Оцінювання якості ОПП «Інформаційна та кібернетична безпека»

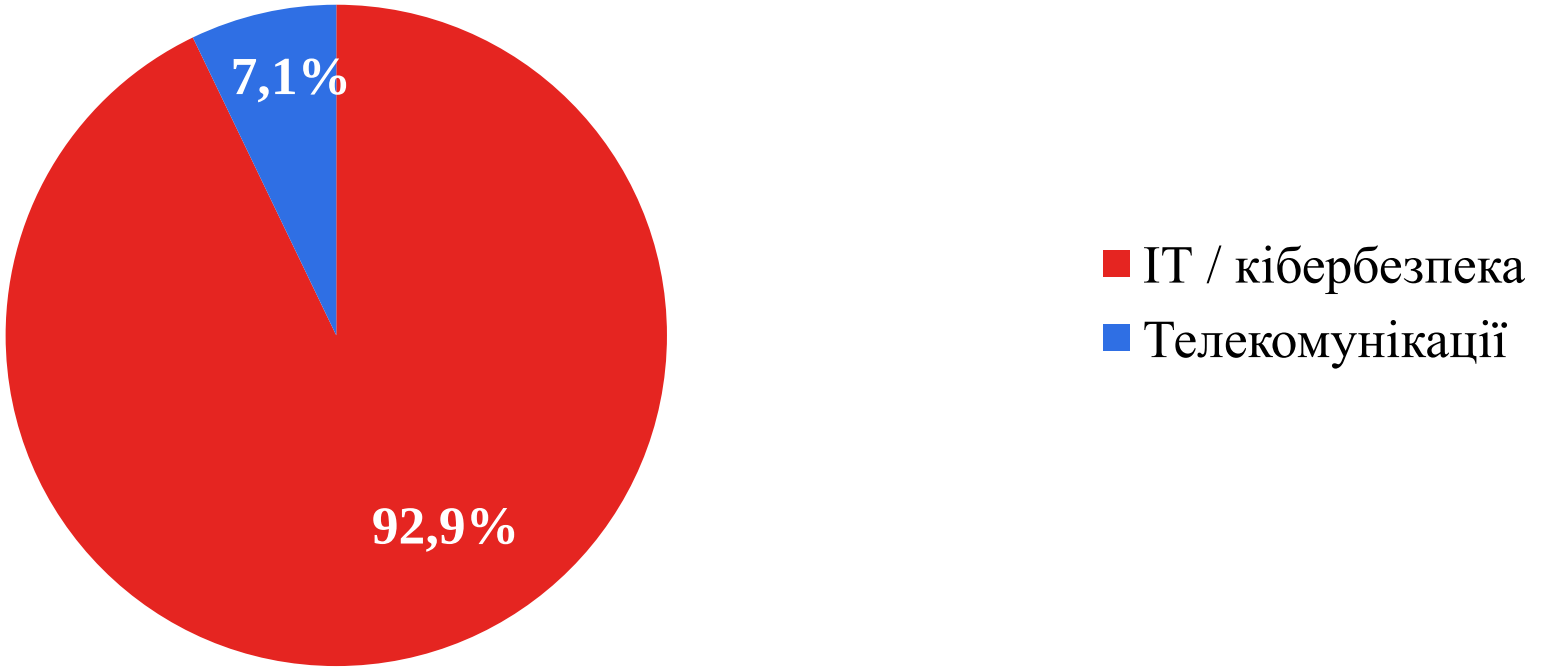
Результати опитування роботодавців та зовнішніх стейкголдерів

СТ-02. Ваша роль щодо ОПП.

Висновки:

Серед респондентів найбільше представників організацій-партнерів (57,1%), роботодавців (42,9%) та експертів/консультантів (35,7%). Це забезпечує оцінювання ОПП з різних позицій зовнішніх стейкголдерів.

СТ-03. Сектор діяльності Вашої організації.



Висновки:

Абсолютна більшість респондентів (92,9%) представляє сектор IT / кібербезпеки. Отже, оцінки та пропозиції переважно сформовані фахівцями профільної галузі.

СТ-04. Назва організації.

