МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної роботи
_____ Віктор ЛОПАТОВСЬКИЙ
_____ 2023 р.

ПРОГРАМА ФАХОВОГО ІСПИТУ

для вступу на навчання для здобуття ступеня доктора філософії на основі раніше здобутого ступеня вищої освіти магістра

Галузь знань: 12 Інформаційні технології
Спеціальність: 126 Інформаційні системи та технології
Спеціалізація (за наявності):
Освітня програма: Інформаційні системи та технології

Схвалено на засіданні кафедри комп'ютерної інженерії та інформаційних систем
протокол № 11 від 13.04 2023 р.

Зав. кафедри Тетяна ГОВОРУЩЕНКО

Гарант ОП Тетяна ГОВОРУЩЕНКО

Програма розглянута та схвалена на засіданні вченої ради факультету інформаційних технологій
протокол № 4 від 14.04 2023 р.

Голова вченої ради факультету Олег САВЕНКО

Хмельницький – 2023

Загальні положення

Вступний фаховий іспит для вступу на навчання для здобуття ступеня доктора філософії за спеціальністю 126 «Інформаційні системи та технології», ОНП «Інформаційні системи та технології» проводиться приймальною комісією Хмельницького національного університету.

Під час виконання завдання перевіряються знання, вміння та навички студентів щодо розв'язання певних завдань з управління ІТ-проектами, технологій проектування інформаційних систем, ІТ-інфраструктур, безпеки та захисту інформаційних систем і технологій, методологічних основ створення інформаційних систем і технологій.

Мета вступного фахового іспиту полягає у перевірці здатності до опанування ОНП «Інформаційні системи та технології» третього (освітньо-наукового) рівня вищої освіти на основі здобутих раніше компетентностей.

Технологія проведення вступного фахового іспиту

Вступний іспит (вступне випробування) проводиться у формі тестування із комп'ютерною обробкою результатів. Система проведення вступних іспитів є оригінальною розробкою ХНУ і захищена свідоцтвом про авторське право № 39534 від 08.08.2011 р. Вона розроблена на підставі таких документів: Закону України «Про вищу освіту», «Положення про приймальну комісію ХНУ», Порядку прийому до вищих навчальних закладів України та Правил прийому до Хмельницького національного університету.

Основні положення системи тестування із комп'ютерною обробкою результатів викладені нижче. Бази даних тестових завдань створюються для всіх дисциплін, з яких проводиться тестування, щорічно поповнюються і вдосконалюються.

Бази даних тестових завдань або навчальні програми, за якими вони створені, є відкритими. Університет щорічно оприлюднює їх у паперовому або в електронному вигляді.

Відповідальність за зміст і якість тестових завдань покладається на голову предметної комісії.

Екзаменаційний білет може містити тестові завдання одного або різних рівнів складності. Для автоматизованого формування білетів використовують комплекс комп'ютерних програм, які компонують бази даних тестових завдань з кожної дисципліни, формують екзаменаційні білети за допомогою випадкової вибірки та роздруковують їх.

Екзаменаційні білети, що включають тестові завдання, формують і тиражують комп’ютерними засобами перед початком тестування. Сформовані білети засвідчуються печаткою приймальної комісії.

Номер кожного екзаменаційного білета збігається з номером талона відповідей, який додається до нього.

Організація автоматизованого формування комплекту екзаменаційних білетів до вступних іспитів, контроль за ним покладається на відповідального секретаря Приймальної комісії або його заступника.

Тестування проводиться відповідно до розкладу в аудиторіях, що обладнані необхідними технічними засобами.

Пропуск вступників до аудиторії тестування проводить відповідальний секретар ПК та його заступники. При цьому перевіряється паспорт та перепустка, у якій вказана особа вступника, дата і час тестування.

Кожний учасник тестування витягує номер, який вказує його місце в аудиторії. Всі місця за столами пронумеровані.

В аудиторії тестування дозволяється присутність громадських спостерігачів (батьків вступників).

