі конфігурації VLAN у середовищі з багатьма комутаторами. Вміє налаштувати порт комутатора для призначення до відповідної VLAN. Вміє налаштувати транковий (магістрального) порту на комутаторі локальної мережі. Вміє налаштувати протокол динамічного транкування.	1
2.4. Маршрутизація між VLAN Знає варіанти налаштування маршрутизації між VLAN. Вміє налаштувати метод Router-on-a-Stick для маршрутизації між VLAN. Вміє налаштувати маршрутизацію між VLAN за допомогою комутатора Рівня 3. Вмяє виявити і усунути типові проблеми з конфігурацією маршрутизації між VLAN.	1
2.5. Принципи роботи протоколу STP Знає типові проблеми із надлишковістю, які виникають у комутованих мережах другого рівня. Розуміє як працює Rapid PVST+. Розуміє принципи роботи протоколу STP у простій комутованій мережі.	1
2.6. EtherChannel Розуміє технологію EtherChannel. Вміє налаштувати EtherChannel. Вмяє виявити і усунути несправності в роботі EtherChannel.	1
2.7. DHCPv4 Розуміє як DHCPv4 працює в кількох локальних мережах. Вміє налаштувати маршрутизатор як сервера та як клієнта DHCPv4.	2
2.8. Поняття SLAAC та DHCPv6 Знає як вузол IPv6 може отримати конфігурацію IPv6. Розуміє принципи роботи SLAAC та DHCPv6. Вміє налаштувати сервер DHCPv6 зі збереженням і без збереження стану.	0
2.9. Принципи роботи протоколу FHRP Знає призначення та роботу протоколів резервування першого переходу. Розуміє принцип роботи HSRP.	0

2.10. Принципи безпеки LAN Знає як захист кінцевих точок здатен запобігти виникненню атак. Розуміє яким чином AAA і 802.1X використовуються для автентифікації кінцевих точок і пристроїв локальної мережі. Вміє визначити вразливості канального рівня. Розуміє як атака на таблицю MAC-адрес підриває безпеку локальної мережі. Роуміє як атаки на локальну мережу знижують рівень її захищеності.	2
2.11. Налаштування безпеки на комутаторі Розуміє як налаштувати DTP і native VLAN для стримування нападів на віртуальні локальні мережі. Знає налаштування PortFast і BPDU Guard допомагають запобігти STP-атакам. Вміє реалізувати захист портів для пом'якшення атак на таблиці MAC- адрес. Вміє налаштувати відстеження DHCP для запобігання атакам за участі DHCP. Вміє налаштувати перевірку ARP для пом'якшення ARP-атак.	2
2.12. Принципи та налаштування WLAN Знає технології та стандарти бездротової локальної мережі. Знає компоненти інфраструктури бездротової локальної мережі. Знає механізми забезпечення безпеки бездротових локальних мереж. Розуміє роль технології бездротового зв'язку в роботі бездротової локальної мережі. Розуміє як контролер бездротової локальної мережі використовує CAPWAP для керування кількома точками доступу. Розуміє принципи керування каналом у бездротовій локальній мережі. Знає загрози для бездротових локальних мереж. Вміє налаштувати WLAN за допомогою бездротового маршрутизатора і WLC.	1
2.13. Принципи маршрутизації Знає як маршрутизатори визначають найкращий шлях та пересилають пакети до місця призначення. Описує структуру таблиці маршрутизації. Може порівняти статичні і динамічні концепції маршрутизації. Вміє налаштувати базові параметри на маршрутизаторі Cisco під керуванням IOS.	1
