МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

"ЗАТВЕРДЖУЮ"
Заступник керівника
(проректор з науково-педагогічної роботи)
_____
Микола АФАНАСЬЄВ

ПРОГРАМА
переддипломної практики

Галузь знань	***12 Інформаційні технології***
Спеціальність	***125 Кібербезпека***
Освітній рівень	***другий (магістерський)***
Освітня програма	***Кібербезпека***

Завідувач кафедри
кібербезпеки та
інформаційних технологій _____ *Сергій ЄВСЕЄВ*

Харків
2020

ЗАТВЕРДЖЕНО
на засіданні кафедри *кібербезпеки та інформаційних технологій*
Протокол № 2 від 31.08.2020 р.

Розробники:
Євсеєв С. П., д.т.н., проф. кафедри КІТ.
Мілов О.В., к.т.н., проф. кафедри КІТ.
Гаврилолва А.А., ст. викладач кафедри КІТ.
Король О.Г., к.т.н., доцент кафедри КІТ.

Лист оновлення та перезатвердження
програми з переддипломної практики

Навчальний рік	Дата засідання кафедри –розробника РПНД	Номер протоколу	Підпис завідувача кафедри

ВСТУП

Переддипломна практика для магістрів спеціальності 125 ″Кібербезпека″, входить до складу базових дисциплін та повинна проходити у строки, які встановлені в графіку навчального процесу.

Проходження переддипломної практики є найважливішою частиною й невід'ємним етапом для формування кваліфікованого й професійно компетентного фахівця - випускника навчального закладу. Професійна компетентність формується на основі синтезу теорії й практики й проявляється в стані актуалізації здатності особистості висувати й вирішувати професійні проблеми. Незважаючи на те, що випускник вузу не може розглядатися як фахівець, що досяг певного рівня професійної майстерності, проте, він повинен мати особистісні ресурси, що сприяють його професійному розвитку.

Завданням вищого навчального закладу є формування таких особистісних якостей випускника, які б сприяли надалі його переходу на більше високі рівні професійної компетентності.

Особливу значимість на етапі професійної підготовки майбутнього фахівця здобуває проблема включення студентів у процес практичного оволодіння професійною діяльністю та придбання навичок рішення комплексних професійних проблем. Переддипломна практика дає студентові реальну можливість узагальнити й систематизувати засвоєні студентом знання і направити їх на реальне рішення комплексу проектних, соціокультурних і науково-дослідних завдань.

Переддипломна практика студентів проводиться в установах, організаціях і підприємствах різних організаційно-правових форм та різних сфер діяльності. Основною вимогою до місця проходження практики є відповідність спеціальності студента, профілю діяльності або всього підприємства, або одного з його підрозділів.

Переддипломна практика магістрів, яка проводиться на другому році навчання, є підсумковим етапом усього навчання, який являє собою проведення всеосяжного аналізу системи безпеки об′єкта дослідження з точки зору можливості реалізації несанкціонованого доступу до секретної та конфіденційної інформації, стороннього деструктивного впливу та доцільності використання відомих методів захисту.

Характеристика навчальної дисципліни

Курс	**2М**
Семестр	**2**
Кількість кредитів ECTS	**8**
Форма підсумкового контролю	**ЗВІТ**

Компетентності та результати навчання за дисципліною

Компетентності	Результати навчання
ЗК 7. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для	ПРН-1 – постійно вдосконалювати та застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; ПРН-2 – планувати, аналізувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; ПРН-20 – усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

активного відпочинку та ведення здорового способу життя	
СК 1. Здатність розробляти та впроваджувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти з метою здійснення професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	ПРН-4 – діяти на основі законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності; ПРН-18 – проводити науково-освітню діяльність, розробляти та впроваджувати систему науково-прикладних досліджень в галузі захисту інформації у відповідності до сучасних норм, вимог, внутрішніх правил і політики безпеки організації (підприємства).
СК 3. Здатність розробляти й впроваджувати систему менеджменту інформаційної безпеки та/або кібербезпеки організації, формувати стратегію і політики інформаційної безпеки різних рівнів на базі світових й вітчизняних стандартів з урахуванням кращих практик галузі інформаційних технологій та їх безпеки.	ПРН-2 – планувати, аналізувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; ПРН-3 – аналізувати та адаптувати професійну діяльність в умовах частої зміни та прогресу інформаційних технологій, що застосовуються в організації, планувати і прогнозувати кінцевий результат; ПРН-7 – виявляти, описувати та використовувати систему аналізу зв'язків між інформаційними потоками та ресурсами (в.ч. критичними) в контурі бізнес-процесів організації (підприємства); ПРН-10 – аналізувати та впроваджувати системи класифікації загроз інформаційним ресурсам (активам), проводити їх ранжування у відповідності до різних класів параметрів (за ймовірністю появи, вартістю, якісними і кількісними показниками, тощо); ПРН-13 – розробляти, планувати, аналізувати та впроваджувати систему аудиту і контролю ефективності функціонування інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки.
СК 9. Здатність розробляти та впроваджувати методи і заходи протидії кіберінцидентам, а також здійснювати процедури управління, контролю та розслідування, надавати рекомендації щодо попередження та аналізу кіберінцидентів.	ПРН-2 – планувати, аналізувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; ПРН-8 – проектувати, впроваджувати, та супроводжувати системи захисту інформаційних систем та ресурсів, інфраструктури установи, розробляти сучасні архітектури використання інформаційних технологій та їх безпеки (архітектури безпеки, моделі інформаційної безпеки, режими безпечного функціонування, методи оцінки якості функціонування відкритих та закритих систем, тощо).

