**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**Волинський національний університет імені Лесі Українки**
**Факультет інформаційних технологій і математики**
**Кафедра комп'ютерних наук та кібербезпеки**

# СИЛАБУС
## нормативного освітнього компонента
# ВИРОБНИЧА ПРАКТИКА З ОРГАНІЗАЦІЇ ЗАХИСТУ ІНФОРМАЦІЇ

**підготовки здобувачів освіти**
**першого (бакалаврського) рівня**
**галузі знань 12 Інформаційні технології**

**за спеціальністю 125 Кібербезпека та захист інформації**

**Освітня кваліфікація: Бакалавр з кібербезпеки та захисту інформації**

Луцьк – 2024

**Силабус освітнього компонента «Виробнича практика з організації захисту інформації»** підготовки бакалавра, галузі знань 12 Інформаційні технології, спеціальності 125 Кібербезпека та захист інформації, за освітньою програмою Кібербезпека та захист інформації.

**Розробник:**
Онищук О.О., кандидат технічних наук, доцент кафедри комп'ютерних наук та кібербезпеки

**Погоджено**
Гарант освітньо-професійної програми:  Чернящук Н.Л.

**Силабус освітнього компонента затверджено на засіданні кафедри комп'ютерних наук та кібербезпеки**

протокол № 4 від 21.11.2024 р.

Завідувач кафедри:  Гришанович Т. О.

## І. ОПИС ОСВІТНЬОГО КОМПОНЕНТА

<table>
<tr><th>Найменування показників</th><th>Галузь знань, спеціальність, освітня програма</th><th>Характеристика освітнього компонента</th></tr>
<tr><td rowspan="2">Денна форма навчання</td><td rowspan="5">12 Інформаційні технології<br>125 Кібербезпека та захист інформації<br>Кібербезпека та захист інформації бакалавр</td><td>Нормативна</td></tr>
<tr><td>Рік навчання 1</td></tr>
<tr><td>Кількість годин/кредитів 180 / 6</td><td>Семестр 8-ий</td></tr>
<tr><td rowspan="3">ІНДЗ: немає</td><td>Самостійна робота 168 год.</td></tr>
<tr><td>Консультації 12 год.</td></tr>
<tr><td>Форма контролю: залік</td></tr>
<tr><td colspan="2">Мова навчання: українська</td><td></td></tr>
</table>

## ІІ. ІНФОРМАЦІЯ ПРО КЕРІВНИКА ПРАКТИКИ

| | |
|---|---|
| ПІП | Онищук Оксана Олександрівна |
| Науковий ступінь | кандидат технічних наук |
| Вчене звання | доцент |
| Посада | доцент кафедри комп’ютерних наук та кібербезпеки |
| Контактна інформація | (096) 6943585,onyshchuk.oksana@vnu.edu.ua |
| Дні занять | за розкладом http://94.130.69.82/cgi-bin/timetable.cgi?n=700 |

## ІІІ. Мета і завдання освітнього компонента

Освітній компонент «**Виробнича практика з організації захисту інформації**» є невід’ємною складовою освітньо-професійної програми Кібербезпека та захист інформації підготовки бакалаврів за спеціальністю 125 Кібербезпека та захист інформації. Під час практики здобувачі освіти повинні набути навичок експлуатації та захисту інформації, що спрямовані на підготовку до самостійної роботи із розв’язання практичних завдань на підприємстві. Виробничу практику здобувачі проходять на підприємствах різних форм власності під керівництвом викладачів кафедри і працівників відповідних підприємств. Така організація керівництва практикою дає змогу здобувачам поглибити теоретичні знання і набути досвіду практичної роботи. Під час практики здобувачі збирають необхідну інформацію про діяльність підприємства та її результати, здійснюють аналіз результатів діяльності підприємства і визначають наявність проблем. Завданням практики є формулювання рекомендацій для підприємства щодо усунення недоліків у діяльності із організації захисту інформації або покращення такої діяльності. Результати роботи здобувачі оформлюють у вигляді звіту з практики. Оцінюють результати роботи спочатку

керівники практики від ЗВО та підприємства у вигляді відгуку, а потім — комісія із захисту практики. Для проходження виробничої практики **з** організації захисту інформації здобувачі направляються до підприємств, організацій та установ, що мають у своєму складі підрозділи, які займаються кібербезпекою. Здобувачі вищої освіти можуть самостійно обирати для себе місце проходження практики або скористатися базами практик, що пропонуються кафедрою. Базами практики можуть бути організації, з якими Волинським національним університетом імені Лесі Українки укладено відповідні угоди.

