Звіт про громадське обговорення
проєкту програми єдиного державного кваліфікаційного іспиту зі спеціальності 125 «Кібербезпека» галузі знань «Інформаційні технології» на першому (бакалаврському) рівні вищої освіти

1. Найменування органу виконавчої влади, який проводив обговорення:

Міністерство освіти і науки України.

2. Зміст питання або назва проєкту документа, що виносили на обговорення:

Проєкт програми єдиного державного кваліфікаційного іспиту зі спеціальності 125 «Кібербезпека» галузі знань «Інформаційні технології» на першому (бакалаврському) рівні вищої освіти (далі – проєкт програми ЄДКІ).

ЄДКІ зі спеціальності 125 «Кібербезпека» галузі знань «Інформаційні технології» на першому (бакалаврському) рівні вищої освіти (далі – ЄДКІ) є обов'язковим компонентом атестації здобувачів вищої освіти за спеціальністю «Кібербезпека».

Метою ЄДКІ є оцінювання готовності випускника закладу вищої освіти самостійно розв'язувати складні задачі і проблеми у сфері кібербезпеки шляхом встановлення відповідності досягнутих здобувачем вищої освіти результатів навчання вимогам стандарту вищої освіти за спеціальністю 125 «Кібербезпека» галузі знань 12 «Інформаційні технології» на першому (бакалаврському) рівні вищої освіти, затвердженого наказом Міністерства освіти і науки України від 4 жовтня 2018 року№ 1074.

Проєкт програма ЄДКІ містить перелік питань: законодавча та нормативно-правова база України в галузі інформаційної та /або кібербезпеки; міжнародні стандарти в галузі інформаційної та /або кібербезпеки; інструментальні та прикладні застосунки в інформаційній та/або кібербезпеці; методи і засоби обробки інформації; операційні системи; моделі безпеки в інформаційній та/або кібербезпеці; захист інформації, що обробляється та зберігається в ІКС; програмні та програмно-апаратні комплекси ЗЗІ; відновлення функціонування ІКС після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження; моніторинг процесів функціонування ІКС; механізми безпеки комп'ютерних мереж; проєктування, створення, супровід КСЗІ; моделі загроз та моделі порушника; оцінка захищеності інформації в ІКС; управління кіберінцидентами; управління ризиками в інформаційній та / або кібербезпеці; аудит інформаційної та/або кібербезпеки; забезпечення безперервності бізнес-процесів; математичні основи криптографії та стеганографії; симетричні

криптосистеми; асиметричні криптосистеми; криптографічні протоколи; цифрова стеганографія; технічні канали витоку інформації; методи та засоби технічного захисту інформації.

Громадське обговорення проводилося у формі електронних консультацій. Проєкт програми ЄДКІ було розміщено 31 грудня 2021 року на офіційному вебсайті Міністерства освіти і науки України за посиланням:

https://mon.gov.ua/ua/news/mon-proponuye-do-gromadskogo-obgovorennya-proyekt-programi-yedinogo-derzhavnogo-kvalifikacijnogo-ispitu-zi-specialnosti-125-kiberbezpeka-dlya-pershogo-bakalavrskogo-rivnya-vishoyi-osviti

Зауваження та пропозиції до проєкту програми ЄДКІ приймалися до 13 січня 2022 року на електронну адресу: mruga@mon.gov.ua.

3. Інформація про осіб, що взяли участь в обговоренні: Протягом встановленого для обговорення з громадськістю терміну надійшли зауваження та пропозиції від п’ятнадцяти адресантів: Олександра Манжая, завідувача кафедри протидії кіберзлочинності Харківського національного університету внутрішніх справ; Дмитра Ланде, професора, завідувача кафедри інформаційної безпеки Навчально-наукового фізико-технічного інституту Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»; Галини Гайдур, доктора технічних наук, професора, завідувача кафедри інформаційної та кібернетичної безпеки Державного університету телекомунікацій; представників факультету кібербезпеки, комп'ютерної та програмної інженерії Національного авіаційного університету; Володимира Лужецького, доктора технічних наук, професора, завідувача кафедри захисту інформації Вінницького національного технічного університету; Олесі Войтович, кандидата технічних наук, доцента, доцента кафедри захисту інформації, директора Центру забезпечення якості освіти Вінницького національного технічного університету; Олександра Лаптєва, доктора технічних наук, старшого наукового співробітника, доцента кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка; Шпатара П.М., кандидата технічних наук, доцента, завідувача кафедри радіотехніки та інформаційної безпеки Чернівецького національного університету ім. Ю.Федьковича, Ластівки Г.І., кандидата технічних наук, доцента, доцента кафедри радіотехніки та інформаційної безпеки Чернівецького національного університету ім. Ю.Федьковича; Рождественської М.Г., доцент кафедри радіотехніки та інформаційної безпеки Чернівецького національного університету ім. Ю.Федьковича; denisdpua@i.ua; yaromenko2304@gmail.com; Андрія Єфіменка, кандидат технічних наук, доцент, завідувач кафедри комп'ютерної інженерії та кібербезпеки Державного університету

«Житомирська політехніка»; Любчак В., завідувача кафедри Кібербезпеки СумДУ; колектива кафедри робототехнічних і телекомунікаційних систем та кібербезпеки Черкаського державного технологічного університету.

4. Інформація про пропозиції, що надійшли до Міністерства освіти і науки України за результатами обговорення:

Пропозиції Олександра Манжая, завідувача кафедри протидії кіберзлочинності Харківського національного університету внутрішніх справ:

Тема та її зміст	**Зауваження та пропозиції**
1.1. Законодавча та нормативно-правова база, державні та міжнародні вимоги, практики і стандарти в галузі інформаційної та/або кібербезпеки	Зовсім відсутні документи, які регламентують захист службової інформації та персональних даних, наприклад, Закон України «Про захист персональних даних» від 01.06.2010, Типова інструкція про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, затверджена Постановою Кабінету Міністрів України від 19.10.2016 № 736 тощо
1.2.1. Регламенти ЄС в галузі кібербезпеки	Які конкретно регламенти ЄС в галузі кібербезпеки маються на увазі? Скільки регламентів? У Темі 1.1. «Законодавча та нормативно-правова база України в галузі інформаційної та /або кібербезпеки» визначений вичерпний перелік актів, що дозволяє визначити сферу знань Доцільно також визначити вичерпний перелік регламентів ЄС в галузі кібербезпеки. Наприклад, Регламент Європейського Парламенту і Ради (ЄС) 2019/881 від 17 квітня 2019 року «Про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій, а також про скасування Регламенту (ЄС) № 526/2013 (Акт про кібербезпеку)»