СК 11. Здатність розробляти, впроваджувати і супроводжувати системи аудиту та моніторингу якості бізнес/операційних процесів інформаційно-комунікаційних систем та технологій, а також системи менеджменту інформаційної безпеки та/або кібербезпеки організації в цілому	ПРН-8 – проектувати, впроваджувати, та супроводжувати системи захисту інформаційних систем та ресурсів, інфраструктури установи, розробляти сучасні архітектури використання інформаційних технологій та їх безпеки (архітектури безпеки, моделі інформаційної безпеки, режими безпечного функціонування, методи оцінки якості функціонування відкритих та закритих систем, тощо); ПРН-11 – планувати, впроваджувати, забезпечувати та контролювати безперервність бізнес/операційних процесів організації (підприємства), згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації (підприємства); ПРН-12 – розробляти, планувати, аналізувати та впроваджувати систему доступу до інформаційних ресурсів, інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, програмного забезпечення, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-13 – розробляти, планувати, аналізувати та впроваджувати систему аудиту і контролю ефективності функціонування інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-14 – розробляти та впроваджувати заходи протидії кіберінцидентам, а також аналізувати, здійснювати процедури управління та контролю інцидентами, організовувати та проводити розслідування, надавати рекомендації щодо заходів їх попередження та протидії; ПРН-15 – розробляти, впроваджувати та супроводжувати процеси управління процедурами ідентифікації, автентифікації, авторизації користувачів і інформаційних ресурсів, операційних процесів інфраструктури організації (підприємства), згідно встановленої політики інформаційної безпеки та кібербезпеки.
СК 12. Здатність проводити науково-освітню діяльність, розробляти та впроваджувати систему управління персоналом, а також проводити та планувати навчання працівників і наукові дослідження в сфері безпеки інформаційно-комунікаційних систем і технологій у відповідність вітчизняним та світовим стандартам галузі інформаційної безпеки та/або кібербезпеки	ПРН-1 – постійно вдосконалювати та застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації; ПРН-2 – планувати, аналізувати та організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; ПРН-3 – аналізувати та адаптувати професійну діяльність в умовах частої зміни та прогресу інформаційних технологій, що застосовуються в організації, планувати і прогнозувати кінцевий результат; ПРН-4 – діяти на основі законодавчої, нормативно-правової бази України та вимог відповідних міжнародних стандартів і практик щодо здійснення професійної діяльності;

	ПРН-5 – аналізувати та впроваджувати процедури контуру бізнес-процесів підприємства, що базуються на національних та міжнародних стандартах інформаційної та/або кібербезпеки; ПРН-6 – розробляти, впроваджувати та супроводжувати програмні та програмно-апаратні комплекси засобів інформаційної безпеки та/або кібербезпеки в інформаційно-комунікаційних (автоматизованих) системах та у інфраструктурі організації в цілому; ПРН-8 – проектувати, впроваджувати, та супроводжувати системи захисту інформаційних систем та ресурсів, інфраструктури установи, розробляти сучасні архітектури використання інформаційних технологій та їх безпеки (архітектури безпеки, моделі інформаційної безпеки, режими безпечного функціонування, методи оцінки якості функціонування відкритих та закритих систем, тощо); ПРН-9 – проектувати, впроваджувати, супроводжувати системи та комплекси (програмні, програмно-апаратні) захисту застосунків (в.ч. веб-застосунків) з метою забезпечення якісного функціонування інформаційно-комунікаційних систем, згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-10 – аналізувати та впроваджувати системи класифікації загроз інформаційним ресурсам (активам), проводити їх ранжування у відповідності до різних класів параметрів (за ймовірністю появи, вартістю, якісними і кількісними показниками, тощо); ПРН-11 – планувати, впроваджувати, забезпечувати та контролювати безперервність бізнес/операційних процесів організації (підприємства), згідно встановленої політики інформаційної безпеки та/або кібербезпеки і стратегії організації (підприємства); ПРН-12 – розробляти, планувати, аналізувати та впроваджувати систему доступу до інформаційних ресурсів, інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, програмного забезпечення, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-13 – розробляти, планувати, аналізувати та впроваджувати систему аудиту і контролю ефективності функціонування інформаційно-комунікаційних систем (вузлів доступу до глобальних мереж, програмно-апаратних комплексів, підсистем, тощо), згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-14 – розробляти та впроваджувати заходи протидії кіберінцидентам, а також аналізувати, здійснювати процедури управління та контролю інцидентами, організовувати та проводити розслідування, надавати рекомендації щодо заходів їх попередження та протидії; ПРН-15 – розробляти, впроваджувати та супроводжувати процеси управління процедурами ідентифікації, автен-