**Мета і завдання освітнього компонента "Виробнича практика з організації захисту інформації"** є оволодіння студентами сучасними методами, формами організації та інструментальними засобами у галузі інформаційних технологій, формування у них, на базі одержаних у вищому навчальному закладі знань, професійних умінь і навичок для прийняття самостійних рішень під час конкретної роботи в реальних умовах, виховання потреби систематично поновлювати свої знання та творчо їх застосовувати в практичній діяльності, отримання здобувачами практичного досвіду застосування знань, умінь і навичок, набутих під час теоретичного навчання, для вирішення завдань забезпечення кібербезпеки в реальних умовах роботи підприємств, організацій чи установ. Практика спрямована на розвиток професійних компетентностей у сфері захисту інформації, аналізу ризиків, впровадження сучасних технологій безпеки та вдосконалення навичок роботи з відповідним програмним і апаратним забезпеченням.

**Завданнями практики є:**

- Ознайомлення з організаційною структурою, нормативною базою та політиками безпеки організації, знайомство з порядком роботи та умовами праці на підприємстві; отримання досвіду входження в трудовий колектив; ознайомлення з процесом виробництва на підприємствах, в організаціях, установах, компаніях, де доведеться працювати майбутнім спеціалістам; - отримання практичного досвіду за обраною професією; Формування навичок командної роботи у професійному середовищі.
- Засвоєння отриманих у процесі навчання теоретичних знань та практичних умінь і навичок за фахом; узагальнення, закріплення і поглиблення знань, що отримані під час навчання в університеті для використання їх у подальшій роботі та обґрунтованого прийняття рішень; отримання інформації про ринок затребуваних професій; отримання інформації про те, які знання, отримані в університеті, і в якому напрямку необхідно поглиблювати і розвивати; знайомство з новими технологіями в IT- індустрії
- Вивчення методів аналізу вразливостей інформаційних систем та оцінки ризиків кіберзагроз.
- Розробка та реалізація заходів для захисту інформаційних ресурсів.
- Участь у моніторингу, виявленні, аналізі та реагуванні на інциденти кібербезпеки.
- Збір документів (довідок, матеріалів тощо) для оформлення звіту з проходження виробничої практики. та підготовка звітів про виконані завдання та рекомендацій щодо покращення кіберзахисту.

Зміст виробничої практики направлений на формування ***компетентностей***, визначених стандартом вищої освіти зі спеціальності 125 «Кібербезпека та захист інформації»:

**Загальні компетентності:**

**ЗК 1.** Здатність застосовувати знання у практичних ситуаціях.

**ЗК 2.** Знання та розуміння предметної області та розуміння професійної діяльності.

**ЗК 3.** Здатність спілкуватися державною мовою як усно, так і письмово.

**ЗК 4.** Здатність спілкуватися іноземною мовою.

**ЗК 5.** Здатність вчитися і оволодівати сучасними знаннями.

**ЗК 6.** Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав та свобод людини і громадянина в Україні.

**ЗК 7.** Здатність ухвалювати рішення й діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.

**ЗК 8**. 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 активного відпочинку та ведення здорового способу життя.

**Спеціальні (фахові, предметні) компетентності**

**СК1.** Здатність застосовувати законодавчу та нормативно- правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності.

**СК 2.** Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.

**СК 3.** Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.

**СК 4.** Здатність забезпечувати захист інформації інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.

**СК 5.** Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.

**СК 6.** Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.)

**СК 7.** Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.

**СК 8.** Здатність застосовувати методи та засоби криптографічного захисту інформації на об’єктах інформаційної діяльності.

**СК 9.** Здатність застосовувати методи та засоби технічного захисту інформації на об’єктах інформаційної діяльності.

**СК 10.** Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки

**РН 1.** Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов’язків.

**РН 2.** Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.

**РН 3.** Застосовувати принципи неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності.

**РН 4.** Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв’язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.

**РН 5.** Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

**РН 6.** Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.

**РН 7.** Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.

**РН 8.** Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.

**РН 9.** Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.

**РН 10.** Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

**РН 11.** Планувати підготовку та забезпечувати неперервність бізнес-процесів в

організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.

