Київський університет імені Бориса Грінченка

Факультет інформаційних технологій та математики

Кафедра інформаційної та кібернетичної безпеки

імені професора Володимира Бурячка

«ЗАТВЕРДЖУЮ»
Проректор з науково-методичної
та навчальної роботи
_____ Олексій ЖИЛЬЦОВ
«___»_____ 2023 р.

ПРОГРАМА ПРАКТИКИ
«ВИРОБНИЧА (ТЕХНОЛОГІЧНА) ПРАКТИКА»

для студентів

спеціальності	125 Кібербезпека
освітнього рівня	першого (бакалаврського)
освітньої програми	125.00.01 Безпека інформаційних і комунікаційних систем

КИЇВСЬКИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА
Ідентифікаційний код 02136554
Начальник відділу
моніторингу якості освіти
Програма № 0978/23
(підпис) (прізвище, ініціали)
«09» 2023

2023 – 2024 навчальний рік

Розробники:

Платоненко Артем Вадимович, кандидат технічних наук, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка, гарант освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем.

Єрмошин Валерій Віталійович, директор департаменту ПрАТ «Національна енергетична компанія Укренерго».

Романюк Олександр Миколайович, здобувач другого (магістерського) рівня освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем.

Складанний Павло Миколайович, кандидат технічних наук, завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Коршун Наталія Володимирівна, доктор технічних наук, професор, професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Програму практики розглянуто і затверджено на засіданні Вченої ради Факультету інформаційних технологій та математики

Протокол від 19.10.2022 р. № 1

Секретар ___(підпис)___ Світлана СЕМЕНЯКА

Робочу програму розглянуто і затверджено на засіданні кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка

Протокол від 01.09.2022 р. № 12

Завідувач кафедри _____(підпис)_____ Павло СКЛАДАННИЙ

Робочу програму погоджено з гарантом освітньої програми (керівником освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем)

___.___. 2022 р.

Керівник освітньої програми _____(підпис)_____ Артем ПЛАТОНЕНКО

Програму практики перевірено

___.___. 2022 р.

Заступник декана _____(підпис)_____ Євген ІВАНІЧЕНКО

Пролонговано:

на 2023/2024 н.р. _____(підпис)_____ (Складанний П.М.), «23» 08 2023 р., протокол № 8

на 20__/20__ н.р. _____(підпис)_____ (_____(ПІБ)_____), «____»____ 20___ р., протокол № ___

на 20__/20__ н.р. _____(підпис)_____ (_____(ПІБ)_____), «____»____ 20___ р., протокол № ___

на 20__/20__ н.р. _____(підпис)_____ (_____(ПІБ)_____), «____»____ 20___ р., протокол № ___

1. Опис практики

Найменування показників	Характеристика за формами навчання	
	денна	заочна
Вид практики	Виробнича (технологічна)	
Загальний обсяг кредитів / годин	6/180	
Курс	3	-
Семестр	6	-
Кількість змістових компонентів з розподілом	3	-
Обсяг кредитів	6	-
Обсяг годин, в тому числі:	180	-
Тривалість (у тижнях)	4	-
Форма семестрового контролю	залік	-

2. Бази практики

Виробнича (технологічна) практика проводиться на підприємствах, в організаціях, науково-дослідницьких та інших установах, що спеціалізуються на наданні послуг в сфері інформаційних технологій та інформаційної безпеки, банках, страхових компаніях, компаніях-операторах зв'язку та інших, що мають у складі своєї структури підрозділ, що відповідає за інформаційну безпеку, або в будь-яких організаціях, де використовуються технічні засоби обробки, зберігання та передачі конфіденційної інформації.

Закріплення баз практики повинно сприяти встановленню та зміцненню довгострокових контактів університету з підприємствами, а також розвитку кооперації між ними з метою якісної підготовки фахівців. Визначенню баз практик повинна передувати постійна робота кафедри щодо вивчення виробничих та економічних можливостей підприємств з точки зору придатності їх для проведення практики студентів за спеціальністю. При цьому повинні враховуватись перспективи сучасних напрямів розвитку ІТ-галузі, економічного, соціального та екологічного розвитку суспільства.

