МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ
Декан факультету
_____ Інна КОНДЮС
«29» серпня 2026 р.

ЗАТВЕРДЖУЮ
Перший проректор
_____ Надія КОВАЛЬЧУК
«29» серпня 2026 р.

СИЛАБУС

з освітнього компонента «Управління інформаційною безпекою»
ступінь вищої освіти – бакалавр
галузь знань – 12 Інформаційні технології
спеціальність – 125 Кібербезпека та захист інформації
освітня програма – Кібербезпека

Кафедра кібербезпеки

Силабус склав(ла) асистент (ПП) кафедри кібербезпеки Олег КУЛАКЕВИЧ

Силабус затверджений на засіданні кафедри кібербезпеки, протокол № 2 від «28» серпня 2026 р.

Завідувач кафедри к.т.н., доцент Сергій КОСТЮЧКО

Розглянуто та схвалено групою забезпечення освітньої програми «Кібербезпека», протокол № 2 від «28» серпня 2026 р.

Гарант ОП «Кібербезпека» к.т.н., доцент Сергій КОСТЮЧКО

Схвалено науково-методичною радою університету, протокол № 1/а від «29» серпня 2026 р.

Затверджений силабус онлайн:
https://e.lntu.edu.ua/syllabus/3018

Луцьк – 2026

СИЛАБУС ОСВІТНЬОГО КОМПОНЕНТА «Управління інформаційною безпекою»

Освітня програма	Кібербезпека
Галузь знань / Спеціальність	12 Інформаційні технології / 125 Кібербезпека та захист інформації
Рівень вищої освіти	перший (бакалаврський)
Статус дисципліни	нормативна
Мова викладання	українська
Обсяг	4 кредити ECTS / 120 годин, семестр 5
Форма контролю	екзамен
Викладач(і)	асистент (пп) Олег КУЛАКЕВИЧ

1. Мета і завдання дисципліни

Мета: Метою викладання є систематизація інформації щодо розроблення, впровадження та експлуатації систем захисту інформації на об’єктах інформаційної діяльності, формування навичок аналізу систем забезпечення інформаційної безпеки з метою впровадження найкращих практик захисту інформації; формування у майбутніх фахівців здатності діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.

Завдання: Завдання дисципліни полягає в поглибленні знань в області безпеки комп’ютерних мереж та систем. Предмет присвячений вивченню та засвоєнню сучасних технологій, які використовуються для організації кібербезпеки.

Пререквізити: Нормативно-правове забезпечення кібербезпеки, Основи кібербезпеки

2. Компетентності

СК02 — Здатність до використання інформаційно комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.

СК05 — Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

СК08 — Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

СК12 — Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

3. Структура дисципліни, розподіл годин, зв'язок тем з компетентностями

№	Назва теми	**Лекції** денна/ заочна	**Лаб.** денна/ заочна	**Самост. робота** денна/ заочна	**Разом**	**Методи навчання**	**Методи оцінювання**	**ЗК та СК**
Змістовий модуль 1.								

№	Назва теми	Лекції денна/ заочна	Лаб. денна/ заочна	Самост. робота денна/ заочна	Разом	Методи навчання	Методи оцінювання	ЗК та СК
1	Тема 1. Передумови та основні напрямки розвитку менеджменту у сфері інформаційної безпеки. Управління кіберінцидентами.	1/–	2/0,25	5/5	8/5,25	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК02, СК05, СК08, СК12
2	Тема 2. Діяльність міжнародних організацій в сфері інформаційної безпеки.	1/–	2/0,25	5/5	8/5,25	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК02, СК05, СК12, СК08
3	Тема 3. Стандартизація в сфері менеджменту інформаційної безпеки.	1/–	2/0,25	5/5	8/5,25	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК02, СК05, СК08, СК12
4	Тема 4. Роботи спеціалізованих міжнародних організацій та об'єднань в галузі інформаційної безпеки. Управління ризиками в інформаційній та кібербезпеці.	1/0,25	2/0,25	5/5	8/5,5	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК02, СК05, СК08, СК12
5	Тема 5. Управління інформаційною безпекою на рівні великих постачальників інформаційних систем.	1/0,25	2/0,25	5/5	8/5,5	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК02, СК05, СК08, СК12
6	Тема 6. Організаційне забезпечення інформаційної безпеки на Державному рівні: практика США.	1/0,25	2/0,25	5/5	8/5,5	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК02, СК05, СК08, СК12

