ЗВЕДЕНА ТАБЛИЦЯ

пропозицій та зауважень, отриманих від стейкголдерів під час громадського обговорення освітньо-професійної програми «Аналіз вразливостей інформаційних систем» першого (бакалаврського) рівня вищої освіти спеціальності F5 Кібербезпека та захист інформації та результати їх обговорення на засіданні кафедри мультимедійних систем (протокол № 3 від 10.03.2026 р.)

№	Пункт ОП	Стейкголдери	Пропозиції / зауваження	Враховано / частково враховано / відхилено	Нова редакція
1.	Передмова. Склад проєктної групи; рецензії та залучені стейкголдери	Члени проєктної групи, викладачі кафедри мультимедійних систем та факультету інформатики	Оновити склад проєктної групи та залучити до розроблення ОПП представників усіх груп стейкголдерів (роботодавців, здобувачів, випускників, академічної спільноти); оформити рецензії.	Враховано	Затверджено склад проєктної групи: керівник (гарант) – Савченко Т.В., члени – Глибовець А.М., Глибовець М.М., Гороховський С.С., Жежерун О.П., Бабич Т.А. Додано рецензії/відгуки: Потій О.В., Тимошик Н.П., Лахно В.А. Зазначено залучених роботодавців (Стиран В.С., Сологуб Р.І.), здобувачів та випускників (Звіркова К.О., Курбіна Д.М.), представника академічної спільноти (Пархоменко І.І.).
2.	Профіль ОП. Характеристика ОП (предметна область)	Члени проєктної групи	Привести опис предметної області у відповідність до Стандарту вищої освіти за спеціальністю F5 (наказ МОН № 1547 від 29.10.2024 р.).	Враховано	Викладено за Стандартом: об’єкти вивчення, цілі навчання, теоретичний зміст предметної області, методи, методики та технології, інструменти та обладнання. Замінено попередні формулювання («сучасні методи та алгоритми…»).
3.	Профіль ОП. Придатність до працевлаштування	Члени проєктної групи	Узгодити перелік посад і результатів навчання з професійними стандартами «Фахівець з реагування на інциденти кібербезпеки» та «Кібероператор» (наказ ДССЗЗІ від 23.01.2024 р. № 38).	Враховано	За ДК 003:2010 визначено посади 2139.2 «Фахівець з реагування на інциденти» та 4113 «Кібероператор» (у редакції 2025 р. – «Аналітик з оцінки вразливостей»). Розширено перелік можливостей подальшого навчання та підвищення кваліфікації.

№	Пункт ОП	Стейкголдери	Пропозиції / зауваження	Враховано / частково враховано / відхилено	Нова редакція
4.	Профіль ОП. Викладання та оцінювання	Члени проєктної групи	Деталізувати підходи до викладання, форми поточного й підсумкового контролю та систему оцінювання; зазначити засоби дистанційного навчання; узгодити формулювання щодо ЄДКІ зі Стандартом.	Враховано	Описано компетентнісний, студентоцентрований та проблемно-орієнтований підходи, тренінгові та інтерактивні технології, платформу Moodle (DistEdu), форми контролю; зазначено порядок оцінювання за 100-бальною рейтинговою системою відповідно до положень НаУКМА; ЄДКІ – за результатами навчання, визначеними Стандартом.
5.	Профіль ОП. Інтегральна компетентність	Члени проєктної групи	Привести інтегральну компетентність до формулювання Стандарту вищої освіти № 1547 від 29.10.2024 р.	Враховано	«Здатність розв’язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації» (замість формулювання про «комплексність та неповну визначеність умов»).
6.	Профіль ОП. Загальні компетентності (ЗК)	Члени проєктної групи	Оновити перелік загальних компетентностей відповідно до чинного Стандарту № 1547 від 29.10.2024 р. https://mon.gov.ua/static-objects/mon/sites/1/vishcha-osvita/zatverdzeni%20standarty/2024/30-10-2024/125-kiberbezpeka-bakalavr-1547-vid-29-10-2024.pdf	Враховано	ЗК1–ЗК8 викладено за Стандартом (зокрема, окремо: ЗК3 – державна мова, ЗК4 – іноземна мова, ЗК5 – здатність вчитися, ЗК7 – принцип неприпустимості корупції); збережено ЗК11 «Здатність до національного спротиву». Вилучено формулювання «вміння виявляти, ставити та вирішувати проблеми» та «здатність до пошуку, оброблення та аналізу інформації».
7.	Профіль ОП. Спеціальні (фахові) компетентності (СК1–СК10)	Члени проєктної групи	Замінити перелік фахових компетентностей (СК1–СК12 у редакції 2025 р.) компетентностями Стандарту № 1547 від 29.10.2024 р.	Враховано	СК1–СК10 викладено за Стандартом (законодавча база, ІТ та методи кібербезпеки, неперервність бізнес-процесів, захист інформації в ІС та ІКС, відновлення після кібератак, комплексні системи захисту, система управління кібербезпекою, криптографічний і

