галузі, створює сприятливі умови щодо професійного розвитку викладачів, побудови індивідуальної освітньої траєкторії, визначення власних освітніх цілей та їх досягнення, реалізації принципу «освіти впродовж життя».

3. Питання запровадження технологій дистанційного навчання в систему підвищення кваліфікації викладачів є актуальними, дискусійними та потребують подальшого поглибленого вивчення.

Посилання

1. Маслов В. Енциклопедія освіти [голов. ред. В. Г. Кремень]. – К.: Юрінком Інтер, 2008.
2. Биков В.Ю. Моделі організаційних систем відкритої освіти: монографія. – К.: Атіка, 2009.
3. Ляхоцька Л. Дистанційне навчання як педагогічна технологія неперервної освіти / Л. Ляхоцька // Педагогічні науки: збірник наукових праць. – Полтава: Вид-во Полтавського педагогічного університету, 2014.
4. Колос К. Р. Система MOODLE як засіб розвитку предметних компетентностей учителів інформатики в умовах дистанційної післядипломної освіти: дис. кан. пед. наук: 13.00.10 «Інформаційно-комунікаційні технології в освіті» / Колос К. Р. – Житомир: Держ. ун-т імені Івана Франка.
5. Ярковий А.О., MOODLE - Електронна Система керування навчальним процесом: Навчальний посібник. Частина І. (дисципліна: Виготовлення презентаційних матеріалів). Київ: ІПДО НУХТ, 2020. 43 с.
6. Положення про дистанційне навчання: Наказ МОН України від 25.04.2013 № 466 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/z0703-13
7. Петренко О.Я., Ярковий А.О. Працюємо в Microsoft Teams: Навчальний посібник. / О.Я. Петренко, А.О.Ярковий – К. ІПДО, 2021. – 59 с.
8. Захар Ольга. Особливості застосування технологій дистанційного навчання в системі підвищення кваліфікації вчителів інформатики [Електронний ресурс]. – Режим доступу: https://science.lpnu.ua/sites/default/files/journal-paper/2019/jun/16829/08-23-27.pdf

ІННОВАЦІЙНІ ПІДХОДИ ПРИ ВИКЛАДАНІ КІБЕРБЕЗПЕКИ У ВИЩИХ НАВЧАЛЬНИХ ЗАКЛАДАХ

Доц., канд. фіз.-мат наук І.А. Петрушко, асистент І.В. Поліщук
ДВНЗ «Ужгородський національний університет», м. Ужгород, Україна

Вступ

Тенденції сучасного ринку праці демонструють зростаючий попит на ІТ фахівців з кібербезпеки. Крім фахових навичок у таких працівників необхідно формувати навички командної роботи, гнучкість у прийнятті рішень, критичне мислення. В даній роботі представлено результати інноваційного

підходу при викладанні одного з курсів циклу кібербезпеки в Ужгородському університеті на прикладі хробака Mirai botnet [1-3]. Mirai botnet є прикладом DDos атаки, яка вражає слабозахищені прилади інтернету речей (IoT).

Мета

Метою даного педагогічного експерименту було застосувати при вивченні хробака Mirai botnet інноваційного підходу:

1) спільно розглянути анатомію даного хробака, на цій основі підготувати таблицю з пустими полями, яку студенти самостійно мають заповнити;

2) розділити студентів на команди, всередині кожної з команд поставити завдання колективно знайти рішення по захисту від хробака (мозговий штурм); також розробити тести по основних поняттях даної теми – 10 питань;

3) командне заповнення таблиці на основі виконаного пошуку;

4) представлення на практичному занятті отриманих результатів, їх обговорення;

5) перехресне розв’язання і обговорення тестів, підготованих студентами.

Результати

Групу студентів було розбито на команди так, щоб інтелектуальний склад кожної з команд був приблизно однаковим. Також, важливо призначити в кожній з команд лідера, який розподіляє завдання відповідно до рівня членів команди, слідкує за станом виконання, а також надає необхідну підтримку. Викладачеві достатньо підтримувати і моніторити лідерів команд. Зазначимо, що такий підхід дає можливість студентам скоординовано шукати методи захисту від хробака Mirai botnet, причому є можливість взяти до уваги різні точки зору, звести їх в єдину цілісну картину – в нашому випадку таблицю. Також, студенти запропонували «підглянути» рішення в області організації інформаційних процесів в живих системах з метою знайти свіжі рішення. Такий підхід називається біоніка. Наприклад найоптимальнішу форма крила деяких літальних апаратів запозичено в комах, адже принципи аеродинаміки однаково діють і на літальний апарат, і на крило комахи [4]. Зазвичай, студенти використовують соціальні мережі для організації комунікацій та систему контроля версіями GitHub для зберігання різних версій проекту.

Розглянемо детальніше аналогії організації інформаційних процесів в живих та технічних системах. Наприклад, виявлення інфекційних агентів:

у живих організмах рецептори на поверхні клітин розпізнають патогени та активують сигнальні шляхи, що вказують на наявність інфекції;

у мережевих системах алгоритми ШІ виявляють аномальну активність мережевих пристроїв або трафіку, і сигналізують про наявність ботнету або кібератаки.