2.14. Статична маршрутизація IP Знає синтаксис команд для статичних маршрутів. Вміє налаштувати статичні маршрути IPv4 і IPv6. Вміє налаштувати змінний статичний маршрут для забезпечення резервного з'єднання. Вміє налаштувати статичні хост-маршрути IPv4 та IPv6, які направляють трафік до певного вузла.	1
2.15. Виявлення і усунення неполадок з маршрутами статичними та за замовчуванням Знає як маршрутизатор обробляє пакети, коли налаштовано статичний маршрут. Вміє усунути типові неполадки з конфігурацією маршрутів статичних та за замовчуванням.	1
3. Побудова, безпека і автоматизація корпоративних мереж	
3.1. Основи протоколу OSPFv2 для однієї зони. Знає основні особливості та характеристики OSPF. Знає типи пакетів, які використовуються в OSPF для однієї зони. Розуміє принципи роботи протоколу OSPF для однієї зони. Вміє налаштувати ID маршрутизатора в OSPFv2. Вміє налаштувати OSPFv2 для однієї зони у мережі типу "точка-точка". Вміє налаштувати на інтерфейсі пріоритет OSPF для впливу на обрання DR/BDR у мережах з множинним доступом. Може Запровадити модифікації для зміни роботи OSPFv2 для однієї зони. Вміє налаштувати OSPF для поширення маршруту за замовчуванням.	1
3.2. Поняття мережної безпеки Знає сучасний стан кібербезпеки та вектори втрати даних. Знає типи суб'єктів загроз, які використовують вразливості мереж. Знає інструменти, що використовуються суб'єктами загроз для втручання у мережі. Знає типи шкідливого програмного забезпечення. Знає найбільш поширені мережні атаки. Знає найкращі методи захисту мережі. Розуміє як нападники використовують вразливості IP. Розуміє як суб'єкти загроз користуються вразливостями TCP та UDP. Розуміє як IP-сервіси використовуються суб'єктами загроз. Знає поширені криптографічні процеси, які використовуються для захисту даних під час передавання.	2
3.3. Принципи роботи та налаштування ACL для IPvACL Розуміє як фільтрується трафік за допомогою ACL. Розуміє як використовуються шаблонні маски в ACL. Може порівняти особливості стандартних та розширених ACL для IPv4. Вміє налаштувати стандартні ACL для IPv4, щоб здійснити фільтрацію трафіку відповідно до вимог мережі. Вміє використати порядкові номери для редагування існуючих стандартних ACL для IPv4. Вміє налаштувати стандартний ACL для захисту доступу до VTY. Вміє налаштувати розширені ACL для IPv4, щоб здійснити фільтрацію трафіку відповідно до вимог мережі.	1
3.4. NAT для IPv4 Знає призначення та функції NAT. Знає переваги і недоліки NAT. Розуміє принципи роботи різних типів NAT. Вміє налаштувати статичний NAT за допомогою інтерфейсу командного рядка (CLI). Вміє налаштувати динамічний NAT за допомогою CLI. Вміє налаштувати PAT за допомогою CLI.	1
3.5. Організація WAN. Знає типи під'єднання до мережі Інтернет. Розуміє призначення WAN. Розуміє як працюють технології глобальних мереж. Розуміє традиційні способи під'єднань до глобальної мережі. Розуміє сучасні способи під'єднання до глобальної мережі.	2
3.6. Функціонування VPN та IPsec. Знає типи та переваги технології VPN. Розуміє як VPN та IPsec допомагають захистити з'єднання між віддаленими системами.	2

