Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

Затверджено

наказом ректора

від \_\_\_\_\_\_\_ № \_\_\_\_\_\_\_

Тимчасовий стандарт вищої освіти

другий рівень вищої освіти, магістр

за освітньо-професійною програмою за спеціальністю

125 – “Кібербезпека”

Схвалено Вченою радою університету “\_\_\_\_\_\_\_” \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ року, протокол №\_\_.**Тимчасовий стандарт підготовки:** вища освіта, магістр

**за спеціальністю:**

125 – “Кібербезпека”;

**спеціалізаціями:**

* “Безпека інформаційних і комунікаційних систем”;
* "Контроль якості програмного забезпечення"

**Тип диплому:** одиночний.

**Обсяг програми:** 90 кредитів ЄКТС.

**Нормативний термін навчання – 1,5** роки.

**Вимоги до рівня освіти осіб, які можуть розпочати навчання за програмою, і вимоги до професійного відбору вступників:**

 попередній рівень освіти або(та) професійної підготовки:

* (перелік 2010 р.) базова вища освіта за напрямом– 6.170101 “Безпека інформаційних і комунікаційних систем”;
* (перелік 2015 р.) – галузь знань –12 – Інформаційні технології;
* абітурієнти повинні мати державний документ про освіту або(та) професійну підготовку встановленого зразка;
* для забезпечення цілей підготовки фахівця, які подані в освітньо-кваліфікаційній характеристиці, абітурієнт повинен:

**Знати:**

* основні закони фізики і вищої математики;
* основи електроніки, теорії кіл, сигналі та процесі в електроніці, принципів побудови мікропроцесорів та їх застосування;
* математичний апарат теорії чисел, груп, полей, кілець, якій необхідний для засвоєння та практичного використання криптографічних методів;
* основи прикладної криптології;
* теоретичні основи побудови та оцінки якості сучасних інформаційних технологій та програмних систем;
* основні мови програмування, існуючі засоби розробки баз даних та забезпечення їх захисту;
* принципи побудови та функціонування систем технічного захисту інформації і комплексних систем захисту інформації у загальної системі забезпечення кібербезпеки;
* стеганографічні методи захисту інформації;
* компоненти складних комп’ютерних мереж;
* основні положення нормативно-правового забезпечення кібербезпеки
* сучасні технології забезпечення та оцінки якості програмного забезпечення

**Уміти:**

* здійснювати оцінки захищеності інформації в кіберсистемах;
* виконувати аналіз ризиків та джерел загроз;
* застосовувати кодування інформаційних повідомлень, використовуючи методи побудови економних та завадостійких кодів;
* вибирати основні методі та способі захисту інформації відповідно до вимог сучасних стандартів інформаційної безпеки щодо критеріїв безпеки інформаційних технологій, застосовуючи системний підхід та знання основ теорії кібербезпеки;
* вибирати та застосовувати стандартні криптографічні алгоритми та протоколи для захисту інформації у кіберсистемах;
* використовувати методі і засобі щодо протидії несанкціонованому отриманню інформації відповідно до вимог нормативних документів системи технічного захисту інформації;
* проводити оцінки відповідності системи управління інформаційною безпекою своєму призначенню відповідно до вимог діючих стандартів та нормативних документів;
* розробляти календарні плані щодо робіт по створенню комплексних систем кибербезпеки;
* моделювати складні системи захисту і обробки інформації;
* оцінювати пропускну спроможність каналів передавання прихованої інформації;
* оцінювати стійкість стеганографічних систем;
* використовувати технології та інструментарій забезпечення і контролю якості (у тому числі автоматизовані) програмного забезпечення.

**Володіти навичками:**

* конспектування лекцій;
* самостійної роботи з літературою;
* написання рефератів, доповідей.

**Для професійної діяльності протипоказані властивості:**

* психологічні відхилення від нормального стану людини;
* нездатність переносити довгі психологічні навантаження та стреси;
* фізичні недоліки, відповідно встановленим медичним нормам.

**Мета програми.**

**Тимчасовий стандарт вищої освіти** є нормативним документом Харківського національного університету імені В.Н. Каразіна, у якому визначається нормативний термін та зміст навчання, встановлюються вимоги до змісту, обсягу й рівня освіти та професійної підготовки фахівця відповідного освітньо-кваліфікаційного рівня певної галузі знань, спеціальності й спеціалізацій.