	тифікації, авторизації користувачів і інформаційних ресурсів, операційних процесів інфраструктури організації (підприємства), згідно встановленої політики інформаційної безпеки та кібербезпеки; ПРН-16 – розробляти, впроваджувати, та організовувати реалізацію процесів з використанням методів та засобів криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності, згідно встановленої політики інформаційної безпеки та/або кібербезпеки; ПРН-17 – розробляти, впроваджувати та супроводжувати процеси виявлення та ідентифікації кібератак, їх аналізу та впроваджувати процедури реагування і управління інцидентами інформаційної і/або кібербезпеки; ПРН-18 – проводити науково-освітню діяльність, розробляти та впроваджувати систему науково-прикладних досліджень в галузі захисту інформації у відповідності до сучасних норм, вимог, внутрішніх правил і політики безпеки організації (підприємства); ПРН-19 – розробляти, впроваджувати, супроводжувати систему управління персоналом з інформаційної безпеки та/або кібербезпеки на підприємстві.

1. Мета і завдання переддипломної практики

Переддипломна практика за фахом є одним із завершальних етапів у системі підготовки фахівців другого (магістерського) освітнього рівня за спеціальністю 125 «Кібербезпека».

Метою проходження переддипломної практики є узагальнення, систематизація, закріплення та поглиблення теоретичних знань студентів за профілюючими дисциплінами, що вивчені, за спеціальністю ″Кібербезпека″, отримання навичок проведення аналізу сучасної системи захисту конкретного об'єкта з метою самостійного моделювання можливих кіберзагроз та розроблення плану кіберзахисту інформаційної системи.

Завдання переддипломної практики:

1. Зібрати матеріал за темою дипломного проекту для оцінювання стану системи захисту об′єкта управління.

2. Вивчити на практиці сучасні методи реалізації несанкціонованого доступу (НСД) та захисту інформації від стороннього впливу.

3. Вивчити специфіку інформаційного потоку конкретного об'єкта управління що підлягає захисту.

4. Розробити вимоги щодо захисту інформації об'єкта управління від НСД.

5. Проаналізувати сучасні існуючі засоби захисту інформації в інформаційно-комунікаційних системах (ІКС) від витоку її технічними каналами.

6. Розробити вимоги щодо використання засобів захисту інформації в ІКС від витоку її технічними каналами за об'єктом управління.

Унаслідок проходження переддипломної практики студент повинен **знати:**

сучасні засоби фізичного захисту інформації;

методи реалізації НСД;

методи реалізації захисту інформації від стороннього деструктивного впливу;

сучасні вимоги щодо захисту інформації від НСД;

засоби захисту інформації в ІКС від витоку її технічними каналами;

вміти:

проводити аналіз проблеми безпеки інформації за науково-технічними джерелами;

проводити оцінку стану захищеності ІС;

розробляти вимоги щодо захисту інформації від НСД,

застосовувати засоби захисту інформації в ІКС;

здобути навички:

застосування фізичних засобів захисту інформації в ІКС;

аналізу захищеності ІС;

робити обґрунтовані висновки щодо необхідності модернізації і розвитку системи інформаційної безпеки;

розробляти пропозиції по модернізації системи інформаційної безпеки.

2. Зміст і структура переддипломної практики

Зміст переддипломної практики визначається її керівником на основі робочої програми, теми дипломного проекту і відображається в індивідуальному плані студента.

Студент під час проходження переддипломної практики зобов'язаний:

повністю виконати завдання, передбачені програмою практики, враховуючи індивідуальне завдання;

виконувати чинні на підприємстві правила внутрішнього розпорядку;

пройти інструктаж і суворо дотримуватися правил охорони праці, техніки безпеки і виробничої санітарії;

виконувати та нести відповідальність за виконану роботу на підприємстві за дорученням керівника практики нарівні зі штатними співробітниками;

вести щоденник практики за етапами її проходження;

подати на кафедру письмовий звіт про виконання переддипломної практики та індивідуального завдання разом із відгуком, підписаним керівником (куратором) практики від підприємства;

захистити основні положення, відображені у звіті.

