



СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Менеджмент в системі корпоративної інформаційної безпеки

Рівень вищої освіти	Другий (магістерський)
Код та назва спеціальності, галузь знань	F5«Кібербезпека та захист інформації», F «Інформаційні технології»
Тип та назва освітньої програми	Освітньо-професійна програма «Кібербезпека та захист інформації»
Статус навчальної дисципліни	Обов'язкова компонента (ОК-5)
Курс, семестр викладання	1 курс, 2 семестр
Трудомісткість навчальної дисципліни	Денна (очна) форма навчання (5 кредитів ЄКТС (150 годин)): лекції – 28 год., практ. зан. – 28 год., самост. роб. – 94 год. Заочна форма навчання (5 кредитів ЄКТС (150 годин)): лекції – 18 год., практ. зан. – 18 год., самост. роб. – 114 год.
Мова викладання	Українська
Кафедра	Кібербезпеки та технічного захисту інформації
Факультет	Інформаційних технологій та кібербезпеки

Викладачі



Васіліу Євген Вікторович, професор кафедри кібербезпеки та технічного захисту інформації, д. т. н., професор
E-mail: y.v_vasiliu@suitt.edu.ua
Тел.: +380673029949
Консультації: щоп'ятниці з 14:00 до 16:00 год., ауд. 313.
(головний корпус)



Стайкуца Сергій Володимирович, доцент кафедри кібербезпеки та технічного захисту інформації, к. філ. н., доцент
E-mail: s.v_staikutsa@suitt.edu.ua
Консультації: щоп'ятниці з 14³⁰ до 15³⁰ год., ауд. 218
(головний корпус)

Мета дисципліни	– формування у здобувачів вищої освіти системи знань та практичних навичок щодо принципів і методів менеджменту корпоративної інформаційної безпеки, організації та стратегічного планування системи безпеки,
-----------------	---

	управління інформаційними ризиками, розроблення та впровадження політик, стандартів і процедур безпеки, управління персоналом, а також управління бізнес-процесами та забезпечення неперервності бізнесу, зокрема розроблення програм і планів забезпечення неперервності та оцінювання готовності організації до кризових ситуацій.
Компетентності, формуванню яких сприяє дисципліна	ЗК1. Здатність застосовувати знання в практичних ситуаціях. ЗК3. Здатність до абстрактного мислення, аналізу та синтезу. СК2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. СК4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог. СК5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. СК7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. СК12. Здатність ефективно використовувати на практиці різні теорії в області навчання технологіям, засобам та організаційним аспектам безпеки інформаційних і комунікаційних систем та мереж. СК16. Здатність аналізувати потреби та вимоги користувачів (замовників) щодо захисту інформації та кіберзахисту з метою впровадження систем та комплексів захисту інформації.
Програмні результати навчання	ПРН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. ПРН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення. ПРН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. ПРН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки. ПРН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. ПРН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень. ПРН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи

кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.

ПРН24. Розроблювати плани аварійного відновлення та безперервності операцій в інформаційних, електронних, комунікаційних та інформаційно-комунікаційних системах.

ПРН34. Приймати участь в організації та навчанні (підвищенні кваліфікації) працівників структурних підрозділів підприємства (організації), до функцій яких входять питання захисту інформації та кібербезпеки, з відповідних питань.

Програма навчальної дисципліни

Тема 1. Основи менеджменту корпоративної інформаційної безпеки та організаційна модель безпеки.

- 1.1. Поняття та завдання менеджменту інформаційної безпеки. Взаємозв'язок цілей безпеки з цілями та місією організації. Безперервний процес управління безпекою.
- 1.2. Організаційна модель безпеки. Комплекс технічних, адміністративних і фізичних компонентів, процедур та бізнес-процесів. Конфіденційність, цілісність і доступність інформації.
- 1.3. Операційні, тактичні та стратегічні цілі безпеки. Підхід «зверху-вниз» та роль вищого керівництва.

Тема 2. Адміністрування корпоративної інформаційної безпеки та захисні заходи.