Вступникам видаються титульні листи і проводиться роз’яснення щодо їх заповнення.

Після розміщення учасників тестування в аудиторії вступники особисто вибирають екзаменаційні білети, що розкладені на столі.

Після отримання екзаменаційних білетів вступники працюють над розв’язком завдань протягом встановленого часу.

Талони відповідей надаються кожному вступнику в одному екземплярі. Забороняється видача вступнику другого талона. Талон відповідей заповнюється вступником відповідно до роз’яснення щодо їх заповнення.

Після закінчення роботи над тестами, або добігання до кінця часу, відведеного на тестування, вступники здають підписані роботи разом з талонами відповідей, які до початку сканування знаходяться на столі екзаменатора.

Сканування талонів відповідей починається після здачі робіт всіма вступниками у їх присутності. Процес сканування талонів відповідей демонструється за допомогою проектору на великому екрані.

Після закінчення сканування та комп'ютерної обробки талонів відповідей результати тестування демонструються на екрані у вигляді екзаменаційної відомості, в якій відсутні прізвища вступників, а є лише номер екзаменаційного білета. Далі персонал приймальної комісії вносить в комп’ютер інформацію про відповідність номера екзаменаційного білета

прізвищу вступника. На екрані демонструється екзаменаційна відомість з прізвищами вступників, яка роздруковується і завіряється відповідальним секретарем приймальної комісії.

Критерії оцінювання вступних іспитів затверджуються на засіданні Приймальної комісії та наводяться в додатку до Правил прийому.

Перелік освітніх компонентів (навчальних дисциплін), на базі яких складається іспит

1 Управління ІТ-проектами

Проєкт і специфіка проєктної діяльності. Сутність управління проєктами. Фази життєвого циклу проєкту. Методичні основи планування проєкту. Організаційні форми управління проєктами. Управління ресурсами проєкту. Управління якістю проєктів. Управління проєктною командою.

Пошук донорів. Фандрейзинг. Життєвий цикл проєкту. Планування та управління ризиками в проєктах. Дослідницькі проєкти. Вибір теми наукового дослідження. Управління дослідницькою групою. Бюджет проєкту. Оцінка проєктної заявки донором.

ІТ бізнес – специфіка та особливості організації. Особливості реалізації ІТ-проєктів. Ризики. Статистика успішності проєктів з розроблення програмного забезпечення (ПЗ). Планування та його роль в організації та веденні бізнесу. Винаходи. Інновації. Стартапи. Основи підприємництва. 24 кроки від запуску до стабільного бізнесу.

Юридичні особливості відкриття ІТ-бізнесу в Україні. Відкриття ІТ-компанії в Україні. Розробка програмного забезпечення: договір про виконання робіт та надання послуг. Особливі договори та поради щодо їх укладення в ІТ-сфері. Стартап в Україні: погляд з позиції ІТ-права.

Основні фази розроблення програмного забезпечення (ПЗ). Сучасні технології проєктування програмного забезпечення. Методологія розроблення ПЗ Microsoft Solutions Framework (MSF). Гнучкі методології розроблення ПЗ. Функціональні можливості та архітектура Team Foundation Server (TFS). Аналіз методології Scrum, робочі елементи шаблону Microsoft Visual Studio Scrum. Організація колективу у методології Scrum.

Список рекомендованої літератури

1. «Управління проєктами»: навчальний посібник до вивчення дисципліни / Уклад.: Л.Є. Довгань, Г.А.Мохонько, І.П Малик. – К.: КПІ ім. Ігоря Сікорського, 2017. – 420 с.

2. Aulet B. Disciplined Enterpreneurship: 24 Steps to a Successful Startup. Workbook. Wiley, 2017. – 288 p.

3. Основи ІТ-права: навчальний посібник / Т. В. Бачинський, Р. І. Радейко, О. І. Харитонова та ін. ; за заг. ред. Т. В. Бачинського. – Київ: Юрінком Інтер, 2017. – 208 с.