Цей стандарт використовується при:

* розробці та корегуванні відповідних навчальних планів і програм навчальних дисциплін;
* розробці засобів діагностики рівня освітньо-професійної підготовки фахівця;
* визначенні змісту навчання як бази для опановування новими спеціальностями, кваліфікаціями;
* визначенні змісту навчання в системі перепідготовки та підвищення кваліфікації.

**Характеристики програми:**

* галузь знань: 12 “Інформаційні технології”;
* основна зорієнтованість програми: забезпечення кібербезпеки, безпеки інформаційних процесів і технологій в складних розподілених комп’ютеризованих системах, забезпечення якості програмних продуктів, проведення аудиту якості програмних систем;
* спрямованість програми: академічна, практична, прикладна;
* відмінності від інших подібних програм: велика увага приділяється застосуванню високих наукоємних технологій та сучасних прикладних програмно-аналітичних методів.

**Програмні компетентності**

* професійне володіння комп’ютером та інформаційними технологіями;
* здатність до самостійної науково-дослідної діяльності (аналіз, співставлення, систематизація, абстрагування, моделювання, перевірка достовірності даних, прийняття рішень та ін.), готовність генерувати та використовувати нові ідеї;
* здатність протягом життя самостійно вчитися, забезпечувати особистісний та професійний розвиток;
* здатність планувати та здійснювати власне наукове дослідження, присвячене суттєвій проблемі сучасної науки у галузі кибербезпеки та оцінки якості програмних продуктів;
* готовність представляти результати досліджень у вигляді звітів і публікацій на державній та одній з іноземних мов;
* здатність до викладання у вищому навчальному закладі предметів, що відносяться до сучасних методів побудови та забезпечення якості і кіберсистем;
* здатність виконувати роботи з проектування складних комплексів засобів захисту та управління безпекою інформаційних і комунікаційних систем відповідно до сфери їх застосування;
* здатність здійснювати та детально обґрунтовувати вибір структури, принципів організації, комплексів засобів і технологій забезпечення безпеки інформаційних і комунікаційних систем;
* здатність упроваджувати в інформаційні і комунікаційні системи сучасні методи забезпечення інформаційної безпеки відповідно до вимог вітчизняних та міжнародних стандартів;
* володіння науковими та практичними методами створення систем моніторингу якості та безпеки в кіберсистемах;
* обґрунтування вибору, реалізації й аналіз криптографічних механізмів та систем захисту інформаційних і комунікаційних систем;
* здатність здійснювати та детально обґрунтовувати вибір структури, принципів організації, комплексів засобів і технологій забезпечення безпеки бездротових мереж;
* здатність здійснювати та детально обґрунтовувати вибір архітектури інфраструктури відкритих ключів (ІВК), що проектується;
* здатність обґрунтовувати доцільність та забезпечувати ефективність взаємовідносин з відповідними зовнішніми організаціями щодо забезпечення економічної безпеки;
* знання наукових та практичних основ адміністрування та експлуатації захищених інформаційних і комунікаційних систем, методів контролю якості програмних систем.

**Програмні результати навчання**

Знання і розуміння

* знання і розуміння математичних методів моделювання та оптимізації процесів;
* знання і розуміння методів аналізу криптосистем та протидії ним;
* знання і розуміння базових архітектур ІВК, основ стандартизації у галузі ІВК, положень політики сертифікації, групи протоколів ІВК;
* знання основ моніторингу та аудиту інформаційно-комунікаційних систем;
* знання теорії розподілених інформаційних ресурсів і розуміння здійснення вибору методів і засобів для побудови захищених розподілених інформаційно-телекомунікаційних систем;
* знання і розуміння загальних принципів побудови систем захисту, завдань, вихідних даних та факторів, які необхідно враховувати при проектування систем захисту;
* знання і розуміння основних технологій і стандартів бездротових мереж, особливості їх використання;
* знання і розуміння правових основ захисту інтелектуальної власності та основ нормативної бази охорони безпеки праці персоналу, зайнятого в галузі інформаційних систем і технологій;
* знання основ економічної безпеки;
* знання основ захисту інформації в банківських системах з урахуванням можливих каналів витоку інформації для конкретних систем;
* знання основних положень філософських проблем наукового пізнання, педагогіки і методики викладання у вищій школі;
* знання змісту та принципів реалізації технологій забезпечення якості програмних систем на різних етапах життєвого циклу.

