**ТЕМАТИКИ НАУКОВО-ДОСЛІДНИХ РОБІТ**

**кафедра інформаційної безпеки**

**2019-2020**

|  |  |
| --- | --- |
| ПІБ викладача | **125 «Кібербезпека»** |
| **бакалаври** | **магістри** |
| **д.т.н., професор** **Архипов Олександр Євгенійович** | 1. Моделювання інформаційних ризиків.
2. Єволюція методології захисту інформації (за результатами аналізу матеріалів міжнародних стандартів безпеки інформації).
3. Основні стратегії застосування ризик-орієнтованого підходу до побудови СЗІ.
4. Методи обробки експертних даних / Технології обробки даних в задачі експертного оцінювання кількісних показників.
5. Групові оцінки параметрів лінійних регресивних моделей.
6. Оцінювання якості ідентифікації математичних моделей.
7. Імітаційне оцінювання точності параметричної ідентифікації математичних моделей.
 |
| **к.т.н., доцент****Литвинова Тетяна Василівна** | 1.Система захисту інформації організації від несанкціонованого доступу внутрішнього порушника2.Система захищеного електронного обміну інформації в організації3.Захист конфіденційної інформації в приватних організаціях |  Комплексна система захисту інформації організації |
| **к.ек.н., доцент****Ткач Володимир****Миколайович** | * Методи аналізу і обробки великих даних
* Системи глибинного аналізу великих даних, отриманих з мобільних пристроїв
* Виявлення аномалій в SIEM-системах
* Системи розпізнавання образів та комп’ютерне бачення
* Нейро-нечіткі моделі розпізнавання графічної інформації
 |
| **к.т.н., доцент****Барановський Олексій Миколайович** | 1. APT-атаки и их исследования2. Кибербезопасности критической инфраструктуры3. Безопасность блокчейн технологии и использование блокчейн в средствах безопасности4. Информационные потоки в сети Интернет и их анализ5. Тесты на проникновение, компьютерная криминалистика.6. Обработка инцидентов информационной безопасности |
| **к.т.н., доцент****Демчинський Володимир****Васильович** | Аналіз ринків Bitcoin (тенденції руху грошової маси).-Аналіз текстів та виявлення статистик натуральних мов.-Обчислення над зашифрованими даними.-Поведінка статистик в хвостах нормального розподілу (фінанси, ISO9000, ризики, трафіки...).-Моделі самоподібності, спрощена (наближена) генерація Self-similar трафіка.-Генерація трафіка с заданими характеристиками, оцінка продуктивності, QoS.-Мережна система керування доступом (NAC) та кореляція статистик трафіків.-Задача кластеризації в системах авторизації (групи, ролі..).-Алгоритм пошуку для HRU-подібних моделей, формальний пошук вразливостей (аудит) в ACL.-Алгебра віртуалізації.-Шаблони (сігнатури) пошуку вразливостей ПЗ.-Моделювання протокола, контекст-аналіз протокола.-Статистики при аналізі аномального трафіка, статистики та аналіз аномалій.-Аналіз стегоканалів.-Приховані канали в мережних протоколах та їх знешкодження.-Ідентифікація даних в захищеному тунелі.-Аналіз трафіка в VPN та маскування характеристик трафіка.-Аналіз та вдосконалення протокола Tor.-Реалізація сервіса неспростовності в критичній інфраструктурі.-Зхист протоколів маршрутизації (OSPF, HSRP).-Механізми захисту в архітектурі DRM-систем.-Механізми захисту в архітектурі DLP-систем.-Застосування ADFS.-Захист терміналів загального користування.-Суб`єктивні фактори автентифікації.-Політика персонального мережного екрана. |
| **к.т.н.****Ільїн Микола****Іванович** | 1.Моделі та методи класифікації шкідливого програмного забезпечення (malware detection and classification)1. 2. Моделі та методи виявлення мережевих вторгнень (network intrusion detection systems)
2. 3. Моделі та методи автоматичного пошуку вразливостей програмного забезпечення (smart fuzzing)

