ІНФОКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ ТА ЕЛЕКТРОННА ІНЖЕНЕРІЯ
INFORMATION AND COMMUNICATION TECHNOLOGIES, ELECTRONIC ENGINEERING

№ 4 (1), 2024

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

https://doi.org/10.23939/ictee2024.01.001

ДОСЛІДЖЕННЯ КОНТЕКСТНО-ЧУТЛИВОГО АЛГОРИТМУ МОНІТОРИНГУ КІБЕРБЕЗПЕКИ НА ОСНОВІ РЕКУРЕНТНИХ НЕЙРОННИХ МЕРЕЖ

М. Климаш [ORCID: 0000-0002-1166-4182], **А. Сеник, Ю. Пиріг** [ORCID: 0000-0002-8973-4005], **В. Мрак** [ORCID: 0009-0002-6066-5592]

Національний університет «Львівська політехніка», вул. С. Бандери, 12, 79013, Львів, Україна
Відповідальний за рукопис: Андрій Сеник (e-mail: andrii.d.senyk@lpnu.ua)

(Подано 17 січня 2024 р.)

У роботі розглянуто найбільш поширені проблеми, з якими стикаються сучасні інформаційно-комунікаційні системи (ІКС) у контексті боротьби з кіберзагрозами. Визначено основні принципи ефективного захисту систем ІКС від можливих втручань в їхню роботу. Наведено класифікацію кіберзагроз та їхній вплив на функціонування інформаційних систем. Визначено особливості використання сучасних інформаційних технологій, як-от: машинне навчання (Machine learning, ML), рекурентні нейронні мережі (Recurrent neural networks, RNN) для підвищення ефективності виявлення та запобігання таким загрозам, прискорення процесу обчислень великих обсягів інформації про різні аспекти роботи інформаційно-коомунікаційних систем. Досліджено параметри аналізу поведінки ІКС, що свідчать про наявність проблем у кібербезпеці. Запропоновано модифікований контекстно-чутливий алгоритм моніторингу кібербезпеки (CCM-RNN), що базується на RNN та дозволяє враховувати динаміку системних змін у встановленому контексті, наприклад тип або обсяг трафіку від користувачів тощо. Також вдосконалено метод вибору найбільш ефективних параметрів та властивостей ІКС для виявлення кіберзагроз. Результати дослідження ефективності використання модифікованого алгоритму CCM-RNN демонструють його широкі можливості для швидкого та точного виявлення аномалій у роботі ІКС, що можуть загрожувати їхній кібербезпеці. Встановлено, що, змінюючи кількість властивостей роботи алгоритму CCM-RNN, які відповідні характеристикам різних аспектів роботи ІКС, можна досягнути максимальної точності виявлення кіберзагроз. За результатами досліджень зроблено висновок про доцільність використання запропонованого модифікованого алгоритму CCM-RNN для можливості виявляти загрози кібербезпеці в ІКС, гнучко регулюючи кількість та тип параметрів навчання нейпрнних мереж. У такий спосіб оптимізується точність та тривалість обчислень, а також враховуються особливості й контексти роботи інформаційо-комунікційних систем.

Ключові слова: *кібербезпека, рекурентні нейронні мережі, алгоритми моніторингу, інформаційно-комунікаційні системи.*
УДК: 621.126

1. Вступ

В останні роки ми спостерігаємо стрімке впровадження цифрових технологій у різні сфери життя. Водночас зростає кількість кібератак, які постійно ускладнюються та вдосконалюються. У наш час алгоритми атак досить складні, постійно змінюються та використовують багато методів

для досягнення своєї мети. Оскільки за останні кілька років багато галузей усе більше перейшли в Інтернет, кількість користувачів, яким загрожує кібератака, також зросла. Також ускладнилася інфраструктура інформаційно-комунікаційних систем, яка передбачає різні рівні доступу користувачів до мережі залежно від їхнього статусу. Існуючі методи захисту від загроз також необхідно постійно вдосконалювати, щоб запобігти їм і ускладнити діяльність зловмисників. Особливістю кібератак зараз є їхня персоналізація, шляхом вивчення поведінки як окремих користувачів, так і системи загалом. Виявивши можливі вразливості, проти них здійснюють кібератаки, які досить складно передбачити та їм запобігти.