До підприємств - баз виробничої практики висуваються такі вимоги:

- здійснення діяльності дослідження, проектування, впровадження і експлуатації програмних засобів;
- наявність високого рівня технічного забезпечення, використання сучасних інформаційних та інтелектуальних технологій;
- забезпечення проходження практики невеликими групами студентів.

Бази практики повинні мати високий рівень техніки та технологій, використовувати сучасну обчислювальну техніку та інформаційні технології; забезпечувати можливість проведення виробничої/технологічної практики з дотриманням програми; мати науково-технічні зв'язки з закладом вищої освіти (ЗВО).

Орієнтовний перелік баз практики

1. Державне підприємство «Українські спеціальні системи»
2. Акціонерне товариство «Інститут інформаційних технологій»
3. ПрАТ «Національна енергетична компанія Укренерго»
4. Товариство з обмеженою відповідальністю «Центр інформаційної та технічної підтримки «Сапфоріс»
5. Приватне акціонерне товариство «Центр комп'ютерних технологій «ІнфоПлюс»
6. Товариство з обмеженою відповідальністю «АВТОР»
7. Товариство з обмеженою відповідальністю «Криптон-М»
8. Товариство з обмеженою відповідальністю «Д-ЛІНК СЕРВІС»
9. Товариство з обмеженою відповідальністю «СКС ПРОЕКТ»
10. Товариство з обмеженою відповідальністю Науково-дослідний інститут «Автопром»
11. Товариство з обмеженою відповідальністю «РДЛ»

Вибір баз практики здійснюється кафедрою інформаційної та кібернетичної безпеки з урахуванням завдань практики та можливостей їх реалізації. Студенти можуть самостійно, з дозволу кафедри, підбирати для себе місце проходження практики та пропонувати його для використання.

3. Мета і завдання практики

Практична підготовка студентів є важливою складовою сучасного освітнього процесу та спрямована на оволодіння студентами системою професійних вмінь і навичок. Практика формує первинний досвід професійної діяльності та сприяє успішному саморозвитку студента. Така форма практичної підготовки фахівця покликана не тільки забезпечити набуття професійних компетентностей, а також суттєво впливає на формування важливих рис особистості спеціаліста.

Мета виробничої (технологічної) практики – формування у студента професійних практичних навичок, необхідних для роботи на підприємствах, застосування отриманих професійних знань, поглиблення та закріплення теоретичних положень з фахових дисциплін.

Проходження виробничої (технологічної) практики має на меті:

- поглиблення та закріплення теоретичних знань з фахових дисциплін;
- ознайомлення з засобами забезпечення інформаційної безпеки і захисту інформації, що використовуються підприємством;
- вивчення нормативної бази, що регулює забезпечення інформаційної безпеки і захисту інформації, що використовується та обробляється даним підприємством;
- опрацювання наукової, періодичної літератури й методичних матеріалів з питань, що підлягають опрацюванню.

Завдання полягають у формуванні наступних компетентностей:

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 Вміння керувати проектами та вести підприємницьку діяльність;

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 та SMART-технологій, сучасних методів і моделей інформаційної та/або кібербезпеки;

КФ-3 Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) та SMART-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) та SMART-системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки;

КФ-6 Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) та *SMART-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.);

КФ-8 Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

4. Результати проходження практики

В результаті проходження виробничої практики студент повинен досягти наступних програмних результатів навчання:

ПРз-2 - здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних та *SMART-технологій*;
- розробляти та аналізувати проекти *IT* та *SMART-систем* базуючись на стандартизованих технологіях та протоколах передачі даних;
- застосовувати в професійній діяльності знання, навички та практики, щодо структур сучасних обчислювальних систем, методів і засобів обробки інформації, архітектур операційних систем;
- здійснювати захист ресурсів і процесів в ІТС на основі моделей безпеки (кінцевих автоматів, управління потоками, Bell-LaPadula, Biba, Clark-Wilson, та інші), а також встановлених режимів безпечного функціонування *IT* та *SMART-системах*;

