МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Волинський національний університет імені Лесі Українки
Факультет (інститут) інформаційних технологій і математики
Кафедра Комп'ютерних наук та кібербезпеки

СИЛАБУС
ВИРОБНИЧОЇ ПРАКТИКИ

підготовки першого (бакалаврського) рівня
(назва освітнього рівня)
спеціальності 125 Кібербезпека
(шифр і назва спеціальності)
освітньої програми
«Інформаційна безпека»
(назва освітньо-професійної освітньо-наукової/освітньо-творчої програм)

Луцьк – 2020

Силабус виробничої практики підготовки першого (бакалаврського) рівня вищої освіти, галузі знань 12 Інформаційні технології, спеціальності 125 «Кібербезпека», за освітньою програмою «Інформаційна безпека»

Розробник: Сачук Ю.В., ст. викл., к. фіз.-мат.н.

Силабус виробничої практики затверджено на засіданні кафедри
Комп'ютерних наук та кібербезпеки
протокол № _3_ від 5 жовтня 2020 р.

Завідувач кафедри:  (Сачук Ю.В.)

І. ОПИС ПРАКТИКИ ВИРОБНИЧА

Найменування показників	**Галузь знань, спеціальність, освітня** /освітньо-наукова/освітньо-творча **програма, освітній рівень**	**Характеристика виду практики**
Денна форма навчання	Галузь знань: 12 Інформаційні технології Спеціальність: 125 «Кібербезпека» Освітня програма: «Інформаційна безпека» Освітній рівень: бакалавр	**Виробнича**
		Рік навчання 2020-2021
Кількість годин/кредитів 150/5		**Семестр** 8 -ий
		Консультації 10 год.
		Форма контролю: залік

ІІ. Інформація про викладача (- ів)

ПІП Сачук Юрій Володимирович

Науковий ступінь кандидат фізико-математичних наук

Вчене звання

Посада старший викладач

Контактна інформація, телефон: +380666587065, e-mail: sachykyra@gmail.com

Дні занять http://194.44.187.20/cgi-bin/timetable.cgi?n=700

ІІІ. Опис практики

1. Анотація практики

Виробнича практика студентів, які набувають кваліфікаційний рівень бакалавра за спеціальністю 125 Кібербезпека, є невід'ємною складовою навчального процесу. Під час практики студенти мають набути навичок експлуатації та захисту комп'ютерних систем та мереж, тобто здійснюють практичну підготовку до самостійної роботи із розв'язання практичних завдань на підприємстві. Виробничу практику студенти проходять на підприємствах різних форм власності під керівництвом викладачів кафедри і працівників відповідних підприємств. Така організація керівництва практикою дає змогу студентам поглибити теоретичні знання і набути досвіду практичної роботи. Під час практики студенти збирають необхідну інформацію про господарську

діяльність підприємства та її результати, потім здійснюють аналіз результатів діяльності підприємства і визначають наявність проблем. У разі виявлення на підприємстві проблем студенти повинні вказати можливі шляхи їх вирішення. Результати роботи студенти оформлюють у вигляді звіту з практики. Оцінюють результати роботи студентів спочатку керівники практики від університету та підприємства у вигляді відгуку, а потім комісія із захисту практики.

2. Мета і завдання практики

Мета: закріпити і поглибити знання, отримані за попередній час навчання в університеті, і використовувати їх для обґрунтованого прийняття проектних рішень, набути досвіду роботи виконання пошуку і порівняльного аналізу при виборі найбільш прийнятних протоколів, алгоритмів та програм, вдосконалити знання й уміння при проектуванні систем в цілому і практично закріпити навички розробки її базових елементів програмного, інформаційного та технічного забезпечення для комплексів автоматизованого проектування, інформаційно-пошукових систем, комп'ютерних мереж, системи дистанційного навчання, набути досвіду в оформленні проектних і графічних матеріалів, складанні пояснювальних записок, специфікацій, відомостей на програмне забезпечення. Під час проходження практики студенти повинні вивчити організаційну структуру підприємства; ознайомитись зі звітними та іншими інформаційними документами про діяльність підприємства; навчитись приймати управлінські рішення в реальних ситуаціях, які виникають у поточній діяльності підприємства (установи).