4. Єгорченков О. В. Азбука управління проєктами. Планування : навч. посіб. / О. В. Єгорченков, Н. Ю. Єгорченкова, Є. Ю. Катаєва. – Київ : КНУ ім.Т.Шевченка, 2017. – 117 с.

5. Говорущенко Т.О. Організація бізнесу в галузі інформаційних технологій. Методичні вказівки до практичних робіт для здобувачів вищої освіти за ОНП «Комп'ютерна інженерія» спеціальності 123 «Комп'ютерна інженерія» другого (магістерського) рівня вищої освіти. – Хмельницький: ХНУ, 2019. – 133 с.

6. На шляху до бізнесу: 6 кроків, як створити успішний ІТ-стартап. – [Електронний ресурс]. – Режим доступу: http://womo.ua/na-puti-v-biznes-6-shagov-kak-sozdat-uspeshnyiy-it-startap/

2 Технології проектування інформаційних систем

Основні поняття технології проектування інформаційних систем. Архітектура інформаційних систем. Методика опису архітектури інформаційних систем (фреймворки). Паттерн-технологія проектування.

Проектування інформаційних систем з урахуванням особливостей їх призначення, неповної / недостатньої інформації та суперечливих вимог.

Управління вимогами до ІС на основі аналізу бізнес-процесів та аналізу потреб зацікавлених сторін, розробка технічного завдання.

Управління процесами розробки, впровадження та експлуатації ІС, які є складними та непередбачуваними.

Типове проектування інформаційних систем. Параметрично-орієнтоване проектування інформаційних систем. Модельно – орієнтоване проектування інформаційних систем. Методологія функціонального моделювання SADT. Методологія IDEF1. CASE-технології.

Моделювання бізнес-процесів та потоків даних.

Методології гнучкого моделювання. Основи гнучкого моделювання.

Манифест гнучкої розробки. Цінності Agile. Приципи Agile. Практики Agile.

Інформаційні системи критичного застосування та сервіс-орієнтовані інформаційні системи. Якість, відмовостійкість та живучість інформаційних систем.

Реінжинірінг інформаційних систем. Надійність, надмірність, резервування та стійкість інформаційних систем.

Список рекомендованої літератури

1. Rainer R. Kelly Prince Brad. Introduction to Information Systems. JOHN WILEY & SONS. 2022. 560 p.
2. Briony J Oates, Marie Griffiths, Rachel McLean Researching Information Systems and Computing. SAGE. 2022 . 376 p.
3. Проектування інформаційних систем: Загальні питання теорії проектування ІС (конспект лекцій) [Електронний ресурс]: навч. посіб. для студ. спеціальності 122 «Комп'ютерні науки» / КПІ ім. Ігоря Сікорського; уклад.: О. С. Коваленко, Л. М. Добровська. – Електронні текстові дані (1 файл: 2,02 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2020. – 192с.
4. Шаховська Н.Б., Литвин В.В. Проектування інформаційних систем Навчальний посібник. – Львів: "Магнолія-2006", 2018. – 380 с.
5. Берко А.Ю., Верес О.М., Пасічник В.В. Системи баз даних та знань. Книга 1. Організація баз даних та знань. - 2-е вид. Підручник. – Львів: "Магнолія2006", 2018. – 440 с.
6. T. Hovorushchenko, Ye. Hnatchuk, A. Herts, O. Onyshko. Intelligent Information Technology for Supporting the Medical Decision-Making Considering the Legal Basis. CEUR-WS. 2021. Vol. 2853. Pp. 72-82. - https://www.scopus.com/authid/detail.uri?authorId=54420153900 (Q4).

3 IT-інфраструктури

Поняття IT-інфраструктури. Типи IT-інфраструктур. Компоненти IT-інфраструктури: апаратне забезпечення, програмне забезпечення, мережі. Центри обробки даних. Хмара. Grid. Вимоги до IT-інфраструктур. Архітектура підприємства та цифрова трансформація. Проєктування IT-інфраструктур. Вибір технологій при проєктуванні IT-інфраструктур. Ієрархічна структура корпоративної IT-інфраструктури.

