**ЗАТВЕРДЖЕНО**

Вченою радою факультету
факультету інформаційно-
комп'ютерних технологій
31 серпня 2023 р., протокол № 5

Голова Вченої ради
_____ Тетяна НІКІТЧУК

# РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ВК «БЕЗПЕКА LINUX/UNIX СИСТЕМ»

для здобувачів вищої освіти освітнього ступеня «магістр»
спеціальності 125 «Кібербезпека та захист інформації»
освітньо-професійна програма «Кібербезпека»
факультет інформаційно-комп'ютерних технологій
кафедра комп'ютерної інженерії та кібербезпеки

Схвалено на засіданні
кафедри комп'ютерної
інженерії та кібербезпеки
28 серпня 2023 р., протокол № 7

Завідувач кафедри
_____ Андрій ЄФІМЕНКО

Гарант освітньо-
професійної програми
_____ Володимир ВОРОТНІКОВ


Розробник: кандидат педагогічних наук, доцент, доцент кафедри комп'ютерної інженерії та кібербезпеки Олена ГОЛОВНЯ


Житомир
2023 – 2024 н.р.

# 1. Опис навчальної дисципліни

| Найменування показників | Галузь знань, напрям підготовки, освітній ступінь | Характеристика навчальної дисципліни | |
|---|---|---|---|
| | | денна форма навчання | заочна форма навчання |
| Кількість кредитів – 4 | Галузь знань<br>12 «Інформаційні технології» | Нормативна | |
| Модулів – 1 | Спеціальність<br>125 «Кібербезпека та захист інформації» | Рік підготовки: | |
| Змістових модулів – 2 | | I | I |
| | | Семестр | |
| Загальна кількість годин – 120 | | 2-й | 2-й |
| | | Лекції | |
| Тижневих годин для денної форми навчання<br><br>денна форма:<br>аудиторних – 3<br>самостійної роботи – 4,5<br><br>заочна форма:<br>аудиторних – 0,5<br>самостійної роботи – 6,5 | Освітній ступінь «магістр» | 16 год. | 2 год. |
| | | Практичні | |
| | | – | – |
| | | Лабораторні | |
| | | 32 год. | 8 год. |
| | | Самостійна робота | |
| | | 72 год. | 110 год. |
| | | | |
| | | Вид контролю:<br>залік (2-й семестр) | |

Співвідношення кількості годин аудиторних занять до самостійної та індивідуальної роботи становить:

для денної форми навчання – 40% аудиторних занять, 60% самостійної та індивідуальної роботи,

для заочної форми навчання – 9% аудиторних занять, 91% самостійної та індивідуальної роботи.

## 2. Мета та завдання навчальної дисципліни

**Метою навчальної дисципліни** є розвиток компетентностей здобувачів освіти, пов'язаними із забезпеченням захисту комп'ютерних систем та мереж на базі ОС Linux.

**Завданнями вивчення навчальної дисципліни** є:

– поглиблення та доповнення в здобувачів освіти теоретичних знань про будову та функціонування систем та мереж на основі ОС Linux;

– розвиток у здобувачів освіти навичок управління ОС Linux та організації її захисту.

Зміст навчальної дисципліни спрямований на формування наступних **компетентностей**.

**К 1.** Налагодження та посилення захисту облікових записів користувачів у комп'ютерній системі.

**К 2.** Організація надійного та безпечного доступу користувачів до ресурсів мережі.

**К 3.** Захист кінцевих мережних пристроїв від шкідливого ПЗ.

**К 4.** Виявлення вразливостей та протидія вторгненням на кінцевих мережних пристроях.

Також зміст навчальної дисципліни покликаний сприяти розвитку наступних **компетентностей, визначених стандартом** вищої освіти зі спеціальності 125 «Кібербезпека та захист інформації»:

**КЗ1.** Здатність застосовувати знання у практичних ситуаціях.

**КФ1.** Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.

**КФ5.** Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

**КФ6.** Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

**КФ7.** Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю

та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому

**КФ9.** Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому

Знання, уміння та навички з навчальної дисципліни стануть складовими наступних **програмних результатів** навчання:

**РНД 1.1.** Налагодження та посилення парольного захисту облікових записів.

**РНД 1.2.** Налаштування та обмеження адміністративних повноважень в операційній системі.

**РНД 2.1.** Налаштування роботи мережних екранів в операційні системі.

**РНД 2.2.** Організація безпечного мережного з'єднання для віддаленого управління кінцевими мережними пристроями.

**РНД 3.1.** Організація сканування кінцевих мережних пристроїв на предмет наявності шкідливого програмного забезпечення.

**РНД 3.2.** Здійснення аудиту на кінцевих мережних пристроях.

**РНД 4.1.** Шифрування томів та окремих елементів файлової системи.

**РНД 4.2.** Аналіз кінцевих мережних пристроїв на наявність вразливостей.

Також отримані знання з навчальної дисципліни сприяти розвитку наступних програмних **результатів навчання, визначених стандартом** вищої освіти зі спеціальності 125 «Кібербезпека та захист інформації».

