Силабус освітнього компонента
Програма навчальної дисципліни

Методи аналізу артефактів систем безпеки

Шифр та назва спеціальності
125 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій (320)

Освітня програма
Кібербезпека

Кафедра
Кібербезпеки (328)

Рівень освіти
третій (осітньо-науковий)

Тип дисципліни
Вибіркова,

Семестр
4

Мова викладання
Українська

Викладачі, розробники

МІЛОВ Олександр Володимирович

oleksandr.milov@khpi.edu.ua
Доктор технічних наук, професор кафедри кібербезпеки НТУ «ХПІ».

Автор понад 200 наукових та навчально-методичних праць. Науковий керівник з захищених кандидатських робіт, гарант освітньо-професійної програми другого (магістерського) рівня вищої освіти. Провідний лектор з дисциплін: «Математичні основи криптології та криптоаналіз», «Структури даних», «Промисловий та офісний шпіонаж» , «Цифрова криміналістика», у студентів бакалавріата та магістратури, Розділ «Методологія наукової та педагогічної діяльності в науках кіберзахисту» для аспірантів.
Детальніше про викладача на сайті кафедри

ХВОСТЕНКО Владислав Сергійович

vladyslav.khvostenko@khpi.edu.ua
Кандидат економічних наук, доцент кафедри кібербезпека НТУ «ХПІ».

Автор більше 30 публікацій: з них 3 монографії у співавторстві 1 посібник з грифом. Провідний лектор з дисциплін: «Інтелектуальна власність систем безпеки», «Правове регулювання кібербезпеки».
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Вивчення дисципліни спрямовано на формування світогляду, розвитку інтелекту, ерудиції, формування професійних компетенцій зі спеціальності кібербезпека; оволодіння методологією наукової діяльності, теоретичними основами сучасних комп'ютерних методів наукових досліджень та інтелектуальними технологіями аналітичної інформації.

Мета та цілі дисципліни

Формування у аспірантів системи теоретичних знань і практичних навичок з основ, принципів та методів аналізу артефактів систем безпеки, формування навичок до розробки технологій та інструментальних засобів аналізу, прогнозування й інформаційно-аналітичної підтримки процесів прийняття рішень щодо забезпечення безпеки інформації.

Формат занять

Лекції, лабораторні роботи, самостійна робота, індивідуальне завдання, консультації.
Підсумковий контроль – залік.

Компетентності

ІК Здатність продукувати нові ідеї, розв'язувати комплексні проблеми професійної та/або дослідницько-інноваційної діяльності у сфері кібербезпеки та захисту інформації, застосовувати методологію наукової та педагогічної діяльності, а також проводити власне наукове дослідження, результати якого мають наукову новизну, теоретичне та практичне значення.
ЗК-1.Здатність до професійного спілкування іноземною мовою.
ЗК-4. Здатність працювати в міжнародному науковому просторі, розробляти та управляти науковими проектами.
СК-1. Здатність до застосування сучасних інформаційних і безпекових технологій у сфері захисту інформації, створення комплексних систем захисту інформації.
СК-3. Здатність розробляти процеси життєвого циклу інформаційних технологій, виявляти технічні канали витоку інформації, застосовувати засоби захисту інформації.
СК-5. Здатність розробляти та реалізовувати нові конкурентоздатні ідеї в галузі захисту інформації, використовувати методологічні та організаційно-технічні основи забезпечення безпеки.

Результати навчання

РН-1. Вміння формувати і аргументовано відстоювати власну думку з різних проблем філософії науки та методології наукового пізнання, бути критичним і самокритичним.
РН-2. Вміння вести дискусії, здійснювати публічні промови, робити повідомлення і доповіді з питань дисертаційного дослідження, аргументовано викладати власну точку зору державною та іноземною мовами.
РН-3. Вміння читати оригінальну наукову літературу на іноземній мові, опрацьовувати та оформляти інформацію. Вміння та навики працювати з сучасними бібліографічними і реферативними базами даних, а також наукометричними платформами (наприклад, Scopus, Web of Science, Web of Knowledge та ін.).
РН-4. Знання, розуміння, вміння та навички використання правил цитування та посилання на використані джерела, правил оформлення бібліографічного списку, розуміння змісту і порядку розрахунків основних кількісних наукометричних показників ефективності наукової діяльності (індекс цитування, індекс Гірша (h-індекс), імпакт-фактор (ІФ, або IF)).
РН-5. Вміння та навички критично сприймати та аналізувати існуючі наукові теорії та ідеї, шукати власні шляхи вирішення проблеми та завдань, проводити критичний аналіз власних матеріалів, генерувати власні нові ідеї, приймати обґрунтовані рішення.
РН-8. Вміння використовувати кількісні і якісні методи для проведення наукових досліджень.
РН-9. Вміння та навички спілкуватися в діалоговому режимі з широкою науковою спільнотою та громадськістю в галузі наукової та/або професійної діяльності з метою обговорення дискусійних питань, результатів досліджень, узгодження дій і спільної роботи на конференціях, симпозіумах, наукових семінарах, доводити результати досліджень та інновацій до колег, публічно представляти, захищати результати своїх досліджень, обговорювати їх і дискутувати з науково-професійною спільнотою, використовувати сучасні засоби візуальної презентації результатів дослідження..
РН-10. Володіння предметною базою знань та сучасними техніками дослідження, здатність створювати та інтерпретувати нові знання.
РН-11. Вміння розробляти проекти наукових досліджень та моделювати їх структуру, застосовуючи різні способи подання статистичної інформації та результатів.