Основні сучасні концепції та підходи до надання IT-послуг. Аналіз IT-інфраструктури та її елементів як об'єктів управління. Моделі управління IT-інфраструктурою. Аналіз стандартів, протоколів та відомих систем

управління IT-інфраструктурою та рівнем послуг. Задача управління IT-інфраструктурою в розрізі управління рівнем послуг. Узгодження рівня послуг у корпоративних IT-інфраструктурах. Планування ресурсів.

Методи моніторингу IT-інфраструктури. Методи оцінки якості функціонування елементів та підсистем IT-інфраструктури. Загальні принципи та метрики аналізу стану об'єктів IT-інфраструктури. Метрики оцінювання рівня обслуговування користувачів на основі експертних оцінок. Нечітке оцінювання у завданнях управління рівнем обслуговування. Оцінювання стану елементів IT-інфраструктури з використанням нейронних мереж. Управління мережним трафіком корпоративної IT-інфраструктури. Управління потоками інформації у мережі. Моделі управління потоками даних.

Поняття кластера. Архітектура кластера. Класифікація кластерів. Кластери високої доступності. Кластери розподілу навантаження. Обчислювальні кластери. Системи розподілених обчислень. Кластер серверів, організованих програмно. Кластер одного вузла. Кластер декількох вузлів. Програмні засоби для організації кластерних структур. Проєктування та розгортання кластерів в IT-інфраструктурі. Концепція Kubernetes. Кластерна архітектура Kubernetes. Сервіси Kubernetes.

Проблеми балансування навантаження в кластерах. Алгоритми балансування навантаження в кластерах. Методи підвищення продуктивності кластерів з динамічним балансуванням навантаження. Оцінка надійності кластерних структур.

Ключові властивості хмарних обчислень. Моделі розгортання хмарних обчислень. Моделі обслуговування хмарних обчислень. Технології хмарних обчислень. Провідні надавачі хмарних послуг. Хмарні послуги на прикладі Microsoft Azure. Інфраструктурні та платформенні сервіси Microsoft Azure. Обчислення: віртуальні машини (VM), служба додатків, сервіс хостингу веб-сайтів, WebJobs. Сховище: Storage Services, Queue Service, File Service. Робота в мережі: віртуальна мережа, Load Balancer, шлюз додатків, VPN-шлюз, Azure DNS. Мобільні сервіси Azure. Медіа-сервіси Azure. Azure Quantum. SQL Azure. Azure Kubernetes (AKS). Віртуальний робочий стіл Azure. Azure Arc. Azure Blockchain Workbench. Безсерверні обчислення, штучний інтелект та машинне навчання, хмарна міграція та модернізація, дані та аналітика, гібридна хмара та інфраструктура, обмін повідомленнями, Інтернет речей, безпека та адміністрування як сервіси Azure. Галузеві рішення Azure. Впровадження хмарних обчислень в IT-інфраструктуру. Кластери в граничних хмарних архітектурах. Проблеми оптимізації продуктивності хмарних обчислень. Проблеми та методи балансування

навантаження в середовищі хмарних обчислень. Алгоритми балансування навантаження в середовищі хмарних обчислень. Проактивні підходи та реактивні підходи балансування навантаження в середовищі хмарних обчислень. Типи балансувальників навантаження. Проблеми балансування навантаження в хмарних центрах обробки даних. Огляд та класифікація методів прогнозування навантаження у хмарних обчисленнях.

Функціональна безпека. Показники функціональної безпеки і надійності. Аудит IT-інфраструктури. Доступність IT-послуг та компонентів IT-інфраструктури. Надмірність в IT-інфраструктурі. Резервне копіювання критично важливої корпоративної інформації та аварійне відновлення даних в IT-інфраструктурі. Хмарне резервне копіювання. Проблеми та методи балансування навантаження в IT-інфраструктурі.

