

**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ**

Кафедра кібербезпеки та DATA – технологій, факультет № 6

ЗАТВЕРДЖЕНО

Перший проректор

Харківського національного
університету внутрішніх справ

полковник поліції

Олександр МОРГУНОВ

ПРОГРАМА

навчальної практики для студентів 3 курсу, які здобувають вищу освіту за
освітньою програмою першого (бакалаврського) рівня вищої освіти

125 – Кібербезпека (безпека інформаційних та комунікаційних систем)

Харків 2022

ЗАТВЕРДЖЕНО

Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол №12 від 22.12.2022

СХВАЛЕНО

Вченою радою факультету № 6
Протокол №14 від 10.12.2022

ПОГОДЖЕНО

Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол №12 від 21.12.2022

Розглянуто на засіданні кафедри кібербезпеки та DATA – технологій,
факультету № 6 протокол №14 від 10.12.2022

Розробники:

1. Завідувач кафедри, кандидат технічних наук, доцент Юрій ГНУСОВ.
2. Старший викладач кафедри Валерій ПЕРЕСІЧАНСЬКИЙ.

Рецензенти:

1. Завідувач кафедри ЕОМ ХНУРЕ, доктор технічних наук, професор Андрій КОВАЛЕНКО .
2. Професор кафедри ОТП НТУ «ХПІ», доктор технічних наук, професор Георгій КУЧУК

1. Загальні положення

Практика студентів є складовою частиною навчально-виховного процесу і має за мету закріплення, поглиблення та вдосконалення теоретичних знань, набуття умінь та навичок, необхідних для самостійної роботи. Це одна з важливих форм практичної підготовки, в ході якої знання, здобуті студентами у навчальному процесі, закріплюються та максимально наближаються до їх майбутньої повсякденної діяльності.

Навчальна практика (далі **практика**) є обов'язковим компонентом освітньо-професійної програми підготовки фахівців першого ступеня вищої освіти - «бакалавр». Організація та проведення практики здійснюється згідно із Положенням про організацію проходження всіх видів практики студентами та слухачами магістратури (далі – Положення) Харківського національного університету внутрішніх справ (далі – Університет) Наказ Харківського національного університету внутрішніх справ від 02.09.2019 № 534, яке розроблено відповідно до закону України «Про освіту», «Про вищу освіту», вимог нормативно-правових актів Міністерства освіти і науки України, наказу Міністерства освіти України «Про затвердження Положення про проведення практики студентів вищих навчальних закладів України», Статуту Харківського національного університету внутрішніх справ. Положення регулює організацію та проведення всіх видів практики студентів, які навчаються в Університеті.

Практика проходить на 3 курсі (6 семестр) навчання.

2. Програмні компетентності

Інтегральна компетентність	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов.
Загальні компетентності (КЗ)	КЗ.1. Здатність застосовувати знання у практичних ситуаціях.
	КЗ.2. Знання та розуміння предметної області та розуміння професії.
	КЗ.3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.
	КЗ.4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

	КЗ.6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
Фахові компетентності спеціальності (КФ	КФ.12. 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. Програмні результати навчання

ПРН.01	застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.
ПРН.02	організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.
ПРН.03	використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел щодо ефективного розв'язання спеціалізованих задач професійної діяльності.
ПРН.04	аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
ПРН.07	діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та/або кібербезпеки.
ПРН.08	готувати пропозиції до нормативних актів щодо забезпечення інформаційної та/або кібербезпеки.
ПРН.09	впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.

4. Організаційно-методичні вказівки

Студенти можуть проходити навчальну практику в групах боротьби з кіберзлочинністю або технічного захисту інформації підприємств, установ та організації де зберігається, обробляється та передається (циркулює) інформація яка потребує захисту. В разі відсутності в установі, куди було направлено для проходження практики студента, підрозділу технічного захисту інформації та кібербезпеки, студент проходить практику у підрозділу, який займається

інформаційною безпекою на підприємстві. Як виняток практика проходить на кафедрі кібербезпеки та DATA - технологій факультету № 6 ХНУВС. Дата та термін проходження практики визначається навчальним планом.

