**ЗАТВЕРДЖУЮ**

Директор Приватної установи
«Університет науки, підприємництва та технологій»

_____ Ірина Вольницька

01 листопада 2022 року

# КОНЦЕПЦІЯ ОСВІТНЬОЇ ДІЯЛЬНОСТІ

**за освітньою програмою підвищення кваліфікації**
**за спеціальністю 125 Кібербезпека у галузі знань 12 Інформаційні технології**

| **1. Загальна інформація** | |
|---|---|
| **Розробники концепції:** | **Клименко Надія Іванівна** – викладач кафедри інформаційних технологій SET University, інженер з безпеки розробки та тестування вебдодатків Bizzabo, магістр кібербезпеки,<br>**Остапенко Анастасія Валеріївна** – викладач кафедри інформаційних технологій SET University, консультант у сфері інформаційної безпеки, CEO Simple Security & Compliance.<br>**Почебут Максим Валентинович** – викладач кафедри інформаційних технологій SET University, Віце-президент Асоціації IT Ukraine з питань освіти, Chief Learning Officer в Sigma Software Group, кандидат технічних наук, доцент. |
| **Ступінь вищої освіти та назва кваліфікації мовою оригіналу** | Післядипломна освіта для осіб з вищою освітою (вид освітньої діяльності – підвищення кваліфікації за спеціальністю 125 Кібербезпека у сфері післядипломної освіти для осіб з вищою освітою) |
| **Назва галузі знань** | 12 Інформаційні технології |
| **Код та найменування спеціальності** | 125 Кібербезпека |
| **Орієнтовний перелік освітніх програм/курсів** | Освітні програми:<br>- Експерт з кібербезпеки: старт у професію; |
| **Загальний обсяг у кредитах Європейської кредитної трансферно-накопичувальної системи та строк навчання** | Обсяг освітніх програм від 1 кредиту ЄКТС (30 год.). Тривалість навчання відповідно до вимог освітньої програми чи курсу. |
| **2. Мета освітньої програм/курсів** | |
| Підготовка і вдосконалення фахівців, здатних використовувати і впроваджувати технології інформаційної та кібербезпеки, а також цифрових технологій; розв'язувати задачі дослідницького та/або інноваційного характеру.<br>Програма призначена для оволодіння сучасними підходами до розв'язання задач із кібербезпеки та формування у здобувачів можливості відповісти на сучасні виклики в галузі, шляхом використання набутих компетентностей для отримання очікуваних результатів. | |

| 3. Характеристика освітніх програм/курсів | |
|---|---|
| **Особливості освітніх програм** | Орієнтованість на сучасні інформаційні технології та унікальні в галузі кібербезпеки підходи, їх застосування для розв'язку задач з кібербезпеки.<br>Накопичення кредитів ЄКТС на основі індивідуальної траєкторії навчання кожним учасником освітніх програм.<br>Інтерактивна взаємодія з експертами та колегами – учасниками освітніх програм.<br>Кожний елемент освітніх програм описаний у форматі результатів навчання.<br>Окремі елементи освітніх програм можуть реалізуватись англійською мовою.<br>Форма навчання – інституційна. |
| **Професійні стандарти, на дотримання яких планується спрямовувати навчання (в разі наявності)** | Відсутні |
| **Рівень НРК** | Національна рамка кваліфікації України 1-8 рівні. |
| **Вимоги до рівня освіти осіб, які зможуть розпочати навчання** | Початковий рівень (короткий цикл) вищої освіти; перший (бакалаврський) рівень; другий (магістерський) рівень; третій (освітньо-науковий/освітньо-творчий) рівень. |
| **Тип документу** | За умови участі у окремих заходах освітніх програм/курсів здобувач отримує Сертифікат.<br>За умови виконання освітніх програм/курсів здобувач отримує Свідоцтво про підвищення кваліфікації. |
| **4. Викладання та оцінювання** | |
| **Викладання та навчання** | Освітній процес побудований на принципах особистісно орієнтованого навчання із застосуванням системного, компетентнісного, інтегративного підходів з елементами самонавчання та самоорганізації. Підходи, методи та технології, що використовуються, є студентоцентрованими.<br>**Форми навчання:** лекції; інтерактивні лекції; практичні заняття; самостійне навчання; симулятивні ігри; групова робота; елементи дистанційного навчання.<br>**Організаційні форми:** колективне та інтегративне навчання тощо.<br>**Технології навчання:** пасивні (пояснювально-ілюстративні); активні (проблемні, ігрові, інтерактивні, проєктні, позиційне та контекстне навчання, технологія співпраці) тощо.<br>Застосовується проблемно-орієнтоване навчання, використовуються кейси, |