Завдання: знайомство з порядком роботи та умовами праці на підприємстві; отримання досвіду входження в трудовий колектив; отримання інформації про те, які знання, отримані у ЗВО, і в якому напрямі необхідно поглиблювати і розвивати; вивчення умов діяльності підприємства(установи); набуття навичок практичного застосування теоретичних знань для розв'язання завдань надання послуг у сфері кібербезпеки; навчитися аналізувати та прогнозувати результати, планувати заходи та приймати управлінські рішення щодо поліпшення технічного та технологічного стану підприємства (установи); вивчення установчих документи та ознайомлення з положеннями про відділи, посадовими інструкціями технологією управління ресурсами на базі практики; участь у виконанні конкретної роботи, що здійснюється технічними службами підприємства; підготовка рекомендації щодо покращення організації управління кібернетичною безпекою підприємства чи установи; підготувка та захист звіт за результатами проходження виробничої практики.

3. Результати навчання

За результатами практики студенти будуть компетентними у таких питаннях:

- вмітимуть використовувати засоби пошуку та порівняльного аналізу інформації при виборі найбільш прийнятних протоколів, алгоритмів і

програм за економічними та технічними характеристиками;

- знатимуть правила оформлення проектних і графічних матеріалів, специфікацій, відомостей на програмне забезпечення та іншої конструкторської документації;
- вмітимуть працювати зі спеціальною технічною і науковою літературою та правилами оформлення технічної документації з засобів апаратного та прорамного захисту;
- вмітимуть виконати аналіз безпеки комп'ютерної системи або мережі та усунути можливі шляхи несанкціонованого доступу;
- вмітимуть перевірити надійність захисту інформації та стійкості його щодо хакерських атак шляхом моделювання загроз;
- знатимуть, як здійснити організаційні та програмні заходи щодо підвищення рівня безпеки зберігання інформації;
- знатимуть, як підібрати комплекс необхідних апаратно-програмних засобів для захисту комп’ютерної системи та мережі;
- вмітимуть виконувати адміністрування прав доступу до комп´ютерної системи та мережі з метою перешкоди призначення невиправданих привілеїв;
- володітимуть навичками, як підібрати тип та структуру локальної комп’ютерної мережі;

IV. ЕТАПИ ПРАКТИКИ

Етапи	Зміст, основні завдання	Тривалість
Підготовчий	1. Техніка безпеки і охорона праці на об'єкті практики.	4
	2. Знайомство з правилами внутрішнього розпорядку підприємства, інструктаж з техніки безпеки та охорони праці, бесіда спеціалістів.	10
	3. Техніка безпеки і охорона праці у підрозділі.	3
	4. Техніка безпеки і охорона праці на робочих місцях.	3
Всього годин		20
Ознайомлювальний	1. Знайомство з підприємством. Екскурсія по відділам підприємства та службам, що забезпечують його роботу.	2
	2. Вивчення роботи основних структурних підрозділів.	2