3.7. Концепції QoS. Знає мінімальні вимоги до мережі для передавання голосу, відео та даних. Знає алгоритми формування й обслуговування черг, які використовуються мережними пристроями. Знає різні моделі QoS. Розуміє як мережні пристрої реалізують механізм QoS. Розуміє як характеристики передавання даних у мережі впливають на якість. Розуміє як QoS використовує механізми для забезпечення якості передавання.	1
3.8. Керування мережею. Знає принципи роботи протоколів SNMP та Syslog. Вміє використовувати CDP для відображення топології мережі. Вміє використовувати LLDP для відображення топології мережі. Вміє налаштувати протоколу NTP між NTP-клієнтом і NTP-сервером. Вміє иикористовувати команд IOS для резервного копіювання та відновлення конфігураційних файлів. Вміє виконувати оновлення образу операційної системи IOS.	1
3.9. Проектування мережі. Знає типи маршрутизаторів, доступних для мереж малого та середнього бізнесу. Розуміє як інформаційні, голосові та відеодані поєднуються у комутованій мережі. Знає що слід враховувати при проектуванні масштабованої мережі. Розуміє як апаратні функції комутатора забезпечують вимоги до мережі.	1
3.10. Віртуалізація мережі. Знає віртуалізацію мережних пристроїв і сервісів. Знає контролери, що використовуються для програмованих мереж. Розуміє важливість хмарних обчислень та віртуалізації.	1
3.11. Автоматизація мережі. Знає формати даних JSON, YAML і XML. Розуміє як API дозволяють комп'ютеру здійснювати комп'ютерні комунікації. Розуміє як здійснюється автоматизація мережі через інтерфейси RESTful API та інструменти керування конфігураціями. Розуміє як REST забезпечує взаємодію між комп'ютерами. Знає інструменти керування конфігурацією Puppet, Chef, Ansible і SaltStack.	2
4. Забезпечення безпеки мережі	
4.1. Типи загроз та атак. Знає еволюції мережевих загроз. Знає різні типи інструментів атак, які використовують зловмисники. Знає типи шкідливого програмного забезпечення. Вміє розпізнавати загальні мережеві атаки. Розуміє атаки типу "Відмова в обслуговуванні", переповнення буфера та ухиляння.	2
4.2. Зменшення загроз. Знає методи та ресурси для захисту мережі. Знає засоби, платформи та сервіси безпеки. Розуміє типи політик мережевої безпеки. Розуміє методи зменшення загальних мережевих атак.	2
4.3. Забезпечення безпечного доступу до пристроїв. Розуміє як захистити периметр мережі. Вміє налаштувати безпечний адміністративний доступ. Вміє використовувати команди для налаштування підвищеної безпеки для віртуальних входів. Вміє налаштувати SSH для безпечного віддаленого управління.	3
4.4. Призначення адміністративних ролей. Вміє налаштувати авторизації команд за допомогою рівнів привілеїв і на основі ролей CLI. Вміє використовувати команди для налаштування рівнів адміністративних привілеїв для контролю доступності команд. Вміє використовувати команди для налаштування доступу до CLI на основі ролей для контролю доступності команд.	2
4.5. Моніторинг та управління пристроями. Знає аутентифікацію протоколів маршрутизації. Розуміє конфігурації NTP та SNMP. Вміє налаштувати аутентифікацію протоколів маршрутизації. Вміє налаштувати syslog для реєстрації подій системи. Вміє налаштувати NTP для забезпечення точного відміткового позначення між всіма пристроями. Вміє налаштувати SNMP для моніторингу статусу системи.	2
4.6. Аутентифікація, авторизація та облік(AAA). Знає характеристики та протоколи аутентифікації, авторизації та обліку. Вміє налаштовувати AAA аутентифікації для перевірки користувачів у локальній базі даних. Вміє налаштувати аутентифікацію, авторизацію та облік на основі сервера.	2
4.7. Керування списками доступу. Знає стандартні та розширені ACL IPv4. Розуміє як ACL використовують маски зворотних бітів. Вміє налаштувати та змінити списки доступу. Вміє використовувати списки доступу для зниження типових мережевих атак. Вміє налаштувати ACL для IPv6 за допомогою командного рядка (CLI).	2
4.8. Технології брандмауерів. Знає принцип використання брандмауерів для забезпечення безпеки мереж. Розуміє аспекти проектування для впровадження технологій брандмауерів. Знає зонові брандмауери з політиками. Вміє використовувати зонові брандмауери з політиками для забезпечення безпеки мережі. Вміє налаштувати зоновий брандмауер з політиками за допомогою командного рядка (CLI)	2
4.9. Технології IPS (системи запобігання вторгнення). Знає характеристики систем IDS та IPS. Знає сигнатури IPS. Розуміє функції та роботу систем IDS та IPS. Вміє налаштувати систему IPS. Знає принципи захисту кінцевих точок та відповідних технологій.	2

