

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ І ЗВ'ЯЗКУ

Факультет Інформаційних технологій та кібербезпеки

Кафедра Кібербезпеки та технічного захисту інформації

НАСКРІЗНА ПРОГРАМА ПРАКТИКИ

Освітньо-професійна програма Кібербезпека та захист інформації

Спеціальність F5 Кібербезпека та захист інформації
Галузь знань F Інформаційні технології

Рівень вищої освіти Другий (магістерський)

Наскрізна програма практики за ОПП «Кібербезпека та захист інформації» [для здобувачів другого (магістерського) рівня вищої освіти зі спеціальності F5 Кібербезпека та захист інформації] / Авт.-уклад.: В. Кільдішев, С. Стайкуца, М. Івахненко. Одеса : ДУІТЗ, 2026. 11 с.

Автори-укладачі:

Кільдішев Віталій Йосипович, доцент кафедри кібербезпеки та технічного захисту інформації, д.т.н., доц.;

Стайкуца Сергій Володимирович, доцент кафедри кібербезпеки та технічного захисту інформації, к.філ.н., доц.;

Івахненко Максим Сергійович, викладач кафедри кібербезпеки та технічного захисту інформації.

Наскрізна програма практики за ОПП «Кібербезпека та захист інформації» для здобувачів другого (магістерського) рівня вищої освіти зі спеціальності F5 Кібербезпека та захист інформації розглянута на засіданні кафедри кібербезпеки та технічного захисту інформації (протокол від 17 червня 2026 р. № 14).

Завідувач кафедри



Володимир КОРЧИНСЬКИЙ

Погоджено з гарантом ОПП «Кібербезпека та захист інформації» зі спеціальності F5 Кібербезпека та захист інформації для здобувачів другого (магістерського) рівня вищої освіти



Віталій КІЛЬДІШЕВ

Наскрізна програма практики за ОПП «Кібербезпека та захист інформації» зі спеціальності F5 Кібербезпека та захист інформації ухвалена рішенням Навчально-методичної ради Державного університету інтелектуальних технологій і зв'язку (протокол від 19 червня 2026 р. №4).

Голова Навчально-методичної ради



Світлана ХАДЖИРАДЄВА

ВСТУП

Наскрізна програма практики за ОПП «Кібербезпека та захист інформації» зі спеціальності F5 Кібербезпека та захист інформації для здобувачів другого (магістерського) рівня вищої освіти розроблена відповідно до Закону України «Про вищу освіту», статті 51 «Практична підготовка осіб, які навчаються у закладах вищої освіти» (Відомості Верховної Ради, 2014, № 37–38), освітньо-професійної програми «Кібербезпека та захист інформації» зі спеціальності F5 Кібербезпека та захист інформації для здобувачів другого (магістерського) рівня вищої освіти, навчального плану та Положення про порядок проведення практичної підготовки здобувачів вищої освіти Державного університету інтелектуальних технологій і зв'язку, затвердженого Вченою радою ДУІТЗ (протокол від 10.02.2023 № 1). <https://suitt.edu.ua/polozennja-duitz>.

Практична підготовка здобувачів другого (магістерського) рівня вищої освіти за ОПП «Кібербезпека та захист інформації» зі спеціальності F5 Кібербезпека та захист інформації здійснюється на підставі укладених договорів із базами практики, а саме:

- Освітній фонд «Кіпсолід»;
- ТОВ «Роберт Бош ЛТД»;
- ПП «Ардо»;
- ТОВ Багатопрофільна фірма «Секрет Сервіс»;
- ТОВ «Консалтингова компанія «СІДКОН»;
- Департамент кіберполіції Національної поліції України;
- ТОВ «ГОФЕР КОРПОРЕЙШН»;
- ПП «Південна телекомунікаційна компанія»;
- Головне управління Пенсійного фонду України в Одеській області;
- Одеський обласний центр зайнятості;
- Департамент інформації та цифрових рішень Одеської міської ради;
- Комунальне підприємство «Обласний інформаційно-аналітичний центр»;
- Управління поліції охорони в Одеській області;
- та інші бази практики.

Перелік баз практики визначається відповідно до ОПП, навчального плану, програми практики та умов, необхідних для виконання її завдань.