Забезпечення бізнес-процесів ресурсами із певним рівнем надійності. Рівні надійності центрів обробки даних. Резервування ресурсів центрів обробки даних. Управління навантаженням та розподілом обмежених ресурсів. Аналіз методів пошуку несправностей у IT-інфраструктурах. Вплив несправностей в IT-інфраструктурі на якість IT-послуг. Проблема поширення впливу несправності на якість IT-послуг.

Список рекомендованої літератури

1. Ролік А.І., Теленик С.Ф., Ясочка М.В. Управління корпоративною IT-інфраструктурою. К.: Наукова думка, 2018. 576 с.
2. Halabi S. Hyperconverged Infrastructure Data Centers: Demystifying HCI (Networking Technology). Cisco Press; 1st edition, 2019. 545 p.
3. ITIL 4 Foundation. The Stationery Office; 4th edition, 2020. 212 p.
4. Oladeji T. Developing As An Enterprise IT Infrastructure Architect : A Beginner’s Guide. Tryspect Solutions, 2022. 136 p.
5. IT Infrastructure And Business Application Monitoring. A Complete Guide. The Art of Service – IT Infrastructure And Business Application Monitoring Publishing, 2020. 320 p.

4 Безпека та захист інформаційних систем і технологій

Завдання навчальної дисципліни. Основна тематика курсу. Структура курсу. Проблемні завдання курсу та предметної області. Основні поняття і терміни захисту інформації та безпеки комп’ютерних систем, кіберзахисту інформаційних систем і технологій. Поняття: інформаційна безпека, кібернетична безпека (кібербезпека), захист інформації. Властивості

інформаційної безпеки. Принципи забезпечення інформаційної безпеки. Крите́рії оці́нки інформаці́йної безпе́ки. Методологічна база для визначення вимог захисту комп'ютерних систем від несанкціонованого доступу, створення захисних систем та оцінки ступеня захищеності. Чотири групи вимог захисту проти певних типів загроз. Стандарт ISO/IEC 15408 «Загальні критерії оцінки безпеки інформаційних технологій». Загрози безпеці інформації. Види захисту інформації. Руйнуючі програмні впливи. Причини трудомісткості рішення задачі забезпечення безпеки програмних систем. Зловмисне програмне забезпечення та комп’ютерні атаки. Методи захисту від руйнуючих програмних впливів та їх виявлення. Покоління антивірусних програм. Типова архітектура програмних засобів антивірусного захисту. Критерії ефективності програмних засобів антивірусного захисту. ROC-аналіз в задачах виявлення зловмисного програмного забезпечення та комп’ютерних атак. Недоліки існуючих засобів захисту та перспективні методи захисту від руйнуючих програмних впливів.

Основні поняття і терміни з предметної області «комп’ютерні атаки». Міжмережні екрани (firewall), антивіруси, системи виявлення атак (СВА) (Intrusion Detection System, IDS), системи контролю цілісності, криптографічні засоби захисту. Типи атак. Моделі атак. Класифікація комп’ютерних атак. Основні типи аномалій в IP-мережах. Етапи реалізації атак. Основні механізми реалізації атак. Вивчення оточення. Ідентифікація топології мережі. Ідентифікація вузлів. Ідентифікація сервісів або сканування портів. Ідентифікація операційної системи. Визначення ролі вузла. Визначення вразливості вузла. Реалізація атак: проникнення, встановлення контролю. Цілі реалізації атак. Завершення атаки. Засоби досягнення мети атаки. Застосування технологій безпечного програмування.

Основні поняття про системи виявлення вторгнень. Класифікація систем виявлення атак. Системи виявлення атак рівня мережі. Класифікація систем виявлення вторгнень. Характеристики систем виявлення вторнень. Системи контролю цілісності. Монітори реєстраційних файлів. Архітектура систем виявлення вторгнень. Основні елементи локальної та глобальної архітектур систем виявлення вторгнень.

