Київський столичний університет імені Бориса Грінченка

Факультет інформаційних технологій та математики

Кафедра інформаційної та кібернетичної безпеки

імені професора Володимира Бурячка

«ЗАТВЕРДЖУЮ»
Проректор з науково-педагогічної
та навчальної роботи
_____ Олексій ЖИЛЬЦОВ
«___»_____ 2024 р.

ПРОГРАМА ПРАКТИКИ
ВИРОБНИЧА ПРАКТИКА

для студентів

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

КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА
Код ЄДРПОУ 45307965
Програма № 3456/24
Начальник відділу моніторингу якості освіти
(підпис) (прізвище, ініціали)
«__» _____ 2024 р.

Київ – 2024

Розробники:

Платоненко Артем Вадимович, кандидат технічних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського столичного 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, випускник другого (магістерського) рівня освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем.

Соболенко Ізабелла Андріївна, студентка першого (бакалаврського) рівня освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем.

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

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

Протокол від 24.01.2024 р. № 1

Секретар ___(підпис)___ Світлана СЕМЕНЯКА

Програму практики розглянуто і затверджено на засіданні кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка

Протокол від 03.01.2024 р. № 1

Завідувач кафедри _____(підпис)_____ Павло СКЛАДАННИЙ

Програму практики погоджено з гарантом освітньої програми (керівником освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем)

___.___. 20___ р.

Гарант освітньої програми _____(підпис)_____ Артем ПЛАТОНЕНКО

Програму практики перевірено

___.___. 20___ р.

Заступник директора/декана _____(підпис)_____ Євген ІВАНІЧЕНКО

Пролонговано:

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

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

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

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

1. Опис практики

Найменування показників	Характеристика за формами навчання	
	денна	заочна
Вид практики	виробнича	
Загальний обсяг кредитів / годин	12/360	
Курс	4	-
Семестр	8	-
Кількість змістових компонентів з розподілом	3	-
Обсяг кредитів	12	-
Обсяг годин, в тому числі:	360	-
Тривалість (у тижнях)	8	-
Форма семестрового контролю	залік	-

2. Бази практики

Виробнича 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 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 ім. професора В.Бурячка 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

Виробнича практика студентів є завершальним етапом навчання, що проводиться на випускному курсі з метою закріплення та поглиблення теоретичних знань, формування професійних умінь, навичок приймати самостійні рішення на певних ділянках роботи (або з конкретних питань) у реальних виробничих умовах шляхом виконання окремих функцій і завдань, властивих майбутній професії, оволодіння професійним досвідом і підготовки до самостійної трудової діяльності.

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

Проходження виробничої практики має на меті:

- поглиблення та закріплення теоретичних знань з фахових дисциплін;
- застосування отриманих у процесі навчання знань безпосередньо в межах організаційної структури, де проходить практика (бази виробничої практики);
- формування прикладних професійних навичок, необхідних для здійснення майбутньої професійної діяльності;
- доповнення знань за окремими питаннями практичного характеру;
- набуття навичок самостійної роботи за спеціальністю;
- перетворення фундаментальних і прикладних знань за фахом у професійні функції, формування досвіду професійної діяльності;
- опанування навичок командної роботи, а також самостійного прийняття рішень, дотримання норм і правил професійної етики.

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;

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) та *SMART-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 встановленої політики інформаційної та/або кібербезпеки.

4. Результати проходження практики

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

ПРз-1 - готувати пропозиції до нормативних актів і документів з метою забезпечення встановленої політики інформаційної та/або кібербезпеки;
- розробляти проектну документацію, щодо програмних та програмно-апаратних комплексів захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) та *SMART-систем*;
- виконувати аналіз реалізації прийнятої політики інформаційної та/або кібербезпеки;

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-6 - вирішувати задачі управління процесами забезпечення неперервності бізнесу з використанням процедур резервування програмного забезпечення та безпосередньо інформаційних ресурсів;
- вирішувати задачі корекції цілей, стратегій, планів забезпечення неперервності бізнесу після здійснення кібератак, збоїв та відмов різних класів;
- створювати і впроваджувати плани процесу забезпечення неперервності бізнесу;
- виконувати аналіз налаштувань елементів інформаційних систем та комунікаційного обладнання;

ПРз-7 - вирішувати задачі супроводу та впровадження комплексних систем захисту інформації, а також протидії несанкціонованому доступу до ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*;
- здійснювати оцінку рівня захищеності інформації що обробляється в *IT* та *SMART-системах* використовувати інструментальні засоби оцінювання наявності потенційних вразливостей;
- вирішувати задачі управління комплексною системою захисту інформації в інформаційних та інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*;
- вирішувати задачі експертизи, випробування КСЗІ;

ПРз-8 - вирішувати задачі попередження та виявлення, ідентифікації, аналізу та реагування на інциденти в інформаційних, інформаційно-телекомунікаційних (автоматизованих) та *SMART-системах*;
- проводити розслідування інцидентів інформаційної та/або кібербезпеки базуючись на національних та міжнародних регулюючих актах, процедурах та положеннях в сфері інформаційної та/або кібербезпеки;
- забезпечувати дотримання політики ведення журналів реєстрації подій та інцидентів з встановленим рівнем деталізації;

