Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

Введено в дію наказом від „\_\_\_” 20\_\_ р.

№ \_\_\_\_\_

Ректор \_\_\_\_\_\_\_\_\_\_\_\_\_\_ В. С. Бакіров

 «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ р.

 Освітньо-наукова програма

«Кібербезпека»

Спеціальність 125 – Кібербезпека

третій (освітньо-науковий) рівень вищої освіти

Затверджено вченою радою університету “\_\_\_\_\_\_\_” \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ року, протокол №\_\_.

**ЛИСТ ПОГОДЖЕННЯ**

**освітньо-професійної (освітньо-наукової) програми**

* 1. Вчена рада факультету комп’ютерних наук: протокол № 10 від «18» лютого 2019 р.

Голова Вченої ради факультету\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(В.Т. Лазурик)

* 1. Методична комісія факультету комп’ютерних наук:

протокол № 5 від « 24 » січня 2019 р.

Голова методичної комісії факультету\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(А.Г. Бердніков)

* 1. Кафедра безпеки інформаційних систем і технологій:

 протокол № 7 від «28» січня 2019 р.

Завідувач кафедри \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(С.Г. Рассомахін)

**ПЕРЕДМОВА**

Розроблено робочою групою у складі:

|  |  |  |
| --- | --- | --- |
| Прізвище, ім’я, по батькові | Найменування посади (для сумісників – місце основної роботи, посада) | Науковий ступінь, вчене звання, за якою кафедрою (спеціальністю) присвоєно |
| Керівник робочої групи |  |  |
| Рассомахін Сергій Геннадійович | Завідувач кафедри безпеки інформаційних систем і технологій | Доктор технічних наук (05.13.06 - Інформаційні технології), доцент за кафедрою автоматизованих систем управління |
| Члени робочої групи |  |  |
| Єсін Віталій Іванович | Професор кафедри безпеки інформаційних систем і технологій | Доктор технічних наук (05.13.06 - Інформаційні технології), доцент за кафедрою спец. дисциплін |
| Кузнецов Олександр Олександрович | Професор кафедри безпеки інформаційних систем і технологій | Доктор технічних наук (05.13.21 – системи захисту інформації), професор за спеціальністю 20.02.12 - військова кібернетика, системи управління та зв'язок |
| Колованова Євгенія Павлівна | Доцент кафедри безпеки інформаційних систем і технологій | Кандидат технічних наук (05.13.21 – системи захисту інформації) |

1. **Профіль освітньої програми**

**«Кібербезпека»**

**зі спеціальності 125 – Кібербезпека**

|  |
| --- |
| **1 – Загальна інформація** |
| **Ступінь вищої освіти та назва кваліфікації**  | третій (освітньо-науковий) рівень,доктор філософії з кібербезпеки |
| **Офіційна назва програми** | Кібербезпека |
| **Тип диплому та обсяг освітньої програми** | 40 кредитів (1200 годин) |
| **Наявність акредитації** | - |
| **Цикл/рівень** | Третій |
| **Передумови** | Наявність другого освітнього рівня – магістра |
| **Мова викладання** | державна |
| **Термін дії освітньої програми** | 4 роки |
| **Інтернет-адреса постійного розміщення опису освітньої програми** | csd.univer.kharkov.ua |
| **2 - Мета освітньої програми** |
| **Мета програми**  | Визначення основних компонент, програмних компетентностей та форм атестації випускників. |
| **3 – Характеристика освітньої програми** |
| **Предметна область (галузь знань, спеціальність** | 12 – Інформаційні технології; 125 – Кібербезпека. |
| **Орієнтація освітньої програми** | Науково-прикладна. |
| **Основний фокус освітньої програми та спеціалізації** | Безпека інформаційно-комунікаційних систем і технологій |
| **Особливості програми** | Підготовка науковців, здатних формульовати та вирішувати наукові та науково-прикладні завдання за спеціальністю 125-Кібербезпека. |
| **4 – Придатність випускників до працевлаштування** **та подальшого навчання** |
| **Придатність до працевлаштування** | Об’єкти та посади для професійної діяльності випускників: * об'єкти інформатизації, включаючи комп'ютерні, автоматизовані, телекомунікаційні, інформаційні, інформаційно-аналітичні, інформаційно-телекомунікаційні системи, інформаційні ресурси і технології;
* технології забезпечення безпеки інформації;
* процеси управління інформаційною та/або кібербезпекою об’єктів, що підлягають захисту.