Основні поняття про системи виявлення атак і технології виявлення. Існуючі технології систем виявлення вторгнень. Методи, які використовують сигнатури вторгнень. Продукційні (експертні) системи виявлення вторгнень. Виявлення вторгнень, що базується на моделі. Аналіз переходу системи із стану в стан. Контроль натиснення клавіш. Концепція виявлення комп'ютерних загроз. Підвищення ефективності систем виявлення атак. Фазовий простір комп'ютерних атак. Характеристика напрямків і груп

методів виявлення вторгнень. Типова архітектура системи виявлення атак. Групи методів з виявлення аномалій і зловживань: з контрольованим навчанням («навчання з учителем») і з неконтрольованим навчанням («навчання без учителя»). Некомерційні системи виявлення комп'ютерних атак. Аналіз мережного трафіку і контенту. Програми аналізу та моніторингу мережного трафіку. Отримання і підготовка вихідних даних для аналізу властивостей аномалій трафіку. Аналіз зразків трафіку. Траси і їх аналіз. Тестування програмного забезпечення. Мережні атаки Portsweep, Neptune, Nmap, Mailbomb, Smurf. Типи сканування портів.

Застосування статичних методів в системах виявлення вторгнень. Статистичні методи виявлення аномальної поведінки. Профіль типової поведінки об'єкту. Методи математичної статистики. Класифікація методів виявлення змін. Помилки першого і другого роду в оцінці ефективності алгоритмів виявлення. Рівень значущості і потужність критерію. Статистичні тести. Критерії відповідності та однорідності. Критерій хі-квадрат. Критерії згоди. Критерій Колмогорова-Смірнова. Критерії оцінювання однорідності Вілкоксона-Манна-Уїтні. Параметричний метод реєстрації змін. Контрольні карти. Контрольні карти Шухарта, CUSUM. Виявлення DDoS-атак із застосуванням алгоритму CUSUM. Розподілене вторгнення. Три основні групи методів виявлення DDoS-атак. Виявлення DDoS-атак на основі відповідності між з'єднаннями, що встановлюються і закриваються. Вибір параметрів алгоритму CUSUM. Моніторинг різних IP-адрес у вхідному трафіку. Непараметричні багатовимірні CUSUM тести для швидкого виявлення DoS-атак в комп'ютерних мережах. Непараметричний багатовимірний CUMSUM алгоритм. Непараметричні методи. Контрольні карти EWMA. Критерії аномальної поведінки та їх практичне застосування. Відсоткове відхилення. Ентропія. Методи описової статистики. Показник активності. Розподіл активності в записах аудиту. Вимірювання категорій. Порядкові виміру. Пошук і оцінка аномалій мережного трафіку на основі циклічного аналізу. Перевірка циклів з точки зору статистичної значущості. Комбінування і проектування циклів в майбутнє. Виявлення аномалій методом головних компонент. Сингулярний спектральний аналіз. Метод головних компонент і виявлення аномалій у великих розподілених системах. Переваги та недоліки статистичних методів. Проєктування систем виявлення вторгнень із застосуванням статистичних методів виявлення аномальної поведінки мережного трафіку.

Застосування методів кратномасштабного аналізу в системах виявлення вторгнень. Основи теорії вейвлетів. Неперервне вейвлет-перетворення. Дискретне вейвлет-перетворення. Алгоритм Малла. Аналіз методів

виявлення аномалій мережного трафіку на основі вейвлет. Алгоритм виявлення аномалій методом дискретного вейвлет-перетворення. Алгоритм виявлення аномалій за критерієм Фішера для викидів дисперсій. Алгоритм виявлення аномалій на основі критерію Кохрана–Кокса. Алгоритм виявлення аномалій за критерієм Фішера для викидів середніх значень. Вибір порогів виявлення. Дискретне вейвлет-пакетне перетворення. Виявлення DoS- і DDoS-атак методами мультифрактального аналізу. Фрактальні властивості телекомунікаційного трафіку. Виявлення DoS- і DDoS-атак методом мультифрактального аналізу. Проєктування систем виявлення вторгнень із застосуванням методів кратномасштабного аналізу для виявлення аномальних викидів мережного трафіку.