	3. Ознайомлення з обчислювальним центром підприємства.	2
	4. Ознайомлення з підрозділами підприємства.	2
	5. Вивчення особливостей роботи окремого структурного підрозділу	6
	6. Ознайомлення з обов'язками згідно з місцем роботи у підрозділі підприємства.	4
	7. Ознайомлення з обов'язками фахівця з захисту інформації.	6
Всього годин		24
Основний	1. Робота зі стандартним обладнанням та програмним забезпеченням.	8
	2. Робота в середовищі сучасних операційних систем та баз даних.	8
	3. Налаштування обладнання комп'ютерних систем та мереж, апаратних, програмних, локальних та мережевих засобів	8
	4. Робота дублером адміністратора комп'ютерних систем та мереж.	8
	5. Обслуговування засобів комп'ютерних систем та мереж	8
	6. Аналіз роботоспроможності мережі та пошук в них вразливостейй за допомогою спеціального програмного забезпечення.	6
	7. Робота дублером ремонтника апаратних засобів комп'ютерних систем та мереж.	8
	8. Аналіз апаратних засобів комп'ютерних систем та мереж.	6
	9. Аналіз апаратних засобів комп'ютерних систем та мереж спеціальним програмним забезпеченням.	6
	10. Аналіз вразливостей комп'ютерних систем та мереж.	5
	11. Оцінка вразливостей в комп'ютерних системах та мережах.	5
	12. Вивчення наукових розробок в напрямку виявлених вразливостей на підприємстві	5

	13. Використовування електронної пошти та телеконференцій для спілкування	5
	14. Вивчення впровадження нових моделей базових захисту інформаційних процесів та висунення пропозицій щодо оптимізації, удосконалення та розвитку існуючих	8
Всього годин		94
Підсумковий	1. Узагальнення та систематизація матеріалу щодо проходження виробничої практики. Підготовка необхідної документації.	7
	2. Оформлення щоденника та звіту практики.	3
	3. Захист практики	2
Всього годин		12
Всього		150

V. ВИДИ (ФОРМИ) ІНДИВІДУАЛЬНИХ ЗАВДАНЬ

1. Ознайомлення з програмою практики. Знайомство з підприємством, його структурою. Інструктаж з техніки безпеки

Практиканти повинні ознайомитися з програмою практики, її основними тематичними розділами. Отримати від керівника практики індивідуальні завдання та документи які потрібно оформити під час проходження практики.

Після прибуття на підприємство практикант повинен ознайомитися: з відомчим підпорядкуванням бази практики, основними нормативно-правовими документами, що лежать в основі її діяльності; з режимом роботи і правилами внутрішнього розпорядку; з вимогами, які пред'являються до працівників бази практики, їх професійних компетентностей в сфері інформаційних технологій та захисту інформації; з основними обов'язками працівників та посадових осіб бази практики;

Керівник практики від бази, ознайомлює з порядком проходження, розпорядком роботи. На основі запропонованого орієнтовного тематичного плану, враховуючи конкретні умови роботи університету, складається орієнтовний графік проходження практики. У разі потреби при виконанні індивідуальних завдань студент складає і затверджує особистий план.

Практиканти проходять інструктаж з техніки безпеки під час проходження практики.

2. Нормативно-правове регулювання забезпечення інформаційної безпеки.

Практиканти повинні визначити перелік нормативних актів що регулюють питання інформаційної безпеки бази практики (міжнародні нормативно-правові акти, закони Верховної Ради України, постанови Кабінету

Міністрів України, Укази президента України, та інші нормативно-правові акти що стосуються інформаційної безпеки бази практики а також внутрішні накази, положення, інструкції бази практики). Після цього необхідно проаналізувати основні положення цих нормативно-правових актів.

Далі практиканти аналізують основні міжнародні та державні стандарти якими повинно керуватися підприємство в галузі інформаційної безпеки.

3. Забезпечення комп'ютерною технікою. Периферійне обладнання та комп'ютерна мережа.

Практиканти повинні проаналізувати рівень комп'ютерного забезпечення підприємства (установи): кількість серверів, персональних комп'ютерів, ноутбуків, інших обчислювальних пристроїв, особливості їх архітектури, апаратну конфігурацію, інтерфейси та ін.

Далі проводиться аналіз периферійного (пристрої вводу-виводу, їх функціональні характеристики) та мережевого обладнання (маршрутизатори, комутатори, wifi-роутери, модеми, тощо), локальної комп'ютерної мережі бази практики (топологія, передавальне середовище, тип підключення до глобальної комп'ютерної мережі Internet) та ін.