У процесі переддипломної практики студенти повинні виконати наступні завдання.

1. Описати напрямки діяльності об'єкта управління.
2. Проаналізувати стан системи безпеки об'єкта управління.
3. Проаналізувати існуючі методи реалізації НСД, які можуть бути застосовані для об'єкта управління.
4. Проаналізувати існуючі методи захисту інформації від НСД.
5. Розробити вимоги щодо захисту інформації від НСД.
6. Проаналізувати технічні канали інформаційно-комунікаційної системи об'єкта управління.
7. Запропонувати необхідні засоби захисту інформації в ІКС від витоку її технічними каналами.

3. Організація та терміни проведення практики

Переддипломна практика може проводитися в державних, муніципальних, громадських, комерційних і некомерційних організаціях чи підприємствах, де можливий збір і вивчення матеріалів, пов'язаних із виконанням сучасних бізнес-процесів, а також у навчальних та наукових підрозділах університету за напрямом підготовки студентів.

Організація практики на всіх етапах спрямована на забезпечення безперервності і послідовності оволодіння студентами навичками та вміннями професійної діяльності відповідно до вимог згідно з рівнем підготовки бакалавра. Практика проводиться відповідно до індивідуальної програми переддипломної практики, узгодженою студентом та науковим керівником на основі загальних підходів до її змісту та структури.

Перед початком практики проводяться консультаційні збори, на яких надається вся необхідна інформація з порядку проведення переддипломної практики та консультація з тех-

ніки безпеки (уповноваженим від кафедри ″Природоохоронних технологій, екології та безпеки життєдіяльності″). За результатами зборів студенти заповнюють щоденники, в яких наводять таке: відомості про себе, назву бази практики, вид практики, період проходження практики, календарний графік із переліком запланованих до виконання робіт (див. додаток А). Календарний графік студенти завіряють підписом керівника від університету, підписом декану факультету та печаткою факультету. За необхідності студентом на базу практики надається направлення від університету (див. додаток Б).

На першому тижні практики студент повинен:

отримати завдання для проходження переддипломної практики;

узгодити графік консультацій зі своїм керівником на кафедрі та ознайомитися з графіком відвідувань даної бази практики уповно-важеними викладачами-консультантами;

завірити підписом календарний графік у завідувача кафедри «Кібербезпеки та інформаційних технологій» або уповноваженою ним особою (для тих, хто проходить практику на кафедрі), або у керівника іншої бази практики (для тих, хто проходить практику за межами університету);

завірити підписом та печаткою керівництва бази практики прибуття студента на практику;

пройти інструктаж із техніки безпеки на базі практики.

На останньому тижні практики студент повинен:

після закінчення терміну проходження практики за результатами виконаних робіт оформити робочі записи у щоденнику та отримати відгуки керівника від кафедри (див. додаток В) та керівника від бази практики (див. додаток Г);

завірити підписом та печаткою керівництва бази практики вибуття студента з практики;

сформувати звіт, титульний аркуш якого підписати з боку студента, керівника від університету та керівника від бази практики; якщо базою практики не є університет, то на підпис керівника від бази практики поставити печатку підприємства (організації, установи) (див. додаток Д).

Індивідуальний план переддипломної практики студента повинен бути узгоджений з планом роботи організації, що є базою практики. У період практики студенти підкоряються всім правилам внутрішнього розпорядку і техніки безпеки, встановленим у підрозділі і на робочих місцях.

Після закінчення практики студенти оформляють всю необхідну документацію відповідно до вимог програми виробничої практики (табл. 1).

Таблиця 1

Програма переддипломної практики з розподілом за днями

№ п/п	Зміст роботи	Кількість днів
1	Проходження інструктажу з техніки безпеки	на початку практики
2	Проведення аналізу систему безпеки ІС підприємства (організації) та її відповідність цілям та задачам бізнес-діяльності	1 тиждень
3	Ознайомлення з методами реалізації НСД	1 тиждень
4	Ознайомлення з методами захисту інформації від стороннього деструктивного впливу	1 тиждень
5	Вивчення типових вимог щодо захисту інформації від НСД	2 тиждень
6	Вивчення технічних каналів як комунікаційної складової інформаційної інфраструктури	2 тижня
7	Проведення аналізу захисту інформації в ІКС через виток її технічними каналами	протягом практики
8	Оформлення звіту згідно з ДСТУ	протягом практики

4. Керівництво та контроль проходження практики

Загальне методичне керівництво практикою здійснюється випускаючим структурним підрозділом – кафедрою «Кібербезпеки та інформаційних технологій». Загальне керівництво переддипломною практикою здійснює науковий керівник від кафедри. Для проходження практики для всіх студентів визначаються куратори від бази практики, під керівництвом яких студенти виконують поставлені в програмі завдання. Керівник переддипломної практики від кафедри надає студенту організаційне сприяння та методичну допомогу у вирішенні завдань.