Первинні посади випускників:* викладач (старший викладач) ВНЗ;
* молодший науковий співробітник;
* керівник дослідницьких груп IT компанії.
 |
| **Подальше навчання** | Можливість продовжити навчання у докторантурі та на курсах підвищення кваліфікації |
| **5 – Викладання та оцінювання** |
| **Викладання та навчання** | Денна (або вечірня) форма навчання |
| **Оцінювання** | За 100-бальною та національною (дворівневою/чотири рівневою) шкалою |
| **6 – Програмні компетентності** |
| **Інтегральна компетентність** | Здатних формульовати та вирішувати наукові та науково-прикладні завдання, які спрямовані на підвищення рівня кібербезпеки, поліпшення експлуатаційних, технічних, економічних та інтегральних показників ефективності інформаційних систем і технологій. |
| **Загальні компетентності** | **ЗК 1** - здатність до абстрактного мислення, аналізу та синтезу;**ЗК 2**- здатність генерувати нові ідеї (креативність);**ЗК 3**- здатність спілкуватися іноземною мовою;**ЗК 4**- здатність до пошуку, оброблення та аналізу інформації з різних джерел;**ЗК 5**- вміння виявляти, ставити та вирішувати науково-технічні проблеми. |
| **Фахові компетентності** | **ФК 1** - здатність використати сучасні досягнення науки і передових технологій;**ФК 2** - здатність користуватися нормативною та законодавчою базою в сфері інтелектуальної власності;**ФК 3** - здатність планувати та здійснювати власне наукове дослідження, присвячене суттєвій проблемі сучасної науки у галузі інформаційно-комунікаційних технологій;**ФК 4** - здатність представляти результати досліджень у вигляді звітів і публікацій на державній та одній з іноземних мов;**ФК 5** - здатність до викладання у вищому навчальному закладі предметів, що відносяться до галузі інформаційно-комунікаційних технологій;**ФК 6** - професійне володіння комп’ютером та інформаційними технологіями;**ФК 7** - здатність виконувати роботи з проектування складних комплексів засобів захисту та управління безпекою інформаційних і телекомунікаційних систем відповідно до сфери їх застосування;**ФК 8** - здатність здійснювати та детально обґрунтовувати вибір структури, принципів організації, комплексів засобів і технологій забезпечення безпеки інформаційних і телекомунікаційних систем;**ФК 9** - здатність здійснювати аналіз та синтез криптографічних примітивів;**ФК 10** - здатність застосовувати моделі і методи комп’ютерної стеганографії при проектуванні комплексів засобів захисту інформаційних і телекомунікаційних систем. |
| **7 – Програмні результати навчання** |
| **Програмні результати навчання** | **ПРН 1** застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;**ПРН 2** Показувати знання основних положень філософських проблем наукового пізнання. Систематизувати методи наукового пізнання, та використовувати їх в дослідженнях. Використовувати знання сутності, принципів, методів, особливостей наукового пізнання для вивчення і розв’язання проблем.**ПРН 3** Демонструвати уміння проводити пошук інформації з різних джерел, її обробку та аналіз із залученням сучасних інформаційних технологій**ПРН 4** Демонструвати уміння представляти результати досліджень на державній та одній з іноземних мов.**ПРН 5** Правильно визначати проблеми інтелектуальної власності та законодавства у цій сфері, шляхи їх подолання, тлумачити та розкривати основні поняття, інститути та категорії інтелектуальної власності.**ПРН 6** Використовувати нормативну та законодавчу базу в сфері інтелектуальної власності**ПРН 7** Застосовувати знання при проведенні досліджень з кибербезпеки, спираючись на сучасні досягнення світової науки і передові технології.**ПРН 8** Показувати знання і розуміння математичних методів моделювання та оптимізації процесів.**ПРН 9** Визначати запобіжні дій щодо протидії загальним методам аналізу криптосистем.**ПРН 10** Показувати знання і розуміння загальних принципів побудови систем захисту, завдань, вихідних даних та факторів, які необхідно враховувати при проектування систем захисту.**ПРН 11** Оцінювати поточний стан рівня безпеки.**ПРН 12** Планувати та здійснювати власне наукове дослідження, присвячене суттєвій проблемі сучасної науки у галузі кибербезпеки.**ПРН 13** Аналізувати фактори ризику та успіху при плануванні та виконанні відповідного проекту складних комплексів засобів захисту та управління безпекою інформаційних і телекомунікаційних систем.**ПРН 14** Оцінювати знання і вміння тих, хто навчається, сприяючи розвитку в них самостійності, творчих здібностей в процесі засвоєння навчальних дисциплін.**ПРН 15** Розробляти математичні моделі завдань забезпечення інформаційної безпеки та захисту інформації.**ПРН 16** Аргументувати вибір та застосовування методів і засобів для побудови захищених інформаційно-телекомунікаційних систем.**ПРН 17** Розробляти рекомендації щодо удосконалення системи інформаційної безпеки, застосування якої дозволить мінімізувати ризики та формулювати перелік уразливостей.**ПРН 18** Упроваджувати в інформаційні і телекомунікаційні системи сучасні методи забезпечення інформаційної безпеки відповідно до вимог вітчизняних та міжнародних стандартів.**ПРН 19** Показувати знання і розуміння методів аналізу криптосистем та протидії ним.**ПРН 20** Показувати знання і розуміння математичних методів синтезу та аналізу криптографічних примітивів.**ПРН 21** Пропонувати обґрунтований вибір та застосовування засобів, необхідних для реалізації та компонування криптографічних систем.**ПРН 22** Моделювати динамічні процеси, використовуючи методи опису та дослідження складних систем.**ПРН 23** Використовувати математичні методи оптимізації з метою одержання найкращих характеристики функціонування засобів та систем.**ПРН 24** Аргументувати вибір та застосовування методів і засобів для побудови захищених інформаційно-телекомунікаційних систем. |
| **8 – Ресурсне забезпечення реалізації програми** |
| **Специфічні характеристики кадрового забезпечення** | Викладання фахових дисциплін забезпечує професорсько-викладацький склад кафедри: 9 докторів та 8 кандидатів наук. |
| **Специфічні характеристики матеріально-технічного забезпечення** | Для навчання використаються спеціалізований комп’ютерний клас та навчальна лабораторія кафедри, навчально-науковий центр сертифікації ключів ЕЦП, реалізація результатів досліджень здійснюється у 6 науково-виробничих підприємств, з якими укладено відповідні договори. |
| **Специфічні характеристики інформаційного та навчально-методичного забезпечення** | Використається навчальний фонд бібліотеки ХНУ, ПЗ дистанційних форм навчання, підручники та навчальні посібники розробки кафедри та провідних світових університетів. |
| **9 – Академічна мобільність** |
| **Національна кредитна мобільність** | Здобувачі мають можливість здійснювати перехід до інших ВНЗ та/або спеціальностей (згідно до положень Закону про освіту та відповідних рішень ВНЗ) з урахуванням накопиченого обсягу кредитів навчання та наукових публікацій. |
| **Міжнародна кредитна мобільність** | Здобувачі мають можливість здійснювати навчання в ВНЗ інших країн у відповідності з домовленостями університетів в рамках міжнародних програм співробітництва та академічної мобільності |
| **Навчання іноземних здобувачів вищої освіти** | Можливим є навчання іноземних студентів за даною програмою з використанням державної, англійської або інших мов викладання |

