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

ЗАТВЕРДЖУЮ»
Заступник Голови
Приймальної комісії,
В.о. ректора Харківського національного
університету імені В. Н. Каразіна

_____Олександр ГОЛОВКО
« »_____ 2024 р.

Програма фахового вступного екзамену
за спеціальністю:
125 «Кібербезпека та захист інформації»
освітньо-наукової програми «Кібербезпека»
для вступників на навчання до аспірантури

Харків 2024

Програма фахових випробувань

1. **Математичні основи**

1. Лінійна алгебра: лінійні простори, базиси, розмірність лінійного простору, підпростори, застосування до систем лінійних рівнянь; лінійні функціонали і оператори, поняття власного значення і вектору лінійного оператора; евклідові (унітарні) лінійні простори; геометрична алгебра, еліптичні криві, їх властивості і загальні параметри, бінарні відображення точок еліптичних кривих.

2. Дискретна математика: множини, відношення і відображення; поняття групи, кільця і поля; скінченні поля Галуа; задача комбінаторики, основні комбінаторні числа; відношення еквівалентності, їх властивості, поняття фактор множини; елементи теорії впорядкованих множин; поняття абстрактного автомату.

3. Теорія ймовірностей і математична статистика: ймовірністна модель, випадкові події і випадкові величини; умовна ймовірність; основні ймовірностні розподіли; центральна гранична теорема; моменти випадкової величини; статистична модель і задача статистики; метод максимальної правдоподібності; елементи теорії перевірки статистичних гіпотез.

4. Методи обчислень: числові методи лінійної алгебри; методи інтерполяції функцій; числові методи диференціювання; числові методи розв'язання рівнянь і систем рівнянь; числові методи інтегрування; числові методи розв'язання диференціальних рівнянь.

Рекомендована література.

1. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Монографія. - Харків: Видавництво «Форт», 2012.
2. Зеліско В. Р. Основи лінійної алгебри і аналітичної геометрії, навчальний посібник. Львів: ЛНУ імені Івана Франка, 2011.
3. Комп'ютерна дискретна математика: підручник \ М. Ф. Бондаренко Н. В. Білоус А. Г. Руккас. - Харків: Компанія СМІТ, 2004.
4. Кривий С. Л. Дискретна математика. Чернівці - Київ: Букрек, 2014.
5. М.Л. Жалдак, Н.М. Кузьміна, Г.О. Михалін. Теорія ймовірностей і математична статистика. Київ: НПУ імені М.П. Драгоманова, 2015.
6. Фельдман Л. П., Петренко А. І., Дмитріева О. А. Чисельні методи в інформатиці. - К.: Видавнича група BHV, 2006.
7. Enge A. Elliplic Curves and Their Applications to Cryptography. – Springer, 2012.
8. Lawrence C. Washington Elliptic Curves: Number Theory and Cryptography, Second Edition. - CRC Press, 2008 - 536 p.
8. Duncan Buell Fundamentals of Cryptography. - Springer Nature Switzerland AG, 2021.

9. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone Handbook of Applied Cryptography. - CRC Press, 2018. - 810 p.
10. William Easttom Modern Cryptography. Applied Mathematics for Encryption and Information Security. - Springer Cham, 2021.
11. Daniel T. Bennett, Paul L. Goethals, Natalie M. Scala Mathematics in Cyber Research. - Chapman and Hall/CRC, 2022.
12. Alko R. Meijer Algebra for Cryptologists. - Springer, 2016. - 301 p.

2. Системи захисту інформації

1. Сучасні моделі у галузі захисту інформації: модель інформаційної безпеки та кібербезпеки, модель загроз, модель захисту інформації, модель порушника інформаційної безпеки.

2. Характеристика інформації як об'єкта захисту; сутність потенційних та реальних загроз інформації; методологія систем захисту інформації.

3. Основні складові забезпечення інформаційної безпеки та кібербезпеки; обгрунтування складу засобів захисту у системі захисту інформації.

Рекомендована література.