№	Назва теми	Лекції денна/ заочна	Лаб. денна/ заочна	Самост. робота денна/ заочна	Разом	Методи навчання	Методи оцінювання	ЗК та СК
7	Тема 7. Забезпечення інформаційної безпеки на державному рівні: практика України.	1/0,25	2/0,5	5/5	8/5,75	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК02, СК05, СК08, СК12
Змістовий модуль 2.								
8	Тема 8. Забезпечення інформаційної безпеки на державному рівні: практика України (криптографічні методи захисту).	1/–	2/0,5	5/8	8/8,5	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК02, СК05, СК08, СК12
9	Тема 9. Забезпечення інформаційної безпеки на державному рівні: практика України (технічні методи захисту). Характеристика кіберзлочинності. Стан кіберзлочинності в Україні. Боротьба із кіберзлочинами.	1/–	2/0,5	5/9	8/9,5	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК02, СК05, СК08, СК12
10	Тема 10. Менеджмент інформаційної безпеки на рівні підприємства: основні напрямки і структура політики безпеки.	1/–	2/0,5	5/10	8/10,5	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК02, СК05, СК08, СК12
11	Тема 11. Зміст деталізованої політики безпеки.	1/–	2/0,5	5/10	8/10,5	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК02, СК05, СК08, СК12
12	Тема 12. Департамент інформаційної безпеки і робота з персоналом.	1/0,25	2/0,5	5/10	8/10,75	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК02, СК05, СК08, СК12

№	Назва теми	Лекції денна/ заочна	Лаб. денна/ заочна	Самост. робота денна/ заочна	Разом	Методи навчання	Методи оцінювання	ЗК та СК
13	Тема 13. Організація реагування на надзвичайні ситуації (інциденти).	1/0,25	2/0,5	5/10	8/10,75	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК02, СК05, СК08, СК12
14	Тема 14. Аудит стану інформаційної безпеки на підприємстві. Надання послуг у сфері інформаційної безпеки (страхування).	1/0,25	2/0,5	5/10	8/10,75	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК02, СК05, СК08, СК12
15	Тема 15. Міжнародний стандарт ISO/IEC 27001 перелік захисних заходів та їх цілей.	1/0,25	2/0,5	5/10	8/10,75	МН1, МН2, МН3, МН4, МН5	МО1, МО2, МО4, МО5	СК02, СК05, СК08, СК12
	Разом	**15/2**	**30/6**	**75/112**	**120/120**			

Легенда: ЗК — загальна компетентність (номер за п. 2); СК — спеціальна (фахова) компетентність (номер за п. 2). Повне формулювання кожного коду наводиться в ОП / стандарті спеціальності.

Методи навчання: МН1 — словесний метод (лекція, дискусія, співбесіда тощо); МН2 — практичний метод (лабораторні та практичні заняття); МН3 — наочний метод (метод ілюстрацій і метод демонстрацій); МН4 — робота з навчально-методичною літературою (конспектування, тезування, анотування, рецензування, складання реферату); МН5 — відеометод у сполученні з новітніми інформаційними технологіями та комп'ютерними засобами навчання (дистанційні, мультимедійні, веб-орієнтовані тощо).

Методи оцінювання: МО1 — екзамен; МО2 — усне або письмове опитування; МО4 — тестування; МО5 — командні проєкти.

4. Результати навчання

ПРН05. адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат;

ПРН08. готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки;

ПРН09. впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;

ПРН16. реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативноправових документів;

ПРН21. вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційнотелекомунікаційних (автоматизованих) системах;

ПРН22. вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційнотелекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки;

ПРН30. здійснювати оцінювання можливості несанкціонованого доступу до елементів

інформаційно-телекомунікаційних систем;

ПРН32. вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;

ПРН34. приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;

ПРН38. інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційнотелекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації;

ПРН40. інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації;

ПРН45. застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;

ПРН51. підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах;

5. Цілі сталого розвитку

ЦСР 8 – Гідна праця та економічне зростання

ЦСР 9 – Промисловість, інновації та інфраструктура

ЦСР 16 – Мир, справедливість та сильні інститути

6. Неформальна освіта

Рекомендовані курси, тренінги, стажування та інші: результати навчання, здобуті у формальній, неформальній чи інформальній освіті, можуть бути визнані відповідно до процедур ЛНТУ. Підтвердженнями можуть бути сертифікати тематичних тренінгів, вебінарів чи онлайн-курсів разом з описом досягнутих результатів навчання та, за потреби, коротке верифікаційне завдання або портфоліо.