1.2.2. ДСТУ ISO 27001	Не зовсім зрозуміло, чому згадується тільки один стандарт, а не вся 27 серія. Оскільки в ДСТУ ISO 27001 містяться лише надзагальні вимоги до побудови системи управління інформаційною безпекою, але не конкретика. Зважаючи на викладене, здобувачам вищої освіти потрібно знати хоча б головні стандарти 27-ї серії
2.2.2.Основи об'єктно-орієнтованого програмування (Класи, Методи, Перевантаження, Наслідування, Делегати, Узагальнення)	Рекомендується «Делегати» вилучити, оскільки не у всіх алгоритмічних мовах присутнє це поняття
2.2.5. Завадостійкі коди	У темі 6.2.2. «Класичні методи шифрування. Шифр Цезаря, Вернама. Квадрат Полібія. Шифр гамування» зазначений вичерпний перелік класичних шифрів Доцільно також визначити вичерпний перелік завадостійких кодів. Наприклад: **двійкові коди, що виявляють помилки** (з перевіркою на парність, з простим повторенням, інверсний (Бауера), кореляційний), **двійкові коди, що виправляють однократні помилки** (Хеммінга, ітеративний (Елайеса), з багатократним повторенням, інверсний, несистематичний код Бергера)
2.3. Операційні системи	Існує велика кількість операційних систем. Їх можна класифікувати за типом апаратної платформи (серверні, десктопні, мобільні, операційні системи інтернету речей), за типом програмної платформи або вендором (Windows, Unix, Linux, Android тощо), роком випуску тощо. Кожен з цих параметрів відповідає своїй власній архітектурі операційної системи, реалізації багатопроцесорності та багатопоточності, керуванню пам'яттю,

	принципам організації файлових систем та механізмам безпеки, які вони використовують. Доцільно чітко вказати тип операційної системи, який має бути розглянутий. Наприклад, десктопні операційні системи сімейства Windows (64-розрядні).
3.5. Механізми безпеки комп'ютерних мереж	Існує два великі класи комп'ютерних мереж: проводові та безпроводові. В залежності від середовища передавання даних мережі будуть використовуватися різні стандарти для побудови таких мереж, забезпечення їх функціонування та захисту. За цим пунктом доцільно розглянути окремо як проводові, так і безпроводові мережі та відповідні механізми захисту.
4. Комплексні системи захисту інформації	Введено цілий розділ «Комплексні системи захисту інформації», але чомусь у програмі жодним чином не згадується «Система управління інформаційною безпекою». Водночас вимогу до знання відповідного стандарту ДСТУ ISO 27001 передбачено у 1 розділі програми. Пояснення. Відповідно до ч. 4 ст. 8 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 державні інформаційні ресурси та інформація з обмеженим доступом, крім державної таємниці, службової інформації та державних і єдиних реєстрів, створення та забезпечення функціонування яких визначено законами, можуть оброблятися в системі ***без*** *застосування комплексної системи захисту інформації* у разі виконання **всіх** таких умов: - підтвердження відповідності *системи управління інформаційною безпекою* за результатами процедури з оцінки відповідності національним стандартам

	України щодо систем управління інформаційною безпекою, яка проведена *органом з оцінки відповідності*, акредитованим національним органом України з акредитації чи національним органом з акредитації іншої держави, якщо і національний орган України з акредитації, і національний орган з акредитації такої держави є членами міжнародної або регіональної організації з акредитації та/або уклали з такою організацією угоду про взаємне визнання щодо оцінки відповідності; - використання для захисту інформації в системі *засобів криптографічного захисту інформації, які мають позитивний експертний висновок* за результатами державної експертизи у сфері криптографічного захисту інформації; - жоден з елементів системи не може бути *розташований на територіях* України, на яких органи державної влади України тимчасово не здійснюють своїх повноважень, на територіях держав, визнаних Верховною Радою України державами-агресорами, на територіях держав, щодо яких застосовано санкції відповідно до Закону України «Про санкції», та на територіях держав, які входять до митних союзів з такими державами; - *виконання особливих вимог*, встановлених Кабінетом Міністрів України до забезпечення захисту інформації в системах залежно від категорії державних інформаційних ресурсів або інформації з обмеженим доступом (вимога щодо захисту якої встановлено законом, що обробляються) Враховуючи викладене, доцільно змінити зміст 4-го розділу програми з урахуванням вимог до побудови системи управління інформаційною безпекою

4.3. Оцінка захищеності інформації в ІКС	Оцінка захищеності інформації в ІКС може відбуватися за різними стандартами та кращими практиками. Їх достатня кількість. Доцільно визначити певний стандарт або визнану методологію. Наприклад, можна визначити один із наведених: «НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»; «ДСТУ ISO/IEC 15408-1:2017 (ISO/IEC 15408-1:2009, IDT). Інформаційні технології. Методи захисту. Критерії оцінки. Частина 1. Вступ та загальна модель»; «ДСТУ ISO/IEC TS 27008:2019 (ISO/IEC TS 27008:2019, IDT) Інформаційні технології. Методи захисту. Настанова щодо оцінювання захисту інформаційної безпеки» тощо
6.2.3. Блокові шифри. DES, AES, ГОСТ 28147, DSTU7624	У темі 6.2.3.4. «ДСТУ 7624:2014 (режими роботи, довжина ключів, довжина блоку вхідного тексту, кількість раундів, крипостійкість)» визначена сфера знань стосовно алгоритму симетричного блокового перетворення. Доцільно також визначити сферу знань (що саме повинен знати, розуміти здобувач) стосовно алгоритмів DES, AES, ДСТУ ГОСТ 28147-2009
5.4. Забезпечення безперервності бізнес-процесів	Не зовсім зрозуміло, про які бізнес-процеси йде мова, оскільки відповідних моделей бізнес-процесів є багато. Слід конкретизувати, наприклад, … бізнес-процесів за методологією IDEF0
6.2.4.1. RC4	Доцільно також визначити сферу знань (що саме повинен знати, розуміти здобувач) стосовно алгоритму RC4.

	Наприклад, як це зроблено для ДСТУ 8845:2019 (довжина ключів, крипостійкість)

Пропозиції Дмитра Ланде, професора, завідувача кафедри інформаційної безпеки Навчально-наукового фізико-технічного інституту Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»;

Просимо сприяти врахуванню в наповненні Програми та тестів ЄДКІ таких зауважень та пропозицій:

Пункт Проєкту Програми	Вміст	Пропозиція/зауваження
П.1.1.4.	ЗУ «Про державну таємницю»	Вивчення деталей цього Закону України не є типовим для всіх освітніх програм спеціальності «Кібербезпека». Пропонуємо замінити його на Закон України «Про електронні довірчі послуги» та/або «Про електронні документи та електронний документообіг»
П. 1.1.6.	Постанова КМУ від 19 червня 2019 року No 518 «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури»	Даний документ був прийнятий відносно нещодавно. В Стандарті освіти відсутні вимоги щодо обізнаності бакалаврів щодо захисту об'єктів критичної інфраструктури. Натомість, така вимога є у стандарті магістрів. Пропонуємо виключити даний документ з Програми ЄДКІ для бакалаврів і включити до Програми ЄДКІ для магістрів