У звіті необхідно описати характеристики зазначеного обладнання. Намалювати схему локальної обчислювальної мережі підприємства.

4. Програмне забезпечення комп'ютерної техніки

Досліджується програмне забезпечення що встановлене на комп'ютерній техніці підприємства (установи): операційні системи, прикладне програмне забезпечення, спеціалізоване програмне забезпечення, службове ПЗ, антивіруси, інше програмне забезпечення що використовується для захисту інформації. Аналізується його конфігурація.

5. Обіг даних та інформації

Практиканти повинні проаналізувати інформаційну систему бази практики з точки зору інформації що в ній обробляється:

Яка конфіденційна інформація збирається, обробляється, зберігається та передається на базі практики (документи, інформація про працівників, клієнтів, товари, послуги, комерційна інформація, проекти, розробки, патенти, тощо).

Яким чином забезпечується її обіг на підприємстві (бази даних, спеціалізоване програмне забезпечення, системи електронного документообігу, технічні канали передачі, тощо).

6. Аналіз основних напрямків забезпечення інформаційної безпеки на підприємстві

Практиканти аналізують основні напрямки забезпечення інформаційної безпеки на підприємстві (установі). Визначають загрози щодо конфіденційної інформації бази практики. Досліджують організаційний та інженерно-технічний захист інформації на нафультеті (інформаційно-обчилювальному центрі).

Визначають яким чином відбувається організація і забезпечення робіт щодо захисту інформації.

7. Висновки щодо рівня інформаційної (кібербезпеки) безпеки бази практики

Внесення пропозицій по підвищенню рівня інформаційної безпеки бази практики на рівні апаратного забезпечення, операційних систем, програмного забезпечення, баз даних, комп'ютерних систем та мереж.

8. Підведення підсумків

Після закінчення терміну практики студенти звітують про виконання програми та індивідуального завдання. Форма звітності студента за практику – заповнений щоденник практики та подання письмового звіту, підписаного і оціненого безпосередньо керівником від бази практики. Щоденник практики разом з іншими документами, установленими навчальним закладом подається на рецензування керівнику практики від навчального закладу.

Щоденник практики та звіт має містити відомості про виконання студентом усіх розділів програми практики та індивідуального завдання. Оформляється щоденник та звіт практики за вимогами, які встановлює вищий навчальний заклад.

VI. ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ ПРАКТИКИ

Зміст роботи, що оцінюється	**Кількість балів**
Ознайомлення з програмою практики. Знайомство з підприємством, його структурою. Інструктаж з техніки безпеки.	5
Нормативно-правове регулювання забезпечення інформаційної (кібербезпеки) безпеки на підприємстві.	5
Забезпечення комп'ютерною технікою. Периферійне обладнання та комп'ютерна мережа.	10
Програмне забезпечення комп'ютерної техніки.	10
Обіг даних та інформація	10
Аналіз основних напрямків забезпечення інформаційної безпеки на підприємстві	15
Технічний захист інформації. Програмний захист інформації.	15
Висновки щодо рівня інформаційної безпеки бази практики.	10
Підведення підсумків. Оформлення щоденника, звіту практики та захист практики.	20
Сума	100

Політика викладача щодо студента (щодо відвідування практики). Відвідування підприємства(установи) бази практики є обов'язковим згідно встановленого графіку керівником від бази практики. За об'єктивних причин (наприклад хвороба) графік може бути скорегований та за погодженням із керівником від бази практики.

Політика щодо академічної доброчесності. Усі письмові роботи та звіти перевіряються на наявність плагіату і допускаються до захисту із коректними текстовими запозиченнями не більше 30%.

Політика щодо дедлайнів та перескладання. Студенту, який не виконав програму практики з поважних, має виконати всі завдання практики за індивідуальним планом та представити результати практики керівнику від бази практики та керівнику практики від ЗВО.

