Міністерство освіти і науки України
Харківський національний університет імені В.Н. Каразіна

ЗАТВЕРДЖУЮ
Голова Приймальної комісії
Харківського національного
університету імені В.Н. Каразіна
_____Віль БАКІРОВ
_____2020 р.

ПРОГРАМА
Фахових випробувань для вступу до аспірантури факультету комп'ютерних наук

з галузі
12 – «Комп'ютерні науки»

за спеціальністю
125 – «Кібербезпека»

Приймальна комісія
Протокол № 3 від 03.02.2020 р.

Харків – 2020

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет імені В.Н. Каразіна

«Затверджую»
Голова приймальної комісії
Ректор Харківського національного
університету імені В.Н. Каразіна

Віль БАКІРОВ
« » _____ 2020 р.

ПРОГРАМА
Фахових випробувань для вступу до аспірантури
факультету комп'ютерних наук

з галузі
12 Комп'ютерні науки

зі спеціальності:
125 Кібербезпека

ХАРКІВ 2020

Програма фахових випробувань

1. Математичні основи:

- теорія чисел та груп, скінченні поля Галуа, особливості застосування в криптографії;
- еліптичні та гіпереліптичні групи, основи застосування в криптографії;
- бінарні відображення (спарювання) точок еліптичних кривих, особливості застосування в криптографії;
- теорія ймовірностей і математична статистика;
- методи обчислень.

Рекомендована література:

Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Монографія. Харків, ХНУРЕ, Форт, 2012 р., 1 та 2 видання, 868 с.
Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Підручник. Харків, ХНУРЕ, Форт, 2013 р., 1 та 2 видання, 878 с
Есин В. И., Кузнєцов А. А., Сорока Л. С. Безопасность информационных систем и технологий – Х.:ООО «ЭДЭНА», 2010.-656с.
Новиков Ф.А. Дискретная математика для программистов. (3-е изд) Питер, 2009. – 384 с.
М.І. Жалдак, Н.М. Кузьміна, Г.О. Михалін. Теорія ймовірностей і математична статистика. Київ. НПУ імені М.П. Драгоманова, 2015. – 705 с.
Фельдман Л. П., Петренко А. І., Дмитрієва О. А. Чисельні методи в інформатиці. — К.: Видавнича група BHV, 2006. — 480 с.

2. Системи захисту інформації:

- загрози інформації, моделі оцінки загроз інформації системи показників вразливостей інформації;
- методологія проектування систем захисту інформації;
- обґрунтування складу засобів захисту у системі захисту інформації;
- технологія функціонування систем захисту інформації;
- основні складові кибербезпеки.

Рекомендована література:

Грушо А.А., Тимотина Е.Е. Теоретические основы защиты информации. М.: Яхтсмен, 1996, 187с.
Мельников В.В. Защита информации в компьютерных системах. М.: Финансы и статистика. Электроинформ, 1997, 364с.
Коваленко М.М. Комп'ютерні віруси і захист інформації. Київ, Наукова думка, 1999.
Петраков Защита и охрана личности, собственности, информации. М.: Радио и связь, 1997, 315 с.

3. Організаційно-правове забезпечення кибербезпеки:

- загальний склад організаційно-правового забезпечення кибербезпеки;
- організаційно-технічні засоби захисту інформації;
- рівні захисту, класифікація автоматизованих систем та вимоги до захисту інформації.

Рекомендована література:

Замула О.А., Горбенко Ю.І., Шумов А.І. Нормативно-правове забезпечення інформаційної безпеки. Комплексні системи захисту інформації»: Навч. посібник. - Харків: ХНУРЕ, 2010 - 98 с.
Замула О.А. Захист держаних секретів. Навчальний посібник. ХНУРЕ – 2004. – 206 с.
Петренко С.А., Петренко А.А. Аудит інформаційної безпеки Internet. – М. ДМК Пресс, 2002-416 с.

4. Основи криптографії:

- місце і роль криптографічних методів у загальній системі кибербезпеки;
- математичні моделі шифрів та їх властивості;
- теоретична і практична стійкість шифрів, досконалі шифри та їх властивості;
- основні поняття і методи стеганографічного захисту інформації;
- управління ключами, формування ключів, протоколи розподілу ключів.

Рекомендована література:

Задірака В. Компьютерная криптологія. Підручник. К, 2002 ,504с.
Бембо Мао. Современная криптографія. Теория и практика. Москва. 2005
Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Изд. Триумф. М., 2003 г. 815 с.
В. Столлингс. Криптография и защита сетей. Принципы и практика. Изд. “Вильямс”. К. 2001. 669 с.
Шеннон К. Работы по теории информации и кибернетике, М., ИЛ, 1963, с. 333-369.