П. 2.4.3.	Модель вразливостей	Пропонуємо сформулювати пункт як «Поняття вразливостей», або «Класифікація вразливостей», оскільки модель вразливостей може передбачати різні бачення, пов'язані із вивченням широкого спектра математичних моделей
П. 2.2.5.	Завадостійкі коди	Теорію кодування не визначено в переліку компетентностей стандарту
П. 4.2.5.	Загрози через соціальну інженерію	В стандарті освіти бакалаврів відсутні прямі вказівки для обізнаності здобувачів у цьому питанні. В ряді освітніх програм предмет «Теорія і методи соціальної інженерії в кібербезпеці» викладається на магістратурі. Пропонуємо виключити даний пункт із програми, або розробити такі тести, які передбачають наявність лише загальних уявлень про сутність загроз соціальної інженерії, без надмірної деталізації класів загроз та їх особливостей
П. 4.3.1.	Концептуальна схема оцінки безпеки інформації	Просимо конкретизувати цей пункт, оскільки він передбачає різні варіанти його розуміння.

П. 4.1.1	Проведення аудиту інформаційної безпеки та визначення на основі звіту з аудиту ризиків ІБ.	Пункт логічніше віднести в категорію «Управління ризиками в інформаційній та/або кібербезпеці». Ризик-орієнтований підхід не є типовим для Комплексних систем захисту інформації (КСЗІ), він притаманний скоріше Системам управління інформаційною безпекою (СУІБ). Для КСЗІ формулювання пункта пропонуємо викласти як «Дослідження середовищ функціонування ІС – середовища користувачів, обчислювальної системи, фізичного середовища, інформаційного середовища та побудова моделі загроз», яке є більш типовим для сталої термінології в області комплексних систем захисту інформації

Пропозиції Галини Гайдур, доктора технічних наук, професора, завідувача кафедри інформаційної та кібернетичної безпеки Державного університету телекомунікацій;

Надаємо зауваження щодо проєкту «ПРОГРАМА ЄДИНОГО ДЕРЖАВНОГО КВАЛІФІКАЦІЙНОГО ІСПИТУ ЗІ СПЕЦІАЛЬНОСТІ 125 «КІБЕРБЕЗПЕКА» ДЛЯ ПЕРШОГО (БАКАЛАВРСЬКОГО) РІВНЯ ВИЩОЇ ОСВІТИ».

В першому розділі «ЗАКОНОДАВЧА ТА НОРМАТИВНО-ПРАВОВА БАЗА, ДЕРЖАВНІ ТА МІЖНАРОДНІ ВИМОГИ, ПРАКТИКИ І СТАНДАРТИ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ ТА/АБО КІБЕРБЕЗПЕКИ» пропонуємо прибрати підпункт 1.2. Міжнародні стандарти в галузі інформаційної та /або кібербезпеки.

Додати підпункт 1.1.7. Державні Стандарти України в галузі інформаційної та/або кібербезпеки, в основі яких покладено міжнародні стандарти ISO серії 27(з конкретним їх переліком).

Додати підпункт 1.1.8. Нормативні документи з технічного захисту інформації (з конкретним їх переліком).

Другий розділ «ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНІЙ ТА/АБО КІБЕРБЕЗПЕЦІ» перейменувати в МЕТОДИ ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ТА /АБО КІБЕРБЕЗПЕКИ,

що відповідає опису предметної області, а саме теоретичному змісту чинного Стандарту вищої освіти України 125 Кібербезпека.

Пункт 2.1 «Інструментальні та прикладні застосунки в інформаційній та/або кібербезпеці» перейменувати в «Основи побудови інформаційно-комунікаційних систем».

Підпункт 2.4. видалити. Він дублюється з підпунктом 4.2.

Третій розділ перейменувати в «ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ». Змістом даного розділу має бути питання створення захищених ІКС, моніторингу та діагностування стану безпеки даних систем, реагування на інциденти інформаційної та /або кібербезпеки, питання відновлення систем та розслідування кіберінцидентів.

Підпункт 3.2. «Програмні та програмно-апаратні комплекси ЗЗІ» має базуватися на конкретних рішеннях (вендорах), тому доцільно засоби захисту розглядати за формулою Призначення-Архітектура-Функції.

В шостому розділі «КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ» видалити питання стеганографії (не є питанням у результатах навчання Стандарту вищої освіти України 125 Кібербезпека) та методи шифрування, які на сучасному етапі розвитку не застосовуються (Шифр Цезаря, Вернама. Квадрат Полібія. Шифр гамування).

Підпункт 6.5. Цифрова стеганографія видалити.

Підпункт 7.2.2. Системи відеоспостереження видалити.

По кожному пункту Програми необхідно зазначати джерело правильної відповіді на поставлені питання, яке буде враховуватися Апеляційною комісією під час розгляду спільних питань.

Пропозиції представників факультету кібербезпеки, комп'ютерної та програмної інженерії Національного авіаційного університету;

№	Програмні питання проєкту ЄДКІ	Пропозиція (об’єднати/вилучити/додати)	Обгрунтування
1	п.2.2.4. Кількісна міра інформації. п.2.2.5. Завадостійкі коди.	Вилучити	Відсутність у стандарті вищої освіти зі спеціальності 125 «Кібербезпека» для першого (бакалаврського) рівня вищої освіти фахової компетентності та результату навчання (вимірювальної характеристики), які відповідають за ці питання та визначають нормативний зміст підготовки здобувача вищої освіти
2	п. 4.1.1. Проведення аудиту інформаційної безпеки та визначення на основі звіту з аудиту ризиків ІБ.	Вилучити	Відсутність у стандарті вищої освіти зі спеціальності 125 «Кібербезпека» для першого (бакалаврського) рівня вищої освіти фахової компетентності та результату навчання (вимірювальної характеристики), які відповідають за ці питанні та визначають нормативний зміст підготовки здобувача вищої освіти
3	п. 5.3. Аудит інформаційної та/або кібербезпеки.	Вилучити	Відсутність у стандарті вищої освіти зі спеціальності 125 «Кібербезпека» для першого (бакалаврського) рівня вищої освіти фахової компетентності та результату навчання (вимірювальної характеристики), які відповідають за дані питанні та визначають нормативний зміст підготовки здобувача вищої освіти