ПРз-9 - забезпечувати неперервність бізнес-процесів організації на базі системи управління інформаційною безпекою, згідно вітчизняних та міжнародних вимог і стандартів;

- забезпечувати функціонування системи управління інформаційною та/або кібербезпекою організації на основі керування інформаційними ризиками, здійснення процедур їх кількісної і якісної оцінки;

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 інструменттального 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 практики за індивідуальним планом	330
	Разом	**330**
Етап ІІІ. Підсумки виробничої практики		
5	Підготовка звітних матеріалів про проходження практики	5
6	Аналіз результатів проходження практики, оцінка власних фахових компетентостей, пошук шляхів розв’язання проблемних питань	5
7	Участь в звітній конференції	10
	Разом	**20**
	Усього годин	**360**

6. Зміст практики

Етап 1. Організаційний етап виробничої практики

Організаційні заходи щодо проходження виробничої практики

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

Складання індивідуальних планів проходження виробничої 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 практики

Виконання програми виробничої практики

Збір, систематизація й узагальнення теоретичного, методичного та практичного матеріалу з урахуванням специфіки бази практики. Розроблення та обґрунтування конкретних практичних положень, що можуть бути використані у подальшій діяльності фахівця. Звіт перед науковим керівником за результатами першої половини виробничої практики.

Етап 3. Заключний етап виробничої 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 практика проводиться відповідно до індивідуальної програми практики, узгодженої з науковим керівником. Організаційне та навчально-методичне керівництво практикою, виконання програми практики забезпечують викладачі кафедри разом з фахівцями від підприємств, установ та організацій, які є базою практики. До керівництва практикою залучаються досвідчені викладачі кафедри.

Перед початком виробничої практики випускова кафедра проводить установчу конференцію, на якій студентам роз'ясняють мету, завдання, зміст, форми організації, порядок проходження практики і вимоги до звіту. Після закінчення практики проводиться звітна конференція з аналізом її підсумків, керівники від університету та бази практики затверджують звіт студента і дають відгук щодо його роботи

протягом виробничої практики. За результатами проходження практики, наявності і якості звітних документів з практики студенти складають диференційований залік.

Зміст виробничої практики визначається індивідуальним планом проходження виробничої практики, що розробляється студентом разом з науковим керівником виробничої практики 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 практики мають бути:

− ознайомлення та вивчення практики забезпечення інформаційної безпеки і захисту інформації, що обробляється інформаційно-телекомунікаційними системами, автоматизованими системами, що функціонують на основі інформаційно-комунікаційних технологій (ІКТ);

− набуття практичних навичок забезпечення та реалізації організаційно-технічних заходів і заходів забезпечення інформаційної безпеки і захисту інформації, що обробляється ІКТ на об'єкті інформатизації;

− набуття практичних навичок забезпечення та реалізації програмно-апаратних засобів і заходів забезпечення інформаційної безпеки і захисту інформації, що обробляється на об'єкті інформатизації;

− набуття практичних навичок забезпечення та реалізації інженерно-технічних засобів і комплексів забезпечення інформаційної безпеки і захисту інформації, що обробляється на об'єкті інформатизації.

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

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

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 випусковій кафедрі, виходячи зі специфіки діяльності бази практики, схильностей, здібностей, особливостей студентів та їх уподобань.

Індивідуальне завдання є особистим для кожного студента, визначається керівником практики. Індивідуальні завдання студенти виконують 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.

Перелік індивідуальних завдань на виробничу практику:

1. Захист інформаційних каналів управління автоматизованою системою супутникового зв'язку.
2. Розробка типового проекту захисту локальної обчислювальної мережі підприємства.
3. Інформаційна безпека підприємства.
4. Комплексний захист інформації на підприємстві.
5. Комплексне забезпечення інформаційної безпеки при реалізації загрози спроби доступу в віддалену систему.
6. Концепція політики безпеки і систем контролю доступу для локальних обчислювальних мереж.
7. Розробка алгоритму та програмного забезпечення маскування даних.
8. Розробка комплексної системи захисту комерційної інформації.
9. Розробка проекту по створенню захищеної корпоративної мережі з застосуванням технологій VPN.
10. Розробка системи захисту персональних даних на підприємстві.

6.3. Обов'язки студентів під час проходження практики

Студенти при проходженні виробничої 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 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 практики від Університету:

- розподіляє разом із завідувачем випускової кафедри студентів на місця проходження практики;
- надає методичні рекомендації щодо складання індивідуальних планів проходження практики студентами 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 практики студентів, оцінює роботу кожного студента, складає рецензії за результатами проведеної ним практики і надає їх завідувачу випускової кафедри.

Керівник виробничої 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 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 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 практики студент повинен надати наступні звітні матеріали:

1) Індивідуальний план проходження виробничої 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 практики.

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

7.3 Вимоги до звіту про практику

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

Звіт про проходження виробничої 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 практику, яка заноситься до залікової відомості і до залікової книжки студента. Підсумки виробничої 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 столичний 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 – 2024

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

ЗВІТ
про проходження виробничої 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.