Шкала оцінювання студентів:

Оцінка в балах за всі види навчальної діяльності	**Оцінка**	
	для екзамену	**для заліку**
90 – 100	Відмінно	Зараховано
82 – 89	Дуже добре	
75 - 81	Добре	
67 -74	Задовільно	
60 - 66	Достатньо	
1 – 59	Незадовільно	Незараховано (з можливістю повторного складання)

VII. ПІДСУМКОВИЙ КОНТРОЛЬ

Звіт по практиці необхідно представити на кафедру не пізніше встановленого терміну на випусковій кафедрі. Захист звіту відбувається в терміни, встановлені кафедрою. Захист звіту про практику відбувається перед комісією, до якої входять керівники практики від кафедри і інші викладачі. По результатах захисту звіту студентові виставляється відмітка про залік, яка записується у залікову книжку. Неподання звіту є підставою для повторного проходження практики за індивідуальним графіком, а у випадку зневажливого ставлення до практики і порушення дисципліни - для відрахування з вузу.

VIII. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

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. Державний стандарт України. ДСТУ 3008-2015 «Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання») /[На заміну ДСТУ 3008-95; чинний від 2017-07-01].- Київ: ДП «УкрНДНЦ», 2016. 31 с. URL: http://www.knmu.kharkov.ua /attachments/3659_3008-2015.PDF

4. Державний стандарт України. ДСТУ 8302:2015 "Інформація та документація. Бібліографічне посилання. Загальні вимоги та правила складання" URL:http://lib.npu.edu.ua/files/dstu-8302-2015.pdf

5. Стандарти з інформації, бібліотечної і видавничої справи. URL:http://wwvv.library.univ.kiev.ua/ukr/about/dstu.html

6. ДСТУ ISO 5807:2016 Обробляння інформації. Символи та угоди щодо документації стосовно даних, програм та системних блок-схем, схем мережевих програм та схем системних ресурсів (ISO 5807:1985, IDT).

7. Положення про проведення практики студентів Волинського національного університету імені Лесі Українки, схваленого Вченою радою, протокол №10 від 28 серпня 2020 р.

8. Положення про проведення практики студентів Волинського національного університету імені Лесі Українки, схваленого Вченою радою, протокол №10 від 28 серпня 2020 р.

IX. ДОДАТКОВІ ВКАЗІВКИ ТА РЕКОМЕНДАЦІЇ

Календарний графік проходження практики

№ з/п	Назви робіт	Тижні проходженя практики						Відмітки про виконання
		1	2	3	4	5	6	

Обов'язки здобувачів вищої освіти при проходженні практики зобов'язані:

1. отримати направлення на практику з індивідуальним завданням, пройти інструктаж про порядок проходження практики та з техніки безпеки, консультації щодо оформлення усіх необхідних документів;
2. отримати та заповнити щоденник практики;
3. своєчасно прибути на базу практики;

4. виконувати правила внутрішнього розпорядку бази практики, розпорядження адміністрації та керівників практики.

5. в повному обсязі виконати програму практики;

6. дотримуватися правил охорони праці, техніки безпеки й виробничої санітарії;

7. нести відповідальність за виконану роботу;

8. своєчасно подати щоденник та звіт про проходження практики та захистити його;

Рекомендована структура звіту наступна:

- титульний аркуш;
- зміст;
- вступ;
- текст індивідуального завдання;
- висновки та рекомендації;
- список літератури;
- додатки.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВОЛИНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ЛЕСІ УКРАЇНКИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І МАТЕМАТИКИ

Кафедра комп’ютерних наук та кібербезпеки

ЗВІТ

про проходження виробничої практики

студента IV курсу денної форми навчання

“_”група

_____

прізвище, ім’я та по-батькові

_____

(база пратики)

Період з “____ р.” до “_____ р.”

Керівник практики:
від підприємства
_.
від кафедри
_.

Луцьк 2021