4	п.6.1. Математичні основи криптографії та стеганографії.	Вилучити	Відсутність у стандарті вищої освіти зі спеціальності 125 «Кібербезпека» для першого (бакалаврського) рівня вищої освіти фахової компетентності та результату навчання (вимірювальної характеристики), які відповідають за ці питанні та визначають нормативний зміст підготовки здобувача вищої освіти
5	п.6.3.4. Електронний цифровий підпис DSA.	**Додати в п.6.3.4** Електронний цифровий підпис DSA, **ДСТУ 4145:2000**	Оскільки ДСТУ 4145:2000 Національний стандарт України, що описує процедури формування та верифікації електронно-цифрового підпису на базі еліптичних кривих
6	п.6.3.2. Шифри RSA, EG.	**Додати в п.6.3.2** Шифри RSA, EG, **ECC**	Оскільки алгоритм ECC відноситься до асиметричних криптосистем та на сьогодні є популярним до використання в протоколах SSL/TLS, HTTPS
7	п.6.5. Цифрова стеганографія.	Вилучити	Відсутність у стандарті вищої освіти зі спеціальності 125 «Кібербезпека» для першого (бакалаврського) рівня вищої освіти фахової компетентності та результату навчання (вимірювальної характеристики), які відповідають за дані питанні та визначають нормативний зміст підготовки здобувача вищої освіти
8	п.3.5. Механізми безпеки комп'ютерних мереж. 6.4. Криптографічні протоколи.	Об’єднати п. 3.5 та п.6.4. **Викласти п. 3.5. в такій редакції:** 3.5. Механізми безпеки комп'ютерних мереж.	Об’єднання обумовлено тим, що IPSec та https – належать до механізмів безпеки комп’ютерних мереж

		3.5.1. Віртуальні приватні мережі (VPN). 3.5.2. Протоколи автентифікації RADIUS. 3.5.3. Протоколи SSL/TLS. 3.5.4. Протоколи захисту мережевого трафіка IPSec. 3.5.5. Протоколи безпечної передачі даних прикладного рівня: https.	

Пропозиції Володимира Лужецького доктора технічних наук, професора, завідувача кафедри захисту інформації Вінницького національного технічного університету; Олесі Войтович, кандидата технічних наук, доцента, доцента кафедри захисту інформації, директор Центру забезпечення якості освіти Вінницького національного технічного університету;

№	Зміст	Зауваження	Пропозиції
1	1.1 Законодавча та нормативно-правова база України в галузі інформаційної та /або кібербезпеки	Відсутні Закони України «Про захист персональних даних», «Про електронні довірчі послуги», «Про критичну інфраструктуру». Вони є також базовими для забезпечення кібербезпеки	Додати ЗУ «Про захист персональних даних», «Про електронні довірчі послуги», «Про критичну інфраструктуру»
2	1.2.1 Регламенти ЄС в галузі кібербезпеки.	Не зрозуміло, чому саме регламенти ЄС, які саме (зараз багато директив перебувають у стадії обговорення та перезатвердження). Якщо інші пункти цього розділу мають посилання на конкретні назви законів та актів, то тут занадто загально.	Конкретизувати директиви ЄС, додати інші міжнародні стандарти, наприклад ISO/IEC 15408, X800 тощо
3	1.2.2 ДСТУ ISO 27001.	Якщо тут мова йде про міжнародні стандарти, то чому вказаний ДСТУ?	Варто говорити про всю серію ISO 27k

4	3.5. Механізми безпеки комп'ютерних мереж	Запропоновані механізми безпеки дуже обмежені	Додати «протоколи віртуальних приватних мереж VLAN», «міжмережеве екранування», «списки доступу ACL», «протоколи на мережевому рівні, наприклад IPSec», тощо
5	3.5.2.Протоколи автентифікації RADIUS	Чому увага зосереджена саме на цьому протоколі? Є багато інших протоколів віддаленої автентифікації. RADIUS лише один з них, далеко не найкращій, хоча і масовий.	Пропонується: «3.5.1. Протоколи віддаленої автентифікації»
6	3.5.3. Протоколи SSL/TLS	Протоколи SSL/TLS.	Пропонується «Протоколи безпеки на сеансовому/транспортному рівні (зокрема SSL/TLS)»
7	4.3.Оцінка захищеності інформації в ІКС	Якщо мова йде про НД ТЗІ 2.5-004-99, то можливо вказати повністю	Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу
8	4.3.1. Концептуальна схема оцінки безпеки інформації	Не зрозуміло, про яку «концептуальну схему оцінки» йде мова, в НД ТЗІ такої не має.	Переформулювати відповідно до законодавства про КСЗІ.

Пропозиції Олександра Лаптєва, доктора технічних наук, старшого наукового співробітника, доцента кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка;

Іспит не буде викреслювати захист бакалаврської роботи. Вважаю, що саме бакалаврська робота – це вирішення технічного завдання. Вона свідчить про наявність технічного мислення та можливості вирішувати технічне завдання. Також як контроль, саме вона може свідчити про наявність

«Плагіату», та може бути перевірена у будь-який час. Інакше для чого проводиться перевірка на плагіат. Саме зараз це питання дуже актуальне.

Стосовно тем та зміст програми іспиту. Вважаю, що програма потребує доробки. Одразу кидається в очі дуже широке коло питань стосовно криптографії. Я ні в якому разі не принижую роль Харківської школи. Вони дійсно у цьому напрямку головні і не тільки у нашій Державі, а ще і у Світі. Але, на мою думку треба більш розгорнуто сформулювати 7 розділ Програми. Додати додаткові теми.

Чому я так вважаю, тому що виток інформації, частіш за все, здійснюється за рахунок використання технічних каналів та технічних засобів отримання інформації. Приклади завжди наведені у відкритій пресі. Аудіо запис Л.Д. Кучми, запис телефонних розмов депутатів та їх дітей, фото, відеозаписи, які оприлюднюють постійно журналісти. Ця інформація не є легко доступною, але вона дуже часто з'являється у пресі. Тому я вважаю, що інженерно-технічному захисту треба приділити значно більшу увагу, а саме пункту 7.

Стосовно пункту 7. Технічний захист інформації, пропоную:

7.1.1. Акустичний (мовний) канал витоку інформації-мовний- видалити- є ще азбука Морзе та інші методи передачі інформації по акустичним каналам.

7.1.2.Електричний канал витоку інформації - що маєте на увазі? Пропоную поєднати з п.7.1.3.

П.7.1.2 Викласти у такий редакції:

7.1.2. Електромагнітний та електричний канал витоку інформації.

7.2. Методи та засоби технічного захисту інформації.

7.2.1. Пасивні методи та засоби захисту інформації від витоку технічними каналами.

7.2.2. Активні методи та засоби захисту інформації від витоку технічними каналами.

7.2.3. Методи пошуку та блокування засобів негласного отримання інформації.

7.2.4. Методика пошуку та блокування засобів негласного отримання інформації.

7.2.5. Пристрої та засоби технічного захисту інформації від витоку акустичними каналами, принципи роботи та умови використання.

7.2.6. Пристрої та засоби технічного захисту інформації від витоку електромагнітними та електричними каналами, принципи роботи та умови використання.

7.2.7. Пристрої та засоби технічного захисту інформації від витоку оптичними та оптоелектронними каналами, принципи роботи та умови використання.

7.2.8. Пристрої та засоби технічного захисту інформації від витоку параметричними каналами, принципи роботи та умови використання.