**РН 12.** Застосовувати методи та засоби захисту інформації в інформаційних та інформаційно-комунікаційних системах відповідно до встановленої політики інформаційної безпеки.

**РН 13.** Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних й інформаційно-комунікаційних систем та\або інфраструктури організації в цілому.

**РН 14.** Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.

**РН 15.** Збирати, обробляти, зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводити аналіз та дослідження кіберінциденту зметою оперативного відновлення функціонування інформаційної системи.

**РН 16.** Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.

**РН 17.** Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.

**РН 18.** Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об’єктах інформаційної діяльності.

**РН 19.** Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.

**РН 20.** Визначати загрози створення технічних каналів витоку інформації на об’єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.

**РН 21.** Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та

використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах

## IV. ЕТАПИ ПРАКТИКИ ТА ЗМІСТ ПРАКТИКИ

| Етапи | Зміст, основні завдання, тривалість | Консультації | Самостійна робота |
|---|---|---|---|
| Підготовчий | Настановча конференція; | 2 | 2 |
| | Консультація з керівником практики та знайомство з колом обов'язків та завданнями практики; | | 4 |
| | Розробка індивідуального графіку роботи студента-практиканта. | | 2 |
| Основний | Ознайомлення з основними видами діяльності бази виробничої практики. | 1 | 24 |
| | Визначення переліку питань для формування індивідуального завдання під час виробничої практики. | 1 | 12 |
| | Робота над індивідуальним завданням, вибір програмних, технічних і організаційних засобів для вирішення поставленої задачі. Виконання індивідуального завдання. | 2 | 80 |
| | Підготовка та виступ із повідомленням про хід виконання індивідуального завдання на виробничій нараді підрозділу установи (бази практики), де проходить виробнича практика. | 1 | 10 |
| | Узагальнення та систематизація матеріалу щодо проходження виробничої практики. Підготовка звітної документації. | 2 | 12 |
| Підсумковий | Оформлення звіту про практику за поданим зразком. | 2 | 10 |
| | Представлення звіту про практику та його затвердження. | 1 | 6 |
| | Захист практики. | | |
| Всього | | 12 | 168 |

***Зміст виробничої практики з організації захисту інформації:***

| № з/п | Найменування розділів практики і перелік виконуваних робіт | Кількість годин |
|---|---|---|
| | **Розділ 1. Техніка безпеки і охорона праці** | **6** |
| 1 | Техніка безпеки і охорона праці на базі практики Знайомство з правилами внутрішнього розпорядку підприємства, інструктаж з техніки безпеки та охорони праці, бесіда спеціалістів. | 2 |
| 2 | Вивчення техніки безпеки і охорони праці у структурному підрозділі | 2 |
| 3 | Вивчення техніки безпеки і охорони праці на робочих місцях. Інструктаж з техніки безпеки та охорони праці на робочому місці. | 2 |
| | **Розділ 2. Загальні відомості про об'єкт практики** | **12** |
| 4 | Знайомство з підприємством. Екскурсія по відділам підприємства та службам, що забезпечують його роботу. | 2 |
| 5 | Вивчення роботи основних структурних підрозділів. | 2 |
| 6 | Ознайомлення з обчислювальним центром підприємства (організації, установи, компанії). | 2 |
| 7 | Ознайомлення з підрозділами підприємства. Вивчення особливостей роботи окремого структурного підрозділу | 2 |
| 8 | Вивчення запропонованої керівником документації (вимоги, стандарти, звіти) у сфері кібербезпеки, які можуть бути необхідні або корисні при виконанні навчально-виробничих завдань. | 2 |
| 9 | Вивчення процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур на підприємстві (в організації чи установі). | 2 |
| | **Розділ 3. Виконання обов'язків згідно посади практики на підприємстві (організації, установі, компанії)** | **102** |
| 10 | Ознайомлення з обов'язками згідно з місцем роботи у підрозділі підприємства (організації, установи, компанії). | 4 |
| 11 | Робота дублером фахівця з захисту інформації. | 4 |