ПРз-3 - забезпечувати процеси захисту інформаційно-телекомунікаційних (автоматизованих) та *SMART-систем* шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту;
- забезпечувати функціонування спеціального програмного забезпечення, щодо захисту даних від руйнуючих програмних впливів, руйнуючих кодів в інформаційних, інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*;
- виконувати розробку експлуатаційної документації на КЗЗ;

ПРз-4 - вирішувати задачі супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно принципів, критеріїв доступу та встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*;
- реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*;
- вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах* на основі моделей управління доступом (мандатних, дискриційних, рольових);
- вирішувати задачі централізованого і децентралізованого адміністрування доступом до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*;
- забезпечувати введення підзвітності системи управління доступом інформаційних ресурсів і процесів в *IT* та *SMART-системах*;

ПРз-5 обирати основні методи та засоби захисту інформації відповідно до вимог сучасних стандартів інформаційної і кібербезпеки, та критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії захисту інформації;
- вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації, користувачів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах;*
- проектувати та реалізувати комплексні системи захисту інформації в АС організації (підприємства) відповідно до вимог нормативних документів системи технічного захисту інформації;
- вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*;
- визначати рівень захищеності інформаційних ресурсів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*;

- використовувати інструментальні засоби оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*;

ПРз-10
- аналізувати та визначати можливість застосування технологій, методів та засобів криптографічного захисту інформації;
- аналізувати та визначати можливість застосування технологій, методів та засобів технічного захисту інформації;
- виявляти небезпечні сигнали технічних засобів;
- вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю захищеності інформації від витоку технічними каналами;
- визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації;
- інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик *IT* та *SMART-систем* відповідно до вимог нормативних документів системи технічного захисту інформації;
- обґрунтовувати можливість створення технічних каналів витоку інформації на об'єктах інформаційної діяльності;
- впроваджувати заходи та засоби технічного захисту інформації від витоку технічними каналами;

ПРз-11
- забезпечувати процеси моніторингу доступу до ресурсів і процесів *IT* та *SMART-систем*;
- забезпечувати конфігурування та функціонування систем моніторингу ресурсів та процесів в *IT* та *SMART-системах*;

ПРз-12
- виконувати впровадження та підтримку систем виявлення вторгнень та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних, інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*;
- аналізувати ефективність систем виявлення та протидії несанкціонованому доступу до ресурсів і процесів в *IT* та *SMART-системах*;
- аналізувати та впроваджувати системи захисту від зловмисних програмних кодів.

ПРз-13
- застосовувати знання державної та іноземних мов для забезпечення ефективності комунікації на засадах дотримання етичних норм суспільної поведінки, професійного дискурсу та культури лідерства;
- знати особистісні та соціальні засади збереження та зміцнення індивідуального здоров'я;
- усвідомлювати цінності демократичного громадянського суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні;
- вміти прогнозувати кінцевий результат та адаптуватися в умовах частої зміни технологій професійної діяльності;
- діяти на основі законодавчої та нормативно-правової бази України та вимог галузевих стандартів, в тому числі міжнародних;
- створювати та впроваджувати бізнес-проекти, а також забезпечувати неперервність бізнес процесів.