Керівник практики від кафедри:

погоджує програму переддипломної практики і тему завдання з науковим керівником;

надає консультації студентам за попередньо узгодженим графіком та проводить перевірку проходження практики студентами та надає їм консультації на тих базах практики, які зазначені в графіку виїзду;

встановлює зв'язок із керівниками практики від організації і спільно з ними складає робочу програму проведення практики;

розробляє завдання згідно з темою дипломного проекту;

сприяє формуванню загальної схеми виконання завдання, графіка проведення практики, режиму роботи студентів і здійснює систематичний контроль ходу практики і роботою студентів;

бере участь у розподілі студентів за робочими місцями або переміщення їх за видами робіт;

несе відповідальність разом із керівником практики від організації за дотримання студентами правил техніки безпеки;

здійснює контроль дотримання термінів практики та її змісту;

надає методичну допомогу студентам під час виконання ними індивідуальних завдань і збору матеріалів для дипломного проекту;

оцінює результати виконання студентами програми практики та вносить їх як у вигляді оцінки, так і у вигляді відгуку за результатами роботи студента (див. додаток В).

Керівник практики від бази практики:

погоджує програму переддипломної практики згідно зі встановленою темою дипломного проекту;

надає консультації студентам щодо організації збору необхідної інформації за темою завдання;

установлює зв'язок із керівниками практики від університету;

розробляє тематику індивідуальних завдань;

сприяє виконанню режиму роботи студентів і здійснює систематичний контроль проведення практики і роботи студентів;

бере участь у розподілі студентів за робочими місцями або переміщення їх за видами робіт;

несе відповідальність разом із керівником практики від університету за дотримання студентами правил техніки безпеки;

здійснює контроль дотримання термінів практики та її змісту;

оцінює результати виконання студентами програми практики та вносить їх як у вигляді оцінки, так і у вигляді відгуку за результатами роботи студента у щоденник з практики (див. додаток Г).

Науковий керівник студента:

координує постановку завдань із самостійної роботи студентів у період практики за виданим індивідуальним завданням зі збору необхідних матеріалів, надає відповідну консультаційну допомогу;

дає рекомендації щодо вивчення спеціальної літератури;

бере участь у роботі конференції з ведення підсумків переддипломної практики.

Студент під час проходження практики отримує від керівника практики, а також від свого наукового керівника вказівки, рекомендації та роз'яснення з усіх питань, пов'язаних з організацією та проходженням практики, звітує про виконання робіт відповідно до графіка проведення практики.

Студент:

проводить збір матеріалів за обраним завданням відповідно до графіка практики та режимом роботи підрозділу – місця проходження практики;

отримує від керівника практики вказівки, рекомендації та роз'яснення з усіх питань, пов'язаних з організацією та проходженням практики;

звітує про виконану роботу відповідно до встановленого графіка.

5. Звітність за результатами практики, її захист і підсумковий контроль

За підсумками переддипломної практики студент надає на кафедру:

щоденник переддипломної практики студента;

розгорнутий звіт про результати переддипломної практики, який складається з титульного листа, завдання на практику, змісту, вступу, основної частини у встановленій формі, висновків (самостійної оцінки роботи), списку використаної літератури, додатків;

презентацію та текст підготовленої доповіді за матеріалами переддипломної практики.

Атестацію за підсумками практики проводять на підставі захисту результатів, отриманих у ході переддипломної практики.

Захист звітів із переддипломної практики здійснюється або на конференції, присвяченій підсумкам переддипломної практики в дні, встановлені керівником від кафедри.

За підсумками захисту студенту виставляється диференційований залік згідно зі встановленою університетом шкалою оцінювання.

Оцінку за переддипломну практику заносять в екзаменаційну відомість і залікову книжку, прирівнюється до оцінок (заліків) із теоретичного навчання і враховується під час підведення підсумків загальної успішності студентів.

Атестація практики здійснюють за 100-бальною шкалою. Рівень оцінки відповідає рівню виконаної роботи і поданих матеріалів у частині опрацьованої літератури, зібраних і оброблених матеріалів, їх відповідності темі дипломного проекту.

Оцінка ″відмінно″ (90 – 100 балів) виставляється за умови повного виконання вимог з виробничої практики в становлений термін, готовності для включення поданих матеріалів у дипломний проект.

Оцінка ″добре″ (74 – 89 балів) виставляється в разі наявності окремих недоробок, неповноти поданих матеріалів.

Оцінка ″задовільно″ (60 – 73 балів) виставляється в разі некомп-лектного і неякісного подання матеріалів, слабкої готовності для включення в дипломний проект.