4.Моделі та методи виявлення та протидії новим загрозам інформаційної безпеки (APT mitigation) |
| **к.т.н., доцент****Коломицев Михайло****Володимирович** | Захист інформації в базах даних. Захист інформації в автоматизованих інформаційних системах. Захист програмного забезпечення. |
| **к.т.н., доцент****Родіонов Андрій****Миколайович** | 1. Розподілені обчислення2. Розподілені системи3. Великі данні4. Машинне навчання |
| **к.т.н., доцент****Стьопочкіна Ірина Валеріївна** | 1. Підвищення ефективності попередження витоку конфіденційної інформації підприємства на основі технології DLP
2. Особливості архітектури інформаційної системи підприємства та впровадження SIEM рішень
3. Цифрова імунна система із використанням SOC (security operation centers)
4. Антивірусні техніки в розробці цифрової імунної системи
5. Протидія атакам на основі соціальної інженерії
6. Передбачувальна аналітика подій безпеки із використанням SIEM
7. Фрактальні показники в задачах оцінки захищеності інформаційної системи
8. Принципи дії атак на інтернет речей та засоби протидії
9. Протидія інтелектуальним видам шкідливого ПЗ
10. Моделювання односторонніх процесів дифузії та тепломасообміну
11. Моделювання фізичних процесів в умовах великої розмірності модельної системи
12. Підвищення ефективності обчислень при моделюванні фізичних процесів
 |
| **д.т.н., професор Качинський Анатолій Броніславович** | 1. Математичне моделювання оцінок стану захищеності складних систем
2. Аналіз структур складних систем безпеки
3. Математичне моделювання систем забезпечення безпеки
4. Розробка основних системних принципів і функцій діяльності системи забезпечення безпеки

5. Розробка кількісних оцінок складності систем безпеки за допомогою методів самоорганізованої критичності1. Аналіз нелінійних моделей складних систем безпеки
2. Системний аналіз закономірностей реалізації загроз
3. Аналіз мереж небезпечних подій
4. Діахронний аналіз конфліктних ситуацій
5. Розробка математичних методів ранжування загроз складних систем безпеки
6. Кількісна оцінка стійкості систем безпеки за допомогою граничних значень
7. Розробка статистичних методів оцінки ризику
8. Розробка експертних методів оцінки ризику
9. Розробка стохастичних методів керування стратегічними ризиками
10. Розробка кількісних методів визначення величини прийнятного ризику
11. Ухвалення рішень в умовах ризику: стохастичні та експертні методи
12. Розробка кількісних оцінок регіональних загроз
13. Розробка методів системного аналізу та розробки сценаріїв політики безпеки
14. Стратегічне планування систем забезпечення безпеки за допомогою *SWOT*-аналізу
15. Застосування методів машинного навчання для оцінки небезпечних ситуацій.
 |
| **к.ф.-м.н., доцент Грайворонський Микола Владленович** | * Дослідження і удосконалення моделей керування доступом (рольова політика, тематичний доступ, типізована матриця доступу) і практичне застосування (КСЗІ, програмні засоби захисту)
* Дослідження і удосконалення моделей безпеки сучасних операційних систем (різні дистрибутиви Linux, Android, перспективні розробки з відкритим кодом)
* Дослідження і моделювання функціювання шкідливих програм (вірусів, експолоітів, руткітів тощо)
* Розробка КСЗІ для певних типових ІКС (за вибором) — переважно, тема для заочників
 | * Розвиток існуючих або розробка нових моделей керування доступом, моделей систем захисту, моделей процесів захисту у контексті кібербезпеки (переважно для магістрів)
* Дослідження і удосконалення моделей безпеки сучасних операційних систем (різні дистрибутиви Linux, Android, перспективні розробки з відкритим кодом) — (переважно для магістрів)
* Дослідження і моделювання функціювання шкідливих програм (вірусів, експолоітів, руткітів тощо)
* Застосування машинного навчання у системах виявлення аномальної поведінки користувачів, поведінкового аналізу програмного коду, тощо.
* Розробка методик застосування міжнародних стандартів з безпеки та(або) їх зіставлення з вітчизняними стандартами (переважно для магістрів-професіоналів)
* Розробка і удосконалення засобів захисту для операційних систем (переважно для магістрів-професіоналів )
 |
| **к.ф-м.н., доцент****Орєхов Олександр Арсенійович** | * - дослідження механізмів захисту в сучасних системах автентифікації та авторизації та розробка методів їх вдосконалення
 |  |
| **к.т.н., доцент Гальчинський Леонід Юрійович** | * Дослідження вразливостей рівня UEFI та розробка методів їх зниження
* Розробка комплексної системи захисту інформації для визначених ІС
* Методи та моделі ідентфікації фішингу
* Дослідження системних механізмів дії зловмисних програм
* Непараметричні методи оцінки рівня інформаційної безпеки для організацій у визначених галузях
 |