- ESET / ESET Ukraine / ESET в Україні (кілька представників)
- НДУ «Кібербезпека»
- КНУ імені Тараса Шевченка
- ТОВ «Security Expert Group» / ГС «Український кластер кібербезпеки»
- ТОВ «ЄВРОТЕЛЕКОМ»
- ТОВ «Світ ІТ»
- ТОВ «Хуавей Україна»
- Представники організацій, назву яких не розкрито через NDA

Висновки:

В опитуванні представлені роботодавці, ІТ- та кібербезпекові компанії, академічна установа й професійне об’єднання. Це забезпечує різноманітність зовнішніх оцінок ОПП.

СТ-05. Ваша посада або сфера професійної відповідальності.

- Керівні ролі: директор, технічний директор, CISO, керівник відділу.
- Технічні ролі: технічний і провідний спеціаліст, фахівці з кібербезпеки.
- Проєктна та освітня діяльність: Junior Cybersecurity Project Manager Specialist, професор кафедри, інструктор академії / керівник кластеру кібербезпеки.

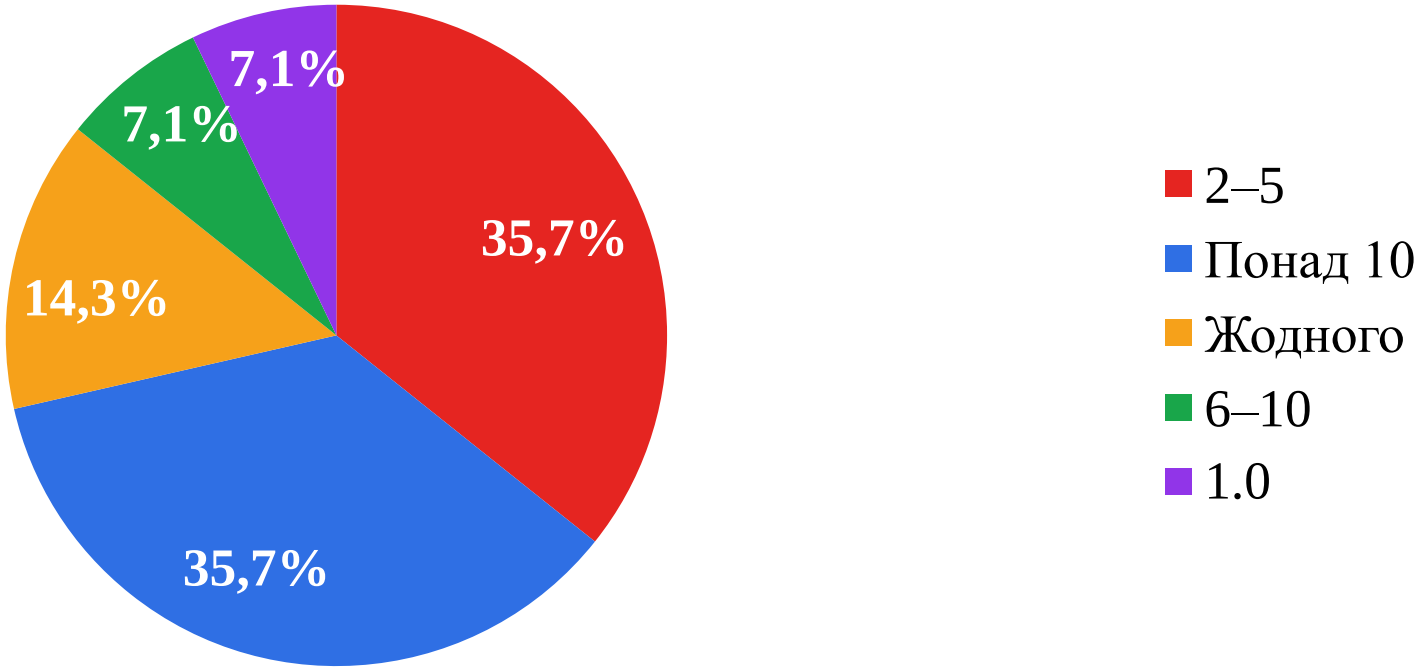
Висновки:

Серед респондентів представлені керівники, технічні фахівці, CISO, представники академічного середовища та проєктного управління, тобто оцінювання охоплює різні рівні професійної відповідальності.

СТ-06. У яких формах Ви взаємодіяли з ОПП або кафедрою?

Висновки:
Респонденти мають різноплановий досвід взаємодії з ОПП: працевлаштування випускників, проведення гостьових занять, керівництво практикою, участь у перегляді програми та спільних активностях.