4.10. Засоби безпеки для зниження атак на рівні 2. Знає загрози безпеки на рівні 2. Розуміє атаки на таблицю MAC-адрес. Розуміє принцип роботи протоколу Spanning Tree. Вміє налаштувати захист портів. Вміє знижувати атаки на VLAN, DHCP, ARP та STP.	1
4.11. Криптографічні сервіси. Знає сутність понять криптографія, криптоаналіз, криптологія. Розуміє як типи шифрування, хеш-функції та цифрові підписи працюють разом для забезпечення конфіденційності, цілісності та аутентифікації. Вміє забезпечувати безпечний зв'язк, включаючи цілісність, аутентифікацію та конфіденційність даних.	2
4.12. Основи цілісності та аутентифікації. Розуміє роль криптографії у забезпеченні цілісності та аутентифікації даних. Знає як криптографічні підходи покращують конфіденційність даних. Розуміє як криптографія використовується для забезпечення цілісності та аутентифікації даних.	2
4.13. Віртуальні приватні мережі (VPN). Знає топології та переваги VPN. Розуміє відмінності між VPN з віддаленим доступом та VPN між сайтами. Знає протокол IPsec та його основні функції. Розуміє відмінності протоколів AH та ESP. Розуміє процес обміну ключами в Інтернеті. Знає 5 етапів налаштування VPN. Вміє налаштовувати VPN між сайтами з аутентифікацією на підставі передзазначеного ключа за допомогою командного рядка.	2
4.14. Брандмауер ASA та його конфігурації. Знає 3 сценарії розгортання ASA. Вміє порівнювати рішення ASA з іншими технологіями маршрутизаційних брандмауерів. Вміє налаштувати параметри керування та служб на брандмауері ASA. Розуміє як налаштувати групи об'єктів на ASA. Вміє використовувати відповідні команди для налаштування.	
5. CyberOps.	
5.1. Загрози Знає особливості кібербезпекових інцидентів. Розуміє мотивації загроз, що стоять за конкретними кібербезпековими інцидентами. Розуміє вплив загроз та можливі наслідки атак на мережеву безпеку. Знає сучасний центр операцій з безпеки та його місії. Знає ресурси, доступні для підготовки до кар'єри в сфері кібербезпеки.	1
5.2. Операційна система Windows. Знає функції безпеки операційної системи Windows. Розуміє архітектуру та операції Windows. Розуміє як налаштовувати та моніторити Windows. Вміє забезпечити безпеку Windows.	2
5.3. Операційна сиситема Linux. Розуміє чому вміння працювати з Linux є важливим для моніторингу та розслідування кібербезпеки мережі. Вміє використовувати оболонку Linux для роботи з текстовими файлами. Розуміє як функціонують мережі клієнт-сервер у Linux. Розуміє як адміністратор Linux знаходить та обробляє журнали безпеки. Вміє управляти файловою системою та дозволами Linux. Розуміє основні компоненти графічного інтерфейсу Linux. Вміє використовувати інструменти для виявлення шкідливого програмного забезпечення на хості Linux.	3
5.4. Мережеві протоколи. Знає процес мережевої комунікації. Розуміє основні операцій передачі даних у мережі. Розуміє як протоколи комунікації забезпечують роботу мережі. Знає як укладання даних дозволяє транспортувати дані через мережу.	3
5.5. Ethernet та Протокол Інтернету (IP). Знає як Ethernet та протокол IPv4 підтримує мережеву комунікацію. Розуміє як IP-адреси дозволяють мережеву комунікацію. Знає різні типи IPv4-адрес, що дозволяють мережеву комунікацію. Знає як основний шлюз дозволяє мережеву комунікацію. Розуміє як протокол IPv6 підтримує мережеву комунікацію.	3
5.6. Принципи мережевої безпеки та перевірка з'єднання. Знає як ICMP використовується для перевірки мережевого з'єднання. Вміє використовувати інструменти Windows, ping та traceroute для перевірки мережевого з'єднання.	3
5.7. Протокол ARP (Протокол вирішення адрес). Знає ролі MAC-адреси та IP-адреси. Розуміє як ARP-запити впливають на мережеву та хостову продуктивність.	3
5.8. Транспортний рівень. Знає характеристики транспортного рівня. Розуміє як протоколи транспортного рівня підтримують мережеву комунікацію. Розуміє як транспортний рівень встановлює сеанси комунікації. Знає як транспортний рівень забезпечує надійність комунікації.	3
5.9. Мережеві служби. Знає як мережеві служби DHCP, DNS та NAT забезпечують мережевий функціонал. Знає служби передачі та обміну файлами. Розуміє як служби електронної пошти та HTTP забезпечують мережевий функціонал.	3
5.10. Пристрої мережевого зв'язку. Знає як пристрої мережевого зв'язку забезпечують провідну та бездротову мережеву комунікацію.	2
5.11. Інфраструктура мережевої безпеки. Знає як пристрої та служби мережевої інфраструктури використовуються для підвищення безпеки мережі. Розуміє як мережеві служби підвищують мережеву безпеку.	2