№	Пункт ОП	Стейкголдери	Пропозиції / зауваження	Враховано / частково враховано / відхилено	Нова редакція
					технічний захист, моніторинг та оцінка вразливостей).
8.	Профіль ОП. Додаткові спеціальні компетентності за професійними стандартами (СК11–СК15)	Роботодавці	Розширити ОП спеціальними компетентностями, визначеними професійними стандартами з кібербезпеки: «Фахівець з реагування на інциденти кібербезпеки» та «Кібероператор».	Враховано	Додано СК11–СК12 («Фахівець з реагування на інциденти кібербезпеки») та СК13–СК15 («Кібероператор»). У розділі 6 «Пояснювальна записка» наведено їх розкриття через знання, уміння, комунікацію, відповідальність і автономність.
9.	Профіль ОП. Програмні результати навчання (РН1–РН21)	Члени проєктної групи	Привести програмні результати навчання у відповідність до чинного Стандарту № 1547 від 29.10.2024 р. (замість РН1–РН54 у редакції 2025 р.).	Враховано	РН1–РН21 викладено за Стандартом; збережено РН11 щодо готовності до виконання громадянського обов’язку (національний спротив). Систему матриць компетентностей та РН оновлено.
10.	Профіль ОП. Додаткові програмні результати навчання за професійними стандартами (РН22–РН27)	Роботодавці	Включити до ОП результати навчання, що забезпечують формування компетентностей за професійними стандартами.	Враховано	Додано РН22–РН27: оцінка дій противника та його методів (ТТП), методики для різних типів інцидентів, запобігання наслідкам інцидентів і виправлення вразливостей, виявлення сильних сторін та вразливостей мережі, віддалена експлуатація, виявлення експлойтів проти цільових мереж і хостів.
11.	Профіль ОП. Ресурсне забезпечення (матеріально-технічне та інформаційне)	Члени проєктної групи Здобувачі вищої освіти	Врахувати умови воєнного стану та забезпечення безпеки освітнього процесу; уточнити інформаційні ресурси.	Враховано	Додано відомості про систему сповіщення про повітряну тривогу, бомбосховища в корпусах, відповідність кількості місць у гуртожитках, наявність полігонів; уточнено використання платформи DistEdu, ресурсів Наукової бібліотеки НаУКМА та необмеженого доступу до мережі Інтернет.