РН-12. Вміння оцінювати конкурентоспроможність отриманих результатів.
РН-13. Вміння узагальнювати і критично оцінювати результати, отримані вітчизняними і зарубіжними дослідниками.
РН-14. Вміння приймати обґрунтовані рішення, бути здатним їх оцінювати та забезпечувати якість виконуваних робіт.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 20 год., лабораторні роботи – 20 год., самостійна робота – 80 год.

Передумови вивчення дисципліни (пререквізити)

Вища математика, Розробка та аналіз алгоритмів, Конкретна математика, Штучний інтелект та експертні системи, Основи програмування, Комбінаторна оптимізація.

Особливості дисципліни, методи та технології навчання

Аспірант зобов'язаний відвідувати всі заняття згідно розкладу, не спізнюватися. Дотримуватися етики поведінки. Працювати з навчальною та додатковою літературою, з літературою на електронних носіях і в Інтернеті. При пропуску лекційних занять проводиться усна співбесіда за темою. З метою оволодіння необхідною якістю освіти з дисципліни потрібно відвідуваність і регулярна підготовленість до занять. Без особистої присутності аспіранта підсумковий контроль не проводиться.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Аналіз артефактів у системах безпеки.
Комп'ютерна безпека. Збір даних. Машинне навчання. Огляд рішень для кібербезпеки: рішення для проактивної безпеки, рішення для реактивної безпеки (виявлення неправомірного використання/підпису, виявлення аномалій, гібридне виявлення, виявлення сканування, модулі профілювання). Класифікація методів аналізу артефактів (набори даних: екземпляри та змінні, контрольоване навчання: класифікація та регресія, неконтрольоване навчання: кластеризація та виявлення закономірностей). Навчання дереву рішень (кластеризація k-середніх, навчання правил асоціації). Аналіз послідовності та епізоду (інтелектуальний аналіз послідовності, аналіз епізоду, інші підходи). Якість результуючих моделей (вимір продуктивності класифікатора, перехресна перевірка, бритва Оккама).
Тема 2. Класичні парадигми машинного навчання для аналізу артефактів.
Основи методів машинного навчання з учителем (класифікація правил асоціації, штучна нейронна мережа, машини опорних векторів, дерева рішень, байєсовська мережа, прихована марківська модель, фільтр Калмана, початкове завантаження, бегінг та AdaBoost, випадковий ліс). Популярні методи машинного навчання без вчителя (кластеризація k-середніх, максимальне очікування, k-найближчий сусід, SOM ANN, аналіз основних компонентів, кластеризація підпростору). Удосконалення методів машинного навчання (нові алгоритми машинного навчання, повторна вибірка, методи вибору ознак, методи оцінки, перехресна перевірка). Проблеми аналізу артефактів (моделювання великомасштабних мереж, виявлення загроз, мережна динаміка та кібератаки, збереження конфіденційності при інтелектуальному аналізі даних). Проблеми машинного навчання (навчання з учителем та навчання без вчителя) (методи онлайн-навчання для динамічного моделювання мережевих даних, моделювання даних зі спотвореним розподілом класів для обробки виявлення рідкісних подій, вилучення ознак для даних з характеристиками, що розвиваються). Напрями досліджень (розуміння фундаментальних проблем методів машинного навчання в кібербезпеці, додаткове навчання в кіберінфраструктурах, вибір/витяг функцій для даних з характеристиками, що розвиваються, інтелектуальний аналіз даних зі збереженням конфіденційності)Колективність та спадкоємність у науковій роботі.
Тема 3. Машинне навчання для виявлення аномалій.