7. Критерії та форми контролю

Оцінювання — за 100-бальною шкалою (національна шкала / ЄКТС). Підсумковий бал = поточний контроль (30 %) + модульний контроль (30 %) + екзамен (40 %).

Академічна доброчесність: самостійне виконання завдань; коректне посилання на джерела; позначення частин тексту, згенерованих засобами ШІ. Порушення академічної доброчесності не толеруються.

8. Зміст тем

Тема 1. Передумови та основні напрямки розвитку менеджменту у сфері інформаційної безпеки. Управління кіберінцидентами.

Передумови становлення та розвитку менеджменту інформаційної безпеки. Основні поняття, принципи та завдання управління інформаційною безпекою. Системний і ризик-орієнтований підходи до забезпечення інформаційної безпеки. Основні етапи розвитку систем менеджменту інформаційної безпеки. Поняття та класифікація кіберінцидентів. Організація процесів виявлення, аналізу, локалізації та усунення кіберінцидентів. Життєвий цикл управління інцидентами інформаційної безпеки.

Тема 2. Діяльність міжнародних організацій в сфері інформаційної безпеки.

Роль міжнародного співробітництва в забезпеченні інформаційної та кібербезпеки. Діяльність ООН, НАТО, Європейського Союзу та Ради Європи у сфері кібербезпеки. Міжнародні ініціативи щодо протидії кіберзагрозам і кіберзлочинності. Механізми обміну інформацією про кіберінциденти. Міжнародне співробітництво у сфері захисту критичної інформаційної інфраструктури. Участь України в міжнародних програмах і проєктах із кібербезпеки.

Тема 3. Стандартизація в сфері менеджменту інформаційної безпеки.

Мета та завдання стандартизації інформаційної безпеки. Міжнародні та національні стандарти управління інформаційною безпекою. Структура та основні положення стандартів серії ISO/IEC 27000. Вимоги ISO/IEC 27001 до системи менеджменту інформаційної безпеки. Практичне застосування ISO/IEC 27002 та ISO/IEC 27005. Використання NIST Cybersecurity Framework для управління кібербезпекою. Сертифікація, аудит та оцінювання відповідності систем менеджменту інформаційної безпеки.

Тема 4. Роботи спеціалізованих міжнародних організацій та об'єднань в галузі інформаційної безпеки. Управління ризиками в інформаційній та кібербезпеці.

Діяльність ENISA, FIRST, CERT та CSIRT у сфері інформаційної безпеки. Міжнародна координація реагування на кіберінциденти. Обмін інформацією про вразливості, загрози та індикатори компрометації. Поняття та класифікація ризиків інформаційної безпеки. Методи ідентифікації, аналізу та оцінювання кіберризиків. Кількісні та якісні методи оцінювання ризиків. Стратегії оброблення ризиків і моніторинг ефективності заходів захисту.

Тема 5. Управління інформаційною безпекою на рівні великих постачальників інформаційних систем.

Особливості менеджменту інформаційної безпеки у великих IT-компаніях. Корпоративні політики та моделі управління кібербезпекою. Практики забезпечення інформаційної безпеки компаній Microsoft, Google, Amazon та інших постачальників інформаційних систем. Управління ідентифікацією та доступом. Захист хмарної інфраструктури та корпоративних інформаційних ресурсів. Забезпечення безпеки життєвого циклу програмного забезпечення. Управління вразливостями, кіберінцидентами та безперервністю бізнес-процесів.

Тема 6. Організаційне забезпечення інформаційної безпеки на Державному рівні: практика США.

Державна політика США у сфері інформаційної та кібербезпеки. Організаційна структура національної системи кібербезпеки. Повноваження та функції CISA, NIST, NSA та інших державних установ. Нормативно-правове регулювання захисту державних інформаційних ресурсів. Організація захисту критичної інформаційної інфраструктури. Національні механізми реагування на кіберінциденти. Державно-приватне партнерство у сфері забезпечення кібербезпеки.

