

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

СИЛАБУС
ПРАКТИКА ТЕХНОЛОГІЧНА

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)

1. ІНФОРМАЦІЙНИ ОПИС ПРАКТИКИ

| Найменування показників | Галузь знань, спеціальність, освітня програма, освітній ступінь | Характеристика навчальної дисципліни |
|---|---|--------------------------------------|
| Денна форма навчання | Шифр і назва галузі знань: <i>12 Інформаційна безпека</i> Спеціальність: <i>125 Кібербезпека</i> Освітньо-професійна програма <i>Інформаційна безпека</i> | Нормативна |
| | | Рік навчання: <i>третій</i> |
| | | Семестр <i>6</i> |
| | | Консультації <i>6 год.</i> |
| Кількість годин/кредитів <i>60/2</i> | Освітній ступінь бакалавр | Самостійна робота <i>54 год.</i> |
| | | Форма контролю: залік |

2. КОМПЕТЕНЦІЇ

За результатами практики студенти будуть компетентними у таких питаннях:

- вмітуть виконати аналіз безпеки комп'ютерної системи або мережі та усунути можливі шляхи несанкціонованого доступу;
- вмітуть 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.
- навчатимуться 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;

3. ЕТАПИ ПРАКТИКИ

| Етапи | Зміст, основні завдання, тривалість |
|---------------------|---|
| 1. Підготовчий | <ol style="list-style-type: none">1. Проходження інструктажу з техніки безпеки2. Ознайомлення з техніко-економічними характеристиками підприємства (закладу, організації) та організаційною структурою управління.3. Ознайомлення з положенням про функціональний підрозділ, комплексом задач, які реалізують функції управління. |
| 2. Ознайомлювальний | <ol style="list-style-type: none">1. Вивчення проектної документації на діючу АІС об'єкту, характеристик функціональної й забезпечуючої складових АІС2. Вивчення складу автоматизованих задач підсистеми, їх інформаційного, програмного, технічного забезпечень3. Проведення інформаційного аналізу та моделювання предметної області підсистеми4. Вивчення інфраструктури корпоративної інформаційної системи підприємства (організації) |
| 5. Основний | <ol style="list-style-type: none">1. Проаналізувати систему безпеки ІС підприємства(організації) та її відповідність цілям та задачам бізнес-діяльності2. Робота на АРМ спеціаліста функціонального підрозділу чи робочому місці спеціаліста відділу комп'ютеризації та інформаційних технологій |
| 6. Підсумковий | <ol style="list-style-type: none">1. Оформлення звіту згідно з ДСТУ |

4. ВИДИ (ФОРМИ) ІНДИВІДУАЛЬНИХ ЗАВДАНЬ

Перед початком проходження навчальної практики студенти одержують від викладачів кафедри індивідуальні завдання, які вони повинні виконати в період проходження практики.

Індивідуальне завдання видається з метою формування у практикантів навичок самостійної роботи, уміння використовувати теоретичні знання в конкретних видах діяльності, аналізувати і оцінювати рівень інформаційної безпеки бази практики на основі теоретичних знань, які вони одержали в навчальному закладі, надбання студентами під час практики умінь та навичок самостійного розв'язання завдань, пов'язаних з використанням комп'ютерної техніки в своїй роботі, активізації діяльності студентів, розширення їх світогляду.

Теми завдань видаються з урахуванням умов роботи установи – бази практики на основі теоретичних знань, які вони одержали в університеті.

Формами індивідуальної роботи можуть бути:

- написання рефератів на певну тему;
- складання задач;
- проведення досліджень.

Індивідуальні завдання розробляються викладачами кафедри національної безпеки.

Спеціальний час для написання індивідуального завдання не відводиться, воно виконується одночасно з проходженням тем практики.

5. ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ ПРАКТИКИ

| Зміст роботи, що оцінюється | Кількість балів |
|--|-----------------|
| 1. Техніка безпеки і охорона праці на об'єкті практики: Знайомство з правилами внутрішнього розпорядку інструктаж з техніки безпеки та охорони праці, бесіда спеціалістів. | 5 |
| 2. Загальні відомості про об'єкт практики Вивчення роботи основних структурних підрозділів. Ознайомлення з інформаційно-обчислювальним центром | 5 |
| 3. Виконання індивідуальних завдань | 20 |
| 4. Виконання обов'язків згідно з місцем проходження практики в університеті: Ознайомлення з обов'язками фахівця з захисту інформації. Робота зі стандартним обладнанням та програмним забезпеченням. Робота в середовищі сучасних операційних систем та баз даних. Налаштування обладнання телекомунікаційних систем та мереж, апаратних, програмних, локальних та мережевих засобів. Аналіз роботоспроможності мережі та пошук в них уразливостей за допомогою спеціального програмного забезпечення. | 20 |
| 5. Підготовка і оформлення звітних матеріалів та захист практики Узагальнення та систематизація матеріалу щодо проходження виробничої технологічної практики. Підготовка необхідної документації. Оформлення пояснювальної записки звіту з технологічної практики | 10 |
| Сума | 60 |

Шкала оцінювання

| 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) |

7. МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ЩОДО ПРОХОДЖЕННЯ ПРАКТИКИ

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.

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.

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

Практиканти повинні проаналізувати рівень комп'ютерного забезпечення університету (факультету): 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, wi-fi-роутери, модеми, тощо), локальної комп'ютерної мережі бази практики (топология, 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.

Програмне забезпечення комп'ютерної техніки

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

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 в університеті (бази даних, спеціалізоване програмне забезпечення, системи електронного документообігу, технічні канали передачі, тощо).

Аналіз основних напрямків забезпечення інформаційної безпеки на підприємстві

Практиканти аналізують основні напрямки забезпечення інформаційної безпеки в університеті. Визначають загрози щодо конфіденційної інформації бази практики. Досліджують організаційний та інженерно-технічний захист інформації на факультеті (інформаційно-обчислювальному центрі).

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

Висновки щодо рівня інформаційної 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.

Підведення підсумків

Практиканти закінчують виконання індивідуальних завдань практики. Оформлюють та підписують звітну документацію (звіт про проходження практики, звіт про виконання індивідуального науково-дослідного завдання)

8. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна література:

1. Stallings, William (2008). Computer Organization & Architecture. NewDelhi: Prentice-Hall of India Private Limited. p. 267. ISBN 978-81-203-2962-1.
2. Ануфрієнко К.П. Електронний документообіг [Текст]Ж Навчальний посібник / К.П. Ануфрієнко, Ю.Б. Коваленко. – К – НАУ, 2015. – 176с.
3. Бабак В. П. Інформаційна безпека та сучасні мережеві технології :Англо - українсько - російський словник термінів К.: НАУ, 2003
4. Бондаренко М. Ф. Операційні системи : навч. посіб. Харків: КомпаніяСМІТ, 2008
5. Вдовин М.Л. Математичне програмування: теорія та практикум : навч. посіб. Львів: Новий Світ, 2009
6. Войтюшенко Н., Остапець А.І. Інформатика та комп'ютерна техніка К. Юрінком Інтер, 2006
7. Гайна Г. А. Основи проектування баз даних : навч. посібник К.: Кондор, 2008
8. Глибовець А.М. Практикум з мови програмування Сі: навчальний посібник: рекомендовано МОН України К.: Києво-Могилянська академія, 2010
9. Головань С.М., Петров О.С., Щербак Л.М., Хорошко В.О Основи організації електронного документообігу. Луганськ: Вид. СХУ ім. В.Даля, 2011. -468 с.
10. Голубничий Д.Ю. Системне програмування і операційні системи : навч. посібн. Ч. 1 / Д. Ю. Голубничий, В. Ф. Третяк. – Х. : Вид. ХДЕУ, 2004. – 192 с.
11. Голубничий Д.Ю. Системне програмування та операційні системи : навч. посібн. Ч. 2 / . Ю. Голубничий, В. Ф. Третяк, С. В. Кавун. – Х. : Вид. ХНЕУ, 2005. – 264 с.
12. Грищук Ю.С. Мікропроцесорні пристрої: навч. посібник : рекомендовано МОН України Харків: НТУ "ХПІ", 2008
13. Джонсон М. Разработка приложений в среде Linux / М. Джонсон, Э. Троян ; пер. с англ. – М. : ООО "И.Д. Вильямс", 2007. – 544 с.
14. Злобін Г.Г. Основи інформатики, комп'ютерної техніки і комп'ютерних технологій:

Підручник К.: Каравела, 2007

15. Коваленко Б.Д. Інженерна та комп'ютерна графіка : навчальний посібник К.: Каравела, 2008
16. Кормич Б.А. Інформаційна безпека: організаційно-правові основи К.: Кондор, 2004. - 384 с.
17. Кравчук С.О. Основи комп'ютерної техніки. Компоненти, системи, мережі : навч. посібник : рекомендовано МОН України К. : Політехніка, Каравела, 2005
18. Кубрак А.І. Комп'ютерне моделювання та ідентифікація автоматичних систем : навч. посібник К. : Політехніка, 2004
19. Маклин Й. Установка и настройка Windows 7. Учебный курс Microsoft / Й. Маклин, Т. Орин. – М. : Русская редакция, 2011. – 848 с.
20. Матвієнко О. В. Основи організації електронного документообігу : навч. посібник К. : Центр учбової літ-ри, 2008
21. Михайленко В. Є. Інженерна та комп'ютерна графіка : підручник : затверджено МОН України К.: Каравела, 2010
22. Олифер В. Г. Сетевые операционные системы / В. Г. Олифер, Н. А.Олифер. – СПб. : Питер, 2002. – 544 с.
23. Пасічник В.В. Організація баз даних та знань : Підручник для вузів К.: Вид. група ВНУ, 2006
24. Побегайло А. П. Системное программирование в Windows / А. П.Побегайло. – СПб. : БХВ-Петербург, 2006. – 1056 с.
25. Секунов Н. Ю. Программирование на С++ в Linux / Н. Ю. Секунов. – СПб.: БХВ-Петербург, 2004. – 368 с.
26. Сорокина С. И. Программирование драйверов и систем безопасности : учебн. пособ. / С. И. Сорокина, А. Ю. Тихонов, А. Ю. Щербаков. – СПб. : БХВ-Петербург, 2003. – 256 с.
27. Соснін О.В. Проблеми державного управління системою національних інформаційних ресурсів з наукового потенціалу України: К.: Інститут держави і права ім. В.М.Корецького НАН України, 2003. – 572 с
28. Таненбаум Э. Современные операционные системы / Таненбаум Э. – СПб. : Питер, 2010. – 1120 с.
29. Терещенко Т.О. Мікропроцесорна техніка : підручник для студентів технічних спеціальностей вузів К. : Кондор, 2008
30. Третьяк В. Ф. Основи операційних систем : навч. посібн. / В. Ф. Третьяк, Д. Ю.Голубничий, С. В. Кавун. – Х. : Вид. ХНЕУ, 2005. – 228 с.
31. Шеховцов В. А. Операційні системи : Підручник для вузів К.: Вид. група ВНУ, 2005
32. Шпак З.Я. Програмування мовою С: навч. посібник Львів: Оріяна- Нова, 2006

8. Додаткова література:

1. Autonomic Systems: Concept for Self-Managing IT Infrastructure White Paper. Fujitsu Siemens Computers, March 2003.
2. Brassard G. Modern Cryptology. - N.Y.: Springer-Verlag, 1988. - 107 p.
3. Cisco Systems, Designing a Campus Network for High Availability. – 2006 – 60с.
4. Cisco Systems, Campus Design: Analyzing the Impact of Emerging Technologies on Campus Design. – 2006. – 91с.
5. Cisco Systems, Understanding Rapid Spanning Tree Protocol (802.1w)(Document ID: 24062). -2006. – 14с.
6. Cisco Systems, Understanding Multiple Spanning Tree Protocol (802.1s)(Document ID: 24248). – 2005. – 14с.
7. David Hucaby. CCNP Self-Study: CCNP BCMSN Exam Certification Guide, Third Edition. – Cisco Press, 2005. – 624с.
8. Dave Hucaby, Steve McQuerry. Cisco Field Manual: Catalyst Switch Configuration. – Cisco

Press, 2002. – 560c.

9. Eric Ouellet, Robert Padjen, Arthur Pfund, Ron Fuller, Tim Blankenship —Building a Cisco Wireless LAN - Syngress Publishing, Inc, 2002.

10. ДОДАТКОВІ ВКАЗІВКИ ТА РЕКОМЕНДАЦІЇ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ СХІДНОЄВРОПЕЙСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ЛЕСІ УКРАЇНКИ

ЗВІТ

про виконання програми наскрізної технологічної
(навчальної) практики

студента_

(прізвище, ім'я, по батькові)

групи_

напряму підготовки
(спеціальність)_

спеціалізація_кваліфікаційний рівень

Керівник практики _

(посада, прізвище, ініціали)

Луцьк – 2020