Найбільший інтерес являє собою "Data Science. Наука о данных с нуля" автора Грас Д., де наведено практичні рекомендації стосовно не тільки проблеми перенавчання даних. Також висвітлені питання вирішення супутньої проблеми недонавчання даних (underfitting), наведені практичні рекомендації покращення моделей із застосуванням мови програмування Python.

Висновок. Автори у своєму дослідженні звертаються до контрольованих моделей (тобто таких, де є сукупність даних, позначена правильними відповідями, на яких відбувається засвоєння); до неконтрольованих моделей (де правильні відповіді відсутні), до напівконтрольованих моделей (де тільки деякі дані позначені правильними відповідями), а також до онлайнових моделей (у яких модель повинна безперервно самоналаштовуватися до даних, що надходять). Інші типии моделей не розглядалися.

Вищенаведені методи можна використовувати як окремо, так і в комбінації один з одним, щоб запобігти перенавчанню та покращити продуктивність моделі на нових даних.

УДК 004.056.5

ФІКСАЦІЯ ДЕСТРУКТИВНОЇ ДЕЗІНФОРМАЦІЇ В КІБЕРПРОСТОРІ ЗА УЧАСТІ СТУДЕНТІВ СПЕЦІАЛЬНОСТІ «КІБЕРБЕЗПЕКА»

Анатолій Давиденко[1], Олена Висоцька[2], Володимир Щербина[2]
[1]Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, davidenkoan@gmail.com,
[2]Національний авіаційний університет, lek_vys@ukr.net

В умовах війни актуальними проблемами є виявлення, моніторинг та фіксація російської дезінформаційної діяльності. Ці питання мають політичні, організаційні та технологічні аспекти. Для перемоги на інформаційному фронті принципово важливим є своєчасно виявляти та фіксувати дезінформацію, а також передбачити можливі наслідки для попередження руйнівного впливу цієї дезінформації. Українське суспільство має дуже важливі та необхідні для перемоги властивості самоорганізації, але цілеспрямованість та наполегливість дій принципово залежить від чистоти інформаційного впливу від випадкової або навмисної дезінформації. Необхідною складовою формування суспільства є навчання молоді основам кібергігієни. Студенти та школярі в першу чергу вразливі до інформаційного впливу, тому вони мають бути залучені до процесу виявлення дезінформації, з метою формування у них імунітету до її впливу.

Метою роботи є розробка методичних матеріалів для навчання студентів фіксації деструктивної дезінформації в кіберпросторі.

На останніх курсах бакалаврату студенти технічного напряму мають достатній досвід використання інформаційних технологій але їм потрібна чітка

фіксація проблеми протидії дезінформації, тому є актуальною задача розробки практичних лабораторних робіт з вияву російської дезінформації.

Розробка лабораторних робіт за тематикою виявлення, моніторингу та фіксації російської дезінформаційної діяльності для здобувачів вищої освіти ОС «Бакалавр» спеціальності 125 «Кібербезпеки» сприяє залученню молоді безпосередньо до процесу протидії російської дезінформаційної діяльності. Наявність іноземних студентів в групах, які навчаються в рамках навчального курсу Incident Management in Cyberspace (НАУ) робить процес протидії більш публічним та незалежним.

Досвід останніх років показав, що розглядати тільки технологічні аспекти процесу виявлення, моніторингу та фіксації російської дезінформаційної діяльності недостатньо. Крім навчання студентів навичкам пошуку, аналізу та збереження фейкової інформації, необхідним є формування у студентів розуміння ознак фейкової інформації та вміння її виявлення в ручному режимі. Крім того, важливим є навчитись здійснювати пошук першоджерела інформації, визначення головних напрямів інформаційної атаки та вивчення характерних ознак та методів розповсюдження фейкової інформації. Важливим є вміти своєчасно зафіксувати факт дезінформації. Не менш важливим етапом є навчити студентів навичкам копіювання інформації зі збереженням її автентичності. Це копіювання у вигляді дзеркала веб-сайту з обов'язковою фіксацію дати копіювання та адреси, забезпечення цілісності копії, наприклад за допомогою хешування та накладення цифрового підпису, надійне збереження знайденої інформації в хмарному або грід середовищі.