Таблиця 1 – Анатомія Mirai botnet, методи захисту та аналогії з сфери живих організмів

Етап розгортання атаки	Методи захисту/пом'якшення атаки, запропоновані студентами	Процеси аналогічної природи в живих організмах
1	2	3
1. Розвідка: збір IP-адрес. Одна з ключових функцій Mirai - це постійний пошук та збір IP-адрес з веб-камер, маршрутизаторів та інших IoT-пристроїв, які використовують стандартні логіни та паролі за замовчуванням або мають вразливості в програмному забезпеченні.	Зміна стандартних логінів та паролів; оновлення програмного забезпечення; вимикання непотрібних послуг; використання файерволів; використання мережевих рішень безпеки: Intrusion Detection/Prevention Systems (IDS/IPS) або систем контролю доступу (Access Control Systems), щоб виявляти та блокувати аномальну активність; моніторинг мережі на предмет аномальної активності та спроб несанкціонованого доступу; шифрування для всіх з'єднань до вашого пристрою, особливо для важливих і конфіденційних даних; відключення від Інтернету пристроїв, які не потребують постійного підключення до мережі; встановлення обмеження на доступ до мережі; навчання користувачів про правильні методи безпеки-кібергігієна.	Вторгнення молекул у клітину або організм. Наприклад, вірус може використовувати свою оболонку для взаємодії з рецепторами клітини та вбудовування свого генетичного коду в ДНК господаря. Наприклад, вірус СНІДу «хакає» (обманює) імунну систему організму.
2. Перехоплення управління скомпрометованими (зламаними) IoT пристроями	Аналогічно до п.1 таблиці. Регулярний аудит безпеки – пошук вразливостей в системі з метою їх усунення – penetration testing (Kali Linux, Nmap і т. д.). Впровадження BlockChain при авторизації [3].	Паразити різної природи модифікують природні програми поведінки клітин використовуючи вразливості у захисних механізмах організму, щоб отримати доступ і контроль над клітинами або системами організму-господаря; це веде до розвитку різноманітних захворювань або втрати функціональності організму.

Продовження таблиці 1

1	2	3
3. Після успішного захоплення IoT пристроїв, Mirai формує мережу ботів і використовує їх для виконання розподілених атак з відмовою в обслуговуванні (DDoS). Ці атаки можуть спричинити недоступність сервісів в Інтернеті шляхом перенасичення цільового сервера трафіком від ботів.	Аналогічно до п.1 таблиці. Сегментація мережі. Ізоляція скомпрометованих IoT приладів – карантин.	Клітини, вражені вірусами, атакують клітини та системи організму, що може спричинити серйозне захворювання або навіть смерть.
4. Mirai використовує досить прості алгоритми атаки, що дозволяє йому швидко заражати та керувати великою кількістю пристроїв.	Залучення арсеналу ШІ для ефективного розпізнання аномальної активності мережного трафіку. Сегментація мережі, щоб ефективно організувати ізоляцію і відновлення інфікованих кластерів мережі. Налаштування автоматичного резервного копіювання в хмарних сервісах для швидкого відновлення навіть у випадку успішної атаки. Розслідування і документування інцидентів безпеки для оптимізації майбутньої роботи безпекової служби; навчання персоналу навичкам безпечної поведінки в кіберпросторі, а також найпростішим сценаріям реагування на кіберінциденти.	Будова біологічного віруса максимально проста- це просто ДНК в білковій капсулі. ДНК віруса є біологічним чіпом з інформацією, який вбудовується в ДНК господаря, внаслідок чого програму господаря змінено так, що клітина господаря починає клонувати віруси. Вірус не має ні дихання, ні травлення, ні системи відтворення – він простий.
5. Автоматичне оновлення: Однією з особливостей Mirai є його можливість автоматичного оновлення. Він може самостійно оновлюватися за допомогою вбудованого механізму, що дозволяє йому використовувати нові вразливості та методи атаки.	Адміністративно налаштувати періодичне оновлення ПЗ IoT системи (щоб IoT прилади мали ПЗ без багів). Якщо є економічна доцільність, то можна скористатися платними хмарними безпековими послугами Cisco Umbrella, DNA, Meraki, Talos, XDR , і т. д. Ці сервіси автоматизують безперервний процес безпекових заходів. Максимальне застосування туманних обчислень – чим менше трафік ззовні всередину мережі, тим менше імовірність проникнення (збільшення автономності).	Генетичні мутації та механізми рекомбінації ДНК можуть спричиняти зміни в геномі організмів-нападників. Ці зміни можуть призвести до виникнення нових властивостей та стійкості до зовнішніх факторів (резистентність до антибіотиків).

Важливою є і аналогія в механізмах розпізнання атаки:

в живих організмах, імунна система мобілізує відповідь на інфекцію за допомогою сигнальних шляхів та вироблення специфічних антитіл та цитокінів; у мережевих системах аналізатори трафіку та алгоритми машинного навчання обробляють дані для виявлення зловмисних дій та вибору оптимальної стратегії відповіді використовуючи алгоритми нечіткої логіки [5].