**РН1.** Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

**РН2.** Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

**РН3.** Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

**РН4.** Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

**РН6.** Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

**РН7.** Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

**РН8.** Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

**РН9.** Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

**РН10.** Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

**РН11.** Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

**РН12.** Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.

**РН13.** Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.

**РН14.** Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.

**РН16.** Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.

**РН18.** Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.

**РН19.** Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.

**РН20.** Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.

**РН21.** Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

**РН22.** Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.

**РН23.** Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

## 3. Програма навчальної дисципліни

### Модуль 1. БЕЗПЕКА UNIX/LINUX СИСТЕМ

### Змістовий модуль 1. Базовий захист у Linux

#### Тема 1. Захист облікових записів користувачів у Linux

Обліковий запис root та механізм sudo. Файл /etc/sudoers та команда visudo. Таймер для sudo. Закриття доступу до домашніх каталогів користувачів. Налаштування вимог до паролів. Обмеження термінів існування облікових записів та паролів. Захист від атак на паролі методом грубої сили (brute-force password attacks). Роль та налаштування банерів та повідомлення дня (MOTD).

#### Тема 2. Брандмауер у Linux

Брандмауер. Компонент netfilter. Утиліта iptables. Утиліта ufw. Утиліта nftables.

#### Тема 3. Шифрування у Linux. Захист SSH-з'єднання в Linux

GNU Privacy Guard. Поєднання GPG та утиліти tar для створення зашифрованих резервних копій. Використання приватних та публічних ключів для асиметричного шифрування та цифрових підписів. Підписування файлів без шифрування. Використання LUKS для шифрування дискових розділів у Linux. Створення зашифрованого тому під час встановлення Ubuntu Linux. eCryptfs. Шифрування окремих каталогів. VeraCrypt.

## Змістовий модуль 2. Розширений захист Linux

### Тема 4. Вибіркове керування доступом у Linux

Поняття вибіркового керування доступом (Discretionary access control, DAC). Команди chown та chmod. Механізми SUID та SGID та пов'язані з ними ризики. Використання розширених атрибутів.

### Тема 5. Розширені списки керування доступом у Linux

Базові та розширені ACL у Linux. Керування успадкуванням ACL. Вибіркове вилучення дозволів за допомогою масок FACL. Особливості архівування файлів з розширеними ACL. Спільні каталоги у Linux.

### Тема 6. Мандатний контроль доступу у Linux

SELinux. Налаштування контекстів безпеки для файлів та каталогів. Політики SELinux. Вирішення проблем з SELinux. AppArmor. Політики AppArmor. Вирішення проблем з AppArmor.

### Тема 7. Розширені прийоми і засоби захисту Linux

Ситуація зі шкідливим ПЗ для Linux. Роль сканування та аудиту. ClamAV. maldet, SELinux, Rootkit Hunter, OpenSCAP. Сканування на вразливості та протидія вторгненням у Linux. Snort. Security Onion. Lynis. OpenVAS. Nikto.

# 4. Структура (тематичний план) навчальної дисципліни

| Змістові модулі і теми | Кількість годин | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | денна форма | | | | заочна форма | | | |
| | усього | лекції | лабораторні | самостійна робота | усього | лекції | лабораторні | самостійна робота |
| **Модуль 1** | | | | | | | | |
| **Змістовий модуль 1. Базовий захист у Linux** | | | | | | | | |
| Тема 1. Захист облікових записів користувачів у Linux | 20 | 2 | 4 | 14 | 20 | 1 | 2 | 17 |
| Тема 2. Брандмауер у Linux | 20 | 2 | 4 | 14 | 20 | 0 | 2 | 18 |
| Тема 3. Шифрування у Linux. Захист SSH-з'єднання в Linux | 20 | 4 | 8 | 8 | 20 | 0 | 0 | 20 |
| ***Разом за змістовий модуль 1*** | **60** | **8** | **16** | **36** | **60** | **1** | **4** | **55** |
| **Змістовий модуль 2. Розширений захист Linux** | | | | | | | | |
| Тема 4. Вибіркове керування доступом у Linux | 15 | 2 | 2 | 11 | 15 | 1 | 1 | 13 |
| Тема 5. Розширені списки керування доступом у Linux | 15 | 2 | 4 | 9 | 15 | 0 | 1 | 14 |
| Тема 6. Мандатний контроль доступу у Linux | 15 | 2 | 4 | 9 | 15 | 0 | 1 | 14 |
| Тема 7. Розширені прийоми і засоби захисту Linux | 15 | 2 | 6 | 7 | 15 | 0 | 1 | 14 |
| ***Разом за змістовий модуль 2*** | **60** | **8** | **16** | **36** | **60** | **1** | **4** | **55** |
| **ВСЬОГО** | **120** | **16** | **32** | **72** | **120** | **2** | **8** | **110** |