Після закінчення практики студенти складають письмові звіти і здають їх разом із щоденником практики та відгуком на студента-практиканта керівника практики від підприємства на кафедру.

Рекомендується складати звіт про переддипломну практику за структурою, наведеною в табл. 2.

У ″Вступі″ необхідно визначити суть та актуальність проблеми дослідження та визначити шляхи її вирішення за рахунок удосконалення системи інформаційної безпеки.

У першому розділі необхідно описати сферу діяльності бази практики та її інформаційні потоки, які підлягають захисту.

У другому розділі проаналізувати систему захисту об′єкта управління.

У третьому розділі необхідно провести огляд і аналіз існуючих методів реалізації та захисту інформації від стороннього деструктивного впливу.

У четвертому розділі необхідно проаналізувати засоби захисту інформації в ІКС від витоку її технічними каналами.

У висновках необхідно визначити недоліки та проблеми існуючої системи захисту інформації на об′єкті управління.

Зміст звіту з практики визначається особистим завданням, що видано студенту під час від'їзду до бази практики.

Таблиця 2

Структура звіту з переддипломної практики

Розділ	Кількість сторінок
Титульний аркуш	1
Завдання на практику	1
Зміст	1
Вступ	1
1. Коротка характеристика об'єкта управління	3
2. Опис системи захисту об'єкта управління	5
3. Огляд і аналіз існуючих методів реалізації та захисту інформації від стороннього деструктивного впливу	6
4. Засоби захисту інформації в ІКС від витоку її технічними каналами	6
Висновки	1
Список літератури	2
Додатки	

Перший аркуш звіту з практики є титульним. Зразок його оформлення наведено в додатку Д. Другий аркуш має назву ″Завдання на практику″ і повинен містити перелік завдань, які повинні бути вирішені в ході проходження практики. Цей аркуш повинен бути підписаний студентом, який має виконати ці завдання, та викладачем-керівником (див. додаток Е).

Увесь текст звіту з практики повинен бути оформлений згідно з п. 2 додаток Ж.

У рекомендованій літературі (див. п. 2 додаток Ж) повинно бути вказано не тільки перелічені ДСТУ, які було використано під час виконання завдань практики та оформлення бібліографічного опису, але й джерела, в яких розкриваються питання предметної області, що аналізується за обраною тематикою завдання.

Список використаної літератури необхідно оформити згідно з рекомендаціями, наведеними в п. 2 додатку Ж.

Виставлення підсумкової оцінки здійснюється за шкалою, наведено в таблиці "Шкала оцінювання: національна та ЄКТС".

Форми оцінювання та розподіл балів наведено у таблиці "Рейтинг-план навчальної дисципліни".

Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	A	відмінно	зараховано
82 – 89	B	добре	
74 – 81	C		
64 – 73	D	задовільно	
60 – 63	E		
35 – 59	FX	незадовільно	не зараховано

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Великий тлумачний словник української мови / уклад. і голов. ред. В. Т. Бусел. – Київ; Ірпінь : Перун, 2009. – 1736 с.

2. Вимоги до оформлення курсових і дипломних проектів: методичні рекомендації для студентів галузі знань 12 ″Інформаційні технології″ / уклад. А. А. Гаврилова, С. П. Євсеєв, Г. П. Коц, О. Г. Руденко. – Харків : ХНЕУ ім. С. Кузнеця, 2018. – 50 с.

3. ДСТУ 7093:2009 Бібліографічний запис. скорочення слів і словосполук, поданих іноземними європейськими мовами. – Київ : Кн. палата України, 2017. – 17 с.

4. ДСТУ 3582:2013 Бібліографічний опис. Скорочення слів і словосполучень українською мовою. Загальні вимоги та правила. – Київ: Мінекономрозвитку України, 2014. – 15 с.

5. ДСТУ 8302:2015 Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання. – Київ : ДП ″УкрНДНЦ″, 2016. – 17 с.

6. ДСТУ 3008-15 Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання. – Київ : ДП ″УкрНДНЦ″, 2016. – 31 с.

7. ДСТУ 3651.0-97 Метрологія. Основні одиниці фізичних величин Міжнародної системи одиниць. Основні положення, назви та позначення. – Київ : ДП ″УкрНДНЦ″, 1997. – 14 с.

8. ДСТУ 1.5:2015 Національна стандартизація. Правила розроблення, викладання та оформлення нормативних документів. – Київ : ДП ″УкрНДНЦ″, 2015. – 65 с.

9. Женченко М. Загальна і спеціальна бібліографія: навч. посіб. / М. Женченко. – Київ : Жнець, 2011. – 255 с.