5. Структура практики

№ з/п	Етапи проходження практики та види діяльності студентів	Усього годин
Етап 1. Організаційний етап. Розробка планів і ознайомлення зі змістом практики		
1	Участь в установчій конференції	2
2	Організаційні заходи щодо проходження практики, ознайомлення з програмою, завданнями, формами звітності з практики	3
3	Розробка планів і визначення змісту практики	5
	Разом	**10**

№ з/п	Етапи проходження практики та види діяльності студентів	Усього годин
Етап ІІ. Виконання завдань за планом практики		
4	Виконання програми виробничої (технологічної) практики за індивідуальним планом	150
	Разом	**150**
Етап ІІІ. Підсумки виробничої (технологічної) практики		
5	Підготовка звітних матеріалів про проходження практики	10
6	Участь в звітній конференції.	10
	Разом	**20**
	Усього годин	**180**

6. Зміст практики

Етап 1. Організаційний етап виробничої (технологічної) практики

Організаційні заходи щодо проходження виробничої (технологічної) практики

Визначення баз проходження практики. Закріплення студентів за базами практики та науковими керівниками практики. Проведення організаційних заходів щодо проходження виробничої/ технологічної практики. Проведення установчої конференції. Розробка методичних рекомендацій та індивідуальних завдань на проходження практики з урахуванням особливостей баз практики.

Складання індивідуальних планів проходження виробничої (технологічної) практики

Знайомство з базами практики та уточнення індивідуальних завдань на проходження практики. Розробка плану проходження практики та узгодження його з керівниками баз практики. Складання індивідуальних планів проходження практики. Затвердження індивідуальних планів проходження практики.

Етап 2. Виконання програми виробничої (технологічної) практики

Виконання програми виробничої (технологічної) практики

Збір, систематизація й узагальнення теоретичного, методичного та практичного матеріалу з питань застосування технологій, методів та засобів криптографічного захисту інформації, технічного захисту інформації, моніторингу доступу до ресурсів і процесів ІТС, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації тощо. Закріплення практичних навичок аналізу програмного забезпечення з метою оцінки на відповідність встановленим вимогам інформаційної та/або кібербезпеки в ІТС, коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту, вирішення задачі супроводу системи управління доступом, реалізації заходів з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в ІТС, використання інструментальних засобів оцінювання можливості реалізації потенційних загроз інформації, що обробляється в ІТС. Розроблення та обґрунтування конкретних практичних положень та рекомендацій Звіт перед науковим керівником за результатами першої половини виробничої/технологічної практики.

Етап 3. Заключний етап виробничої (технологічної) практики

Підготовка до захисту і захист звітних матеріалів про проходження практики

Оформлення комплекту звітних матеріалів про проходження практики. Затвердження результатів практики науковим керівником. Підготовка до захисту і захист звітних матеріалів про проходження практики. Обговорення результатів практики на звітній конференції. Підведення підсумків практики. Проведення заліку.

6.1 Особливості організації та проведення практики

Виробнича/технологічна практика передбачає безперервність та послідовність її проведення,

формування у студентів необхідного і достатнього обсягу практичних знань і вмінь відповідно до освітнього ступеня бакалавра. На цій практиці студент всебічно вивчає забезпечення інформаційної безпеки діяльності підприємств, виконує індивідуальні завдання, збирає практичний матеріал та створює підґрунтя для виконання в подальшому бакалаврської роботи та її захисту.

Зміст виробничої/технологічної практики визначається індивідуальним планом проходження виробничої/технологічної практики, що розробляється студентом разом з науковим керівником і затверджується на засіданні випускової кафедри. Індивідуальний план має передбачати систематичну звітність про проходження практики перед науковим керівником.

Основними напрямами діяльності студента під час виробничої/технологічної практики мають бути:

- робота по збору й обробці теоретичних і методичних матеріалів з метою закріплення отриманих знань;
- систематизація й обробка практичного матеріалу стосовно стандартизованих технологій та протоколів передачі даних, структур сучасних обчислювальних систем, методів і засобів обробки інформації, архітектур операційних систем;
- напрацювання практичних навичок вирішення задач управління процедурами ідентифікації, автентифікації, авторизації, користувачів і процесів, встановлення рівня захищеності інформаційних ресурсів, використання інструментальних засобів оцінювання можливості реалізації потенційних загроз інформації та систем виявлення вторгнень;
- розробка і обґрунтування практичних рекомендацій. Рекомендації повинні мати теоретичний, методичний та практичний характер, грамотно сформульовані й письмово оформлені.