Використання методів інтелектуального аналізу даних при проєктуванні підсистем систем виявлення вторгень. Методи Data Mining. Метод опорних векторів. Виявлення аномалій трафіку із застосуванням нейронних мереж. Виявлення аномалій мережної активності із застосуванням апарату штучних нейронних мереж. Застосування нейронних мереж в задачах виявлення вторгнень. Архітектурні рішення СВВ. Результати експериментів. Методи штучного інтелекту в задачах забезпечення безпеки комп'ютерних мереж. Багатоагентні системи. Системи аналізу захищеності. Методи штучних імунних систем і нейронних мереж для виявлення комп'ютерних атак. Побудова штучної імунної системи для виявлення комп'ютерних атак. Метод функціонування імунних нейромережних детекторів. Алгоритм функціонування системи виявлення вторгнень на основі штучних імунних систем і нейронних мереж. Візуальний аналіз даних. Аналіз методів візуалізації.

Визначення комп’ютерного вірусу на основі модельного підходу. Моделі на основі абстрактних «обчислювачів». «Екзотичні» віруси. Міфічні віруси. Batch-віруси. Віруси в початкових текстах. Графічні віруси. Віруси в інших операційних системах. Віруси в UNIX-подібних системах. Віруси для мобільних телефонів. Інша вірусна «екзотика». Поширення вірусів. Епідемії мережних worm-вірусів. Проста SI-модель експоненціального розмноження. SI-модель розмноження в умовах обмеженості ресурсів. SIS-модель примітивного протидії. SIR-модель кваліфікованої боротьби. Інші моделі епідемій. Моделювання заходів пасивної протидії. Моделювання «контр worm-вірусу». Епідемії поштових worm-вірусів, файлових і завантажувальних вірусів. Епідемії мобільних worm-вірусів.

Виявлення комп’ютерних вірусів. Аналіз непрямих ознак. Прості сигнатури. Контрольні суми. Питання ефективності. Вибір файлових позицій. Фільтр Блума. Метод половинного ділення. Розбиття на сторінки.

Використання сигнатур для детектування поліморфних вірусів. Апаратне трасування. Емуляція програм. Протидія емуляції. «Глибина» трасування і емуляції. Аналіз поліморфних вірусів і їх класифікація. Метаморфні віруси і їх детектування. Етап «виділення та збору характеристик». Етап «обробки і аналізу». Аналіз статистичних закономірностей. Евристичні методи детектування вірусів. Виділення характерних ознак. Логічні методи. Синтаксичні методи. Методи на основі формули Байеса. Методи, які використовують штучні нейронні мережі. Концепція сучасного антивірусного детектора. Боротьба з вірусами без використання антивірусів. Файлові «ревізори». Політики розмежування доступу. Криптографічні методи. Гарвардська архітектура ЕОМ. Перспективи розвитку і використання комп'ютерних вірусів. Віруси як «кіберзброя». Корисні застосування вірусів. Засоби і методи захисту від програмних закладок. Проєктування систем захисту інформації з використанням «приманок» (honeypots, honeynet).

Список рекомендованої літератури

1. Закон України «Про основні засади забезпечення кібербезпеки України» (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403) {Із змінами, внесеними згідно із Законом № 2469-VIII від 21.06.2018, ВВР, 2018, № 31, ст.241}

2. Міжнародний стандарт ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity: [Електронний ресурс]. – Режим доступу: https://webstore.iec.ch/preview/info_isoiec27032%7Bed1.0%7Den.pdf.

3. National Institute of Standards and Technology (NIST). (2010a). Guide to Aplying the Risk Management Framework to Federal Information Systems, NIST Special Publication 800-37.

4. National Institute of Standards and Technology (NIST). (2010b). Security and Privacy Controls for Federal Information Systems and Organizations, Building Effective Security Assessment Plans, NIST Special Publication 800-53A.

5. Савенко О.С. Теорія та практика створення розподілених систем виявлення зловмисного програмного забезпечення в локальних комп’ютерних мережах / Дис. на здобуття наук. ступеня докт. техн. наук за спеціальністю 05.13.05 – комп’ютерні системи та компоненти. – Львів. Національний університет «Львівська політехніка». – 2019.