Завданнями **практики** є:

- послідовне знайомство з практичною діяльністю підрозділів підприємства, які займаються інформаційною безпекою та кібербезпекою;
- придбання навичок користуватись типовими інструкціями, положеннями та обчислювальною технікою;
- придбання навичок складання документів з питань технічного захисту інформації;
- застосування і закріплення на практиці знань з діловодства;
- закріплення на практиці знань з організації охорони інформації з обмеженим доступом на об'єктах інформаційної діяльності;
- участь у проведенні перевірок стану технічного захисту інформації в підприємств, організацій, установ, або інших структур.

Студент може проходити **практику** в службах безпеки державних, банківських та комерційних структур, підприємств, установ, організаціях та в практичних органах внутрішніх справ та ЗВО МВС України.

5. Права та обов'язки осіб, які беруть участь в організації, проведенні та проходженні практики

Керівник **практики** від ХНУВС забезпечує укладання договорів за базами практик, оформлення листів, що направляють на бази практик студентів, здійснює загальний контроль за ходом практики та прийом кінцевих індивідуальних звітів студентів.

На початку **практики** керівник від ХНУВС організує та проводить настановний інструктаж для студентів, що розподіляються на практику, пояснює план проходження та зміст практики, а також роз'яснює зміст та порядок оформлення звітних матеріалів. Забезпечує проходження студентами необхідного інструктажу, здійснює їх розподіл по базам практики, знайомить з керівниками практики на базах практики.

По закінченні **практики** безпосередній керівник практики дає відгук про роботу студента за час проходження навчальної практики. У висновку керівника практикою повинно бути зазначено відношення студента до проходження практики, відвідуваність, ступінь активності й самостійності в рішенні завдань, рівень показаних їм знань, умінь і навичок. Також керівник відзначає основні зауваження і побажання в оцінці результатів практики.

Студент-практикант зобов'язаний дотримуватись режиму діяльності тієї установи, на якій він проходить практику, сумлінно відноситися до своїх обов'язків, виконати програму практики в повному обсязі.

Відповідальність за організацію і проведення **практики**, а також безпосередній контроль за нею покладається на керівників практики від кафедри кібербезпеки та DATA–технологій факультету № 6 ХНУВС.

6. Зміст та порядок оформлення звітних матеріалів

На захист студент-практикант надає комісії наступні документи, що відбивають хід і зміст його діяльності в процесі проходження практики:

1. План - завдання про проходження практики (підписи керівника Базис практики про виконання).
2. Щоденник проходження практики, у якому відбивається зміст завдань практики на щодня.
3. Звіт студента – практиканта про виконання програми схемотехнічної практики .
4. Характеристика керівника з місця практики, що відбиває відношення практиканта до практики, виконання їм завдань практики, зауваження, аналіз помилок і успіхів студента, рекомендації з удосконалювання процесу проходження практики; (підпис керівника, печатка – Базис практики).
5. Копія або виписка з наказу про зарахування на практику студента до відповідної установи.
6. Додатки до звіту про проходження практики.
7. Зразки плану - завдання про проходження практики, звіту студента – практиканта про виконання програми практики, та щоденника проходження практики див. додаток.

7. Захист матеріалів практики та критерії його оцінювання

Кінцевим результатом **практики** є оцінка за захист студентом звіту та матеріалу практики.

Наказом ректора ХНУВС призначається комісія, до складу якої входять: керівник кафедри (голова комісії) та викладачі кафедри кібербезпеки та DATA–технологій факультету № 6.

Захист матеріалів практики проводиться в присутності всієї комісії або її більшості де студент доповідають про всю зроблену ними під час проходження практики роботу, викладає зміст свого звіту і відповідає на питання членів комісії.

Члени комісії перевіряють відповідність поданих матеріалів програмі

практики, правильність складання документів, надають до них зауваження та оцінюють матеріали практики. В разі неповноти звіту висловлюють пропозиції щодо його доробки.

Проходження студентами **практики** оцінюється на підставі звітних матеріалів, наданих ними, а також висновків викладача-керівника практики, які відображені в характеристиці стажиста. Оцінка за стажування вноситься до залікової книжки.