7.2.9. Інженерно-технічні системи. Системи відеоспостереження, охоронних сигналізацій, контроля доступу та інші технічні системи захисту інформації.

Пропозиції Шпатара П.М., кандидата технічних наук, доцента, завідувача кафедри радіотехніки та інформаційної безпеки Чернівецького національного університету ім. Ю.Федьковича, Ластівки Г.І., кандидата технічних наук, доцента, доцента кафедри радіотехніки та інформаційної безпеки Чернівецького національного університету ім. Ю.Федьковича; Рождественської М.Г., доцент кафедри радіотехніки та інформаційної безпеки Чернівецького національного університету ім. Ю.Федьковича

№ п/п		**Тема та її зміст**	**Зауваження та/або пропозиції**
1		**2**	**3**
	Зауваження загального характеру		
1		Різні	Пропонуємо конкретизувати зміст тем 2, 3, 4, 5, 7 аналогічно до теми 6 «Криптографічний захист інформації»
2		3. БЕЗПЕКА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ	Додати до теми 3 «Безпека інформаційно-комунікаційних систем» підпункти, пов’язані з класифікацією зловмисного програмного забезпечення (ПЗ) та атак на ІКС. Наприклад, додати як підпункт 4.2.6. Вага – 2% (відсотки пропонуємо врахувати на підставі пропозиції №7 даної таблиці). Або розшифрувати зміст підпунктів, в яких ці питання передбачені до розгляду
3		Різні	Просимо, за можливості, розшифровувати абревіатури,

			оскільки вони можуть залишитись у складі екзаменаційних питань і під час іспиту можуть викликати невірну трактовку здобувачами
1	2	3	
Зауваження за темами			
4.	Різні	Якщо загалом не передбачається уточнення (конкретизація) підпунктів за темами, просимо навести детальніше зміст наступних пунктів: 2.1.2. – Віртуалізація (принципи, гіпервізори). 2.1.3. - Архітектура комп'ютерів. 2.2.4. - Кількісна міра інформації. 2.2.5. - Завадостійкі коди. 2.3.1. - Архітектура операційних систем. 2.3.4. - Файлові системи. 3.2. - Програмні та програмно-апаратні комплекси ЗЗІ (усі підпункти). 5.4.1. - Поняття бізнес-процесу. 5.4.2. - Модель бізнес-процесу. 7.2.1. - Пасивні та активні методи і засоби захисту інформації від витоку технічними каналами	
5.	2.4. Моделі безпеки в інформаційній та/або кібербезпеці.	Пропонуємо перенести до п. 4.2. - Моделі загроз та моделі порушника. Або просимо розшифрувати детальніше вміст даних підпунктів	
6.	3.3.3. Політики резервного копіювання даних.	Пропонуємо перенести даний підпункт до пункту 3.1. - Захист інформації, що обробляється та зберігається в ІКС як підпункт 3.1.3	

7.	5.3. Аудит інформаційної та/або кібербезпеки.	Зменшити вагу підпунктів 5.3.2, 5.3.3, 5.3.4, до 1%
8.	6.1.6. Обчислення в системі чисел з плаваючою точкою.	Пропонуємо викласти даний підпункт у редакції: 6.1.6. - Обчислення в системі чисел з фіксованою та плаваючою точкою
9.	7.2.2. Системи відеоспостереження.	Пропонуємо зменшити вагу даного підпункту до 1%
10	7.2. Методи та засоби технічного захисту інформації.	Пропонуємо додати підпункт 7.2.3. – Методи виявлення та інструментального оцінювання (пошуку) технічних каналів витоку інформації. Вага – 1%
11	3.3.1. Організаційно-технічні заходи відновлення функціонування ІКС.	Пропонуємо збільшити вагу даного підпункту до 2%

Пропозиції denisdpua@i.ua

Щодо проєкту програми ЄДКІ зі спеціальності 125 «Кібербезпека» для першого (бакалаврського) рівня вищої освіти є такі пропозиції:

1) п. 3.2.3. «Системи контролю та управління доступом». Прохання уточнити в програмі, які конкретно системи маються на увазі. Можливо, мова йде про методи та/або механізми управління доступом в ІКС. Якщо ні, то вважаємо доцільно доповнити п. 3.1 відповідним п.п. (наприклад, «Методи управління доступом в ІКС»).

2) п. 4.1.2. «Вибір методів та засобів забезпечення необхідного рівня ІБ». Прохання уточнити в програмі, на чому має ґрунтуватися вибір, що означає «необхідний рівень ІБ» (наприклад, функціональні профілі захищеності або перелік послуг безпеки і т.ін.).

3) п. 4.1.1. «Проведення аудиту інформаційної безпеки та визначення на основі звіту з аудиту ризиків ІБ». Питання аудиту ІБ дублюються в п. 5.3. «Аудит інформаційної та/або кібербезпеки». В рамках КСЗІ доцільніше розглядати питання обслідування об’єкта.

4) п. 4.3. «Оцінка захищеності інформації в ІКС». Прохання уточнити в програмі, на основі чого має проводитися така оцінка, вказати нормативні документи (наприклад, відповідні НДТЗІ).

Пропозиції yaromenko2304@gmail.com.

До проєкту програми ЄДКІ зі спеціальності 125 «Кібербезпека» для першого (бакалаврського) рівня вищої освіти, що оприлюднений для обговорення є наступне зауваження: в проєкті наявний пункт 6.5. «Цифрова стеганографія», однак у Стандарті спеціальності 125 «Кібербезпека» для першого (бакалаврського) рівня вищої освіти стеганографія не розглядається, тобто не є обов'язковою для вивчення. Таким чином, є пропозиція або видалити вказаний пункт з програми, або залишити лише запитання з найпростішого методу – методу модифікації найменшого значущого біта.

Пропозиції Андрія Єфіменка, кандидата технічних наук, доцента, завідувача кафедри комп'ютерної інженерії та кібербезпеки Державного університету «Житомирська політехніка»

Прохання розглянути такі пропозиції щодо змін у Програмі ЄДКІ 125 КБ Бакалавр:

I. Зменшити до 5 % обсяг п.1. ЗАКОНОДАВЧА ТА НОРМАТИВНО-ПРАВОВА БАЗА, ДЕРЖАВНІ ТА МІЖНАРОДНІ ВИМОГИ, ПРАКТИКИ І СТАНДАРТИ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ ТА/АБО КІБЕРБЕЗПЕКИ

II. Усунути пункти 1.1.1. ЗУ про інформацію, про науково-технічну інформацію та 1.1.3. ЗУ «Про доступ до публічної інформації», оскільки вони є мало дотичними до спеціальності. Додати до п. 1 ЗУ «Про захист інформації в інформаційно-комунікаційних системах» (https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text).

III. Збільшити до 20% обсяг п. 2."ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНІЙ ТА/АБО КІБЕРБЕЗПЕЦІ;

IV. Розділити п. 2.1.1 на два підпункти Мережева модель OSI

Основні протоколи стеку TCP/IP та встановити їх обсяг відповідно 1% та 3%.