5. Основи технічного захисту інформації:

- класифікація технічних каналів витоку інформації та їх моделі;
- методи і засоби захисту об’єктів від витоку інформації по технічних каналах;
- захист технічних засобів від витоку інформації по побічних електромагнітних випромінюваннях.

Рекомендована література:

Организация и современные методы защиты информации. М.: Концерн «Банк Деловой Центр», 1998, 465 с.
Корченко А.Г. Несанкционированный доступ к компьютерным системам и методы защиты. Учебное пособие. Киев, 1998, КМУГА, 115 с.
Зегжда Д.П., Ивашко А.М. Как построить защищённую информационную систему. Санкт-Петербург, НПО «Мир и семья – 95», 286с.
Хорев А.А. Защита информации от утечки по техническим каналам. Часть 1.

Технические каналы утечки информации. Учебное пособие. М.: Гостехкомиссия России, 1998. – 320 с.
ДСТУ 3396.0-96 Державний стандарт України. Захист інформації. Технічний захист інформації. Основні положення.

6. Реалізація систем забезпечення кібербезпеки та їх фрагментів:

- методи захисту програмного забезпечення від вірусів, несанкціонованого використання, тощо;
- реалізація методів захисту інформації в стандартних мережевих операційних системах;
- стандартні система захисту інформації в локальних та глобальних мережах, захист інформації в Internet;
- особливості використання методів захисту у банківських технологіях та віртуальній торгівлі.

Рекомендована література:

Горфинкель С., Стеффорд Дж. Безопасность Web и электронная коммерция. М.: Book Media Publisher, 1999, 563с.
Эдвардс М.Дж. Безопасность в Интернете на основе Windows NT. М.: Русская Редакция, 1999, 618 с.
Горфинкель С., Стеффорд Дж. Практическое руководство по безопасности UNIX и Интернет. М.: Book Media Publisher, 1999, 478 с.
Тайли Э Безопасность персонального компьютера. Минск: Попурри, 1997, 477с.
Барсуков В.С. Обеспечение информационной безопасности. М.: Технология электронных коммуникаций. 1996, 94с.

КРИТЕРІЇ ОЦІНЮВАННЯ ФАХОВОГО ВИПРОБУВАННЯ

Бали	Вимоги
30-33 (34)	Тверде засвоєння теоретичного матеріалу, глибокі та вичерпні знання змісту програмного матеріалу по суті питання, розуміння сутності та взаємозв'язку розглянутих процесів і явищ, тверде знання основних положень суміжних питань. Уміння самостійно використовувати математичний апарат для аналізу та вирішення практичних завдань, робити правильні висновки з отриманих результатів. Логічність і грамотність викладення. Відсутність помилок і неточних формулювань.
23-29	Тверді і досить повні знання теоретичного матеріалу по суті питання, правильне розуміння сутності та взаємозв'язку розглянутих процесів і явищ, розуміння основних положень суміжних питань. Уміння самостійно застосовувати математичний апарат до вирішення практичних завдань. Окремі неточності у формулах, графіках, логікі та мові відповіді, що не ставлять під сумнів принципову вірність відповіді. Логічність і зрозумілість викладення. Відсутність значних помилок, допустимі 1-3 неточності. Не більше як 4 припущені неточностей при відсутності помилок або одна значна помилка і 1-2 неточності

17-22	Тверді у основі та загалом задовільні знання і розуміння теоретичного матеріалу по суті питання, зрозумілість викладення. Правильні конкретні відповіді на поставлені питання за наявності кількох помилок і неточностей при висвітленні окремих положень. Уміння застосовувати теоретичні знання до вирішення основних практичних завдань, які не потребують самостійного застосування складного математичного апарату або творчого підходу до інформаційних технологій. припущення тільки однієї, однак грубої, помилки або тільки двох суттєвих помилок. Не більше однієї грубої помилки при 1-2 значних помилках або не більше 4 значних помилок за відсутності грубих.
0-16	Недостатнє розуміння суті розглянутих процесів і явищ, наявність кількох грубих помилок або значної кількості суттєвих помилок у відповіді. Невміння зрозуміло викладати відповіді на питання. Невміння застосовувати знання при вирішенні практичних завдань.

Білет фахового вступного випробування містить три питання, два з яких оцінюється максимум 33 бала, третє питання оцінюється максимум 34 бала. Вступник допускається до участі у відборі за умови успішного складання фахового вступного випробування за сто бальною шкалою оцінювання, якщо набраний бал складає не меньше 50 балів.

Голова предметної комісії Сергій РАССОМАХІН

Відповідальний секретар приймальної комісії Ольга АНОЩЕНКО