| | | |
|---|---|---|
| 12 | Робота зі стандартним обладнанням та програмним забезпеченням. | 4 |
| 13 | Робота в середовищі сучасних операційних систем та баз даних. | 4 |
| 14 | Налаштування обладнання комп'ютерних систем та мереж, апаратних, програмних, локальних та мережевих засобів, між мережевих екранів. | 6 |
| 15 | Робота дублером адміністратора комп'ютерних систем та мереж. | 4 |
| 16 | Обслуговування засобів комп'ютерних систем та мереж | 6 |
| 17 | Аналіз працездатності мереж та пошук в них вразливостей за допомогою спеціального програмного забезпечення. | 6 |
| 18 | Робота дублером ремонтника апаратних засобів комп'ютерних систем та мереж. | 6 |
| 19 | Аналіз апаратних засобів комп'ютерних систем та мереж. | 6 |

| | | |
|---|---|---|
| 20 | Аналіз апаратних засобів комп'ютерних систем та мереж спеціальним програмним забезпеченням. | 8 |
| 21 | Аналіз вразливостей комп'ютерних систем та мереж | 6 |
| 22 | Визначення задач захисту інформації, що обробляється в інформаційно-телекомунікаційних системах підприємства (організації, установи), що використовують чи потребують використання сучасних методів та засобів криптографічного захисту інформації. | 6 |
| 23 | Аналіз та оцінка ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах в згідно встановленої політики інформаційної та\або кібербезпеки. | 8 |
| 24 | Розробка рекомендацій щодо покращення захищеності комп'ютерних систем та мереж | 8 |
| 25 | Розробка пропозицій по заходах з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах підприємства (організації, установи). | 8 |

| | | |
|---|---|---|
| 26 | Розробка пропозицій щодо реалізації комплексної системи захисту інформації в АС організації (підприємства) відповідно до вимог нормативно правових документів. | 8 |
| | **Розділ 4. Робота над індивідуальним завданням** | **40** |
| 27 | Виконання теоретичної частини (розбір статей, інформаційних схем, комп'ютерних програм і відповідної документації, пошук інформації з літератури та Інтернету, складання оглядів і т.п.). | 10 |
| 28 | Виконання практичної частини. | 10 |
| 29 | Підбір фактичного матеріалу на підприємстві (організації, установі, компанії) для написання курсових і наукових робіт. | 10 |
| 30 | Вирішення інших питань відповідно до індивідуального завдання. | 10 |
| | **Розділ 5. Підготовка і оформлення звітних матеріалів** | **20** |
| 31 | Заповнення щоденника виробничої практики. | 4 |
| 32 | Отримання відгуку керівника практики від підприємства. | 2 |
| 33 | Отримання відгуку керівника практики від університету. | 2 |
| 34 | Узагальнення та систематизація матеріалу щодо проходження виробничої практики. | 6 |
| 35 | Оформлення звіту з виробничої практики. | 6 |
| | **Диференційований залік Всього** | **180** |

## V. ВИДИ (ФОРМИ) ІНДИВІДУАЛЬНИХ ЗАВДАНЬ

У період проходження здобувачами виробничих практик на відповідній базі практикант виконує індивідуальне завдання з більш глибокого вивчення окремих аспектів діяльності досліджуваного об'єкту – бази практики. Індивідуальне завдання розробляється для кожного студента та узгоджується з керівником практики від кафедри в перші дні проходження практики. Формування індивідуального завдання для виробничої практики (з розробки програмно забезпечення) направлено на розробку програмного забезпечення, сформульоване керівником від бази практики та узгоджене керівником від кафедри. Матеріали, отримані практикантом під час виконання індивідуального завдання, можуть бути використані надалі при підготовці доповідей, наукових статей, підготовки студентських наукових робіт та написанні кваліфікаційної роботи.

## VI. ФОРМИ КОНТРОЛЮ ТА ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ ПРАКТИКИ

**Форми контролю.** До видів контролю виконання завдань виробничої практики з організації захисту інформації відносяться:

- контроль за вчасним проведенням робіт, що зазначені у індивідуальному завданні та календарному плані виробничої практики;
- вчасне надання керівнику матеріалів виробничої практики відповідно до індивідуального завдання;
- контроль за якістю підготовки здобувачем письмового звіту про виконання завдань виробничої практики;
- контроль за вчасним поданням керівнику на перевірку письмового звіту про виконання завдань виробничої практики;
- контроль за підготовкою студента до захисту на кафедрі результатів виробничої практики згідно вимог індивідуального завдання.

Матеріали проходження виробничої практики з організації захисту інформації повинні бути здані керівнику практики від випускової кафедри не пізніше ніж за 3 дні після завершення терміну виробничої практики.