10. Основные стандарты для современного книгоиздательского дела / Рос. кн. палата ; сост. : А. А. Джиго,. С. Ю. Калинин, Г. П. Калинина. – Київ: М. Сухоруков, 2008. – 656 с.

11. Про затвердження Вимог до оформлення дисертації: Наказ від 12.01.2017 р. № 40 [Електронний ресурс] // База даних ″Законодавство України″ / ВР України. – Режим доступу до журн. : http://zakon2.rada.gov.ua/laws/show/z0155-17/print1509912703741 483 (дата звернення: 10.04.2018).

12. Словник книгознавчих термінів / уклад.: В. Я. Буран, В. М. Медведєва, Г. І. Ковальчук, М. І. Сенченко. – Київ : Аратта, 2003. – 160 с.

13. Отенко І. П. Основи наукових досліджень : конспект лекцій / І. П. Отенко. – Х. : ХНЕУ, 2010. – 79 с.

Додаткова

14. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” (1994);

15. Закон України “Про захист персональних даних” (2010)

16. СТРАТЕГІЯ національної безпеки України (затверджена Указом Президента України від 26 травня 2015 року № 287/2015)

17. Закон України “Про національну безпеку (2018)

18. ISO/IEC 27001. "Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью.

19. ISO/IEC 27002. "Информационные технологии. Методы обеспечения безопасности. Практические правила управления информационной безопасностью."

20. ISO/IEC 27005. "Информационные технологии. Методы обеспечения безопасности. Управление рисками информационной безопасности

ДОДАТКИ

Додаток А

Щоденник проходження практики

ЩОДЕННИК ПРАКТИКИ

студента _____
(прізвище, ім'я, по батькові)

факультет Економічної інформатики

кафедра Кібербезпеки та інформаційних технологій

освітньо-кваліфікаційний рівень бакалавр/магістр

спеціальність 125 «Кібербезпека»
(шифр і назва)

курс 3/4/1 р.н./2 р.н., група _____

Рис. А.1. **Приклад заповнення першої сторінки щоденника з виробничої / переддипломної практики**

2. Календарний графік проходження практики

№ з/п	Назви робіт	Тижні проходження практики															Відмітки про виконання
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	Проходження інструктажу з ТБ																
2	Ознайомлення з об'єктом управління та його організаційною структурою керування																
3	Дослідження існуючої системи управління інформаційною безпекою (СУІБ)																
4	Ознайомлення з проектною документацією СУІБ																
5	Ознайомлення з політикою безпеки та профілями безпеки																
6	Дослідження можливих загроз інформаційним ресурсам організації, каналів витоку інформації																
7	Аналіз результатів виробничої практики																
8	Оформлення звіту																

Рис. А.2. **Приклад заповнення четвертої сторінки щоденника з переддипломної практики**

Додаток Б

Направлення на переддиплому практику

_____
(назва бази практики)

_____
(П. І. Б. керівника бази практики)

_____
(адреса бази практики)

НАПРАВЛЕННЯ НА ПРАКТИКУ
/є підставою для зарахування на практику/

Згідно з угодою від ″___″ _____20__ року № ____, яку укладено з _____
(назва бази практики)

направляємо на практику студента(ку) __ курсу факультету економічної інформатики _____, який(а)
(П. І. Б.)

навчається за спеціальністю 125 ″Кібербезпека″ для проходження
(шифр) (назва)

переддипломної практики.
Строки практики з ″__″ _____ 20__ року по ″__″ _____ 20__ року.

Керівник практики від
кафедри кібербезпеки
та інформаційних технологій _____

Керівник виробничої практики ЗВО _____

Заступник керівника
(проректор з науково-педагогічної роботи) _____

Додаток В

Відгук керівника від університету про проходження переддипломної практики

У відгуку керівника практики від університету обов'язково повинно бути зазначено таке:

- вказується відповідність виконання поставлених завдань встановленим строкам календарного графіка;
- наголошується на ступені повноти вирішення питань, які розглядаються в роботі;
- звертається увага на обсяг і якість виконаної студентом роботи,
- звертається увага на своєчасність і правильність ведення щоденника практики;
- зазначається обов'язковість відвідування консультацій, які проводив керівник;
- ураховуються відгуки спеціалістів із бази практики, які надаються керівнику під час відвідування бази практики.

Додаток Г

Відгук куратора практики від підприємства

У відгуку керівника практики від підприємства повинно бути зазначено таке:

- повнота виконання студентом програми проходження переддипломної практики;
- якість написання студентом звіту про проходження практики, його відповідність установленим вимогам, реаліям бази практики;
- рівень підготовленості практиканта до професійної діяльності за теоретичними знаннями і практичними навичками;
- відношення студента до роботи, його організованість і дисциплінованість;
- практична значимість пропозицій практиканта, викладених у звіті, щодо поліпшення певних аспектів завдань, що вирішуються тощо;
- вміння працювати в колективі, рівень комунікабельності, громадську позицію та інші особисті риси, що проявились під час практики.