- 2.1. Організація адміністрування безпеки. Розподіл обов'язків, структура підзвітності, контроль і моніторинг.
- 2.2. Адміністративні, технічні (логічні) та фізичні заходи захисту. Взаємодія захисних механізмів і процедур.
- 2.3. Основні принципи безпеки. Вимоги до захисту інформації та обмеження підходу «безпека через невідомість».

Тема 3. Цілі, організаційне та стратегічне планування корпоративної інформаційної безпеки.

- 3.1. Цілі та плани організації, місія організації та її вплив на планування безпеки. Стадії процесу управління.
- 3.2. Стратегічне планування інформаційної безпеки. Взаємозв'язок бізнес-цілей, ІТ-цілей і цілей безпеки.
- 3.3. Формулювання функціональних стратегій, SWOT-аналіз та планування дій у кризових ситуаціях.

Тема 4. Управління інформаційними ризиками в корпоративному середовищі.

- 4.1. Поняття інформаційного ризику та основні категорії ризиків: фізичний збиток, дії людини, несправності обладнання, внутрішні та зовнішні атаки, неправильне використання і втрата даних, програмні помилки.
- 4.2. Управління інформаційними ризиками (IRM): виявлення та оцінювання ризиків, зниження їх до прийнятного рівня та підтримання цього рівня.
- 4.3. Політика управління інформаційними ризиками та IRM-група. Прийнятний рівень ризику, розподіл ролей, ресурси, бюджет, метрики та зв'язок зі стратегічним плануванням.

Тема 5. Аналіз та обробка ризиків корпоративної інформаційної безпеки.

- 5.1. Цілі та етапи аналізу ризиків. Ідентифікація активів, їх цінності, загроз і вразливостей. Оцінювання можливого впливу на бізнес.
- 5.2. Кількісний та якісний аналіз ризиків. Визначення пріоритетів ризиків та економічне обґрунтування захисних заходів.
- 5.3. Методи аналізу збоїв і дефектів, зокрема FMEA та аналіз дерева збоїв. Загальний і залишковий ризик, вибір та обробка ризиків.

Тема 6. Політики,

- 6.1. Програма безпеки та її основні компоненти. Політика інформаційної безпеки як основа програми безпеки, її

стандарти, базиси, керівництва та процедури корпоративної інформаційної безпеки.	цілі, область дії та відповідальність. 6.2. Стандарти, базиси, методичні вказівки та процедури. Вимоги до їх розроблення, впровадження, актуалізації та контролю виконання. 6.3. Впровадження програми безпеки, управління змінами, відповідність законодавчим і регуляторним вимогам, планування реагування на інциденти.
Тема 7. Класифікація інформації та розподіл відповідальності в корпоративній системі безпеки.	7.1. Класифікація інформації та управління класифікованими даними. Визначення вимог до доступу, маркування, зберігання, резервного копіювання та належного знищення інформації. 7.2. Рівні відповідальності в організації: вище керівництво, функціональне та оперативне керівництво. 7.3. Ролі у системі управління безпекою: власник даних, відповідальний за зберігання даних, власник системи, адміністратор та аналітик безпеки, власник процесу, користувач, аудитор та інші.
Тема 8. Управління персоналом та навчання з питань корпоративної інформаційної безпеки.	8.1. Людський фактор як складова ризику інформаційної безпеки. Структура обов'язків, розмежування повноважень і принцип розподілу обов'язків. 8.2. Безпека персоналу: вимоги під час прийому на роботу, контроль співробітників, посадові інструкції, управління доступом та заходи безпеки при звільненні. 8.3. Навчання та підвищення обізнаності з питань безпеки. Види тренінгів, оцінювання результатів навчання та спеціалізована підготовка персоналу.
Тема 9. Бізнес-процеси корпоративної системи.	Класифікація та структурно-ієрархічна модель бізнес-процесів. Життєвий цикл бізнес-процесів та їх роль у забезпеченні інформаційної безпеки.
Тема 10. Основи управління неперервністю бізнесу.	Поняття, принципи та цілі управління неперервністю бізнесу (BCM). Основні етапи побудови системи управління неперервністю бізнесу.
Тема 11. Міжнародні стандарти та практики управління неперервністю бізнесу.	Міжнародні стандарти та кращі практики BCM. Вимоги до системи управління неперервністю бізнесу. Управління ризиками в системі BCM.
Тема 12. Корпоративна програма управління неперервністю бізнесу (ЕСР).	Етапи розроблення та впровадження ЕСР. Компонентний склад, пріоритети та ресурси. Плани забезпечення неперервності бізнесу.
Тема 13. Забезпечення неперервності бізнесу в кризових та нетипових умовах.	«Чорні лебеді» та інші непередбачувані події. Вплив пандемій, воєнних дій, масштабних кібератак та інших кризових ситуацій на неперервність бізнесу. Адаптація планів BCM до кризових умов.
Тема 14. Оцінювання стану безпеки та	Експрес-аудит стану безпеки підприємства. Виявлення та оцінювання загроз і вразливостей. Оцінювання готовності до кризових ситуацій. Методи та засоби підвищення стійкості бізнес-процесів.