1. **Перелік компонент освітньо-наукової програми**

**та їх логічна послідовність**

* 1. Перелік компонент ОНП

|  |  |  |  |
| --- | --- | --- | --- |
| Код н/д | Компоненти освітньої програми (навчальні дисципліни, курсові проекти (роботи), практики, кваліфікаційна робота) | Кількість кредитів | Форма підсумкового контролю |
| **Обов’язкові компоненти ОНП** |
| ОК 1. | Філософські засади та методологія наукових досліджень | 5 | Залік |
| ОК 2. | Іноземна мова для аспірантів | 10 | ІспитЗалік |
| ОК 3. | Реєстрація прав інтелектуальної власності | 3 | Залік |
| ОК 4. | Підготовка наукових публікацій та презентація результатів досліджень | 4 | Залік |
| ОК 5. | Математичні методи в кібербезпеці | 6 | Іспит |
| **Загальний обсяг обов’язкових дисциплін** |  28 |
| **Вибіркові компоненти ОНП** |
| *Вибірковий блок А* |
| ВБ 1.1. | Методи синтезу та аналізу захищених телекомунікацій | 6 | Залік |
| ВБ 1.2. | Математичні методи синтезу та аналізу криптографічних примітивів | 6 | Іспит |
| *Вибірковий блок Б* |
| ВБ 2.1. | Методи побудови телекомунікаційних протоколів фізичного та канального рівнів | 6 | Залік |
| ВБ 2.2. | Моделі і методи комп’ютерної стеганографії | 6 | Іспит |
| **Загальний обсяг вибіркових дисциплін** |  12 |
| **ЗАГАЛЬНИЙ ОБСЯГ ОСВІТНЬОЇ ПРОГРАМИ** |  40 |

* 1. Структурно-логічна схема ОНП

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Рік навчання | 1-й | 2-й | 3-й | 4-й |
| Семестр | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| ОК 1. |  |  |  |  |  |  |  |  |
| ОК 2. |  |  |  |  |  |  |  |  |
| ОК 3. |  |  |  |  |  |  |  |  |
| ОК 4. |  |  |  |  |  |  |  |  |
| ОК 5. |  |  |  |  |  |  |  |  |
| ВБ 1.1. |  |  |  |  |  |  |  |  |
| ВБ 1.2. |  |  |  |  |  |  |  |  |
| ВБ 2.1. |  |  |  |  |  |  |  |  |
| ВБ 2.2. |  |  |  |  |  |  |  |  |