№	Пункт ОП	Стейкголдери	Пропозиції / зауваження	Враховано / частково враховано / відхилено	Нова редакція
12.	Перелік освітніх компонентів. Структура ОП	Члени проєктної групи	Структурувати перелік компонентів на цикли загальної та професійної підготовки, виокремити компонент практичної підготовки та атестацію; узгодити співвідношення обов'язкових і вибіркових компонентів.	Враховано	Обов'язкові компоненти – 180 кредитів (цикл загальної підготовки – 42 кр., цикл професійної підготовки – 120 кр., практики – 6 кр., кваліфікаційна робота – 12 кр.); вибіркові компоненти – 60 кредитів (дисципліни професійної підготовки – 40 кр., вільного вибору – 20 кр.). У редакції 2025 р.: 172 і 68 кредитів відповідно.
13.	Освітні компоненти.	Здобувачі вищої освіти	Запровадити на початку навчання вступну дисципліну «Вступ до кібербезпеки», що формує цілісне уявлення про галузь кібербезпеки.	Враховано	Введено ОК 1.2.1 «Вступ до кібербезпеки» (3 кр., залік).
14.	Освітні компоненти. Реагування на інциденти (професійний стандарт «Фахівець з реагування на інциденти кібербезпеки»)	Роботодавці	Додати компоненти, що забезпечують формування СК11–СК12 та РН22–РН24: моніторинг, аналіз та реагування на кіберінциденти, відновлення систем.	Враховано	Введено ОК 1.2.9 «Моніторинг та реагування на кіберінциденти» (4 кр., екзамен) та ОК 1.2.21 «Аналіз та реагування на кіберінциденти» (5 кр., екзамен).
15.	Освітні компоненти. Мережева розвідка та аналіз вразливостей (професійний стандарт «Кібероператор»)	Роботодавці	Додати компоненти, що забезпечують формування СК13–СК15 та РН25–РН27: аналіз вразливостей мереж, ОС та пам'яті, техніки експлуатації та закріплення.	Враховано	Введено ОК 1.2.24 «Вразливості корпоративних мереж» (5 кр.), ОК 1.2.25 «Вразливості привілеїв та конфігурації ОС» (5 кр.), ОК 1.2.27 «Техніки закріплення та стійка присутність» (5 кр.), ОК 1.2.16 «Зворотна інженерія та вразливості пам'яті» (4 кр., замість ОК «Низькорівневі вразливості програмного забезпечення», 4 кр.). У складі обов'язкових компонентів

№	Пункт ОП	Стейкголдери	Пропозиції / зауваження	Враховано / частково враховано / відхилено	Нова редакція
					більше не передбачено ОК «Етичний хакінг» (3 кр.) та «Безпека операційних систем» (4 кр.).
16.	Освітні компоненти. Системне адміністрування, інфраструктура та хмарні сервіси	Роботодавці	Посилити практичну підготовку з адміністрування операційних систем, доменної інфраструктури, автоматизації розгортання та безпеки хмарної інфраструктури.	Враховано	Введено ОК 1.2.8 «Адміністрування ОС сімейства *nix» (4 кр.), ОК 1.2.18 «Доменна інфраструктура та служби каталогів» (4 кр.), ОК 1.2.19 «Автоматизація розгортання та інфраструктури» (3 кр.), ОК 1.2.22 «Хмарна інфраструктура та сервіси» (3 кр.), ОК 1.2.26 «Безпека хмарної інфраструктури» (3 кр.). ОК «Адміністрування розподілених систем» (4 кр.) та обов'язкова ОК «Хмарні технології» (4 кр.) у складі обов'язкових не збережені; «Хмарні технології» перенесено до вибіркових (ВБ 2.1.61, 4 кр.).
17.	Освітні компоненти. Технічний захист та управління інформаційною безпекою	Члени проєктної групи	Забезпечити формування СК7 та СК9 окремими обов'язковими компонентами.	Враховано	Введено ОК 1.2.30 «Технічний захист інформації» (4 кр., екзамен) та ОК 1.2.32 «Управління інформаційною безпекою» (3 кр., залік). ОК «Методи та засоби соціальної інженерії» (4 кр.) замінено на ОК 1.2.31 «Соціальна інженерія» (3 кр.); ОК «Методи та засоби збору чутливої інформації» (3 кр.) переведено до обов'язкових (ОК 1.2.14).
18.	Освітні компоненти. Програмування	Члени проєктної групи	Забезпечити базову підготовку з системного програмування та скоригувати обсяг компонентів з програмування.	Враховано	Введено ОК 1.2.15 «Мова програмування С» (4 кр., екзамен) замість ОК «Процедурне програмування» (5 кр.). Обсяг ОК «Мова програмування Python» зменшено з 6 до 5 кр., ОК «Алгоритми та структури даних» – з 6 до 5 кр. ОК «Розробка та впровадження програмних продуктів» (4 кр.) та «Моделі