Методи навчання

У процесі вивчення навчальної дисципліни використовуються такі методи навчання:

Інтерактивні	▪ Наочно-демонстраційні дидактичні комплекси до тем, що вивчаються в межах дисципліни (схеми, таблиці, графіки, діаграми, презентації, відеоматеріали тощо). ▪ Відповіді на запитання та обговорення проблемних питань, дискусії. ▪ Відпрацювання навичок та робота в групах. Виконання спільних завдань з аналізу управлінських ситуацій, ризиків, бізнес-процесів та заходів забезпечення інформаційної безпеки з подальшим представленням результатів.
Практичні	▪ Вправи та практичні завдання з аналізу інформаційних ризиків, визначення загроз і вразливостей, розроблення заходів їх обробки, формування політик та процедур інформаційної безпеки. ▪ Аналіз ситуацій та міні-кейси з управління корпоративною інформаційною безпекою, бізнес-процесами та забезпечення неперервності бізнесу. ▪ Практичне розроблення окремих елементів системи управління інформаційною безпекою, програм і планів забезпечення неперервності бізнесу.
Методи дистанційного навчання	▪ Відеоконференції у форматі лекцій або практичних занять. Зв'язок здобувачів освіти з викладачем забезпечують сучасні платформи, такі як: Zoom, Moodle, Google Meet тощо. ▪ Онлайн-дискусії. ▪ Індивідуальне і групове консультування (викладач надає додаткові роз'яснення щодо виконання завдань через чати та e-mail). ▪ Відеозаписи лекцій і практичних занять. ▪ Онлайн-тестування та опитування.

Стратегія оцінювання результатів навчання

Змістовий контент результатів навчання з дисципліни	Результати навчання з цієї дисципліни, які здобувач може продемонструвати та які можна ідентифікувати, оцінити і виміряти, розглядаються у вимірах 7 рівня Національної рамки кваліфікацій, що відповідає другому циклу вищої освіти Рамки кваліфікацій Європейського простору вищої освіти, а саме: Знання – очікується засвоєння принципів і методів менеджменту корпоративної інформаційної безпеки, організаційного та стратегічного планування системи безпеки, управління інформаційними ризиками, розроблення та впровадження політик, стандартів і процедур інформаційної безпеки, класифікації інформації та розподілу відповідальності. Передбачається розуміння принципів управління бізнес-процесами та забезпечення неперервності бізнесу, міжнародних стандартів і кращих практик у цій сфері, підходів до розроблення програм і планів забезпечення неперервності та підготовки організації до кризових ситуацій. Уміння/навички – формується здатність аналізувати стан корпоративної інформаційної безпеки, виявляти та оцінювати інформаційні ризики, визначати заходи щодо їх обробки, розробляти політики та процедури безпеки, аналізувати бізнес-процеси з урахуванням вимог інформаційної безпеки. Здобувач набуває навичок розроблення окремих елементів програм і
--	---