Керівник виробничої практики від кафедри надає всебічну консультативну допомогу практиканту, здійснює загальний контроль підготовлених студентами матеріалів, контактує з керівництвом бази практики, де проходять практику студенти-практиканти.

Забезпечення якісного проведення виробничої/технологічної практики передбачає виконання певних організаційних заходів, таких як:

- обґрунтоване визначення бази практики;
- розподіл студентів за базами практики з урахуванням їх потреб;
- складання оптимальних індивідуальних планів проходження виробничої/технологічної практики з урахуванням здібностей і схильностей студентів;
- розроблення необхідного навчально-методичного забезпечення виробничої/технологічної практики;
- проведення установчої і звітної науково-практичної конференцій за участю наукових керівників практики і викладачів випускової кафедри.

6.2. Завдання для самостійної роботи та перелік індивідуальних завдань для студентів

В процесі проходження виробничої/технологічної практики студент повинен ознайомитися з характеристикою бази практики та виконати наступні завдання (орієнтовний перелік):

1. Проходження інструктажу з техніки безпеки.
2. Пошук, збір і обробка інформації про підприємство в сфері професійної діяльності.
3. Опис організаційної структури обраного підприємства у сфері професійної діяльності.
4. Формування загального уявлення про інформаційну безпеку підприємства
5. Вивчення запровадженої в організації системи захисту інформації.

Індивідуальне завдання є однією з форм набуття фахових компетентностей, яка має на меті поглиблення, узагальнення та закріплення знань, які студенти отримали у процесі теоретичного навчання, та застосування цих знань в практичній діяльності.

Напрями і тематика індивідуальних завдань для студентів-практикантів розробляються на кафедрі, виходячи зі схильностей, здібностей, особливостей студентів та їх уподобань.

Індивідуальне завдання є особистим для кожного студента, визначається керівником практики. Індивідуальні завдання виконують студенти самостійно у супроводженні керівника

практики. Як правило, індивідуальні завдання виконуються окремо кожним студентом. У тих випадках, коли завдання мають комплексний характер, до їх виконання можуть залучатися кілька студентів.

Приклади індивідуальних завдань на виробничу (технологічну) практику:

1. Захист інформації при використанні електронної пошти
2. Захист від атак типу впровадження SQL-коду
3. Дослідження вразливостей операційних систем
4. Модель системи управління інформаційною безпекою підприємства
5. Модернізація комплексу антивірусного захисту підприємства
6. Організація захисту персональних даних на підприємстві
7. Основні напрямки, принципи та методи забезпечення інформаційної безпеки
8. Побудова типової моделі загроз безпеки інформації підприємства
9. Розробка корпоративної мережі підприємства з підключенням віддалених філій по каналах VPN
10. Розробка заходів з технічного захисту конфіденційної інформації на підприємстві

6.3. Обов'язки студентів під час проходження практики

Студенти при проходженні виробничої/технологічної практики зобов'язані:

- до початку практики одержати від керівника практики консультації щодо її проходження і оформлення всіх необхідних документів;
- у повному обсязі виконувати всі завдання, передбачені програмою виробничої/технологічної практики та індивідуальним планом;
- вести календарно-тематичний план проходження практики, своєчасно оформити всі документи з практики і скласти залік;
- проходити практику за строками, визначеними у наказі по Університету;
- суворо дотримуватись правил охорони праці, техніки безпеки і виробничої санітарії.

6.4. Обов'язки керівників практики від Університету та від бази практики

Керівник виробничої (технологічної) практики від Університету:

- розподіляє разом із завідувачем випускової кафедри студентів на місця проходження практики;
- надає методичні рекомендації щодо складання індивідуальних планів проходження практики і затверджує їх після погодження з завідувачем випускової кафедри;
- забезпечує постійне керівництво та контроль за виконанням індивідуального плану кожним студентом і надає необхідну допомогу;
- надає консультації практикантам щодо виконання індивідуальних завдань і робочої програми практики;
- контролює виконання студентами правил внутрішнього трудового розпорядку, облік відвідування студентами практики;
- повідомляє студента про систему звітності з практики;
- підводить підсумки виробничої (технологічної) практики студентів, оцінює роботу кожного студента, складає рецензії за результатами проведеної ним практики і надає їх завідувачу випускової кафедри.