Тема 7. Забезпечення інформаційної безпеки на державному рівні: практика України.

Основні засади державної політики України у сфері інформаційної та кібербезпеки. Нормативно-правове забезпечення захисту інформаційних ресурсів. Суб'єкти національної системи кібербезпеки та їх повноваження. Діяльність Держспецзв'язку, СБУ, Національної поліції та CERT-UA. Організація захисту державних інформаційних систем і критичної інфраструктури. Координація діяльності суб'єктів забезпечення кібербезпеки. Основні напрями розвитку національної системи кібербезпеки України.

Тема 8. Забезпечення інформаційної безпеки на державному рівні: практика України (криптографічні методи захисту).

Основні принципи та завдання криптографічного захисту інформації. Нормативно-правове регулювання криптографічного захисту інформації в Україні. Симетричні та асиметричні криптографічні алгоритми. Національні стандарти криптографічного захисту інформації. Електронні підписи, сертифікати відкритих ключів та інфраструктура відкритих ключів (PKI). Методи забезпечення конфіденційності, цілісності та автентичності інформації. Організація управління криптографічними ключами. Державний контроль та оцінювання відповідності засобів криптографічного захисту інформації.

Тема 9. Забезпечення інформаційної безпеки на державному рівні: практика України (технічні методи захисту). Характеристика кіберзлочинності. Стан кіберзлочинності в Україні. Боротьба із кіберзлочинами.

Основні принципи та завдання технічного захисту інформації в Україні. Нормативно-правове регулювання технічного захисту інформації. Організаційні та інженерно-технічні методи захисту

інформаційних ресурсів. Захист інформації від витоку технічними каналами. Засоби контролю доступу, мережевого захисту та виявлення несанкціонованих дій. Оцінювання відповідності систем і засобів технічного захисту інформації. Поняття, класифікація та основні види кіберзлочинів. Особливості кіберзлочинності в Україні. Діяльність правоохоронних органів щодо виявлення, розслідування та протидії кіберзлочинам. Міжнародне співробітництво у сфері боротьби з кіберзлочинністю.

Тема 10. Менеджмент інформаційної безпеки на рівні підприємства: основні напрямки і структура політики безпеки.

Мета, завдання та принципи організації менеджменту інформаційної безпеки підприємства. Формування корпоративної системи управління інформаційною безпекою. Організаційна структура та розподіл відповідальності за забезпечення інформаційної безпеки. Основні складові та порядок розроблення політики інформаційної безпеки. Управління інформаційними активами, ризиками та доступом до інформаційних ресурсів. Організація захисту персональних даних і комерційної таємниці. Забезпечення безперервності діяльності та реагування на інциденти кібербезпеки. Контроль виконання політики безпеки, внутрішній аудит та оцінювання ефективності системи менеджменту інформаційної безпеки.

Тема 11. Зміст деталізованої політики безпеки.

Призначення та структура деталізованої політики інформаційної безпеки підприємства. Основні принципи розроблення та впровадження політик безпеки. Класифікація інформаційних активів та визначення вимог до їх захисту. Політика управління доступом та ідентифікації користувачів. Політики парольного захисту, використання корпоративних мереж, електронної пошти та мобільних пристроїв. Забезпечення захисту персональних даних і конфіденційної інформації. Порядок контролю виконання, перегляду та актуалізації політик інформаційної безпеки.

Тема 12. Департамент інформаційної безпеки і робота з персоналом.

Організаційна структура та основні функції департаменту інформаційної безпеки підприємства. Розподіл повноважень і відповідальності між працівниками підрозділу інформаційної безпеки. Функції керівника служби інформаційної безпеки (CISO). Організація взаємодії департаменту інформаційної безпеки з іншими структурними підрозділами. Управління кадровими ризиками інформаційної безпеки. Організація навчання, інструктажів та підвищення обізнаності персоналу з питань кібербезпеки. Протидія соціальній інженерії та внутрішнім загрозам. Контроль дотримання працівниками встановлених політик і процедур інформаційної безпеки.

Тема 13. Організація реагування на надзвичайні ситуації (інциденти).