	планів забезпечення неперервності бізнесу, оцінювання готовності організації до кризових ситуацій та обґрунтування заходів щодо підвищення стійкості бізнес-процесів. Комунікація – здатність аргументовано представляти та обговорювати результати аналізу інформаційних ризиків і стану корпоративної інформаційної безпеки, обґрунтовувати управлінські рішення та заходи безпеки, взаємодіяти з керівництвом, фахівцями структурних підрозділів та іншими зацікавленими сторонами під час організації інформаційної безпеки та забезпечення неперервності бізнесу. Відповідальність і автономія – здатність самостійно приймати обґрунтовані рішення у сфері менеджменту корпоративної інформаційної безпеки, оцінювати ризики та наслідки прийнятих рішень, визначати пріоритети захисту інформаційних активів і бізнес-процесів, організовувати заходи щодо забезпечення їх безпеки та неперервності, демонструючи професійну відповідальність за прийняті рішення та результати діяльності.
Критерії оцінювання	Академічні успіхи здобувачів освіти в межах даної дисципліни оцінюються за бально-рейтинговою шкалою (максимальна кількість – 100 балів), що прийнята в ДУІТЗ, з обов’язковим переведенням кількості балів в оцінки за національною шкалою та за шкалою ECTS. Відмінно (А) – від 90 до 100 балів – здобувач у повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час усних виступів та письмових відповідей, глибоко та всебічно розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов’язкову та додаткову літературу. Правильно вирішив усі або не менше 90% завдань, передбачених програмою навчальної дисципліни. Дуже добре (В) – від 82 до 89 балів – здобувач досить повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, в основному розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов’язкову літературу. Однак під час викладання деяких питань допускаються при цьому окремі несуттєві неточності. Правильно вирішив 80-89% письмових завдань. Добре (С) – від 74 до 81 балів – здобувач достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, в основному розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов’язкову літературу. Однак під час викладання деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки. Правильно вирішив 74-81% письмових завдань. Задовільно (D) – від 64 до 73 балів – здобувач в цілому володіє навчальним матеріалом, викладає його основний зміст під час усних та письмових відповідей, але з не зовсім глибоким та всебічним аналізом, обґрунтуванням та аргументацією, з недостатнім використанням необхідної літератури, допускаючи при цьому окремі неточності та помилки. Правильно вирішив 64-73% письмових завдань. Задовільно (E) – від 60 до 63 балів – здобувач в цілому володіє навчальним матеріалом, викладає його основний зміст під час усних та письмових відповідей, але без глибокого всебічного аналізу, обґрунтування та аргументації, без використання необхідної літератури, допускаючи при цьому окремі суттєві неточності та помилки. Правильно вирішив 60-63% письмових завдань. Незадовільно з можливістю повторного складання (FX) – від 35 до 59 балів – здобувач не в повному обсязі володіє навчальним матеріалом. Фрагментарно, стисло без аргументації та обґрунтування викладає його під час усних виступів та письмових відповідей, поверхово розкриває зміст теоретичних питань та практичних завдань, допускаючи при цьому суттєві неточності. Правильно вирішив 35-59% письмових завдань. Незадовільно з обов’язковим повторним вивченням дисципліни (F) – від 0 до 34 балів – Здобувач частково володіє

	навчальним матеріалом, не у змозі викласти зміст більшості питань теми під час усних виступів та письмових відповідей, допускаючи при цьому суттєві помилки. Правильно вирішив 1-34% письмових завдань.
Форма та методи контролю навчальних досягнень	В межах даної дисципліни передбачено три види контролю: поточний, підсумковий та семестровий (академічний). Поточний контроль здійснюється під час проведення лекційних та практичних занять і має на меті перевірку рівня підготовленості здобувачів до виконання конкретних завдань з тем, що вивчаються. При поточному контролі оцінюється активність роботи здобувача на заняттях, результати виконання практичних та індивідуальних завдань, контрольних робіт, якість виконання завдань під час самостійної роботи. Формами проведення поточного контролю є тестування, опитування, виконання практичних і контрольних завдань, аналіз та розв’язання ситуаційних задач. Курсова робота виконується здобувачем вищої освіти відповідно до тематики навчальної дисципліни та спрямована на поглиблення теоретичних знань і набуття практичних навичок щодо управління корпоративною інформаційною безпекою, інформаційними ризиками, бізнес-процесами та забезпеченням неперервності бізнесу. Оцінювання курсової роботи здійснюється окремо відповідно до встановлених вимог і критеріїв оцінювання. Підсумковий контроль – це накопичена здобувачем сума балів за результатами вивчення навчальних тем та виконання завдань самостійної роботи. Семестровий (академічний) контроль передбачає проведення екзамену, під час якого здобувачу виставляється остаточна оцінка за навчальну дисципліну відповідно до чинної в ДУІТЗ системи оцінювання.