1. МЕТА, ЗАВДАННЯ ТА ОЧІКУВАНІ РЕЗУЛЬТАТИ ПРАКТИЧНОЇ ПІДГОТОВКИ ЗДОБУВАЧІВ

Мета практики: систематизація, закріплення і розширення теоретичних і практичних знань здобувачів зі спеціальності F5 Кібербезпека та захист інформації, формування професійних умінь і навичок для прийняття самостійних рішень у процесі професійної діяльності.

В межах цієї мети реалізуються такі *завдання*:

1) ознайомлення з правилами внутрішнього розпорядку бази практики, проходження інструктажів з охорони праці, пожежної безпеки, електробезпеки та інших вимог безпечної роботи;

2) аналіз об'єкта інформаційної діяльності та інформаційної інфраструктури бази практики, рівня комп'ютерного забезпечення, периферійного та мережевого обладнання, локальної комп'ютерної мережі, а також технічної та нормативної документації;

3) аналіз та оцінювання ризиків кібербезпеки, виявлення та аналіз вразливостей інформаційних систем і мереж, оцінювання рівня їх захищеності;

4) аналіз організації комплексного захисту об'єктів, структури та рівнів мережевої взаємодії, програмно-апаратних рішень у комплексних системах безпеки.

Очікувані результати практичної підготовки здобувачів другого (магістерського) рівня вищої освіти в межах ОПП «Кібербезпека та захист інформації» зі спеціальності F5 Кібербезпека та захист інформації сформульовані з урахуванням трьох складових: загальних компетентностей (ЗК), спеціальних (фахових) компетентностей (СК) та програмних результатів навчання (ПРН), а саме:

- ЗК-1. Здатність застосовувати знання у практичних ситуаціях.
- ЗК-4. Здатність оцінювати та забезпечувати якість виконуваних робіт.
- ЗК-5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
- СК-1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.

- СК-2. 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.
- СК-10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.
- СК-12. Здатність ефективно використовувати на практиці різні теорії в області навчання технологіям, засобам та організаційним аспектам безпеки інформаційних і комунікаційних систем та мереж.
- СК-16. Здатність аналізувати потреби та вимоги користувачів (замовників) щодо захисту інформації та кіберзахисту з метою впровадження систем та комплексів захисту інформації.
- ПРН-2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
- ПРН-15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.
- ПРН-17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.
- ПРН-23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

2. ВИДИ, ЕТАПИ ТА ОПИС ЗМІСТУ ПРАКТИКИ

Відповідно до навчального плану підготовки здобувачів другого (магістерського) рівня вищої освіти за ОПП «Кібербезпека та захист інформації» зі

спеціальності F5 Кібербезпека та захист інформації передбачено проведення виробничої практики в обсязі 15 кредитів ЄКТС (450 год) у 2-3 семестрах (табл. 1).

Таблиця 1 – Види практичної підготовки здобувачів другого (магістерського) рівня вищої освіти за ОПП «Кібербезпека та захист інформації»

№ п/п	Назва практики	Семестр	Кількість кредитів ЄКТС
1	Практика (виробнича)	2	12 (360 год)
2	Практика (виробнича)	3	3 (90 год)

Практична підготовка здобувачів другого (магістерського) рівня вищої освіти за ОПП «Кібербезпека та захист інформації» зі спеціальності F5 Кібербезпека та захист інформації здійснюється в два етапи.

На першому етапі виробничої практики – 2 семестр, 12 кредитів ЄКТС (360 год) – здобувачі освіти опановують такі основні блоки питань:

Інструктаж з техніки безпеки. Інструктаж з охорони праці, пожежної безпеки та електробезпеки. Ознайомлення з правилами внутрішнього розпорядку бази практики, вимогами безпечної роботи на робочому місці та в підрозділі.

Знайомство з базою практики.

Короткий опис бази практики — назва, основні напрями діяльності, послуги або продукція, цілі та завдання. Організаційна структура бази практики, склад структурних підрозділів та їх взаємозв'язок, кадровий склад і назви посад, правила внутрішнього розпорядку, внутрішні нормативні документи та регламенти. Основні бізнес-процеси або процеси діяльності організації. Визначення ключових процесів, пов'язаних із функціонуванням інформаційної інфраструктури та забезпеченням кібербезпеки.

Аудит поточного стану безпеки бази практики. Моделювання загроз кібербезпеці бази практики.

