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

виробничої практики для студентів 4 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, закріпляються та максимально наближаються до їх майбутньої повсякденної діяльності.

Виробнича 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 4 курсі (8 семестр) навчання. Проходження практики є завершальним етапом навчання освітньо-кваліфікаційного рівня «бакалавр» і проводиться після вивчення теоретичної частини навчальних дисциплін з метою підготовки майбутніх бакалаврів до самостійного виконання службових обов'язків на відповідній посаді згідно з отриманою спеціалізацією на кафедрі кібербезпеки та DATA - технологій ХНУВС.

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.5. Здатність до пошуку, оброблення та аналізу інформації.
	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.1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.
	КФ.2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.
	КФ.3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.
	КФ.4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.
	КФ.5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.
	КФ.6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.
	КФ.7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

Фахові компетентності спеціальності (КФ)	КФ.8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.
	КФ.9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.
	КФ.10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності
	КФ.11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.
	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.09	впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.

ПРН.15	використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
ПРН.16	реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.
ПРН.17	забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів із відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.
ПРН.18	використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
ПРН.19	застосовувати теорії та методи захисту щодо забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.
ПРН.30	здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.
ПРН.32	вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем із використанням процедур резервування згідно встановленої політики безпеки.
ПРН.36	виявляти небезпечні сигнали технічних засобів.
ПРН.37	вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації.
ПРН.38	інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.
ПРН.39	проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.
ПРН.40	інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації;

4. Організаційно-методичні вказівки

Практика проходить у формі стажування на посаді фахівця групи по боротьбі з кіберзлочинністю, в окремих випадках у групі 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 по боротьбі з кіберзлочинністю, студент проходить практику на посаді фахівця 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 з кіберзлочинністю (інформаційною безпекою).
- набуття навичок спілкування в колективі, з громадянами та посадовими особами підприємств, установ та організацій;
- набуття навичок у розробці посадових обов'язків для персоналу;
- придбання навичок складання документів з питань боротьби з кіберзлочинністю (технічного захисту інформації);
- можливість брати участь в організації забезпечення обладнання підрозділів боротьби з кіберзлочинністю (інформаційної безпеки) необхідними організаційними та технічними засобами;
- закріплення на практиці знань боротьби з кіберзлочинністю та організації охорони інформації з обмеженим доступом на об'єктах інформаційної діяльності;
- збір матеріалів для виконання кваліфікаційної дипломної роботи по заданій тематиці.

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.

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 виробничої практики, а також безпосередній контроль за нею покладається на керівника 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 виробничої практики:

1. План - завдання про проходження практики (підписи керівника Бази практики про виконання).
2. Щоденник проходження виробничої практики, у якому відбивається зміст завдань практики на щодня.
3. Звіт студента – практиканта про виконанню програми виробничої 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 – Бази практики).
5. Копія або виписка з наказу про зарахування на практику студента до відповідної установи.
6. Додатки до звіту про проходження практики (тобто: копії актів обстеження приміщень, пропозиції по удосконаленню систем ЗІ, розробок обов'язків персоналу та ін.)
7. Зразки плану - завдання про проходження практики, звіту студента – практиканта про виконанню програми практики, та щоденника проходження практики (див. додаток).

7. Захист матеріалів практики та критерії його оцінювання

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

Наказом ректора ХНУВС призначається комісія, до складу якої входять: керівник кафедри кібербезпеки та DATA – технологій факультету № 6 ХНУВС (голова комісії), 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 виробничої 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 виробничої практики наводиться у таблиці (табл. 1).

Розподіл балів між об’єктами оцінювання виробничої практики

Таблиця 1

Об’єкти оцінювання	**Бали**
I. Виконання плану-завдання виробничої практики	**50**
II. Додатковий матеріал до звіту практики	**20**
- копії актів обстеження приміщень де циркулює інформація з обмеженим доступом; *- пропозиції по удосконаленню систем ЗІ;* *- розробки обов’язків персоналу які працюють на об’єктах інформаційної діяльності та інше.*	
III. Дотримання вимог щодо оформлення роботи:	**10**
IV. Захист:	**20**
- ґрунтовність доповіді про виконання виробничої практики; *- аргументованість відповідей на зауваження керівника практики та членів комісії;* *- чіткість, структурованість доповіді;*	
Разом	**100**

Студенти, які не виконали програму виробничої практики або за результатами захисту одержали оцінку “незадовільно” до складання державних іспитів не допускаються. Їм видається довідка про те, що вони прослухали теоретичний курс навчання та відраховуються у встановленому порядку. Результати захисту стажування відбиваються в атестаціях студентів.