## 5. Теми практичних (лабораторних) занять

| № з/п | Назва теми | Кількість годин | |
|---|---|---|---|
| | | денна форма | заочна форма |
| 1 | Лабораторна робота №1. Захист облікових записів користувачів у Linux | 4 | 2 |
| 2 | Лабораторна робота №2. Налаштування брандмауера у Linux | 4 | 2 |
| 3 | Лабораторна робота №3. Шифрування у Linux | 4 | 0 |
| 4 | Лабораторна робота №4. Захист SSH-з'єднання у Linux | 2 | 0 |
| 5 | *Модульна контрольна робота №1* | 2 | 0 |
| 6 | Лабораторна робота №5. Вибіркове керування доступом у Linux | 2 | 1 |
| 7 | Лабораторна робота №6. Розширені списки керування доступом у Linux | 4 | 1 |
| 8 | Лабораторна робота №7. Налаштування мандатного контролю у Linux | 4 | 1 |
| 9 | Лабораторна робота №8. Захист Linux від шкідливого програмного забезпечення | 2 | 1 |
| 10 | Лабораторна робота №9. Сканування на вразливості та протидія вторгненням у Linux | 2 | 0 |
| 11 | *Модульна контрольна робота №2* | 2 | 0 |
| РАЗОМ | | 32 | 8 |

## 6. Завдання для самостійної роботи

У межах самостійної роботи передбачене проходження здобувачами освіти окремих модулів на базі електронної освітньої платформи Rangeforce. Перелік модулів уточнюється та оновлюється відповідно до доступних на момент роботи модулів («Linux User Management», «Linux File Permissions and Ownership», «Linux Execution Context», «Linux Log Management: Systemd», «Deploying Linux Endpoint Protection», «Linux Security Investigation Exercise», «Identifying Linux IOCs» чи подібні). Здійснюється опрацювання здобувачами освіти теоретичних матеріалів, виконання ними практичних завдань та проходження контрольних заходів курсу. Результати підсумкових контрольних заходів модулів на RangeForce враховуються під час обчислення рейтингового балу студента.

## 7. Індивідуальні завдання

Індивідуальні завдання не передбачені навчальним планом.

## 8. Методи навчання

Застосовуються такі форми організації навчання, як лекція-бесіда, лекція-презентація, лабораторна робота, аудиторна та позааудиторна контрольна робота, залік.

Використовуються наступні методи навчання: розповідь, пояснення, бесіда, інструктаж, пояснення, демонстрація, спостереження, лабораторна робота, «мозковий штурм», ситуаційний аналіз.

## 9. Методи контролю

Передбачено заходи поточного та підсумкового контролю. Поточний контроль здійснюється шляхом проходження студентами комп'ютерних тестів, виконання завдань лабораторних робіт, фронтального та індивідуального усного опитування, ситуаційного аналізу. Підсумковий контроль реалізовано у формі електронного тестування та контрольних робіт практичного характеру.

## 10. Розподіл балів

Нарахування балів здійснюється за наступною схемою. 60 балів виділяється на поточне оцінювання, 40 балів – на модульний контроль. Детальний розподіл балів наводиться у рейтингових таблицях і доступний студентам протягом усього періоду вивчення дисципліни.

## Шкала оцінювання

| За шкалою | Екзамен | Залік | Бали |
|---|---|---|---|
| A | Відмінно | Зараховано | 90-100 |
| B | Добре | Зараховано | 82-89 |
| C | | | 74-81 |
| D | Задовільно | Зараховано | 64-73 |
| E | | | 60-63 |
| FX | Незадовільно | Не зараховано | 35-59 |
| F | | Не зараховано | 0-34 |

## 11. Рекомендована література

### *Основна література*

1. Donald A. Tevault. Mastering Linux Security and Hardening. Packt Publishing, 2018.
2. Jay LaCroix. Mastering Ubuntu Server. 4th edition. Packt Publishing, 2022.

3. Tajinder Kalsi. Practical Linux Security Cookbook. Packt Publishing, 2016.

***Допоміжна література***

1. G. Held. Windows Networking Tools. The Complete Guide to Management, Troubleshooting, and Security. – CRC Press, 2013.
2. Daniel J. Barrett, Richard E. Silverman, Robert G. Byrnes. Linux Security Cookbook. O'Relly, 2003.

## 12. Інформаційні ресурси в Інтернеті

1. Linux Professional Institute (LPI). URL: https://www.lpi.org/
2. RangeForce – Team Cyber Readiness. URL: https://www.rangeforce.com
3. Ubuntu Server Guide – Introduction Ubuntu. URL: https://ubuntu.com/server/docs
4. Ubuntu Turtorials – Ubuntu Turtorials. URL: https://ubuntu.com/tutorials.
5. Ubuntu Manpages – Ubuntu Manuals. URL: https://manpages.ubuntu.com/.
6. Stack Exchange. URL: https://stackexchange.com/.

*Індекс структурного підрозділу відповідно до наказу ректора «Про затвердження організаційної структури Державного університету «Житомирська політехніка» (наприклад, 22.06).
** Індекс освітньої програми відповідно до наказу ректора «Про індексацію освітніх програм Державного університету «Житомирська політехніка» (наприклад, 122.00.1/Б).
*** Шифр освітньої компоненти в освітній програмі (наприклад, ОК1).