V. Збільшити до 25% обсяг п. 3."БЕЗПЕКА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ"

VI. Перенести п.6.4. до розділу 3. БЕЗПЕКА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ. А також п. 6.4.1. Об"єднати з пунктом 3.5.1. Віртуальні приватні мережі (VPN) і п. 6.4.2. Об"єднати з пунктом 3.5.3.

VII. Доповнити п. 3.5.2. протоколами аутентифікації Tacacs+, 802.1x.

VIII. Додати до п.3.5. Механізми безпеки комп'ютерних мереж підпункт

Механізми безпеки локальних мереж.

IX. Усунути п. 6.5. Цифрова стеганографія.

X. Зменшити до 15% обсяг п. 5. УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА / АБО КІБЕРБЕЗПЕКОЮ

Пропозиції Любчака В., завідувача кафедри Кібербезпеки СумДУ

1. Пропозиції до теми 1 «ЗАКОНОДАВЧА ТА НОРМАТИВНО-ПРАВОВА БАЗА, ДЕРЖАВНІ ТА МІЖНАРОДНІ ВИМОГИ, ПРАКТИКИ І СТАНДАРТИ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ ТА/АБО КІБЕРБЕЗПЕКИ».

Вважаємо необхідним додати знання Стратегії кібербезпеки України, затвердженої Указом Президента України №447/2021.

Також перелік в пунктах п 1.1.1. – п 1.1.6. конкретних законодавчих актів є обмеженим, наприклад доцільно додати Закон 1882-IX «Про критичну інфраструктуру» (КІ), підписаний Президентом України 10.12 2021р.

2. Пропозиції до теми 2 «ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНІЙ ТА/АБО КІБЕРБЕЗПЕЦІ».

2.1. Згідно ПОСТАНОВИ КАБІНЕТУ МІНІСТРІВ УКРАЇНИ від 7 липня 2021 р. № 762 визначено наступне

Шифр і найменування галузі знань	Код і найменування спеціальності	Код і найменування відповідної деталізованої галузі за Міжнародною стандартною класифікацією освіти	
12 Інформаційні технології	125 Кібербезпека	0612	Database and network design and administration

Для підсилення сутності спеціальності 125 «Кібербезпека» (адаптація до Міжнародних стандартів класифікації освіти) та визначальної ролі інформаційних технологій пропонуємо питому вагу теми №2 збільшити з 16% до 20 %.

Це можливо зробити за рахунок зменшення ваги наступних тем:

•№5 «УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА / АБО КІБЕРБЕЗПЕКОЮ» - з 20% до 18%,

•№6 «КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ» - з 13% до12 % ,

•№7 «ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ» - з 14% до 13% .

2.2. З пункту 2.2 «Методи і засоби обробки інформації» пропонуємо виділити новий пункт 2.5 «Алгоритмізація та програмування» наступного змісту:

2.5. Алгоритмізація та програмування 5%

2.5.1. Типові структури та алгоритми обробки даних 2% В

2.5.2. Програмування (без прив’язки до конкретної мови програмування): базові правила проектування, написання, тестування, налагодження і підтримка комп'ютерних програм

2% C

2.5.3. Основи об’єктно-орієнтованого програмування (класи, методи, інкапсуляція, успадкування, поліморфізм, абстракція)1% B

Пункт 2.2. викласти у наступній редакції:

2.2. Методи збору та обробки інформації. 4%

2.2.1. Математичне моделювання, статистична обробка, прогнозування 1% B

2.2.2. Методи сортування та пошуку даних. 1% B

2.2.3. Кількісна міра інформації. 1% B

2.2.4. Завадостійкі коди. 1% B

2.3. На нашу думку, уточнення потребують пункти 2.4 «Моделі безпеки в інформаційній та/або кібербезпеці» та 4.2 «Моделі загроз та моделі порушників». Зазначені у пп. 4.2.1 - 4.2.5 загрози мають відношення не тільки до комплексних систем захисту (пункт 4), але й до безпеки інформаційно-комунікаційних систем (пункт 3). У зв’язку з цим, вважаємо за доцільне питання щодо моделей загроз, порушника та вразливостей віднести до фундаментальних і додати відповідні питання у п. 2.4 «Моделі безпеки в інформаційній та/або кібербезпеці».

3. Пропозиції до теми 3 «БЕЗПЕКА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ».

Пропонуємо деталізувати пункт 3.2.3. «Системи контролю та управління доступом» на такі 2 складові:

3.2.3. Системи контролю та управління доступом 1% B

3.2.4. Фізична безпека: контроль доступу до об'єктів, контроль доступу персоналу, механізми захисту зовнішнього периметру 1% B

4. Пропозиції до теми 5 «УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА / АБО КІБЕРБЕЗПЕКОЮ».

4.1. Також зазначимо, що п. 4.1.1 «Проведення аудиту інформаційної безпеки та визначення на основі звіту з аудиту ризиків ІБ» частково дублюється з п. 5.3 «Аудит інформаційної та/або кібербезпеки». Можливо доречно п. 4.1.1 повністю перенести до п. 5.3.

4.2. Виникає питання щодо доцільності винесення п. 5.4 «Забезпечення безперервності бізнес-процесів», який є загальним і не містить специфіки спеціальності 125.

5. Пропозиції до теми 7 «ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ».

П.7.2.2. «Системи відеоспостереження» доцільно конкретизувати, на які саме питання буде зроблено акцент: складові систем, типи побудови систем, види фото- та відеофіксації, типи несанкціонованого втручання або фізично-технічні особливості функціонування складових систем відеоспостереження.

Пропозиції колектив кафедри робототехнічних і телекомунікаційних систем та кібербезпеки Черкаського державного технологічного університету

1. Затверджений Стандарт за даною спеціальністю №1074 від 04.10.18 р. не містить конкретних алгоритмів, шифрів, протоколів і т.п., тому кожен навчальний заклад може по своєму інтерпретувати Програмні результати навчання. Пропонується вилучити з Програми такі підпункти, які не отримали свого широкого відображення в навчальній літературі. Наприклад п.6.2.4. «Потокові шифри STRUMOK», який з'явився вже після затвердження самого стандарту і набору слухачів, які будуть проходити тест. З іншого боку, існують ряд стандартів, які є вже застарілими (п.6.2.3. Блокові шифри. DES), які вже не використовуються, і відповідно, можуть не вивчатися в навчальних закладах.

2. З огляду на затверджений Стандарт за даною спеціальністю просимо вилучити п.6.5 «Цифрова стеганографія» з Програми ЄДКІ, оскільки цей розділ не фігурує в Програмних результатах навчання. При внесенні змін до Стандарту можливі зміни і в Програмі, але в поточному варіанті Стандарту такі результати навчання відсутні.