Розподіл балів між об'єктами оцінювання навчальної практики наводиться у таблиці (табл. 1).

Розподіл балів між об'єктами оцінювання навчальної практики

Таблиця 1

Об'єкти оцінювання	Бали
I. Виконання плану-завдання навчальної практики	50
II. Додатковий матеріал до звіту практики	20
<ul style="list-style-type: none"> – копії актів перевірок стану технічного захисту інформації в установі (організації), інструкцій; – пропозиції по удосконаленню систем ЗІ; – перелік комп'ютерних програм, які використовуються в обробці інформації з обмеженим доступом та діловодстві та інше. 	
III. Дотримання вимог щодо оформлення роботи:	10
IV. Захист:	20
<ul style="list-style-type: none"> – ґрунтовність доповіді про виконання навчальної практики; – аргументованість відповідей на зауваження керівника практики та членів комісії; – чіткість, структурованість доповіді. 	
Разом	100

Критерії оцінювання результатів практики

Таблиця 2

Оцінка в балах	Оцінка за національною шкалою	Оцінка за шкалою ECTS	
		Оцінка	Пояснення
97-100	Відмінно ("зараховано")	A	«Відмінно» – необхідні практичні навички сформовані, всі навчальні завдання, які передбачені програмою виконані в повному обсязі, відмінна робота без помилок або з однією незначною помилкою.
94-96			
90-93			
85-89	Добре ("зараховано")	B	«Дуже добре» – необхідні практичні навички в основному сформовані, всі навчальні

80-84			завдання, які передбачені програмою виконані, якість виконання більшості з них оцінено числом балів, близьким до максимального, робота з двома – трьома незначними помилками.
75-79		C	«Добре» – практичні навички роботи в основному сформовані, всі навчальні завдання, які передбачені програмою виконані, якість виконання жодного з них не оцінено мінімальним числом балів, деякі види завдань виконані з помилками, робота з декількома незначними помилками, або з однією – двома значними помилками.
70-74	Задовільно ("зараховано")	D	«Задовільно» – необхідні практичні навички роботи сформовані не повністю, але прогалини не носять істотного характеру, більшість передбачених програмою навчальних завдань виконано, деякі з виконаних завдань містять помилки, робота з трьома незначними помилками.
65-69			
60-64		E	«Достатньо» – деякі практичні навички роботи не сформовані, частина передбачених програмою навчання навчальних завдань не виконані, або якість виконання деяких з них оцінено числом балів, близьким до мінімального, робота, що задовольняє мінімуму критеріїв оцінки.
40-59	Незадовільно („не зараховано”)	FX	«Умовно незадовільно» – необхідні практичні навички роботи не сформовані, більшість передбачених програмою навчальних завдань не виконано, або якість їхнього виконання оцінено числом балів, близьким до мінімального; робота, що потребує доробки.
21-40			
1-20		F	«Безумовно незадовільно» – необхідні практичні навички роботи не сформовані, всі виконані навчальні завдання містять грубі помилки, робота, що потребує повної переробки

Студенти, які не виконали програму навчальної практики або за результатами захисту одержали оцінку “незадовільно” проходять додатково навчальну практику і повторно її захищають.

8. Інформаційне та методичне забезпечення

8.1. Закони України

1. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР
2. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України», від 23.02.2006.
3. Закон України «Про державну таємницю», від 21.01.1994 № 3855-ХІІ.
4. Закон України «Про інформацію», від 02.10.1992 № 2657-ХІІ.
5. Закон України «Про національну безпеку України» від 21.06.2018 № 2469-VIII
6. Закон України «Про доступ до публічної інформації», від 13.01.2011 № 2939-VI
7. Закон України «Про захист інформації в автоматизованих системах»
8. Закон України «Про телекомунікації»
9. Закон України «Про електронні документи та електронний документообіг»
10. Закон України «Про електронні довірчі послуги» від 05.10.2017 р. № 2155-VIII
11. Закон України «Про електронний цифровий підпис»
12. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»
13. Закон України «Про основи національної безпеки України»
14. Закон України «Про Національний банк України»
15. Закон України «Про банки і банківську діяльність»
16. Закон України «Про ліцензування видів господарської діяльності» від 02.03.2015 № 222-VIII
17. Закон України «Про основні засади забезпечення кібербезпеки України»
18. Закон «Про ратифікацію Конвенції про кіберзлочинність» від 07.09.2005, № 284-IV.