Додаток Д

Титульний аркуш з переддипломної практики

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ СЕМЕНА КУЗНЕЦЯ

ФАКУЛЬТЕТ ЕКОНОМІЧНОЇ ІНФОРМАТИКИ

КАФЕДРА КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Звіт

з переддипломної практики

на тему: …

Виконав(ла): студент(ка) 2 р.н., групи <шифр>,
спеціальності 125 "Кібербезпека" ____
_____ П. І. Б. студента _____

Керівник від
бази практики _____ _____
(підпис, печатка) (науковий ступінь, посада, П. І. Б.)

Керівник від ЗВО _____ _____
(підпис) (науковий ступінь, посада, П. І. Б.)

Харків – 20___ рік

Додаток Е

Шаблон завдання на виконання практики

ЗАВДАННЯ НА _____ ПРАКТИКУ
(вид практики)

1. Назва завдання: _____
_____
_____
2. Строк подання звіту _____
3. Вхідні дані до завдання: ДСТУ з оброблення інформації, літературні джерела, технічна документація <назва об'єкта>, матеріали практики.
4. Перелік графічного матеріалу: _____
_____
_____

Керівник від ЗВО _____
(підпис) (посада, П. І. Б.)

Студент _____
(підпис) (П. І. Б.)

Додаток Ж

Список використаної літератури

1. Великий тлумачний словник української мови / уклад. і голов. ред. В. Т. Бусел. – Київ; Ірпінь : Перун, 2009. – 1736 с.
2. Вимоги до оформлення курсових і дипломних проектів: методичні рекомендації для студентів галузі знань 12 ″Інформаційні технології″ / уклад. А. А. Гаврилова, С. П. Євсеєв, Г. П. Коц, О. Г. Руденко. – Харків : ХНЕУ ім. С. Кузнеця, 2018. – 50 с.
3. ГОСТ Р 7.0.12-2011 Библиографическая запись. Сокращение слов и словосочетаний на русском языке. Общие требования и правила. – Москва : Стандартинформ, 2012. – 28 с.
4. ГОСТ 2.105-95 ЕСКД. Общие требования к текстовим документам. – Москва : Стандартинформ, 2005. – 30 с.
5. ДСТУ 7093:2009 Бібліографічний запис. скорочення слів і словосполук, поданих іноземними європейськими мовами. – Київ : Кн. палата України, 2017. – 17 с.
6. ДСТУ 3582:2013 Бібліографічний опис. Скорочення слів і словосполучень українською мовою. Загальні вимоги та правила. – Київ: Мінекономрозвитку України, 2014. – 15 с.
7. ДСТУ 8302:2015 Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання. – Київ : ДП ″УкрНДНЦ″, 2016. – 17 с.
8. ДСТУ 3008-15 Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання. – Київ : ДП ″УкрНДНЦ″, 2016. – 31 с.
9. ДСТУ 3651.0-97 Метрологія. Основні одиниці фізичних величин Міжнародної системи одиниць. Основні положення, назви та позначення. – Київ : ДП ″УкрНДНЦ″, 1997. – 14 с.
10. ДСТУ 1.5:2015 Національна стандартизація. Правила розроблення, викладання та оформлення нормативних документів. – Київ : ДП ″УкрНДНЦ″, 2015. – 65 с.
11. Женченко М. Загальна і спеціальна бібліографія: навч. посіб. / М. Женченко. – Київ : Жнець, 2011. – 255 с.
12. Мильчин А. Э. Издательский словарь-справочник / А. Э. Мильчин. – 2-е изд., испр. и доп. – Москва : ОЛМА-Пресс, 2003. – 560 с.

Закінчення додатка Ж

13. Основные стандарты для современного книгоиздательского дела / Рос. кн. палата ; сост. : А. А. Джиго,. С. Ю. Калинин, Г. П. Калинина. – Київ: М. Сухоруков, 2008. – 656 с.
14. Про затвердження Вимог до оформлення дисертації: Наказ від 12.01.2017 р. № 40 [Електронний ресурс] // База даних ″Законодавство України″ / ВР України. – Режим доступу до журн. : http://zakon2.rada.gov.ua/laws/show/z0155-17/print1509912703741 483 (дата звернення: 10.04.2018).
15. Р 50-77-88 Рекомендации. ЕСКД. Правила выполнения диаграмм. – Москва : Государственный комитет СССР по стандартам, 1989. – 11 с.
16. Словник книгознавчих термінів / уклад.: В. Я. Буран, В. М. Медведєва, Г. І. Ковальчук, М. І. Сенченко. – Київ : Аратта, 2003. – 160 с.