1. John Vacca Cyber Security and IT Infrastructure Protection. - Syngress, 2013. - 380 p.
2. Martti Lehto, Pekka Neittaanmäki Cyber Security. Critical Infrastructure Protection. - Springer International Publishing, 2022.
3. Гулак Г. М. Методологія захисту інформації. Аспекти кібербезпеки: підручник/Г.М. Гулак. – Київ: Видавництво НА СБ України, 2020. – 256 с.
4. Жилін А. В. Технології захисту інформації в інформаційно-телекомуні-каційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с.
5. Єсін В. І., Кузнецов О. О., Сорока Л. С. Безпека інформаційних систем і технологій. - Харків: ХНУ імені В. Н. Каразіна, 2013. - 632 с.
6. Гребенніков В.В. Комплексні системи захисту інформації: проектування, впровадження, супровід. / В.В. Гребенніков — Київ: Вид. «Издательские решения», 2019.

3. Організаційно-правове забезпечення кібербезпеки

1. Загальний склад організаційно-правового забезпечення кібербезпеки.

2. Організаційно-технічні засоби захисту інформації.

3. Класифікація автоматизованих інформаційних систем та вимоги до захисту інформації в них, рівні захисту.

Рекомендована література.

1. Замула О.А., Горбенко Ю.І., Шумов А.І. Нормативно-правове забезпечення. Комплексні системи захисту інформації. – Харків, ХНУРЕ, 2010. – 98 с.

2. John Vacca Managing Information Security. - Elsevier, 2013 . - 372 p.
3. Thomas R. Peltier Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. - CRC Press, 2016. - 312 p.
4. Andy Taylor Information Security Management Principles. - BCS Learning & Development Limited, 2013. - 224 p.
5. Sandy Bacik Building an Effective Information Security Policy Architecture. - CRC Press, 2008. - 368 p.
6. Thomas R. Peltier Information Security Risk Analysis. - CRC Press, 2010. - 456 p.
7. Tony Campbell Practical Information Security Management: A Complete Guide to Planning and Implementation. - Apress, 2016. - 237 p.
8. Sandra Senft, Frederick Gallegos, Aleksandra Davis Information Technology Control and Audit. - CRC Press, 2016. - 776 p.

4. Основи криптографії

1. Стандартизовані криптографічні примітиви, порядок їх розробки та застосування при захисті інформації з обмеженим доступом та наданні електронних транскордонних довірчих послуг в ІТС та ІВК, в тому числі у постквантовий період.

2. Класифікація, основні вимоги та принципи побудування асиметричних криптосистем. Вимоги та застосування асиметричних криптосистем в постквантовий період.

3. Критерії та показники оцінки стійкості, складності тощо реалізації криптосистем та безпечності криптографічних протоколів, включаючи хмарні сервіси.

4. Методи, методики та засоби дослідження стійкості криптосистем та засобів КЗІ, особливості їх розробки та експертизи на національному та міжнародному рівнях.

5. Класифікація, основні вимоги та побудування криптосистем на основі блокових симетричних шифрів (БСШ). Вимоги до БСШ в постквантовий період.

6. Функції гешування, їх застосування та властивості. Порівняльний аналіз перспективних функцій гешування, в тому числі в постквантовий період.

7. Життєві цикли особистих ключів та сертифікатів відкритих ключів. Особливості сертифікації ключів в хмарах.

Рекомендована література.

1. Henk C.A. van Tilborg Fundamentals of Cryptology: A Professional Reference and Interactive Tutorial. - Springer Science & Business Media, 2006 . - 492 p.
2. Bruce Schneier Applied Cryptography: Protocols, Algorithms and Source Code in C. - John Wiley & Sons, 2017. – 784 p.
3. Daniel J. Bernstein, Johannes Buchmann, Erik Dahmen Post-Quantum Cryptography. - Springer Berlin Heidelberg, 2010. - 246 p..

4. Cryptology: Classical and Modern / Richard Klima and oth. - Taylor & Francis Group, 2023. – 496 p.
5. William Stallings Cryptography and network security: principles and practice. - Pearson, 2022. - 766 p.
6. Henk C.A. van Tilborg, Sushil Jajodia Encyclopedia of Cryptography and Security. - Springer Science & Business Media, 2014. - 1416 p.
7. Горбенко Ю.І. Побудування та аналіз систем, протоколівта засобів криптографічного захисту інформації. Монографія. Частина 1. Методи побудування та аналізу, стандартизація та застосування криптографічних систем. Харків, 2016.- 959 с.
8. Кузнецов О.О, Потій О.В., Полуяненко М.О., Горбенко Ю.І. Потокові шифри. Монографія. – Харків: Форт, 2019. - 544 с.
9. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Підручник. - Харків: ХНУРЕ, Форт, 2013. - 878 с.