СТ-07. Скількох здобувачів або випускників цієї ОПП Ви могли безпосередньо оцінювати?



Висновки:
Понад 70% респондентів безпосередньо оцінювали щонайменше 2 здобувачів або випускників ОПП, а 35,7% — понад 10. Це підсилює практичну обґрунтованість оцінок професійної підготовки.

СТ-08. Оцініть актуальність та спрямованість ОПП.

Висновки:

За всіма складовими актуальності та проєктування ОПП переважають високі оцінки. Найбільше максимальних оцінок отримали баланс складових підготовки, врахування потреб кіберстійкості та відновлення України, а також виразна цінність ОПП порівняно з іншими програмами профілю.

СТ-09. Рівень підготовки випускників за професійними компетентностями.

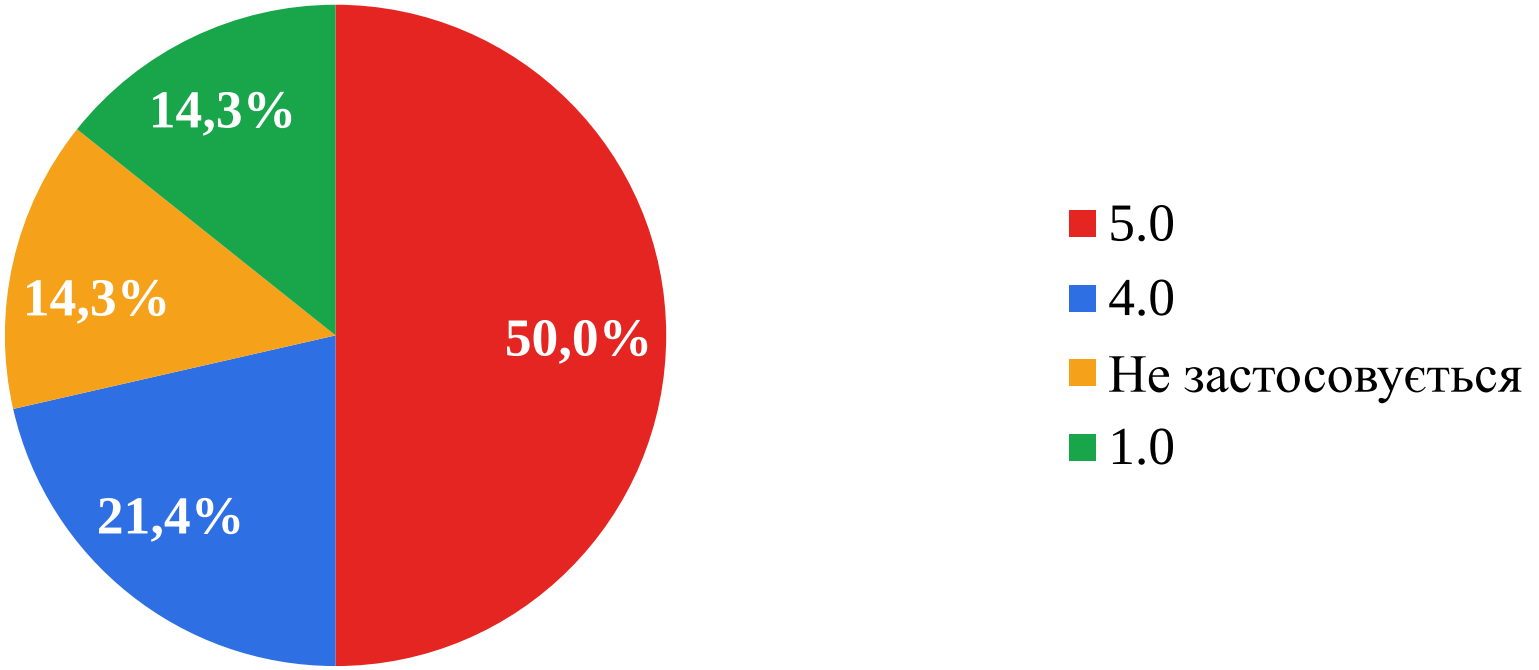
Висновки:
Зовнішні стейкголдери загалом позитивно оцінюють професійні компетентності випускників. Найбільше максимальних оцінок отримали здатність організовувати реагування на кіберінциденти та здатність планувати навчання і розвиток персоналу; за більшістю інших компетентностей також переважають високі оцінки.