Результати проходження практики та звіт здобувачів обговорюються на публічному захисті практики в присутності комісії, затвердженої наказом на практику, та керівника практики від кафедри. Захист практики організовується протягом перших 10 днів після її закінчення. Комісія приймає залік у терміни, що визначені наказом на практику.

**Допуск студента до захисту виробничої практики з організації захисту інформації** здійснює керівник практики від кафедри. Критерієм допуску є:

- наявність заповненого щоденника практики;
- наявність відгуку керівника бази практики в щоденнику;
- наявність письмового звіту про виконання завдань практики, з дотриманням всіх вимог та завіреного керівником бази практики;
- відповідність змісту звіту темі індивідуального завдання;
- наявність розробленої програмної розробки, згідно індивідуального завдання.

Оцінювання результатів проходження виробничої практики відбувається на комісії згідно критеріїв, поданих в табл.

**Критерії оцінювання виробничої практики з організації захисту інформації**

| | **Зміст роботи, що оцінюється** | **Кількість балів** |
|---|---|---|
| 1 | **Теоретична підготовка.** Оцінюється вміння під час проходження практики, правильно використати теоретичні знання, здобуті здобувачами в процесі навчання. Оцінювання здійснюється на основі відгуку керівника від бази практики. | 15 |
| 2 | **Оцінювання процесу проходження практики. Особистісні характеристики.** Враховується формування технічної документації, вміння адаптуватись до вивчення нових технологій, дисциплінованість під час проходження практики, ініціативність, самостійність, професійна спрямованість, інноваційність тощо. Оцінювання здійснюється на основі відгуку керівника від бази практики. | 25 |

| | | |
|---|---|---|
| 3 | **Оцінювання звітної документації.** Оцінюється змістове наповнення всієї звітної документації (письмовий звіт та щоденник практики). | 20 |
| 4 | **Наявність розробленого програмного продукту або його частини (відповідно до індивідуального завдання) з усією супровідною документацією.** Оцінюється якість написання технічного завдання та реалізованих алгоритмів при розробці програмного продукту або його частини. | 10 |
| 5 | **Оцінювання допоміжної документації.** Оцінюється загальне оформлення щоденника, оформлення звіту практики. | 5 |
| 6 | **Захист звіту практики.** Оцінюється змістовність доповіді з чіткими та обґрунтованими відповідями на запитання членів комісії під час захисту. | 25 |
| **Всього** | | 100 |

## Політика оцінювання

### Політика викладача щодо здобувача освіти

Усі учасники освітнього процесу повинні дотримуватись вимог чинного законодавства України, Статуту і Правил внутрішнього розпорядку ВНУ імені Лесі Українки, загально-прийнятих моральних принципів, правил поведінки та корпоративної культури; підтримувати атмосферу доброзичливості, відповідальності, порядності й толерантності.

Проходження практики передбачає відвідування здобувачами настановчої конференції перед початком практики. На настановній конференції здобувачу, надається вся необхідна інформація з порядку проходження практики, проводиться інструктаж з техніки безпеки та видаються щоденники практики. Також здобувачеві видається направлення на проходження практики від університету на базу практики. Протягом перших трьох днів практикант повинен пройти інструктаж із техніки безпеки на базі практики. У період практики здобувачі дотримуються всіх правил внутрішнього розпорядку і техніки безпеки, встановлених у підрозділі і на робочих місцях.

Поставити питання для керівника практики, уточнити завдання, з’ясувати незрозумілі моменти здобувачі освіти можуть на консультаціях, які проводяться керівником практики відповідно до графіку. Кожен здобувач повинен бути учасником дистанційного курсу «Виробнича практика», розміщеного на платформі дистанційного навчання Moodle. (https://moodle-cs.vnu.edu.ua/course/view.php?id=206). Передбачено спілкування керівника практики зі здобувачами через форум дистанційного курсу. До захисту практики допускаються здобувачі, які виконали завдання, оформили звіт практики та завантажили відповідну документацію до дистанційного курсу. Вимоги до структури звіту та його оформлення здобувачі можуть переглянути на дистанційному курсі.

### Політика щодо академічної доброчесності

Під час навчання учасники освітнього процесу зобов’язані дотримуватися академічної доброчесності: етичних принципів та визначених законом правил, якими

мають керуватися учасники освітнього процесу під час навчання, викладання та провадження наукової діяльності.