Керівник виробничої(технологічної) практики від підприємства:

- організує проходження практики закріплених за ним студентів спільно з керівником від Університету;
- ознайомлює студентів з організацією праці на конкретному робочому місці;

- здійснює контроль за роботою практикантів, допомагає виконувати завдання на даному робочому місці, надає консультації щодо виробничих питань;
- контролює ведення щоденників та складає на кожного студента характеристику-відгук керівника практики від підприємства, який заноситься до відповідного розділу щоденника виробничої практики;
- ознайомлюється зі звітом студента та дає оцінку звіту і роботі студента.

7. Контроль навчальних досягнень

7.1 Система оцінювання навчальних досягнень студентів

Навчальні досягнення студентів з виробничої/технологічної практики оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип пооперaційної звітності, обов'язковості модульного контролю, накопичувальної системи оцінювання рівня знань, умінь та навичок, розширення кількості підсумкових балів до 100.

Оцінка за кожний змістовий модуль включає бали за поточну роботу студента на практиці, за виконання індивідуальних завдань, за самостійну роботу. Модульний контроль здійснюється після виконання завдань практики студентами за відповідним змістовим модулем.

№ з/п	Види робіт/діяльності студента	Форма звітності	Максимальна кількість балів		
			За одиницю	Кількість одиниць	Максимальна кількість балів
1	Складання індивідуального плану практики	план	20	1	20
2	Виконання програми виробничої/технологічної практики	робочі матеріали	100	1	100
3	Оформлення звітних матеріалів	звіт	40	1	40
			Разом	-	160
	Захист практики:				30
	Максимальна кількість балів				**190**
	Розрахунок коефіцієнта: k=190/100=1,9				

У процесі оцінювання навчальних досягнень студентів застосовуються такі методи:

- *методи усного контролю: індивідуальне опитування, фронтальне опитування, співбесіда, залік;*
- *методи письмового контролю: реферат, звіт;*
- *комп'ютерного контролю: тестові програми;*
- *методи самоконтролю: уміння самостійно оцінювати свої знання, самоаналіз.*

Кількість балів за виконання завдань практики, індивідуальних завдань, самостійної роботи залежить від дотримання таких вимог:

- *систематичність відвідування бази практики за індивідуальним планом роботи;*
- *своєчасність виконання навчальних та індивідуальних завдань;*
- *повний обсяг їх виконання;*
- *якість виконання навчальних та індивідуальних завдань;*
- *самостійність виконання;*
- *творчий підхід до виконання завдань;*
- *ініціативність у виконанні завдань практики.*

7.2 Перелік звітної документації

На захист звіту про проходження виробничої/технологічної практики студент повинен надати наступні звітні матеріали:

1) Індивідуальний план проходження виробничої/технологічної практики з позначками про виконання/невиконання його пунктів.
2) Календарно-тематичний план проходження практики.
3) Звіт про виконання індивідуального завдання.
4) Відгук керівника практики про результати і якість проходження студентом виробничої/технологічної практики.

Студент, який не надав звітної документації, вважається таким, що не пройшов виробничу/технологічну практику.

7.3 Вимоги до звіту про практику

Після закінчення терміну виробничої/технологічної практики студенти звітують про виконання програми та індивідуальних завдань. Звіт має містити відомості про виконання усіх розділів індивідуального плану проходження виробничої/технологічної практики та індивідуального завдання, мати висновки і пропозиції, список використаних джерел тощо. Оформлюється звіт за вимогами, які встановлені на кафедрі інформаційної та кібернетичної безпеки.