Але крім цих важливих навичок стандартною помилкою студентів під час виконання лабораторних робіт є помилки при ідентифікації інформаційної атаки. По-перше, це фіксація вторинного джерела дезінформації, по-друге, студенти не завжди відрізняють кібервплив від інформаційного. Тому в цьому році студентам були запропоновані додаткові лабораторні роботи, які наочно показують цю різницю.

Важливим аспектом при проведенні лабораторних робіт є розуміння факту, що інформація це зброя, поводження з якою потребує особливої обмеженості. Намагаючись довести фейковість інформації не можна розкривати критичну інформацію (наприклад ЗСУ має тільки n-HIMARS, а РФ говорить, що знищила їх більше ніж існує насправді). Нажаль невдала спроба протидії може спричинити більше шкоди ніж сама фейкова інформація. Тому важливими є фактори самоцензури та знання наслідків розголошення інформації. Перші місяці війні добре навчили нас, що застосування інформаційних технологій без розуміння що саме вони роблять веде до незворотних втрат.

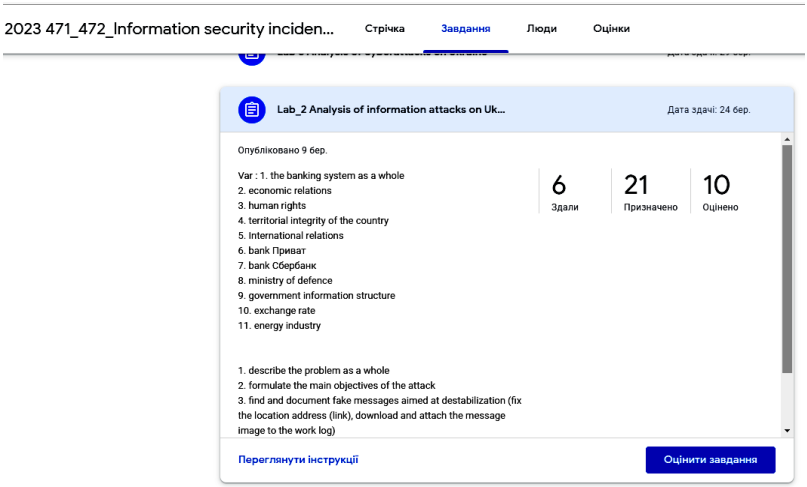

Рис. 1. Лабораторна робота Analysis of information attacks on Ukraine з дисципліни «2023 471_472_Information security incident management», НАУ, 2023 рік

Розробка навчально-методичних матеріалів, їх практична апробація та формування групи фахово-підготовленої молоді, вмотивованої на виявлення, моніторинг та фіксацію російської дезінформаційної діяльності є основними результатами цього року.

УДК 004.274:004.056

ВИКОРИСТАННЯ ПЛІС ДЛЯ ЗАХИСТУ КІБЕРФІЗИЧНИХ СИСТЕМ ЕНЕРГЕТИКИ

Сергій Гільгурт

ІПМЕ ім. Г.Є. Пухова НАН України, hilgurt@ipme.kiev.ua

Цировізація промислового обладнання та кіберфізичні системи останнім часом все частіше використовуються для підвищення ефективності критичної інфраструктури, зокрема, в енергетичній галузі. Цифровізація електричних підстанцій, які є найпоширенішими об'єктами електроенергетики, відбувається згідно низки стандартів МЕК-61850 «Мережі та системи зв'язку на підстанціях», згідно якого єдиним засобом передачі інформації на всіх рівнях підстанції прийнятий стандарт Ethernet. На жаль, пакетна передача даних і протоколи, що на ній засновані, роблять цифрові підстанції більш вразливими для кібератак. Наявний в ІТ-галузі досвід захисту інформації не може буди безпосередньо застосований до цифровізованих промислових систем, але з низкою поправок його доцільно використовувати. До дієвих засобів протидії загрозам безпеки інформації