| | |
|---|---|
| | практикуються ігри з публічним захистом результатів виконання індивідуальних та/чи групових завдань.<br>**Методи, методики та технології.**<br>Методи, моделі, методики та технології створення, обробки, передачі, приймання, знищення, відображення, захисту (кіберзахисту) інформаційних ресурсів у кіберпросторі, а також методи та моделі розробки та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач в галузі інформаційної безпеки та/або кібербезпеки.<br>Технології, методи та моделі дослідження, аналізу, управління та забезпечення бізнес/операційних процесів із застосуванням сукупності нормативно-правових та організаційно-технічних методів і засобів захисту інформаційних ресурсів у кіберпросторі.<br>**Інструменти та обладнання**.<br>Засоби, пристрої, мережне устаткування та середовище, прикладне та спеціалізоване програмне забезпечення, автоматизовані системи та комплекси проектування, моделювання, експлуатації, контролю, моніторингу, обробки, відображення та захисту даних (інформаційних потоків), а також методи і моделі теорії ризиків та управління інформаційними ресурсами при дослідженні і супроводженні об'єктів інформаційної діяльності у галузі інформаційної безпеки та/або кібербезпеки. |
| **Оцінювання** | Форми контролю: тестування, виконання індивідуальних завдань, написання есе, проєктна робота, розв'язання кейсів та проблемних завдань, презентації групових проєктів.<br>Для кожного елементу програми описуються результати навчання. Залежно від змісту та специфіки результатів навчання визначаються релевантні методи оцінювання. Методи оцінювання спільно із результатами навчання зазначаються у описі елементу освітніх програм. |
| **5. Програмні компетентності** | |
| **Інтегральна компетентність:** | здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки. |
| **Загальні компетентності:** | КЗ-1. Здатність застосовувати знання у практичних ситуаціях. |

| | |
|---|---|
| | КЗ-2. Здатність проводити дослідження на відповідному рівні.<br>КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу.<br>КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт.<br>КЗ-5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності). |
| **Фахові компетентності:** | 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.<br>КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.<br>КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.<br>КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.<br>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.<br>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.<br>КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.<br>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.<br>КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки. |

**6. Нормативний зміст підготовки здобувачів вищої освіти, сформульований у контексті результатів навчання**

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.

РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.

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.
РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.
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.
РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об’єктивно оцінювати результати навчання.
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.

## 7. Ресурсне забезпечення реалізації освітніх програм/курсів

| | |
|---|---|
| **Кадрове забезпечення** | Склад проєктної групи, професорсько-викладацький склад, що задіяний до викладання відповідають Ліцензійним умовам провадження освітньої діяльності. |

| | |
|---|---|
| **Матеріально-технічне забезпечення** | Забезпеченість навчальними приміщеннями, комп'ютерними робочими місцями, мультимедійним обладнанням відповідає потребам. |
| **Інформаційне та навчально-методичне забезпечення** | Інформаційне та навчально-методичне забезпечення відповідає Ліцензійним умовам провадження освітньої діяльності. |

**8. Освітні компоненти програми**

Згідно з вимогами Закону України «Про вищу освіту» SET University самостійно визначає перелік дисциплін/курсів, практик та інших видів освітньої діяльності, необхідний для набуття компетентностей та забезпечення нормативного змісту підготовки здобувачів.

| **Найменування освітнього (практичного) компонента програми (освітньої програми)** | **Вид засобу провадження освітньої діяльності** | **Найменування обладнання, устаткування, їх кількість** | **Найменування лабораторії, спеціалізованого кабінету, їх площа, кв. метрів (адреса приміщення, в якому розташовується лабораторія, спеціалізований кабінет)** |
|---|---|---|---|
| 1. Introduction: про курс<br>2. Паролі, хеші та атаки<br>3. Безпека браузера<br>4. Безпекові ресурси браузера<br>5. Самозахист у мережі; Best Practices<br>6. Ключові принципи кібербезпеки: операційні системи та розбір моделей ЦРУ<br>7. Вебсайти та веббезпека<br>8. GDPR. Захист інформації у мережі<br>9. Розвідка: цілі, Maltego, запобігання витоку даних<br>10. Попередження загроз та хакерських атак, частина 1: віруси, шпигуни, DoS та DdoS | Матеріальні, нематеріальні та інші ресурси, що знаходяться у користуванні для провадження освітньої діяльності. | Ethernet точки, WiFi роутер Aruba AP-535 x1, Проектор NEC M403H x1, Моноблок Acer Aspire C22 x1, 1 маркерна дока, 1 фліпчарт мобільний, 15 парт. | SET Classroom<br><br>офіс 712, вул. Солом'янська, 3, м. Київ, 03110 |

| | | | |
|---|---|---|---|
| 11. Попередження загроз та хакерських атак, ч.2: RAT, топ-хакери світу<br>12. Попередження загроз та хакерських атак, ч. 3: методологія зламу, фішинг<br>13. Корисні лайфхаки. | | | |

**Порядок оцінювання результатів навчання**

| Оцінка в балах | Оцінка за шкалою Університету | Пояснення оцінок | |
|---|---|---|---|
| | | **Іспит, диференційований залік** | **Залік** |
| **100** | **A +** | **Відмінно** (відмінне виконання, допускається незначна кількість несуттєвих помилок) | **Зараховано** (виконання основних/мінімальних вимог) |
| **93-99** | **A** | | |
| **91-92** | **A -** | | |
| **88-90** | **B +** | **Добре** (в загальному вірне виконання з незначною кількістю суттєвих помилок) | |
| **79-87** | **B** | | |
| **76-78** | **B -** | | |
| **73-75** | **C +** | **Задовільно** (задовільне виконання із значною кількістю суттєвих помилок, але з дотриманням мінімальних вимог) | |
| **66-72** | **C** | | |
| **60-65** | **C -** | | |
| **0-59** | **F** | **Незадовільно** (невиконання мінімальних вимог) | **Незараховано** (невиконання мінімальних вимог) |