Звіт про проходження виробничої/технологічної практики захищається студентом у комісії, призначеній завідувачем кафедри. До складу комісії входять керівники практики від університету і, за можливості, від бази практики. За результатами захисту і наявності повного комплекту звітних матеріалів виставляється оцінка за виробничу/технологічну практику, яка заноситься до залікової відомості і до залікової книжки студента. Підсумки виробничої/технологічної практики підводяться на звітній конференції.

7.4 Шкала відповідності оцінок

Систему рейтингових балів для різних видів контролю та порядок їх переведення у європейську (ECTS) шкалу подано нижче у таблиці.

Шкала оцінювання ECTS

Сума балів за всі види навчальної діяльності	Оцінка за шкалою ECTS	Значення оцінки
90-100	A	Відмінно — відмінний рівень знань (умінь) в межах обов'язкового матеріалу з, можливими, незначними недоліками
82-89	B	Дуже добре – достатньо високий рівень знань (умінь) в межах обов'язкового матеріалу без суттєвих (грубих) помилок
75-81	C	Добре – в цілому добрий рівень знань (умінь) з незначною кількістю помилок
69-74	D	Задовільно – посередній рівень знань (умінь) із значною кількістю недоліків, достатній для подальшого навчання або професійної діяльності
60-68	E	Достатньо – мінімально можливий допустимий рівень знань (умінь)
35-59	FX	Незадовільно з можливістю повторного складання – незадовільний рівень знань, з можливістю повторного перескладання за умови належного самостійного доопрацювання
1-34	F	Незадовільно з обов'язковим повторним вивченням курсу – досить низький рівень знань (умінь), що вимагає повторного вивчення дисципліни

8. Рекомендовані джерела

1. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Посібник]. / В.Л. Бурячок, С.В.Толюпа, В.В.Семко, Л.В.Бурячок, П.М.Складанний, Н.В. Лукова-Чуйко/ – К. : ДУТ - КНУ, 2016. – 178 с
2. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В.Л. Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко / – К.:ДУТ, 2015. – 345 с.
3. Закон України «Про інформацію» від 02.10.1992 № 2657-XII
4. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР
5. Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 №373
6. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі
7. Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96
8. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі
9. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу
10. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу
11. НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2
12. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу
13. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі
14. 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
15. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

ДОДАТКИ

Додаток А

Зразок оформлення Щоденника навчальної практики студента

Титульна сторінка

Київський університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

ЩОДЕННИК ПРАКТИКИ

студента _____
(прізвище, ім’я та по батькові)

Курс _____

Група_____

Спеціальність: 125 «Кібербезпека»

Освітній рівень: перший (бакалаврський)

Київ – 2022

Продовження Додатку А

Друга і наступні сторінки Щоденника

Календарний графік проходження практики

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

Керівники практики:

від Університету _____ _____

(підпис) (прізвище та ініціали)

Робочі записи під час практики

Продовження Додатку А

Висновок керівника практики від Університету про проходження практики

_____

_____

_____

Дата складання заліку „____”_____20____року

Оцінка:
за національною шкалою _____

кількість балів _____

за шкалою ECTS _____

Керівник практики від Університету

_____ _____
(підпис) (прізвище та ініціали)

Додаток Б

Відгук керівника практики від Університету про роботу студента

_____

ПІБ студента повністю

1. Актуальність і практичне значення виконуваної роботи.
2. Позитивні сторони у роботі.
3. Недоліки або дискусійні питання у роботі.
4. Якість та повнота оформлення звіту з виробничої/технологічної практики.
5. Оцінка особистих якостей студента та отриманих практичних навичок.
6. Загальна оцінка практики.

Додаток В

Зразок оформлення першої сторінки звіту про проходження практики

Київський університет імені Бориса Грінченка
Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

ЗВІТ
про проходження виробничої (технологічної) практики

студента _____ _____
(прізвище, ім'я, по батькові)
групи _____ _____
спеціальність: 125 «Кібербезпека»
Освітній рівень: перший (бакалаврський)

Керівник практики від Університету_____
(посада, прізвище, ініціали)

Звіт захищений з оцінкою_____ *(підпис керівника практики від Університету)*
«_____» _____ 202_ р.