Дотримання академічної доброчесності здобувачами передбачає: самостійне виконання індивідуальних завдань практики (для осіб з особливим освітніми потребами ця вимога застосовується з урахуванням їх індивідуальних потреб і можливостей); посилання на джерела інформації у разі використання ідей, тверджень, відомостей; дотримання норм законодавства про авторське право; надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності.

**Політика щодо дедлайнів та перескладання**

Терміни практики оголошуються керівником практики на настановчій конференції, зазначаються у дистанційному курсі. Матеріали практики, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку. У випадку, коли здобувач освіти не виконав завдання практики у зазначені терміни, він має можливість виконати завдання під час ліквідації академічної заборгованості.

## VII. ПІДСУМКОВИЙ КОНТРОЛЬ

Підсумковою формою контролю освітнього компонента «Виробнича практика (із розробки програмного забезпечення)» є залік. Оцінювання навчальних досягнень здійснюється за 100 бальною шкалою. Оцінювання здійснюється на основі представленого звіту, демонстрації виконання індивідуального завдання, захисту матеріалів практики, що відбувається за присутності усіх студентів-практикантів комісії та керівника практики.

Диференційована оцінка за Виробничу практику (із розробки програмного забезпечення) вноситься в заліково-екзаменаційну відомість, індивідуальний навчальний план (залікову книжку) студента за підписами членів комісії. У разі отримання незадовільної оцінки під час складання заліку студенту надається можливість повторного складання заліку за умови доопрацювання звіту й індивідуального завдання. За умови отримання незадовільної оцінки з практики під час ліквідації заборгованості комісії студент відраховується з університету.

## VIII. ШКАЛА ОЦІНЮВАННЯ

| **Оцінкав балах за всі види навчальної діяльності** | **Оцінка** |
|---|---|
| 90–100 | Зараховано |
| 82–89 | |
| 75–81 | |
| 67–74 | |
| 60–66 | |
| 1–59 | Незараховано (з можливістю повторного складання) |

## IX. РЕКОМЕНДОВАНА ЛІТЕРАТУРА ТА ІНТЕРНЕТ-РЕСУРСИ.

1. Положення про проведення практики студентів Волинського національного університет імені Лесі Українки [Електронний ресурс]. URL: https://vnu.edu.ua/uk/normativno-pravova-baza

2. Закон України «Про вищу освіту», Указ президента України від 04.07.2005р. №1013/2005 «Про невідкладні заходи щодо забезпечення функціонування та розвитку освіти в Україні».
3. Положення про навчання у Волинському національному університеті імені Лесі Українки для здобуття першого (бакалаврського) ступеня на основі раніше здобутих освітньо-кваліфікаційного рівня «молодший спеціаліст», освітнього ступеня «фаховий молодший бакалавр». URL: https://vnu.edu.ua/uk/normativno-pravova-baza
4. Положення про проведення практики студентів вищих навчальних закладів України. URL: https://zakon.rada.gov.ua/laws/show/z0035-93#Text
5. Навчальний план підготовки бакалавра, спеціальності 125 Кібербезпека та захист інформації. URL: https://vnu.edu.ua/uk/faculties-and-institutions/fakultet-informaciynikh-tekhnologiy-i-matematiki
6. Закон України «Про вищу освіту» від 01.07.2014 р. № 1556-VII (Відомості Верховної Ради (ВВР), 2014, № 37-38, ст. 2004).
7. Положення «Про проведення практики студентів вищих навчальних закладів України», затвердженого наказом Міністерства освіти України від 08.04.1993 р. № 93.
8. 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.
9. . Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 №373.
10. 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
11. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі.
12. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу.
13. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.
14. НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу
15. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.
16. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.
17. 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.
18. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
19. Корченко О.Г. Прикладна криптологія : системи шифрування: підручник / О.Г. Корченко, В.П. Сіденко, Ю.О. Дрейс. – К.: ДУТ - ТОВ "Наш формат", 2014. – 448 с.: іл.
20. Горбенко І.Д. Прикладна криптологія. Теорія. Практика. Застосування : монографія / І.Д. Горбенко, Ю.І. Горбенко. – Харків: Видавництво "Форт", 2012. – 880 с.: іл.
21. 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
22. 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.