СТ-10. Оцініть готовність випускників до професійної діяльності.

Висновки:

Переважна більшість оцінок підтверджує високу готовність випускників до професійної діяльності: адаптації до нових технологій, командної роботи, дотримання професійної етики та самостійного розвитку.

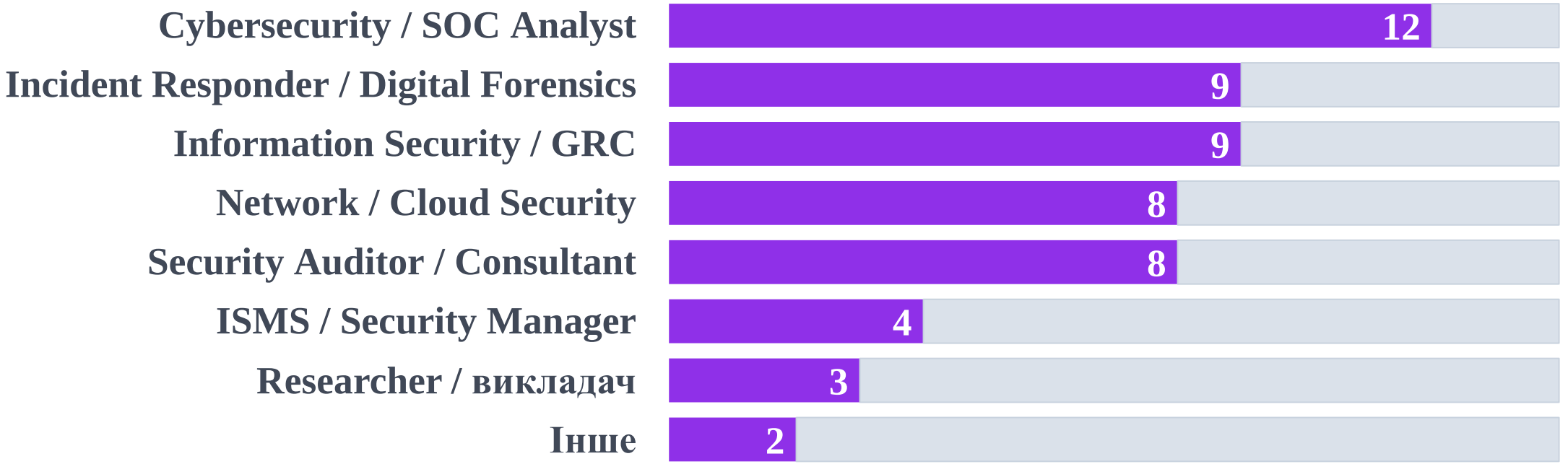
СТ-11. Наскільки Ваша організація зацікавлена у працевлаштуванні випускників цієї ОПП?



Висновки:

71,4% респондентів оцінили зацікавленість у працевлаштуванні випускників на 4–5 балів. Половина опитаних надала максимальну оцінку «5».

СТ-12. Для яких ролей підготовка випускників є найбільш релевантною?



Висновки:

Найбільш релевантною підготовку випускників вважають для ролей Cybersecurity / SOC Analyst (85,7%), Incident Responder / Digital Forensics та Information Security / GRC (по 64,3%), а також Network / Cloud Security і Security Auditor / Consultant (по 57,1%).

СТ-13. Які напрями слід посилити в ОПП у найближчі 2–3 роки?

Висновки:

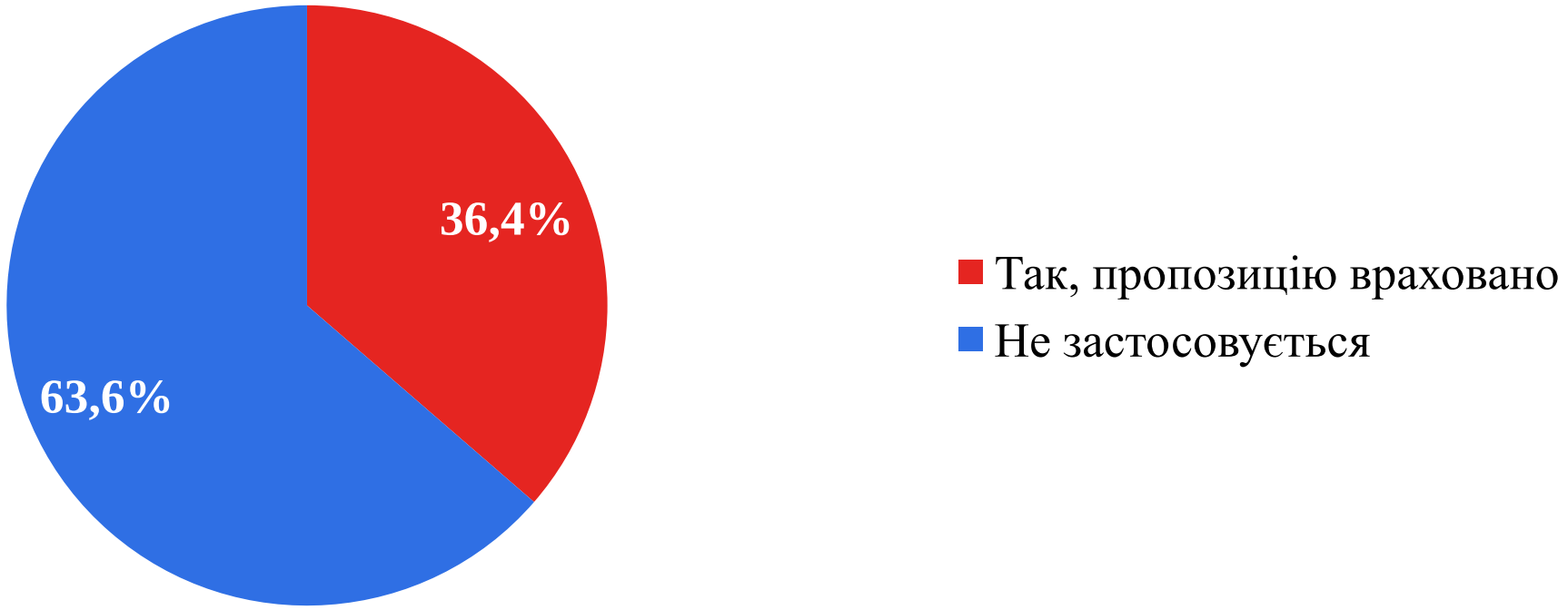
Найбільший запит стейкголдерів — AI/ML у кібербезпеці (71,4%), SOC/SIEM та аналітика подій і реагування на інциденти (по 64,3%), а також мережева безпека та захист інфраструктури (57,1%).

СТ-14. Чи мали Ви можливість надати пропозиції до ОПП?

Висновки:

28,6% респондентів безпосередньо подавали пропозиції до ОПП, ще 28,6% мали таку можливість, але не скористалися нею. Водночас 14,3% не знали про можливість подання пропозицій.

СТ-15. Якщо Ви подавали пропозиції, чи отримали інформацію про результат їх розгляду?



Висновки:

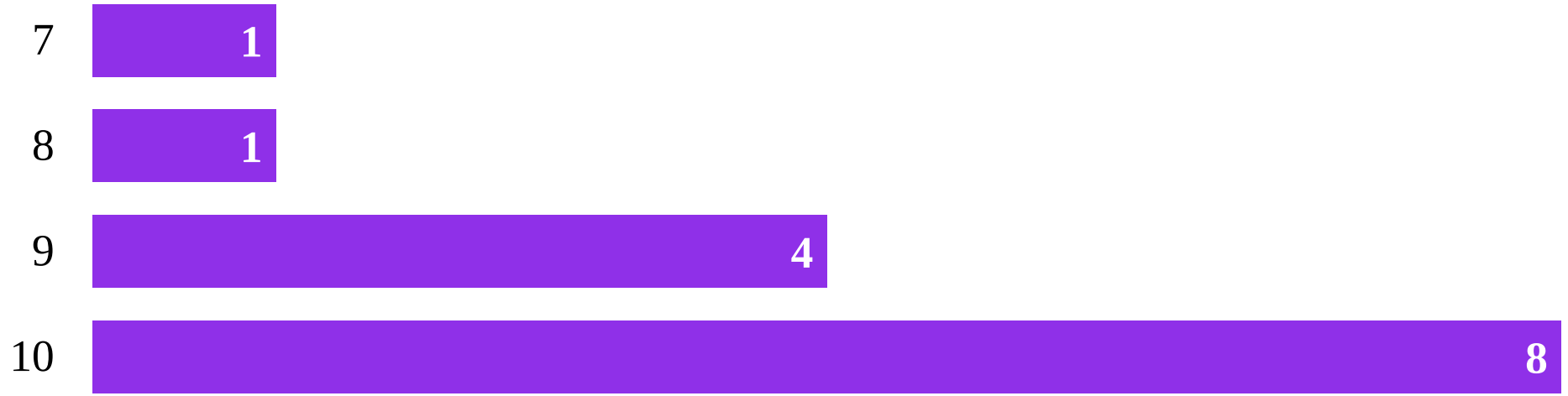
Серед відповідей на це питання 36,4% зазначили, що їхні пропозиції було враховано. Для решти респондентів питання не застосовувалося; негативних варіантів щодо розгляду пропозицій не зафіксовано.