Поняття та класифікація надзвичайних ситуацій та інцидентів інформаційної безпеки. Основні принципи організації реагування на кіберінциденти. Формування команди реагування та розподіл функціональних обов'язків. Розроблення планів реагування на інциденти та забезпечення безперервності діяльності підприємства. Методи виявлення, аналізу, локалізації та усунення наслідків інцидентів. Організація резервного копіювання та відновлення інформаційних систем. Документування інцидентів і проведення післяінцидентного аналізу. Оцінювання ефективності заходів реагування та вдосконалення процедур управління інцидентами.

Тема 14. Аудит стану інформаційної безпеки на підприємстві. Надання послуг у сфері інформаційної безпеки (страхування).

Мета, завдання та основні принципи аудиту інформаційної безпеки підприємства. Види внутрішнього та зовнішнього аудиту інформаційної безпеки. Основні етапи планування, проведення та документування аудиторських перевірок. Методи оцінювання захищеності інформаційних систем і відповідності встановленим вимогам. Аналіз вразливостей, загроз і ризиків інформаційної безпеки. Підготовка аудиторського звіту та рекомендацій щодо вдосконалення системи захисту інформації. Основні види послуг у сфері інформаційної та кібербезпеки. Поняття та принципи кіберстрахування. Оцінювання кіберризиків для визначення умов страхування. Особливості страхового покриття фінансових наслідків кіберінцидентів.

Тема 15. Міжнародний стандарт ISO/IEC 27001 перелік захисних заходів та їх цілей.

Призначення, структура та сфера застосування міжнародного стандарту ISO/IEC 27001. Основні вимоги до системи менеджменту інформаційної безпеки (СМІБ). Ризик-орієнтований підхід до вибору заходів захисту інформації. Структура та призначення Додатка А стандарту ISO/IEC 27001:2022. Організаційні, кадрові, фізичні та технологічні заходи захисту інформації. Визначення цілей застосування захисних заходів. Порядок вибору, обґрунтування та впровадження контролів інформаційної безпеки. Формування декларації застосовності (Statement of Applicability, SoA). Моніторинг, оцінювання результативності та постійне вдосконалення системи менеджменту інформаційної безпеки.

9. Опис ІЗ/КПІЗ

Не передбачено навчальним планом.

10. Загальні вимоги

Освітній процес регулюється академічними правилами ЛНТУ. Здобувачі освіти зобов’язані ознайомитися з вимогами, визначеними Кодексом академічної доброчесності ЛНТУ та Політикою етичного використання штучного інтелекту в ЛНТУ, і дотримуватися принципів академічної доброчесності та етичного використання штучного інтелекту в освітній діяльності.

Академічна доброчесність. Учасники освітнього процесу зобов’язані дотримуватися Закону України «Про академічну доброчесність» від 18.12.2025 № 4742-IX та внутрішніх нормативних документів ЛНТУ. Не допускаються академічний плагіат, фабрикація, фальсифікація, привласнення авторства, несамостійне виконання завдань, а також недоброчесне використання результатів, згенерованих штучним інтелектом.

Використання штучного інтелекту. Інструменти штучного інтелекту можуть використовуватися для пошуку ідей, пояснення методів, попереднього структурування, мовного редагування та допоміжного аналізу неконфіденційних даних, якщо конкретне завдання не передбачає повністю самостійного виконання. Здобувач освіти має зазначати використаний інструмент, мету та етап його застосування, перевіряти факти й розрахунки та самостійно обґрунтовувати висновки.

11. Література

ІІ. Наукові праці

Праці інших авторів:

1. Pascoe C., Quinn S., Scarfone K. The NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg : National Institute of Standards and Technology, 2024. NIST Cybersecurity White Paper No. 29. DOI: 10.6028/NIST.CSWP.29.

2. Nelson A., Rekhi S., Souppaya M., Scarfone K. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. Gaithersburg : National Institute of Standards and Technology, 2025. NIST Special Publication 800-61 Rev. 3. DOI: 10.6028/NIST.SP.800-61r3.

3. NIS2 Technical Implementation Guidance / European Union Agency for Cybersecurity. Heraklion : ENISA, 2025. URL: https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance.

4. ENISA Threat Landscape 2025 / European Union Agency for Cybersecurity. Heraklion : ENISA, 2025. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025.

5. NIS Investments 2025 / European Union Agency for Cybersecurity. Heraklion : ENISA, 2025. URL: https://www.enisa.europa.eu/publications/nis-investments-2025.