5. Основи технічного захисту інформації

1. Класифікація технічних каналів витоку інформації та їх моделі.
2. Методи та засоби захисту інформації від витоку по технічних каналах.
3. Методи захисту інформації від витоку по побічних електромагнітних випромінюваннях.

Рекомендована література.

1. Гулак Г. М. Методологія захисту інформації. Аспекти кібербезпеки: підручник/Г.М. Гулак. – Київ: Видавництво НА СБ України, 2020. – 256 с.
2. Методи та засоби технічного захисту інформації. Опорний конспект лекцій [Електронний ресурс] : навч. посіб. – Київ : КПІ ім. Ігора Сікорського, 2021. – 289 с.
3. ДСТУ 3396.0-96 Державний стандарт України. Захист інформації. Технічний захист інформації. Основні положення.
4. ДСТУ 3396.1-96 Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт.
5. ДСТУ 3396.2-97 Державний стандарт України. Захист інформації. Технічний захист інформації. Терміни та визначення

6. Побудова захищених інформаційно-комунікаційних систем та їх компонентів

1. Основи побудови сучасних операційних систем; загальні моделі безпеки операційних систем; методи та механізми забезпечення безпеки основних операційних систем та застосунків.

2. Основні різновиди зловмисного програмного забезпечення; аналіз шкідливого програмного забезпечення; статичний та динамічний аналіз зловмисного програмного забезпечення та шкідливого коду; методи і засоби

захисту від зловмисного програмного забезпечення, обфускації, дизассемблювання, реверс-інжинірингу.

3. Основні технології сучасної мережевої безпеки, які включають брандмауери, системи виявлення вторгнень і віртуальні приватні мережі. Політика мережевої безпеки та оцінка безпеки мереж, в тому числі – бездротових, за допомогою провідних галузевих стандартів і моделей. Методи і засоби захисту від мережевих атак, в тому числі - в бездротових мережах. Захист даних за допомогою криптографічних відкритих/приватних ключів, цифрових підписів і сертифікатів.

4. Штучний інтелект та інтелектуальний аналіз даних; алгоритми штучного інтелекту такі, як штучні нейронні мережі, нечітка логіка, генетичні алгоритми та гібридні механізми; застосування методів штучного інтелекту та інтелектуального аналізу даних з метою виявлення вразливостей інформаційних систем та протидії атакам на мережеві системи. Ключові механізми та технології, які використовують методи штучного інтелекту та інтелектуального аналізу даних у кібербезпеці.

5. Основи хмарних обчислень і хмарних сервісів; концепції безпеки хмарних середовищ, вразливості, стандарти безпеки та еталонні моделі; методи безпеки для хмарних середовищ для різних моделей хмарних сервісів; методи та механізми керування даними, ідентифікацією та доступом; забезпечення безпеку мереж та реагування на інциденти у хмарних середовищах.

6. Основи побудови децентралізованих комп’ютерних систем і мереж та забезпечення безпеки в розподілених системах і мережевих системах з використанням технології блокчейн; основи, архітектура та проблеми застосування блокчейну для кібербезпеки, в тому числі - в IoT; загрози та вразливості блокчейна; використання блокчейну для онлайн-платежів електронної комерції, систем підтримки платежів.

Рекомендована література.

1. A. Kleymenov, A. Thabet Mastering Malware Analysis: The complete malware analyst's guide to combating malicious software, APT, cybercrime, and IoT attacks. - Packt Publishing Ltd, 2019. - 562 p.
2. Artificial Intelligence for Cybersecurity / Mark Stamp and oth. - Springer Nature, 2022. – 380 p.
3. Behrouz A. Forouzan, Debdeep Mukhopadhyay Cryptography and Network Security. - Mc Graw Hill Education Private Limited, 2015. – 702 p.
4. Cory Beard, William Stallings Wireless Communication Networks and Systems. - Pearson Education, 2015. - 672 p.
5. Abdulrahman Yarali From 5G to 6G: Technologies, Architecture, AI, and Security. - Wiley, 2023.

