МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Харківський національний університет імені В.Н. Каразіна

«Затверджую»

Голова приймальної комісії

Ректор Харківського національного

університету імені В.Н. Каразіна

В. С. Бакіров

« » \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2017 р.

ПРОГРАМА

Фахових випробувань для вступу до аспірантури

факультету комп’ютерних наук

з галузі

12 Комп’ютерні науки

зі спеціальності:

125 Кібербезпека

Програма затверджена

на засіданні Вченої ради

факультету комп’ютерних наук

Протокол № 8 від 14 лютого 2017 р.

Голова Вченої ради

проф. В.Т. Лазурик

ХАРКІВ 2017

**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 c.

**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

Брюc 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, 563c.

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 c.

Тайли Э Безопасность персонального компьютера. Минск: Попурри, 1997, 477с.

Барсуков В.С. Обеспечение информационной безопасности. М.: Технология электронных коммуникаций. 1996, 94с.

Декан факультету комп’ютерних наук В.Т. Лазурик

Гарант освітньо-наукової програми

завідувач кафедрою безпеки інформаційних систем і технологій С.Г. Рассомахін