5.12. Зловмисники та їх інструменти Знає як розвиваються загрози мережі. Знає різні типи атакованих інструментів, використовуваних загрозами.	2
5.13. Загальні загрози та атаки. Знає типи зловмисного програмного забезпечення. Вміє розпізнавати загрози мережі - Розвідка, доступ та соціальна інженерія. Знає мережеві атаки - Відмова в обслуговуванні, переповнення буфера та ухилення.	3
5.14. Спостереження за роботою мережі. Знає інструменти моніторингу мережі. Розуміє важливості моніторингу мережі.важливості моніторингу мережі. Вміє виконати моніторинг мережі.	2
5.15. Атаки на мережу Знає як вразливості TCP/IP забезпечують атаки на мережу. Знає структуру заголовка IPv4 та IPv6. Розуміє вразливості IP, TCP та UDP	2
5.16. Вразливість мережевих програм та служб Знає вразливості мережевих служб IP. Розуміє як вразливості додатків мережі забезпечують атаки на мережу.	2
5.17. Поняття захисту Знає як стратегія оборони в глибину використовується для захисту мережі. Знає політики, нормативи та стандарти безпеки.	2
5.18. Розвідка загроз. Знає джерела інформації, що використовуються для передачі поточних загроз мережі безпеки. Знає різні служби розвідки загроз. В міє використовувати різні джерела розвідки для виявлення поточних загроз безпеки.	2
5.19. Криптографія. Розуміє роль криптографії в забезпеченні цілісності та автентичності даних. Розуміє яким чином криптографічні методи підвищують конфіденційність даних. Знає як функціонує публічна інфраструктура ключів. Розуміє як використання криптографії впливає на операції кібербезпеки.	3
5.20. Захист кінцевих точок Знає як веб-сайт аналізу шкідливих програм генерує звіт про аналіз шкідливих програм. Розуміє методи пом'якшення впливу шкідливих програм. Ідентифікує записи журналів хоста IPS/IDS. Знає безпеку застосунків.	2
5.21. Оцінка вразливості кінцевого обладнання. Знає профілювання мережі та сервера. Розуміє як оцінюються та керуються вразливості кінцевого обладнання. Розуміє як використовуються звіти CVSS для опису вразливостей безпеки. Розуміє як захищені техніки управління пристроями використовуються для захисту даних та активів. Знає як системи управління інформаційною безпекою використовуються для захисту активів.	2
5.22. Технології та протоколи. Розуміє поведінку загальних мережевих протоколів у контексті моніторингу безпеки. Знає як технології безпеки впливають на можливість моніторингу загальних мережевих протоколів.	2
5.23. Дані мережевої безпеки. Знає типи даних, що використовуються у моніторингу безпеки. Розуміє опис елементів файлу журналу кінцевого пристрою та мережевого пристрою.	1
5.24. Оцінка оповіщень. Розуміє процес оцінки оповіщень. Знає джерела та структуру оповіщень. Знає класифікацію оповіщень. Може провести огляд оцінки оповіщень. Знає як дані підготовлюються для використання в системі моніторингу мережевої безпеки. Вміє використовувати інструменти Security Onion для дослідження подій мережевої безпеки. Знає інструменти моніторингу мережі, які поліпшують управління робочим процесом.	1
5.25. Цифрова судова експертиза та аналіз та реагування на інциденти. Розуміє обробку доказів та встановлення атрибуції атаки. Знає класифікацію подій вторгнення за допомогою моделі діамантової аналізу. Вміє застосувати процедури обробки інцидентів для заданого сценарію інциденту.	1
6. Розмовна англійська	
6.1 Правильна побудова фрази з узгодженням часу Вміє використовувати відповідні часові форми дієслів і структури речень для точного вираження часу в комунікації. Здатний правильно використовувати часові форми, такі як Present Simple, Present Continuous, Past Simple, Past Continuous, Future Simple, для передачі правильного значення в повідомленні.	2
6.2 Професійна it термінологія в розмові з замовником Знає і використовує професійні IT-терміни та скорочення, які використовуються в IT-індустрії, для чіткого та зрозумілого спілкування зі замовником. Вміє перекладати складні технічні концепції на доступну мову для замовника, не знайомого з IT-галуззю.	3

6.3 Професійна it термінологія у діловому звіті Знає і використовує спеціалізовану IT-термінологію та фразеологію при написанні ділових звітів. Вміє передати інформацію про технічні питання та проєкти зрозуміло та конкретно, використовуючи адекватні IT-терміни та абревіатури.	2
6.4 Професійна термінологія Знає та розуміє специфічну термінологію, що використовується в галузі кібербезпеки. Вміє використовувати основні терміни для опису та обговорення замовлення з користувачем.	2
6.5 Неформальне спілкування (small talks) Вміє вести неформальну розмову, розпочинати діалоги та підтримувати невимушену атмосферу. Знає загальновживану термінологію та фрази, які використовуються у неформальних розмовах, таких як загальні питання про погоду, цікаві події, особисті захоплення, спорт, фільми тощо.	2

Коментарі до таблиці

Оцінки компетентностей вказані станом на 2023/2024 рр., по шкалі від 0 до 3.

«3» - компетентність вкрай важлива, якщо кандидат нею не володіє, його подальше просування на вакансію неможливе.

«2» - компетентність, знання якої обов'язково знадобиться кандидату при подальшому професійному зростанні.

«1» - некритична компетентність, якою можна знехтувати.

«0» - неактуальна компетентність.