3. Є доцільним відкорегувати зміст п.2. «ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ІНФОРМАЦІЙНІЙ ТА/АБО КІБЕРБЕЗПЕЦІ», оскільки пп.2.1.2 та 2.1.3 мало корелюють зі змістом даного пункту. Аналогічна ситуація і з п.2.2.4, п.2.2.5.

4. В представленій програмі спостерігається розбалансованість між змістом відповідних розділів і часткою розподіленого на них часу навчання. Наприклад, на п.6 «КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ» виділено всього 13%, але за змістовним наповненням і своєю СКЛАДНІСЮ даний матеріал потребує значно більших часових ресурсів. Тому пропонується збільшити розподіл частки матеріалу до 20-25%, або суттєво зменшити змістовне навантаження при 13%. Наприклад, на п.1. «ЗАКОНОДАВЧА ТА НОРМАТИВНО-ПРАВОВА БАЗА...» виділено 8%, що є співрозмірним з 13%, але неможливо навіть порівнювати складність опанування п.6 з п.1.

5. Є доцільним зменшити частку (у % співвідношенні) п.5 «УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА / АБО КІБЕРБЕЗПЕКОЮ» (з 20% до 10%) та п.7. «ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ» (з 14% до 7%), і відповідно, змістовним наповненням цих розділів.

6. п.6.4.1. «Протоколи захисту мережевого трафіку IPSec.» та п.6.4.2. «Протоколи безпечної передачі даних прикладного рівня: https.» мають дуже опосередковане відношення до п.6. «КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ».

7. В Програмі відсутні сучасні напрямки криптографічного захисту інформації, наприклад з використанням алгоритмів із застосуванням Еліптичних кривих. В той же час є досить суперечливим необхідність вивчення застарілого Радянського і Російського стандарту п.6.2.3. ГОСТ 28147. А такий стандарт, як п.6.2.3. ДСТУ 7624:2014 практично

ненаведений і неописаний в навчальних підручниках, і посібниках за даною спеціальністю. Тому є пропозиція уніфікувати цю частину п.6. таким чином, щоб вона була актуальною і доступною для вивчення здобувачами.

8. Деякі із запропонованих стандартів, наприклад п.6.2.4.2 ДСТУ 8845:2019 та інші, були запроваджені тільки з 2019 р. , коли вже були затверджені поточні Освітні програми і Навчальні Плани, які могли не враховувати такі нововведення.

9. Доцільно внести зміни в Стандарт за даною спеціальністю з врахуванням уніфікації Програмних результатів навчання для всіх ЗВО України. Зменшити кількість і конкретизувати Програмні результати навчання, щоб вони корелювали з Програмою ЄДКІ і була реальна можливість надавати здобувачам необхідні знання і вміння.

5. Інформація про рішення, прийняті за результатами обговорення:

Під час доопрацювання проєкту програми ЄФВВ зауваження та пропозиції, отримані під час громадського обговорення, враховано частково, а саме робоча група вирішила:

1. У пункті 1 «ЗАКОНОДАВЧА ТА НОРМАТИВНО-ПРАВОВА БАЗА, ДЕРЖАВНІ ТА МІЖНАРОДНІ ВИМОГИ, ПРАКТИКИ І СТАНДАРТИ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ ТА/АБО КІБЕРБЕЗПЕКИ» збільшити питому вагу до 10%.
2. У пункті 1.1. «Законодавча та нормативно-правова база України в галузі інформаційної та /або кібербезпеки» збільшити питому вагу до 7%.
3. Викласти у такій редакції пункт 1.1.2. «ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основні засади забезпечення кібербезпеки України»».
4. Вилучити пункт 1.1.3. «ЗУ «Про доступ до публічної інформації»».
5. Викласти у такій редакції пункт 1.1.4. «ЗУ «Про державну таємницю». «Про захист персональних даних»».
6. Вилучити пункт 1.1.5 «ЗУ «Про основні засади забезпечення кібербезпеки України»».
7. Додати два пункти з врахуванням зміни нумерації. **Пункт 1.1.5**. «Державні Стандарти України в галузі інформаційної та/або кібербезпеки ДСТУ 3396.0,1,2-97; ДСТУ ISO/IEC 15408-1:2017» з питомою вагою 1%, рівнем В. **Пункт 1.1.6. «**Нормативні документи з технічного захисту інформації НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу», НД ТЗІ 2.5-004-99. «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»» з питомою вагою 2%, рівнем В.

8. У пункті 1.2. «Міжнародні стандарти в галузі інформаційної та /або кібербезпеки» збільшити питому вагу до 3%.
9. Викласти у такій редакції пункт 1.2.1 «Регламенти ЄС в галузі кібербезпеки Регламент Європейського Парламенту і Ради (ЄС) 2019/881 від 17 квітня 2019 року «Про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій»».
10. Викласти у такій редакції пункт 1.2.2 «ISO 27001, ISO 27002, ISO 27003, ISO/IEC 15408- 2, ISO/IEC 15408-3» з питомою вагою 2%, рівнем В.
11. У пункті 2.1. «Інструментальні та прикладні застосунки в інформаційній та/або кібербезпеці» збільшити питому вагу до 4%.
12. У пункті 2.1.1. «Мережева модель OSI. Основні протоколи стеку TCP/IP» збільшити питому вагу до 2%.
13. У пункті 2.2. «Методи і засоби обробки інформації» збільшити питому вагу до 6%.
14. У пункті 2.2.1. «Алгоритмізація та програмування (без прив'язки до конкретної мови програмування)» збільшити питому вагу до 2%.
15. Викласти у такій редакції пункт 2.2.2 «Основи об'єктно-орієнтованого програмування (Класи, Методи, Перевантаження, Наслідування, Узагальнення)» з питомою вагою 2%, рівнем В.
16. У пункті 2.2.3. «Методи сортування та пошуку даних» збільшити питому вагу до 2%.
17. Вилучити пункт 2.2.4. «Кількісна міра інформації».
18. Вилучити пункт 2.2.5. «Завадостійкі коди».
19. У пункті 2.3. «Операційні системи» збільшити питому вагу до 6%.
20. У пункті 2.3.5. «Захисні механізми операційних систем» збільшити питому вагу до 2%.
21. Вилучити пункт 2.4. «Моделі безпеки в інформаційній та/або кібербезпеці».
22. Вилучити пункт 2.4.1. «Модель порушника».
23. Вилучити пункт 2.4.2. «Модель загроз».
24. Вилучити пункт 2.4.3. «Модель вразливостей».
25. Викласти у такій редакції пункт 3.2.1. «Антивіруси, міжмережеві екрани (призначення, архітектура, функції)».
26. Викласти у такій редакції пункт 3.2.2. «IPS, IDS (призначення, архітектура, функції)».
27. Викласти у такій редакції пункт 3.2.3. «Системи контролю та управління доступом в ІКС (Active Directory, ACL)».
28. У пункті 3.4. «Моніторинг процесів функціонування ІКС» зменшити питому вага до 3%.