Аналіз здійснюється за п'ятьма основними напрямками: кадрове забезпечення; взаємодія з контрагентами; інженерний захист та технічні засоби охорони; інформаційна інфраструктура та інформаційна мережа; документообіг і захист персональних даних.

Аналіз та аудит окремих аспектів кібербезпеки здійснюються за погодженням із керівником практики від бази практики, у межах наданого доступу, на основі внутрішніх розпорядчих документів, регламентів, технічної документації та іншої доступної інформації.

Основною метою аналізу є збір первинної інформації для оцінювання поточного стану кібербезпеки бази практики, визначення основних зовнішніх і внутрішніх загроз, потенційних вразливостей та ризиків.

За результатами аналізу здійснюється моделювання загроз, зокрема можливих сценаріїв фізичного проникнення порушника, у межах, визначених завданням практики та дозволеним доступом до інформації.

Основні етапи проведення аудиту безпеки бази практики:

1. Результати аудиту представити у вигляді зведених інформаційних таблиць.

На що звернути увагу:

- локація (будівля, приміщення);
- кількість ПК або ноутбуків (робочих місць);
- тип ПК або ноутбуків (робочих місць);
- активне та пасивне мережеве обладнання (роутери, комутатори, PON-адаптери тощо);
- технічний стан обладнання;
- автономність мережі та її компонентів під час відключень електроенергії;
- тип операційної системи та наявність відповідних ліцензій;
- основне програмне забезпечення на робочих місцях;
- параметри підключення до мережі Інтернет (за наявності відповідного доступу);
- додаткові елементи інформаційної інфраструктури та систем безпеки;
- наявність і основні характеристики засобів захисту інформації.

2. Проаналізувати структуру інформаційної мережі бази практики та основні мережеві компоненти і засоби захисту інформації.

3. Провести аналіз документів, що регламентують функціонування інформаційної інфраструктури та забезпечення кібербезпеки бази практики, зокрема договорів, технічної документації, схем, регламентів, посадових інструкцій та інших документів. Аналіз документів здійснюється за наявності відповідного доступу та з дотриманням установлених на базі практики вимог щодо захисту інформації та нерозголошення інформації з обмеженим доступом.

На другому етапі виробничої практики – 3 семестр, 3 кредити ЄКТС (90 год) –

зміст практичної підготовки акцентується на питаннях:

Опрацювання результатів аналізу та розроблення пропозицій щодо підвищення рівня кібербезпеки бази практики.

Основна мета етапу – визначення доцільних методів і засобів захисту інформації за основними напрямками, визначеними програмою практики, з урахуванням результатів проведеного аналізу, виявлених загроз, ризиків та вразливостей, а також технічних, організаційних і ресурсних можливостей бази практики.

За погодженням із керівником практики від бази практики здобувач розробляє пропозиції щодо вдосконалення інформаційної інфраструктури, програмного забезпечення, організаційних заходів та інших складових системи кібербезпеки.

У пропозиціях обґрунтовуються запропоновані методи та засоби захисту, очікуваний результат їх застосування та можливі обмеження.

3. ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ ПРАКТИЧНОЇ ПІДГОТОВКИ

Результати виробничої практики оцінюються за бально-рейтинговою шкалою, прийнятою в ДУІТЗ, із подальшим переведенням отриманих балів в оцінки за національною шкалою та шкалою ЄКТС.

Підсумкова оцінка за виробничу практику формується з урахуванням результатів виконання програми практики, індивідуального завдання, якості оформлення звітної документації, характеристики (відгуку) керівника практики від бази практики та результатів захисту звіту.

Під час оцінювання враховуються:

- 1) повнота та якість виконання програми виробничої практики;
- 2) виконання індивідуального завдання;
- 3) практичне застосування набутих знань і навичок;
- 4) якість та повнота звіту і щоденника практики;
- 5) характеристика (відгук) керівника практики від бази практики;
- 6) результати захисту звіту та відповіді на запитання.

Максимальна оцінка за виробничу практику становить 100 балів.