1. **Форма атестації здобувачів вищої освіти**

 Атестація випускників освітньо-кваліфікаційного рівня "Доктор філософії" зі спеціальності 125 – «Кібербезпека» проводиться на основі публічного захисту дисертаційної роботи у Спеціалізованої вченої раді університету. До захисту дисертації допускаються здобувачі, які виконали всі вимоги навчального плану. Захист дисертаційної роботи відбувається з метою з‘ясування рівня підготовленості здобувачів для виконання професійних завдань, передбачених стандартом вищої освіти.

1. **Матриця відповідності програмних компетентностей**

**компонентам освітньої програми**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **ОК 1** | **ОК 2** | **ОК 3** | **ОК 4** | **ОК 5** | **ВБ 1.1** | **ВБ 1.2** | **ВБ 2.1** | **ВБ 2.2** |
| **ЗК 1** | **+** |  | **+** | **+** |  |  |  |  |  |
| **ЗК 2** | **+** |  |  |  |  |  |  |  |  |
| **ЗК 3** |  | **+** |  |  |  |  |  |  |  |
| **ЗК 4** |  |  | **+** | **+** | **+** |  |  |  |  |
| **ЗК 5** |  |  |  | **+** |  | **+** | **+** | **+** | **+** |
| **ФК 1** |  |  | **+** |  | **+** | **+** | **+** | **+** | **+** |
| **ФК 2** |  |  |  |  | **+** |  |  |  |  |
| **ФК 3** |  |  |  |  |  |  |  |  |  |
| **ФК 4** |  | **+** | **+** |  |  |  |  |  |  |
| **ФК 5** |  |  |  |  |  | **+** |  | **+** |  |
| **ФК 6** |  |  |  |  | **+** |  | **+** |  | **+** |
| **ФК 7** |  |  |  |  |  | **+** | **+** | **+** | **+** |
| **ФК 8** |  |  |  |  |  | **+** | **+** | **+** | **+** |
| **ФК 9** |  |  |  |  |  |  | **+** |  |  |
| **ФК 10** |  |  |  |  |  |  |  |  | **+** |

1. **Матриця забезпечення програмних результатів навчання (ПРН)**

**відповідними компонентами освітньої програми**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **ОК 1** | **ОК 2** | **ОК 3** | **ОК 4** | **ОК 5** | **ВБ 1.1** | **ВБ 1.2** | **ВБ 2.1** | **ВБ 2.2** |
| **ПРН 1** | **+** |  |  |  |  |  |  |  |  |
| **ПРН 2** |  | **+** |  |  |  |  |  |  |  |
| **ПРН 3** |  |  | **+** | **+** |  |  |  |  |  |
| **ПРН 4** |  | **+** |  | **+** |  |  |  |  |  |
| **ПРН 5** |  |  | **+** |  |  |  |  |  |  |
| **ПРН 6** |  |  | **+** |  |  |  |  |  |  |
| **ПРН 7** |  |  |  | **+** | **+** |  |  |  |  |
| **ПРН 8** |  |  |  |  | **+** |  |  |  |  |
| **ПРН 9** |  |  |  |  |  | **+** | **+** | **+** | **+** |
| **ПРН 10** |  |  |  |  | **+** | **+** |  | **+** |  |
| **ПРН 11** |  |  |  |  | **+** | **+** |  | **+** |  |
| **ПРН 12** |  |  | **+** | **+** | **+** |  |  |  |  |
| **ПРН 13** |  |  |  | **+** | **+** | **+** |  |  |  |
| **ПРН 14** | **+** |  |  |  |  | **+** | **+** | **+** | **+** |
| **ПРН 15** |  |  |  |  | **+** |  |  |  |  |
| **ПРН 16** |  |  |  |  |  | **+** |  | **+** |  |
| **ПРН 17** |  |  |  |  |  |  | **+** |  | **+** |
| **ПРН 18** |  |  |  |  |  | **+** |  | **+** |  |
| **ПРН 19** |  |  |  |  |  |  | **+** |  |  |
| **ПРН 20** |  |  |  |  |  |  | **+** |  |  |
| **ПРН 21** |  |  |  |  |  | **+** |  | **+** |  |
| **ПРН 22** |  |  |  |  | **+** |  |  |  |  |
| **ПРН 23** |  |  |  |  | **+** |  |  |  |  |
| **ПРН 24** |  |  |  |  |  | **+** |  | **+** |  |