29. У пункті 3.4.2. «Система візуалізації та управління подіями (SIEM)» зменшити питому вагу до 1%.
30. У пункті 3.5. «Механізми безпеки комп'ютерних мереж» збільшити питому вагу до 6%.
31. Викласти у такій редакції пункт 3.5.1. «Протоколи безпеки на канальному рівні» з питомою вагою 1%, рівнем В.
32. Викласти у такій редакції пункт 3.5.2. «Протоколи безпеки на мережному рівні (IPSec)» з питомою вагою 1%, рівнем В.
33. Викласти у такій редакції пункт 3.5.3. «Протоколи безпеки на транспортному/сеансовому рівні (SSL/TLS)» з питомою вагою 1%, рівнем В.
34. Викласти у такій редакції пункт 3.5.4. «Протоколи безпеки прикладного рівня (HTTPS)» з питомою вагою 1%, рівнем В.
35. Викласти у такій редакції пункт 3.5.5. «Протоколи автентифікації прикладного рівня (RADIUS)» з питомою вагою 1%, рівнем В.
36. Викласти у такій редакції пункт 3.5.6. «Віртуальні приватні мережі (VPN)» з питомою вагою 1%, рівнем В.
37. Викласти у такій редакції пункт 4.1.1 «Дослідження середовищ функціонування ІС – середовища користувачів, обчислювальної системи, фізичного середовища, інформаційного середовища та побудова моделі загроз».
38. Викласти у такій редакції пункт 4.2.5. «Загрози автентичності».
39. У пункті 4.3. «Оцінка захищеності інформації в ІКС» визначити питому вагу 2%, рівнем В.
40. Вилучити пункт 4.3.1. «Концептуальна схема оцінки безпеки інформації».
41. Вилучити пункт 4.3.2. «Кількісна та якісна оцінки безпеки інформації».
42. У пункті 5. «УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА / АБО КІБЕРБЕЗПЕКОЮ» зменшити питому вагу до 18%.
43. У пункті 5.2. «Управління ризиками в інформаційній та / або кібербезпеці» збільшити питому вагу до 10%.
44. У пункті 5.2.1. «Ризики інформаційної безпеки» збільшити питому вагу до 5%.
45. У пункті 5.2.2. «Аналіз та оцінка ризику. Прийняття ризику. Зменшення ризику. Страхування (перекладання) ризику» збільшити питому вагу до 5%.
46. Викласти у такій редакції пункт 5.3. «Політика інформаційної безпеки» з питомою вагою 4%, рівнем В.
47. Викласти у такій редакції пункт 5.3.1. «Розробка політик ІБ при забезпеченні бізнес-процесів» з питомою вагою 2%, рівнем В.
48. Викласти у такій редакції пункт 5.3.2. «Дотримання політик ІБ при забезпеченні бізнес-процесі» з питомою вагою 2%, рівнем В.
49. Вилучити пункт 5.3.3. «Аудит на основі стандартів ІБ».

50. Вилучити пункт 5.3.4. «Аудит на основі експериментальних досліджень ІС».
51. У пункті 5.4. «Забезпечення безперервності бізнес-процесів» зменшити питому вагу до 2%.
52. Викласти у такій редакції пункт 5.4.1. «Поняття та моделі бізнес-процесів» з питомою вагою 2%.
53. Вилучити пункт 5.4.2. «Модель бізнес-процесу».
54. Викласти у такій редакції пункт 6.2.3. «Блокові шифри. DES, AES, ДСТУ ГОСТ 28147-2009, ДСТУ 7624:2014 (довжина ключів, довжина блоку вхідного тексту, кількість раундів, крипостійкість, режими роботи згідно ДСТУ ISO/IEC 10116:2019)».
55. Вилучити пункт 6.2.3.1. «DES».
56. Вилучити пункт 6.2.3.2. «AES».
57. Вилучити пункт 6.2.3.3. «ДСТУ ГОСТ 28147-2009».
58. Вилучити пункт 6.2.3.4. «ДСТУ 7624:2014».
59. Викласти у такій редакції пункт 6.2.4. «Потокові шифри. RC4, STRUMOK. (довжина ключів, крипостійкість)».
60. Вилучити пункт 6.2.4.1. «RC4».
61. Вилучити пункт 6.2.4.2. «ДСТУ 8845:2019».
62. Вилучити пункт 6.4. «Криптографічні протоколи».
63. Вилучити пункт 6.4.1. «Протоколи захисту мережевого трафіку IPSec».
64. Вилучити пункт 6.4.2. «Протоколи безпечної передачі даних прикладного рівня: https».
65. У пункті 6.5.3. «Відкриті, напівзакриті, закриті стеганосистеми» визначили рівень А.
66. У пункті 6.4.5. «Метод модифікації найменшого значущого біта» визначили рівень В.
67. Вилучити пункт 6.5.6. «Атаки на стеганосистеми».
68. У пункті 7.1. «Технічні канали витоку інформації» зменшити питому вагу до 6%.
69. Викласти у такій редакції пункт 7.1.1. «Вібро-акустичний канал витоку інформації».
70. У пункті 7.1.2. «Електричний канал витоку інформації» зменшити питому вагу до 1%.
71. У пункті 7.1.3. «Електромагнітний канал витоку інформації» зменшити питому вагу до 1%.
72. У пункті 7.1.4. «Оптичний та оптоелектронний канал витоку інформації» зменшити питому вагу до 1%.
73. У пункті 7.1.5. «Параметричний канал витоку інформації» зменшити питому вагу до 1%.

74. У пункті 7.2. «Методи та засоби технічного захисту інформації» збільшити питому вагу до 8%.
75. У пункті 7.2.1. «Пасивні методи та засоби захисту інформації від витоку технічними каналами» зменшити питому вагу до 1%.
76. Викласти у такій редакції пункт 7.2.2. «Активні методи та засоби захисту інформації від витоку технічними каналами» з питомою вагою 1%.
77. Викласти у такій редакції пункт 7.2.3. «Методи пошуку та блокування засобів негласного отримання інформації» з питомою вагою 1%.
78. Викласти у такій редакції пункт 7.2.4. «Методи та засоби технічного захисту інформації від витоку вібро-акустичними каналами» з питомою вагою 1%.
79. Викласти у такій редакції пункт 7.2.5. «Методи та засоби технічного захисту інформації від витоку електромагнітними та електричними каналами» з питомою вагою 1%.
80. Викласти у такій редакції пункт 7.2.6. «Методи та засоби технічного захисту інформації від витоку оптичними та оптоелектронними каналами» з питомою вагою 1%.
81. Викласти у такій редакції пункт 7.2.7. «Методи та засоби технічного захисту інформації від витоку параметричними каналами» з питомою вагою 1%.
82. Викласти у такій редакції пункт 7.2.8. «Системи відеоспостереження, охоронних сигналізацій, контролю доступу» з питомою вагою 1%.