Таблиця 2 – Шкала оцінювання результатів виробничої практики

Кількість балів	Оцінка за шкалою ЄКТС	Національна оцінка
-----------------	-----------------------	--------------------

90–100	A	відмінно
82–89	B	добре
74–81	C	добре
64–73	D	задовільно
60–63	E	задовільно
35–59	FX	незадовільно з можливістю повторного складання
0–34	F	незадовільно

4. ЗАГАЛЬНІ ВИМОГИ ДО ЗВІТІВ ТА ПІДВЕДЕННЯ ПІДСУМКІВ ПРАКТИКИ

Після закінчення терміну практики здобувачі звітують про виконання програми практики у визначені строки. Протягом тижня після закінчення практики здобувач подає керівникові практики від Університету письмовий **звіт про проходження практики** та оформлений за всіма розділами **щоденник практики**, підписаний керівником від бази практики.

Щоденник практики є документом, у якому систематично відображаються виконані роботи, результати діяльності здобувача та набуті практичні навички відповідно до програми практики.

Звіт має містити відомості про виконання здобувачем усіх розділів наскрізної програми практики та індивідуального завдання, результати проведеного аналізу, висновки і пропозиції, список використаної літератури тощо. Текст звіту може містити відповідні розрахунки, пояснення, таблиці, схеми, діаграми та інші матеріали, що підтверджують результати виконання завдань практики.

Звіт оформлюється відповідно до вимог ДСТУ 3008:2015 та інших нормативних документів, що регламентують оформлення текстових документів. Звіт подається на одному боці аркуша білого паперу формату А4 з інтервалом 1,5; шрифт – Times New Roman, розмір – 14 пт. Текст необхідно друкувати, залишаючи поля таких розмірів: ліве – не менше 25 мм, праве – не менше 10 мм, верхнє і нижнє – не менше 20 мм. Текст звіту поділяють на розділи, підрозділи і пункти відповідно до структури програми практики. Складений здобувачем звіт має наскрізну нумерацію сторінок.

Окремим документом до звіту додається характеристика (відгук) керівника практики від бази практики з рекомендованою оцінкою.

Формою підсумкового контролю з практики є залік із захистом звіту. Залік

проводить комісія, призначена завідувачем кафедри. До складу комісії входять керівник практики від Університету, викладачі; за можливості до проведення заліку може бути залучений керівник практики від бази практики.

Залік проводиться протягом перших десяти робочих днів після закінчення практики у формі захисту здобувачем звіту. Оцінка вноситься до залікової відомості та індивідуального навчального плану здобувача з підписами членів комісії.

Здобувач вищої освіти, який не виконав програму практики без поважних причин, вважається таким, що не виконав вимоги навчального плану. У разі невиконання програми практики з поважної причини здобувачу надається можливість пройти практику повторно відповідно до встановленого порядку. У разі отримання негативної оцінки за результатами підсумкового контролю можливість повторного проходження практики визначається відповідно до Положення про порядок проведення практичної підготовки здобувачів вищої освіти ДУІТЗ.

5. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Стайкуца С. В., Белова Ю. В., Сєдов К. С., Севастєєв Є. О. Комплексні системи безпеки : методичні вказівки для виконання лабораторних робіт. Одеса : ДУІТЗ, 2021. 80 с.
2. НД ТЗІ 3.7-003-2023. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі. Київ : Адміністрація Держспецзв'язку, 2023.
3. НД ТЗІ 3.6-004-21. Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці. Київ : Адміністрація Держспецзв'язку, 2021.
4. НД ТЗІ 3.6-005-21. Порядок категоріювання безпеки інформаційної системи та інформації. Київ : Адміністрація Держспецзв'язку, 2021.
5. НД ТЗІ 1.6-005-2013. Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці. Київ : Адміністрація Держспецзв'язку, 2013.

6. НД ТЗІ 2.7-011-2012. Захист інформації на об'єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв. Київ : Адміністрація Держспецзв'язку, 2012.
7. НД ТЗІ 2.6-001-2011. Порядок проведення робіт з державної експертизи засобів технічного захисту інформації від несанкціонованого доступу та комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. Київ : Адміністрація Держспецзв'язку, 2011.
8. НД ТЗІ 2.5-008-2002. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2. Київ : ДСТСЗІ СБУ, 2002.
9. НД ТЗІ 3.6-003-2016. Порядок проведення робіт зі створення та атестації комплексів технічного захисту інформації. Київ : Адміністрація Держспецзв'язку, 2016.
10. ДСТУ 3008:2015. Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання. Київ : ДП «УкрНДНЦ», 2016.
11. Нормативні документи системи ТЗІ : вебсайт. URL: <https://cip.gov.ua/ua/news/normativni-dokumenti-sistemi-tzi2024>