Виявлення аномалій. Машинне навчання у системах виявлення аномалій. Додатки машинного навчання виявлення аномалій (виявлення аномалій з урахуванням правил, нечіткі правила, IHC, методи опорних векторів, навчання з урахуванням найближчих сусідів, прихована марківська модель, фільтр Калмана). Неконтрольоване виявлення аномалій (виявлення аномалій на основі кластеризації, випадкові ліси, аналіз основних компонентів/підпростір, однокласова контрольована векторна машина). Теоретична інформація. Інші методи машинного навчання, що застосовуються для виявлення аномалій. Контрольоване навчання виявлення неправомірного використання/подписи. Виявлення неправильного використання/підпису. Машинне навчання для виявлення неправомірного використання/підпису. Додатки машинного навчання виявлення зловживань (аналіз підписи з урахуванням правил: класифікація з допомогою правил асоціації, з урахуванням нечітких правил). Штучна нейронна мережа. Машини опорних вектори. Генетичне програмування. Дерево рішень та CART (методи дерева рішень, застосування дерева рішень при виявленні зловживань, CART). Байєсовська мережа, байєсівський мережевий класифікатор, наївний байєсовський алгоритм.

Тема 4. Машинне навчання для гібридного виявлення, виявлення сканування та профілювання мережевого трафіку.

Гібридне виявлення. Машинне навчання у гібридних системах виявлення вторгнень. Додатки машинного навчання в гібридному виявленні вторгнень (система виявлення аномалій-неправомірного використання послідовності, правила асоціації в аналізі та видобутку даних аудиту, система виявлення неправильного використання аномалії послідовності, паралельна система виявлення, комплексна змішана система виявлення, інші гібридні системи вторгнень) Сканування та виявлення сканування. Машинне навчання у виявленні сканування. Програми машинного навчання виявлення сканування. Інші методи сканування за допомогою методів машинного навчання. Профілювання мережного трафіку та пов'язані з ним знання про мережний трафік. Машинне навчання та профільування мережевого трафіку. Програми для інтелектуального аналізу даних та машинного навчання у профілюванні мережі. Інші методи профілювання та застосування.

Тема 5. Аналіз артефактів збереження конфіденційності.

Методи збереження конфіденційності у PPDM (позначення, збереження конфіденційності при інтелектуальному аналізі даних). Робочий процес PPDM (Вступ до робочого процесу PPDM, алгоритми PPDM, оцінка продуктивності алгоритмів PPDM). Додатки інтелектуального аналізу даних та машинного навчання в PPDM (правила асоціації для збереження конфіденційності, дерево рішень для збереження конфіденційності, байєсовська мережа для збереження конфіденційності, KNN для збереження конфіденційності, кластеризація k-середніх для збереження конфіденційності, інші методи.

Тема 6. Моделювання та аналіз процесів.

Вибух даних. Обмеження моделювання. Процес майнінгу. Аналіз прикладу журналу. Play-in, Play-out та Replay. Тенденція. Перспектива. Мистецтво моделювання. Моделі процесів (системи переходу, мережі Петрі, мережі робочих процесів, YAWL, нотація моделювання бізнес-процесів (BPMN), ланцюжки процесів, що керуються подіями (EPC), каузальні мережі). Аналіз процесів з урахуванням моделей (перевірка, аналіз продуктивності, обмеження аналізу з урахуванням моделей). Від журналів подій до моделей процесів. Виявлення процесу. Постановка задачі. Джерела даних. Журнал подій. XEC. Зведення реальності до журналів подій. Простий алгоритм виявлення процесів (основна ідея, алгоритм, обмеження α-алгоритму, облік життєвого циклу транзакцій). Нове відкриття моделей процесів. Проблеми (зміщення уявлення, шум і неповнота, чотири конкуруючі критерії якості, вибір правильного двовимірного зрізу тривимірної реальності). Розширені методи виявлення процесів. Огляд характеристики: репрезентативне усунення, здатність характеристики справлятися з шумом, передбачуване поняття повноти, підхід, що використовується. Евристичний аналіз (перегляд причинно-наслідкових мереж, вивчення графа залежностей, вивчення поділу та об'єднання). Генетичний процес майнінгу. Інтелектуальний аналіз на основі регіонів (навчання систем переходу, виявлення процесів із використанням регіонів на основі стану, виявлення процесів із використанням регіонів на основі мови). Історична перспектива.

Тема 7. Нові виклики в галузі кібербезпеки.

Виникаючі кіберзагрози (загрози від шкідливих програм, погрози від ботнетів, погрози від кібервійн, погрози від мобільного зв'язку, кіберзлочини). Моніторинг мережі, профіль та збереження конфіденційності (збереження конфіденційності вихідних даних, збереження

конфіденційності в алгоритмах моніторингу та профілювання мережевого трафіку, збереження конфіденційності даних моніторингу та профілювання, регулювання, закони та збереження конфіденційності, збереження конфіденцій). Нові проблеми в області виявлення вторгнень (уніфікація існуючих систем виявлення аномалій, виявлення аномалій мережного трафіку, проблема незбалансованого навчання та розширені метрики оцінки для IDS, надійні набори даних оцінки або інструменти генерації даних, проблеми конфіденційності при виявленні аномалій мережі).