Політика навчальної дисципліни	
Відвідування	Здобувачі вищої освіти самостійно планують відвідування лекційних занять, що проводяться в межах дисципліни. Присутність на практичних заняттях та контрольних заходах (екзамен) є обов’язковою. Важливим є своєчасне виконання індивідуальних завдань в межах самостійної роботи, передбачених програмою дисципліни.
Дотримання принципів академічної доброчесності	Підготовка усіх завдань, письмових робіт і т. ін., що виконуються в межах дисципліни, здійснюється здобувачем вищої освіти самостійно, на засадах академічної доброчесності. Викладач має право для перевірки робіт застосовувати різні програмні засоби.
Умови зарахування пропущених занять	Відпрацювання академічної заборгованості з дисципліни можливо до початку екзаменаційної сесії. Процедура узгоджується з викладачем, згідно його розкладу консультацій.
Інші умови	Навчально-методичні матеріали дисципліни розміщені на платформі Moodle

Рекомендовані джерела інформації	
Базові підручники та навчальні посібники	1. Корченко О. Г., Шелест М. Є., Казмірчук С. В. та ін. Менеджмент інформаційної безпеки : навч. посіб. Ніжин : ТПК «Орхідея», 2019. 408 с. 2. Євсєєв С. П., Король О. Г., Воропай Н. Менеджмент інформаційної безпеки : навч. посіб. Харків : НТУ «ХП», 2022. 3. Носок С. О., Фаль О. М., Ткач В. М. Управління інформаційною безпекою : конспект лекцій. Київ : КПІ ім. Ігоря Сікорського, 2021. 258 с. 4. Гребенюк А. М., Рибальченко Л. В. Основи управління інформаційною безпекою : навч. посіб. Дніпро : Дніпропетровський державний університет внутрішніх справ, 2020. 144 с.

	- Костюк Ю. В., Складанний П. М., Бебешко Б. Т. та ін. Безпека інформаційно-комунікаційних систем : підручник. Київ : Київський столичний університет імені Бориса Грінченка, 2025. 1016 с. - Довгий С. О., Воробієнко П. П., Гуляєв К. Д. Сучасні телекомунікації: мережі, технології, безпека, економіка, регулювання : монографія / за заг. ред. чл.-кор. НАН України С. О. Довгого. Київ : Азимут Україна, 2013. 607 с.
Методичні рекомендації та розробки викладачів дисципліни	Методи та засоби захисту інформації : навч. посіб. / В. А. Лахно, Є. В. Васіліу, В. М. Гладких, В. М. Домрачев, Н. М. Сивкова. Київ : ЦП «Компринт» О. В., 2021. 444 с.
Інформаційні ресурси	- ДСТУ EN ISO 22301:2021. Безпека та стабільність. Системи управління неперервністю бізнесу. Вимоги (EN ISO 22301:2019, IDT; ISO 22301:2019, IDT). Київ : ДП «УкрНДНЦ», 2022. 18 с. - Керування ризиками на підприємстві / CIDCON CONSULTING COMPANY. Київ, 2012. - ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva : International Organization for Standardization, 2022. - ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls. Geneva : International Organization for Standardization, 2022. - ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks. Geneva : International Organization for Standardization, 2022. - NIST SP 800-37 Rev. 2. Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. Gaithersburg : National Institute of Standards and Technology, 2018.

Рік введення силабусу – 2026-2027 н. р. Затверджено рішенням кафедри кібербезпеки та технічного захисту інформації № 13 від 22.05.2026 р.

Завідувач кафедри КБ та ТЗІ



Володимир КОРЧИНСЬКИЙ

Гарант програми



Віталій КІЛЬДІШЕВ

Викладачі



Євген ВАСІЛІУ



Сергій СТАЙКУЦА