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 завдання, які передбачені програмою виконані, якість виконання більшості з них оцінено числом балів, близьким до максимального, робота з двома – трьома незначними помилками.
80-84			
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

21-40			їхнього виконання оцінено числом балів, близьким до мінімального; робота, що потребує доробки.
1-20		F	**«Безумовно незадовільно»** – необхідні практичні навички роботи не сформовані, всі виконані навчальні завдання містять грубі помилки, робота, що потребує повної переробки

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-XII.
4. Закон України «Про інформацію», від 02.10.1992 № 2657-XII.
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.
19. Кодекс про адміністративні правопорушення від 07.12.1984 № 8073-X
20. Кримінальний кодекс України від 05.04.2001 № 2341-III
21. «Про Положення про технічний захист інформації в Україні»: Указ Президента України від 27.09.1999 № 1229
22. «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» : постанова Кабінету Міністрів України від 29.03.2006 № 373

8.2. Міжнародні правові документи.

23. Європейська Конвенція по кіберзлочинності (злочинність в кіберпросторі) Будапешт, 23 листопада 2001 рік.
24. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи (від 21.07.2006, ВВР, 2006, N 39, ст.328)

8.3. Нормативні документи.

25. НД ТЗІ 2.5-010-03 «Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу»
26. НД ТЗІ 2.5-008-2002 «Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2»
27. 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»
28. НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі»
29. НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу»
30. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу»

8.4. Стандарти

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

8.5. Інформаційні ресурси в Інтернеті

35. Державна служба спеціального зв'язку та захисту інформації України: https://cip.gov.ua
36. Рада національної безпеки і оборони України: https://www.rnbo.gov.ua/
37. Департамент Кіберполіції Національної поліції України: https://cyberpolice.gov.ua/
38. База даних «Законодавство України» / Верховна Рада України. https://zakon.rada.gov.ua/laws

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)

Додаток 2

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

ЩОДЕННИК ПРАКТИКИ

_____
(вид і назва практики)

Студента_____
(ім'я прізвище)

Факультет _____

Кафедра _____

Освітній рівень _____

Спеціальність _____
(назва)

Спеціалізація_____

Наказ про організацію та проведення всіх видів практики студентів (слухачів) Університету _____
(номер та дата видання наказу)

Строк проведення практики з _____ по _____.

Календарний графік проходження практики

№ з/п	Назви робіт	Тижні проходження практики					Відмітки про виконання
		1	2	3	4	5	

Керівники практики:
від університету

_____ _____ _____
(посада) (підпис) (ім’я, прізвище)

Робочі записи під час практики

Примітка: в розділі "Робочі записи під час практики" зазначаються:
- установа (кафедра Університету, кафедри інших ВНЗ, органи державного управління та місцевого самоврядування, правоохоронні та контролюючі органи, підприємства, організації, установи), де здійснено практику, посада та функціональні обов'язки;
- заходи, в яких взято участь;
- практичні навички, отримані при проходженні практики;
- перелік документів, які були складені безпосередньо;
- труднощі та недоліки, що мали місце під час проходження практики;
- інша інформація, що впливає на якість проходження практики.

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:

1. Щоденник заповнюється практикантом особисто, крім розділу відгуку осіб, які перевіряли проходження практики.

2. Формат бланка щоденника А5 (148× 210 мм), брошура 8 сторінок разом з обкладинкою з карткового паперу.

Додаток 3

ЗАТВЕРДЖУЮ

_____

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

_____

_____ _____

(підпис) (ім'я, прізвище)

ЗВІТ
за результатами проходження практики

_____

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

Зміст звіту

Студент

_____ _____

(підпис) (П.І.Б.)

_____

(дата)

Керівник практики від Університету

_____ _____

(підпис) (П.І.Б.)

_____

(дата)

ПОГОДЖЕНО
Керівник практики від бази практики

_____ _____

(підпис) (П.І.Б.)

_____

(дата)