Застосування знань і розуміння

* обґрунтування вибору та застосовування методів і засобів для побудови захищених розподілених інформаційно-телекомунікаційних систем;
* здійснення запобіжних дій щодо протидії загальним методам аналізу криптосистем;
* аналіз факторів ризику та успіху при плануванні та виконанні відповідного ІТ-проекту;
* обґрунтування вибору та застосовування засобів, необхідних для реалізації та компонування криптографічних систем;
* проектування безпечних бездротових мереж, враховуючі особливості побудови мобільних, розподілених транкінгових та супутникових систем;
* обґрунтування вибору архітектури ІВК з урахуванням завдань, що вирішується на рівні держави, відомства, державних установ, приватних організацій, суспільних організацій; визначення функціональної структури, топології центрів сертифікації та обґрунтування вимог безпеки до центрів з метою забезпечення необхідної якості надання послуг;
* оформлення аудиторського звіту, що містить оцінку поточного стану рівня безпеки, інформацію про виявлені проблеми, аналіз відповідних ризиків та рекомендації щодо їх усунення;
* проведення досліджень у галузі інформаційної безпеки та захисту інформації, спираючись на сучасні досягнення світової науки і передові технології;
* проведення досліджень та розробка методів забезпечення та контролю якості програмних систем;
* оцінка знань і вмінь тих, хто навчається, сприяючи розвитку в них самостійності, творчих здібностей в процесі засвоєння навчальних дисциплін.

Формування суджень

* здатність детально обґрунтовувати вибір структури, принципів організації, комплексів засобів і технологій забезпечення безпеки інформаційних і телекомунікаційних систем;
* здатність упроваджувати в інформаційні і телекомунікаційні системи сучасні методи забезпечення інформаційної безпеки відповідно до вимог вітчизняних та міжнародних стандартів;
* здатність здійснювати оцінку поточного стану рівня безпеки з відповідним оформленням аудиторського звіту;
* здатність планувати та здійснювати власне наукове дослідження, присвячене суттєвій проблемі сучасної науки у галузі інформаційних технологій.

**Придатність до працевлаштування:** магістр може займати посади:

* інженера-дослідника, молодшого наукового співробітника в науково-дослідних і проектних організаціях;
* інженера та адміністратора з інформаційної безпеки та оцінки якості програмного забезпечення на підприємствах і фірмах, що займаються розробкою та експлуатацією комп'ютерних систем, баз даних та знань інформаційно-керуючих і комунікаційних систем;
* програміста, інженера по оцінці якості в компаніях та фірмах, які розробляють програмне забезпечення та системи інформаційної безпеки;
* комп'ютерного аналітика і системного адміністратора;
* асистента, викладача вищого навчального закладу.

**Можливості подальшого навчання:** аспірантура за спеціальностями "Комп’ютерні науки та інформаційні технології", "Кібербезпека", курси підвищення кваліфікації за відповідним галузевим напрямом, післядипломна освіта.

**Стиль викладання, навчання та система оцінювання:**

* опис основних підходів, методів та технологій, передбачених програмою: проблемно-орієнтоване, у тому числі самостійне навчання, навчання на основі лабораторної, науково-дослідницької практики;
* методи оцінювання: екзамени, практика, контрольні, курсові та дипломні роботи.

 **Форми атестації здобувачів вищої освіти:**

* Атестація випускників освітньо-кваліфікаційного рівня "Магістр" зі спеціальності 125 – "Кібербезпека", спеціалізацій "Безпека інформаційних і комунікаційних систем", "Контроль якості програмного забезпечення" проводиться Державною екзаменаційною комісією вищого навчального закладу.
* Державна атестація проводиться у вигляді кваліфікаційного екзамену з фундаментальної підготовки та захисту кваліфікаційної магістерської роботи.
* До складання екзамену та до захисту кваліфікаційних робіт допускаються студенти, які виконали всі вимоги навчального плану.
* Кваліфікаційний іспит і захист магістерської роботи мають своєю метою з‘ясування рівня підготовленості випускника для виконання професійних завдань, передбачених відповідними стандартами вищої освіти, і продовження освіти.
* Рішенням Державної екзаменаційної комісії випускникам, які найбільш відзначилися у вирішенні задач діяльності, передбачених даною програмою, може бути виданий документ (диплом освітньо-кваліфікаційного рівня магістр) про закінчення ВНЗ "З ВІДЗНАКОЮ".
* Студенту, який склав екзамен і захистив кваліфікаційну роботу відповідно до вимог освітньо-професійної програми, рішенням державної комісії присвоюється освітньо-кваліфікаційний рівень магістр і видається державний документ про освіту.