М И Н И С Т Е Р С Т В О Н А О Т Б Р А Н А Т А

ИНСТИТУТ ПО ОТБРАНА „ПРОФЕСОР ЦВЕТАН ЛАЗАРОВ”

София, бул. „Проф. Цветан Лазаров” № 2, факс: 02/92 21 808, http://di.mod.bg

УТВЪРЖДАВАМ:

ДИРЕКТОР НА ИНСТИТУТ ПО ОТБРАНА

„ПРОФЕСОР ЦВЕТАН ЛАЗАРОВ”

ПОЛКОВНИК Д-Р /П/ ДИМИТЪР КИРКОВ

___.___2020 г.

П Р О Г Р А М А

ЗА ПРОВЕЖДАНЕ НА КОНКУРСЕН ИЗПИТ ПО СПЕЦИАЛНОСТТА

ПО ДОКТОРСКА ПРОГРАМА „ИНФОРМАЦИОННИ ТЕХНОЛОГИИ И КИБЕР СИГУРНОСТ”, ТЕМА „ОЦЕНКА НА ЩЕТИТЕ ПРИ КИБЕР АТАКИ СРЕЩУ ИНФОРМАЦИОННИ СИСТЕМИ И КОМПЮТЪРНИ МРЕЖИ ЗА СИГУРНОСТ И ОТБРАНА”

В СЪОТВЕТСТВИЕ С ОБЯВЕНИЯ КОНКУРС (МЗ № ОХ-456/17.06.2020 г.) ЗА ОБУЧЕНИЕ В ЗАДОЧНА ФОРМА НА ДОКТОРАНТУРА ПРЕЗ 2021 г.

СОФИЯ
2020

I. РАЗДЕЛ

1. Случайни събития. Вероятност на събитие. Формула за пълна вероятност. Случайни величини. Закони на разпределение. Числени характеристики на случайните величини.
2. Случайни функции. Определение. Закони за разпределение на случайна функция. Характеристики на случайна функция.
3. Общи принципи на моделирането. Класификация на математическите модели.
4. Елементи на дискретните математически модели – множества, списъци, релации, функции.
5. Графи. Дървета. Обхождане на графи.
6. Крайни автомати. Регулярни изрази. Граматики.
7. Алгоритми. Формално и неформално определение. Свойства на алгоритмите.
8. Детерминирани и недетерминирани алгоритми. Сложност и оптималност на алгоритмите. Изчислимост, P и NP класове от задачи.
9. Алгоритми в графи с тегла на ребрата. Оценки за сложност.
10. Архитектура на съвременните компютри. Централен процесор – структура и организация. Инструкции. Типове данни, формати, видове операции, адресация, изпълнение, признаци на резултата.
11. Принципи на операционните системи. Структура на ОС (монолитна структура, слоеста структура, микро ядро). Абстракции на ОС (процес, задача, файл).
12. Архитектура на компютърните мрежи. Основни принципи и характеристики. Еталонен модел на ISO. Модел TCP/IP. Характеристики на нивата и сравнение между двата модела.
13. Бази от данни (БД). Системи за управление на бази от данни (СУБД). Описание и сравнителна характеристика на мрежовия, йерархичния и релационния модели на СУБД.
14. Облачни изчисления (cloud computing) - характеристики, модели, услуги. Инструменти и технологии за реализация.
15. Изкуствен интелект (ИИ) – основни понятия, типове ИИ, основни алгоритми, приложение
16. Сигурност на компютърните системи и мрежи. Тайна, цялостност и наличност на информацията.

II. РАЗДЕЛ

1. Контрол на достъпа и оторизация.
2. Методи за автентификация.
3. Криптографски алгоритми: формални дефиниции, класификация
4. Симетрични криптографски алгоритми.
5. Криптография с публични ключове.
6. ХЕШ функции. Определение. Основни изисквания към функциите. Методи и средства за проверка на функциите. Приложение.
7. Формални модели за сигурност. Модел на Biba.
8. Формални модели за сигурност. Модел на Bell-LaPadula.
9. Формални модели за сигурност. Модел на Clark-Wilson.
10. Формални модели за сигурност. Модел на Graham-Denning.
11. Формален модел за кибер сигурност. Политики, атаки, защита.
12. Теоретични характеристики – модел „Противопоставяща се средата”
13. Теоретични характеристики – модел „Свойства на атаките”
14. Кибер-сигурност на мобилни и безжични устройства и комуникации
15. Социални медии, бот-мрежи и системи за откриване и реакция.
16. Кибер-защита на вградени и SCADA системи

ЛИТЕРАТУРА

1. Боянов Л. и др., Компютърни мрежи и телекомуникации, Авангард Прима, София, 2014
2. Боянов Л. и др., Разпределено управление на слабо свързани системи, Техника, София, 1989
3. Василев Н. и др., Приложна математика, Военно издателство, София, 1985
4. Денев, Й., Р. Павлов, Я. Деметрович, Дискретна математика. Наука и изкуство, София, 1984
5. Котов В. Е., Сети Петри, Наука, Москва, 1984
6. Манев К., Увод в дискретната математика, КЛМН, София, 2005
7. Фаулър, М., UML основи, Софтпрес, 2004
8. Целков В., Н. Стоянов, Защитени криптографски приложения в компютърните системи и мрежи, Издателство „Нова Звезда", София, 2009. ISBN 978-954-8933-20-9
9. Целков В., Н. Стоянов, О. Исмаилов, Международни стандарти и добри практики за защита на информацията, Издателство „За буквите – О писменехь", София, 2010, ISBN 978-954-8887-68-7
10. Booch, G., Object-oriented Analysis and Design with Applications, The Benjamin/Cummings Publishing Company 1994.
11. Carr J., Inside Cyber Warfare, O'Reilly Media, Inc., 2012, ISBN: 978-1-449-31004-2
12. Davis, Sigal, Weyuker, Computability, Complexity and Languages: Fundamentals of Theoretical Computer Science, second edititon, 1994, Morgan Kaufman Publishers, ISBN 0-12- 206382-1.
13. Fisch E., White G., Secure computers and networks, Analysis, Design, and Implementation, CRC PRESS, 2000
14. Graham J., R. Howard, R. Olson, Cyber security essentials, CRC Press, Auerbach book, 2011, ISBN 978-1-4398-5126-5
15. N. Koblitz, A Course in Number Theory and Cryptography, 1998, Springer-Verlag
16. Johannes Buchmann, Introduction to Cryptography (2en edition) 2004, Springer
17. Douglas R. Stinson, Cryptography: Theory and Practice (3rd edition), 2005, Chapman and Hall/CRC
18. Zubairi J., Athar Mahboob, Cyber Security Standards, Practices and Industrial,Applications: Systems and Methodologies, IGI Global, 2012, ISBN 978-1-60960-851-4
19. Carr J., Inside Cyber Warfare, O'Reilly Media, Inc., 2012, ISBN: 978-1-449-31004-2
20. Janczewski L., A. Colarik, Cyber Warfare and Cyber Terrorism, IGI Global, 2008, ISBN 978-1-59140-991-5
21. Graham J., R. Howard, R. Olson, Cyber security essentials, CRC Press, Auerbach book, 2011, ISBN 978-1-4398-5126-5

Програмата е приета на заседание на Научния съвет на Институт по отбрана "Професор Цветан Лазаров" с протокол № / .10.2020 г.