6. P. Porambage, M. Liyanage Security and Privacy Vision in 6G: A Comprehensive Guide. - Wiley, 2023. – 352 p.
7. Charles Pfleeger, Shari Lawrence Pfleeger, Lizzie Coles-Kemp Security in Computing, 6th Edition. - Addison-Wesley/Pearson, 2023. – 960 p.
8. John R. Vacca Cloud Computing Security: Foundations and Challenges. - CRC Press, 2016. – 518 p.
9. Brij B. Gupta Modern Principles, Practices, and Algorithms for Cloud Security. - IGI Global, 2020. – 361 p.
10. W. Stallings, L. Brown Computer Security: Principles and Practice, Global Edition. - Pearson, 2018. – 986 p.
11. H. Bos, A. S. Tanenbaum Modern Operating Systems: Global Edition 4th Edition. – Pearson, 2015. – 1138 p.
12. W. Stallings Operating Systems: Internals and Design Principles, 9th Global Edition. - Pearson Education Limited, 2017. – 1128 p.
13. Blockchain for Cybersecurity and Privacy: Architectures, Challenges, and Applications/ Y. Maleh, and oth. - CRC Press, 2020. - 404 p.
14. Artificial Intelligence and Data Mining Approaches in Security Frameworks/ N. Bhargava and oth. - John Wiley & Sons, 2021. - 320 p.

ІІ. Загальні критерії оцінювання знань.

Оцінка ECTS	**Вимоги**
200-170	Тверде засвоєння теоретичного матеріалу, глибокі та вичерпні знання змісту програмного матеріалу по суті питання, розуміння сутності та взаємозв'язку розглянутих процесів і явищ, твердезнання основних положень суміжних питань. Уміння самостійно використовувати математичний апарат для аналізу та вирішення практичних завдань, робити правильні висновки з отриманих результатів.
169-140	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 для вирішення практичних завдань.
139-100	Тверде знання і розуміння теоретичного матеріалу по суті питання. Правильні і конкретні відповіді на поставлені питання за наявності окремих неточностей і несуттєвих помилок при висвітленні окремих положень. Уміння застосовувати теоретичні знання до вирішення основних практичних завдань при обмеженні математичного апарату.
99-1	Недостатнє розуміння суті розглянутих процесів і явищ, наявність грубих помилок у відповіді. Невміння застосовувати знання при вирішенні практичних завдань.

Білет складається з 3-ох питань теоретичного характеру. Максимальна кількість балів за кожну відповідь дорівнює: 1-е питання – 66 балів, 2-е та 3-є питання – 67 балів.

Шкала оцінки (одне питання екзаменаційного білету)

Кількість балів	Критерії оцінки
0-20	Робота виконана не в повному обсязі. Допущені грубі помилки. Робота виконанане самостійно.
21-33	Абітурієнт має фрагментарні знання при незначному загальному їх обсязі завідсутності сформованих умінь та навичок.
34-46	Абітурієнт має рівень знань вищий, ніж початковий; може відтворити значну частину матеріалу з елементами логічних зв'язків; має стійкі навички виконанняелементарних технологічних застосувань та їх опрацювання.
47-59	Абітурієнт вільно володіє матеріалом, застосовує знання на практиці; вміє узагальнювати і систематизувати інформацію; може аргументовано обратираціональний спосіб виконання завдання.
60-67	Абітурієнт має стійкі системні знання та продуктивно їх використовує, стійкі навички керування інформаційною системою в нестандартних ситуаціях; уміє вільно використовувати нові інформаційні технології для поповнення власних знань та розв'язування задач.

Вступник допускається до участі у конкурсному відборі, якщо його остаточна оцінка становить не менше 100 балів.

РОЗРОБНИКИ ПРОГРАМИ:
д.т.н., професор Горбенко Іван Дмитрович
к.т.н., доцент Громико Ігор Олексійович
к.т.н., с.н.с. Сватовський Ігор Іванович

В.о. завідувача кафедри безпеки інформаційних систем і технологій, к.т.н, доцент Ольга МЕЛКОЗЬОРОВА

Затверджено на засіданні Приймальної комісії Харківського національного університету імені В. Н. Каразіна
Протокол № 2 від « 15 » квітня 2024 р.

Відповідальний секретар
Приймальної комісії Сергій ЄЛЬЦОВ