№	Пункт ОП	Стейкголдери	Пропозиції / зауваження	Враховано / частково враховано / відхилено	Нова редакція
					обчислень в програмній інженерії» (4 кр.) у складі обов'язкових не збережені.
19.	Освітні компоненти. Математична підготовка	Члени проєктної групи Представники академічної спільноти	Узгодити обсяг і склад математичних компонентів зі Стандартом та потребами фахових дисциплін; приведення кредитів.	Враховано	ОК 1.1.4 «Дискретна математика» – 5 кр. (замість «Основи дискретної математики», 4 кр.); ОК 1.1.5 «Алгебра та теорія чисел» – 5 кр. (замість «Лінійна алгебра та аналітична геометрія», 4 кр.); ОК 1.1.6 «Теорія ймовірностей та математична статистика» – 5 кр. (було 4 кр.). У складі обов'язкових не збережені ОК «Основи матаналізу» (4 кр.), «Диференціальні рівняння» (3 кр.), «Теорія алгоритмів і математична логіка» (4 кр.), «Історія української кібернетики» (2 кр.).
20.	Освітні компоненти. Правові, етичні та базові ІТ-компоненти (приведення обсягу кредитів)	Члени проєктної групи	Привести обсяги кредитів окремих компонентів у відповідність до логіки формування компетентностей і навантаження за семестрами.	Враховано	ОК «Етичні аспекти кібербезпеки» – 3 кр. (було 2); «Правове регулювання кібербезпеки» – 3 кр. (було 4; уточнено назву); «Безпека програмних впроваджень» – 3 кр. (було 4); «Основи операційних систем» – 3 кр. (було 4); «Основи мережних технологій» – 4 кр. (було 5). Змінено форму контролю з курсової роботи на «захист»; «Архітектура обчислювальних систем» – екзамен.
21.	Освітні компоненти. Вибіркові компоненти	Здобувачі вищої освіти Роботодавці	Оновити та розширити перелік вибіркових компонентів фахового спрямування з урахуванням сучасних викладів кібербезпеки.	Враховано	Сформовано перелік із 65 дисциплін професійної підготовки (40 кр.), зокрема: «Архітектура нульової довіри», «Аудит та консалтинг у кібербезпеці», «Безпека штучного інтелекту», «Безпека промислових систем управління», «Безпека IoT та вбудованих систем», «Змагальна кібербезпека», «Інженерія виявлення

№	Пункт ОП	Стейкголдери	Пропозиції / зауваження	Враховано / частково враховано / відхилено	Нова редакція
					кіберзагроз», «Поглиблений аналіз шкідливого ПЗ», «Проактивна протидія кіберзагрозам», «Розслідування кіберзлочинів», «Цифрова криміналістика», «Криптоаналіз та постквантова криптографія»; передбачено 20 кр. дисциплін вільного вибору.
22.	Компонент практичної підготовки та атестація	Члени проєктної групи	Виокремити практичну підготовку; привести обсяг та формулювання кваліфікаційної роботи у відповідність до Стандарту.	Враховано	Практики (ПП 3.1 «Практика навчальна», ПП 3.2 «Практика виробнича») – по 3 кр., залік. Кваліфікаційна робота – 12 кр. (було 15 кр.); завдання: «розв'язок спеціалізованого завдання теоретичного або практичного спрямування в галузі кібербезпеки та захисту інформації». Передбачено оприлюднення робіт на сайті університету або факультету, або в репозитарії eKMAIR.
23.	Структурно-логічна схема, матриці, пояснювальна записка	Члени проєктної групи	Оновити структурно-логічну схему та матриці відповідності; додати відповідність дескрипторам НРК та розкриття компетентностей професійних стандартів.	Враховано	Оновлено структурно-логічну схему та матриці ЗК/СК і РН відповідно до нової структури ОК; додано розділ 6 «Пояснювальна записка»: класифікація компетентностей за НРК, матриця відповідності ЗК/СК дескрипторам НРК, розширення ОП спеціальними компетентностями професійних стандартів (СК11–СК15), матриця відповідності РН і компетентностей.