СТ-16. До яких форм співпраці Ви або Ваша організація готові долучатися?

Висновки:

Найбільша готовність до співпраці стосується гостьових лекцій і тренінгів (76,9%), надання баз практики (53,8%), кар’єрних заходів / працевлаштування (46,2%) та експертного перегляду ОПП (38,5%).

СТ-17. Наскільки ймовірно, що Ви порекомендуєте співпрацю з цією ОПП або працевлаштування її випускників?



Висновки:

85,7% респондентів оцінили ймовірність рекомендації на 9–10 балів, з них 57,1% обрали максимальну оцінку «10». Це свідчить про високий рівень довіри до ОПП та її випускників.

СТ-18. Які сильні сторони ОПП та її випускників варто зберегти й розвивати?

- Практична спрямованість, технічна підготовка та професіоналізм випускників.
- Здатність до самовдосконалення, швидкої адаптації та опанування нових технологій.
- Командна робота й комунікативні навички.
- Поєднання фундаментальних знань із системним підходом до захисту інформації та міждисциплінарністю.

Висновки:
Сильні сторони, які доцільно зберігати, пов’язані з фундаментальною та практичною підготовкою, адаптивністю випускників і здатністю працювати в команді. Окремо відзначено доцільність активнішого залучення фахівців галузі.

СТ-19. Які прогалини у підготовці випускників Ви спостерігаєте?

- Недостатній практичний досвід роботи із сучасним інструментарієм, зокрема SIEM та EDR.
- Потреба у більшій практиці з хмарною інфраструктурою, автоматизацією та цифровою криміналістикою.
- Складнощі з кореляцією подій, аналізом трафіку, розслідуванням інцидентів і документуванням цифрових доказів.
- Потреба в розвитку управління проєктами та роботи в розгалужених командах; лабораторна база має швидше реагувати на появу нових вендорів.

Висновки:

Основний напрям удосконалення — збільшення практичного досвіду з актуальними технологіями та інструментами, а також розвиток навичок командної і проєктної роботи.

СТ-20. Яку конкретну зміну до змісту, практик або організації ОПП Ви рекомендуєте першочергово?

- Оперативніше включати до навчання актуальні практики й технології, що вже використовуються у галузі.
- Адаптувати практичну підготовку до запитів роботодавців і посилювати співпрацю з ними.
- Запровадити наскрізний практикум на базі кіберполігону з повним циклом роботи з реалістичним кіберінцидентом.

Висновки:
Пропозиції зосереджені на посиленні практичної складової та її оперативній актуалізації відповідно до потреб роботодавців. Найбільш конкретна рекомендація — наскрізний практикум із повним циклом реагування на кіберінцидент.

СТ-21. Які нові технології, стандарти, загрози або професійні ролі слід врахувати під час наступного перегляду ОПП?

- AI/ML у кібербезпеці та безпека систем штучного інтелекту.
- DevSecOps, автоматизація безпеки, автоматизація SOC, хмарні й контейнерні середовища, Zero Trust.
- Захист ланцюгів постачання ПЗ, OT/ICS, цифрова криміналістика та реагування на актуальні кібератаки.
- NIST CSF 2.0, ISO/IEC 27001:2022, NIS2, ECSF та актуальні вимоги законодавства.

Висновки:
Під час наступного перегляду ОПП доцільно посилити технологічні напрями AI/ML, DevSecOps, хмарної та OT/ICS-безпеки, а також орієнтувати зміст на актуальні міжнародні стандарти й професійні ролі.