Спільна реакція та співпраця:

у живих організмах клітини імунної системи працюють скоординовано для ефективного розпізнавання інфекційної загрози та реакції на неї;

у мережевих системах спільна реакція виявлених пристроїв або користувачів може бути організована через Blockchain -платформу, де рішення приймається на основі консенсусу мережі.

Оновлення та адаптація:

У живих організмах, імунна система може вдосконалюватися та адаптуватися до нових інфекцій шляхом мутацій та пам'яті імунної системи.

У мережевих системах, Blockchain може служити для збереження та оновлення інформації про нові загрози та налаштування безпекових протоколів саме на наявну ситуацію.

Підсумовуючи зазначимо, що не зважаючи на багато спільних рис, технічні системи, на відміну від біологічних, не зданті до самовідворення та передачі спадкової інформації; якісно відрізняється і підхід до кодування сигналів: у живих системах інформація часто кодується у формі хімічних сигналів, таких як різноманітні молекули, гормони, нейромедіатори тощо. Ці сигнали використовуються для передачі сигналів між клітинами, органами та системами організму при селективному каталізові клітинних процесів; сучасні інформаційні системи зазвичай використовують електронні сигнали для передачі даних. Роль нейромедіаторів схожа на мультисценарні цифрові підписи.

Під час обговорення результатів та розв’язання тестів викладач фокусується на формуванні дружньої атмосфери спілкування, всі студенти, які працювали над даним проектом отримують хороші оцінки - формат спілкування win-win. Тести, отримані і апробовані в такий спосіб, викладач може використовувати в подальшій роботі, при підготовці банку питань для модульних та екзаменаційних контрольних завдань.

Висновки

Даний інноваційний підхід добре зарекомендував себе і може застосовуватися для урізноманітнення навчального процесу. Студенти завдяки своєму незаангажованому поглядові продукують свіжі ідеї, які можуть стати новими корисними рішеннями при захистові від Mirai botnet. Також має місце розвиток лідерських якостей у сильних студентів, командних навичок, а також навичок презентувати свою точку зору у всіх студентів. Цінним при застосуванні даного методу є інноваційне бачення на поставлену задачу, обмін думками та розвиток командних навичок.

Посилання

1. https://www.netacad.com/courses/cybersecurity/iot-security
2. Affinito A., Zinno St, Stanco G., Botta A., Ventre G. The evolution of Mirai botnet scans over a six-year period. Journal of Information Security and Applications. Volume 79, December 2023, 103629.
3. Sajjad S.M., Mufti M.R , Yousaf M. , Aslam W. , lshahrani R., Nemri N., Afzal H., Khan M.A , Chen Ch.-M. Detection and Blockchain-Based Collaborative Mitigation of Internet of Things Botnets. Wireless Communications and Mobile Computing Volume 2022, Article ID 1194899, 26 pages https://doi.org/10.1155/2022/1194899
4. Євсєєв В. В. Аналіз конструкції крила робота-орнітоптера / Р. І. Захаров, В. В. Євсєєв // ІІІ-я Міжнародна конференція «Виробництво & Мехатронні системи 2019», м. Харків, 24-25 жовтня 2019 р. – Х. : ХНУРЕ, 2019. – С. 36 – 38.
5. Gavurova B., Kelemen M., Polishchuk V., Mudarri T. and Smolanka V. A fuzzy decision support model for the evaluation and selection of healthcare projects in the framework of competition // Frontiers in Public Health, 2023. -11:1222125.

РОЗРОБКА МАТЕМАТИЧНОЇ МОДЕЛІ КОМПЕНСОВАНОГО ВИПРЯМЛЯЧА З ПАРАЛЕЛЬНИМ АКТИВНИМ ФІЛЬТРОМ

Студ. К.О. Підопрогора, ст. викл. М.В. Антонова, ст. викл. Є.В. Васильєва, доц. А.Є. Казурова, доц. М.Л. Антонов
Національний університет «Запорізька політехніка», м. Запоріжжя, Україна

У багатьох електричних мережах та системах вентильні перетворювачі є одним із основних видів навантаження. Перетворювач є для мережі нелінійним навантаженням, і його робота впливає на режими роботи мережі, особливо якщо потужності перетворювача та мережі можна порівняти [1].

Компенсовані перетворювачі мають низку переваг, завдяки чому дослідження їх характеристик є дуже актуальною темою.

Мета роботи – дослідження енергообміну у дванадцятифазному компенсованому випрямлячі з позиції теорії миттєвої потужності за допомогою комп'ютерного моделювання. Дослідження взаємного впливу активного фільтра та компенсованого випрямляча.

Для покращення енергетичних характеристик та підвищення якості перетворення можуть бути використані компенсовані випрямлячі та активні фільтри.

Для аналізу електромагнітних процесів у компенсованому випрямлячі з паралельним активним фільтром було виконано модель (рисунок 1) у комп'ютерному середовищі MatLab/Simulink (Mathworks Inc). Модуль SimPowerSystems, що входить до складу Simulink, є спеціалізованим додатком для моделювання пристроїв силової електронної техніки.