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Знайомство з аналітичною платформою "Deductor".
Тема 2. Пошук асоціативних правил.
Тема 3. Розпізнавання образів даних (НМ Хеммінгу).
Тема 4. Кластерна обробка даних (НМ Кохонена).
Тема 5. Алгоритми розпізнавання прецедентів.
Тема 6. Фільтрування даних (Фільтр Калмана).
Тема 7. Парціальна обробка даних.

Самостійна робота

Самостійна робота аспіранта є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи аспіранти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних робіт, заліків та іспитів. Аспірантам також рекомендуються додаткові матеріали (відео, статті) для самостійного вивчення та аналізу.

Неформальна освіта

В рамках неформальної освіти згідно відповідного Положення (http://surl.li/pxssv), освітня компонента або її окремі теми можуть бути враховано у разі самостійного проходження професійних курсів/тренінгів, отримання громадянської освіти, онлайн освіти, професійного стажування тощо.
За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

Література та навчальні матеріали

Основна література

1. Josh Patterson and Adam Gibson. Deep Learning // Josh Patterson and Adam Gibson. O'Reilly Media, Inc., 2017. – 532 p. URL: https://www.purestorage.com/content/dam/pdf/en/white-papers/protected/wp-oreilly-deep-learning.pdf
2. Trask A.W. Grokking Deep Learning // Trask A.W. Manning Publications Co., 2019. – 335 p. URL: https://edu.anarcho-copy.org/Algorithm/grokking-deep-learning.pdf
3. Jojo Moolayil. Learn Keras for Deep Neural Networks. A Fast-Track Approach to Modern Deep Learning with Python. Apress Berkeley, CA, 2019. 192 p. URL: http://45.32.33.124/ebook/python/Learn%20Keras%20for%20DL.pdf
4. КІБЕРБЕЗПЕКА: ЛАБОРАТОРНИЙ ПРАКТИКУМ З ОСНОВ КРИПОГРАФІЧНОГО ЗАХИСТУ / С.П. Євсеєв, О.В. Мілов, О.Г. Король – Львів: «Новий Світ- 2000», 2020 . – 241 с. URL: https://drive.google.com/file/d/14fS7nVtD3xieqA8f_rFBiiqcr96_piTe/view?usp=sharing
5. Євсєев С.П. Кібербезпека: основи кодування та криптографії/ С.П. Євсеєв, О.В. Мілов, С.Е. Остапов, О.В. Сєвєрінов. – Харків: Вид. "Новий Світ-2000", 2023. – 657 с. URL: https://drive.google.com/file/d/1694khGjEN1-2PvXFQY27IPPc8Sn4BsLC/view?usp=sharing

Додаткова література

6. Любунь З. М. Основи теорії нейромереж / З. М. Любунь /: Текст лекцій. – Львів: Видавничий центр ЛНУ імені Івана Франка, 2007. –142 с. URL: https://f.eruditor.link/file/236389/

7. Liubun Z. Hover Signal-Profile Detection / Liubun, V. Mandziy, H. Klein, O. Karpin, V. Rabyk // Proceedings of the XV International Scientific and Technical Conference “Computer Science and Information Technologies” – 2020. P. 7 – 10. (Scopus)
8. Бобало Ю.Я., Горбатий І.В. (ред.) Інформаційна безпека. Навчальний посібник. — Львів : Видавництво Львівської політехніки, 2019. — 580 с. — ISBN 978-966-941-339-0. URL: https://drive.google.com/file/d/1xVAWLoZMLes_XiXEd7E_6KT-QA4w2Hw7/view?usp=sharing
9. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. URL: http://monograph.com.ua/pctc/catalog/view/64/52/231-1
10. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p. URL: http://monograph.com.ua/pctc/catalog/view/978-617-7319-72-5/978-617-7319-72-5/746-2
11. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. – Kharkiv: PC TECHNOLOGY CENTER, 2022. – 196 p. URL: http://monograph.com.ua/pctc/catalog/view/978-617-7319-57-2/117/419-2.

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
•лабораторні роботи: 20% семестрової оцінки;
•самостійна робота: 30% семестрової оцінки;
•індивідуальне завдання: 20% семестрової оцінки;
•залік: 30% семестрової оцінки.

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D
60–63	Задовільно	E
35–59	Незадовільно (потрібне додаткове вивчення)	FX
1–34	Незадовільно (потрібне повторне вивчення)	F

Норми академічної етики і політика курсу

Здобувач вищої освіти повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту. Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

Погодження

Силабус погоджено

28.08.2024 — Завідувач кафедри
Сергій ЄВСЕЄВ

28.08.2024 — Гарант ОП
Олександр МІЛОВ