5 Методологічні основи створення інформаційних систем і технологій

Методи розробки моделей інформаційних систем. Технологія структурного аналізу і проєктування інформаційних систем, стандарт SADT. Технологія IDEF (Icam Definition). Застосування діаграми потоків даних Data Flow Diagrams для створення моделей інформаційних систем. Діаграми «сутність–зв'язок» (Entity-Relationship Diagrams). Діаграми переходів станів (State Transition Diagrams). Стратегії розробки інформаційних систем.

Моделювання і моделі інформаційних систем. Поняття моделі і моделювання. Метод "знизу-догори". Метод "згори-донизу". Принципи "дуалізму" і багатокомпонентності. Використання моделей при створенні інформаційних систем. Каскадна модель інформаційних систем. Поетапна (ітераційна) модель з проміжним контролем. Спіральна модель. Автоматизована система моделювання. Класифікація моделей інформаційних систем. Інформаційна (концептуальна) модель інформаційних систем. Логічна модель (модель проектування) інформаційних систем. Функціональна модель інформаційних систем.

Процес побудови задачі моделювання. Моделювання процесів інформаційної системи. Формалізація множин параметрів модельованої інформаційної сиастеми. Побудова алгоритмічної моделі інформаційної системи. Вибір моделі обчислення. Вибір апаратного забезпечення реалізації інформаційної системи. Здійснення симуляції моделі системи. Перевірка/тестування моделі інформаційної системи. Модельно-орієнтоване проектування програмних систем.

Суть технологій аналізу даних в інформаційних системах. Поняття інтелектуального аналізу даних. Етапи та методи знаходження нових знань та їх аналізу. Засоби програмної підтримки аналізу даних.

Сховище даних та OLAP технології. Концепція сховищ даних. Технології побудови сховищ даних. Вітрини та кіоски даних. OLAP-технології. Основні архітектури OLAP-систем.

Нейрокомп'ютерні технології та мережі як засоби аналізу даних в інформаційних системах. Поняття та можливості нейрокомп'ютерних технологій. Архітектура нейронних мереж. Програмні та апаратні засоби реалізації нейрокомп'ютерних технологій аналізу даних.

Аналіз даних для підтримки прийняття рішень інформаційних систем на основі асоціативних правил та дерев рішень. Основні поняття теорії асоціативних правил. Дерева рішень – загальні принципи технології.

Еволюційні технології та генетичні алгоритми аналізу даних.

Концептуальні засади еволюційної теорії. Основні положення теорії генетичних алгоритмів. Моделі генетичних алгоритмів. Мурашині алгоритми та генетичне програмування.

Нечіткі методи аналізу даних. Концепція нечітких обчислень. Нечітка логіка в системах Data Mining. Методи кластеризації даних. Алгоритми машинного навчання.

Список рекомендованої літератури

1. Методологія інформаційних систем та баз даних: теоретичний і практичний підходи : навч. посібник / уклад. Ю.О. Ушенко, М.Л. Ковальчук, М.С. Гавриляк, А.Л. Негрич. – Чернівці : Чернівецький нац. ун-т ім. Ю. Федьковича, 2021. 240 с. ISBN 978-966-423-641-3

2. Додонов О. Г., Коваль О. В., Глоба Л. С., Бойко Ю. Д. Комп'ютерне моделювання інформаційно-аналітичних систем: монографія. Київ: ІПРІ НАН України, 2017. 239 с.

3. Ajit Singh, Ms. Anamika. Object Oriented Modeling and Design Using UML: 2nd Edition. ISBN-13 979-8846348363. 2022. P. 153

4. Jason Bell. Machine Learning: Hands-On for Developers and Technical Professionals, Second Edition, Wiley. 2020.

5. Richard J. Roiger. Just Enough R! An Interactive Approach to Machine Learning and Analytics, CRC Press. 2020.