8.2. Нормативні документи.

19. НД ТЗІ 2.5-010-03 «Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу»
20. НД ТЗІ 2.5-008-2002 «Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2»
21. НД ТЗІ 3.6-001-2000 «Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу»
22. НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі»
23. НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу»
24. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»

25. НД ТЗІ 3.7-001-99 «Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі»

8.3. Стандарти

26. ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ Захист інформації. Технічний захист інформації. Основні положення. ДСТУ 3396.0-96
27. ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96
28. ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ Захист інформації. Технічний захист інформації. Терміни та визначення. ДСТУ 3396.2-97
29. НАЦИОНАЛЬНЫЕ СТАНДАРТЫ ПО БЕЗОПАСНОСТИ СЕТЕВЫХ И ИНФОРМАЦИОННЫХ СИСТЕМ (by admin • 13.06.2017)

8.4. Допоміжна

30. Діордіца І. В. Кібербезпекова політика України: стан та пріоритетні напрями забезпечення. Запоріжжя, Гельветика, 2017. 548 с.
31. Остапов С.Е., Євсєєв С.П., Король О.Г. Кібербезпека: сучасні технології захисту. Навчальний посібник. Новий світ-2000, 2020. 678с.
32. Хорошко В. О. та ін. Проектування комплексних систем захисту інформації. Підручник, Львів, Львівська політехніка, 2020. 320с.
33. Гапак О. М., Балога С.І. Захист інформації в комп'ютерних системах. Підручник. Ужгород: ДВНЗ УжНУ, 2021. 184с.

9. Додатки

Додаток 1

ЗАТВЕРДЖЕНО

Завідувач кафедри кібербезпеки та
DATA-технологій факультету № 6

(підпис)

(ім'я, прізвище)

ІНДИВІДУАЛЬНИЙ ПЛАН

Студента _____ курсу

факультету _____
(назва факультету, № навчальної групи)

(прізвище, ініціали)

на посаді

(назва посади,

підрозділу бази практики)

Строк (термін) проходження практики _____

№ з/п	Заплановані заходи	Відмітка про виконання
1.		
2.		
3.		
4.		

Студент

(підпис)

(ім'я, прізвище)

(дата)

(вид і назва практики)

Строк проведення практики з _____ по _____.

[illegible]

**Відгук і оцінка роботи практиканта на практиці
керівника практики від установи**

Відгук осіб, які перевіряли проходження практики

Висновок керівника практики від Університету про проходження практики

Дата складання заліку " ____ " _____ 20 ____ року

Оцінка:

за національною шкалою (словами)	кількість балів (цифрами і словами)	за шкалою ECTS

Члени комісії прийому практики від Університету

Завідувач кафедри КБ
та DATA-технологій

(підпис)

(ім'я, прізвище)

_____ кафедри КБ
та DATA-технологій

(підпис)

(ім'я, прізвище)

_____ кафедри КБ
та DATA-технологій

(підпис)

(ім'я, прізвище)

Примітки:

- Щоденник заповнюється практикантом особисто, крім розділу відгуку осіб, які перевіряли проходження практики.
- Формат бланка щоденника А5 (148 × 210 мм), брошура 8 сторінок разом з обкладинкою з карткового паперу.

ЗАТВЕРДЖУЮ

(посада керівника установи, де проходять практиканти практику, звання (якщо правоохоронний орган))

(підпис)

(ім'я, прізвище)

3BIT

за результатами проходження практики

(П.І.Б.,повне найменування навчального підрозділу)

Зміст звіту

[illegible]

Студент

(підпис)

(П.І.Б.)

(дата)

Керівник практики від Університету

(підпис)

(П.И.Б.)

(дата)

ПОГОДЖЕНО

Керівник практики від бази практики

(підпис)

(П.И.Б.)

(дата)