Тож необхідно використовувати інноваційні підходи до захисту та моніторингу інформаційно-комунікаційних систем. Якщо раніше було достатньо використовувати статичні методи захисту від кіберзагроз, то зараз їх недостатньо. На зміну приходять адаптивні та комплексні методи кіберзахисту. Для цього використовують методи машинного навчання (Machine Learning, ML) та штучного інтелекту (Artificial Intelligence, AI), зокрема рекурентні нейронні мережі, які дозволяють відстежувати закономірності системних процесів, прогнозувати можливі загрози та пропонувати шляхи їх усунення. В ІКС важливо налагодити механізми взаємодії їхніх компонентів між собою, оскільки це покращує процес виявлення загроз та ефективність їхнього усунення. Для дослідження загроз у таких системах доцільно використовувати рекурентні нейронні мережі, які можуть визначати моделі поведінки та працювати з послідовностями даних. Зміни в процесах з часом часто аналізуються для виявлення потенційних кіберзагроз, а RNN значно прискорює обчислення результатів. RNN також зберігає інформацію про попередні часові інтервали, що дозволяє порівнювати динаміку системи та поведінку користувача. Використання попереднього досвіду системи допомагає підвищити ефективність виявлення загроз кібербезпеці. Адаптивність RNN до нових умов дозволяє вирішувати задачі різного типу та складності. У роботі запропоновано контекстно-чутливий алгоритм моніторингу кібербезпеки на основі рекурентних нейронних мереж, який дозволяє враховувати різні особливості поведінки користувачів і виявляти рівень їхньої потенційної кіберзагрози [1–4].

2. Аналіз та формулювання завдання

Інформаційно-комунікаційні системи – це сукупність методів і засобів збору, зберігання, обробки та передавання інформації. Такі системи зараз широко використовуються, оскільки завдання аналізу та обміну даними актуальні як ніколи.

Для роботи інформаційно-комунікаційних систем використовується як програмне, так і апаратне забезпечення, а також мережеві засоби взаємодії між компонентами. Функції ІКС:

1. Збір даних з пристроїв для подальшої обробки.
2. Обробка даних необхідна для їхнього аналізу та отримання результатів, які приносять цінність системі та її користувачам.
3. Передача даних, що необхідно для обміну між пристроями важливою інформацією та службовими командами.
4. Зберігання інформації для подальшого аналізу.

Завдяки вдосконаленню основних функцій інформаційно-комунікаційних систем вони почали використовуватися в багатьох сферах життя, зокрема в освіті, медицині, бізнесі та ін. Зрозуміло, що для більш ефективної роботи сучасних ІКС їх варто постійно моніторити [5–7].

Питання оптимізації моніторингу ІКС зараз особливо актуальне. Зокрема, виділяють такі проблеми:

1. Обсяги даних, які необхідно обробити, швидко зростають. У зв’язку з масштабуванням інформаційних систем та використанням значної кількості джерел даних особливу увагу варто звернути на методи та засоби моніторингової роботи.
2. Нові загрози для системи та користувачів, зокрема кібератаки. Моніторинг стану ІКС допомагає вирішувати та уникати таких загроз.

3. Оптимізація ресурсів для спрощення завдань їхньої подальшої обробки та моніторингу.

4. Високі вимоги до ефективності інформаційно-комунікаційних систем потребують вдосконалення та оптимізації методів моніторингу.

5. Забезпечення приватності та конфіденційності інформації здійснюється шляхом моніторингу системи та виявлення проблемних ситуацій.

Отже, оптимізація методів моніторингу інформаційно-комунікаційних систем є дуже актуальним завданням сьогодення. Для більш ефективного виявлення загроз у функціонуванні інформаційно-комунікаційних систем використовуються контекстно-залежні алгоритми. Такі алгоритми аналізують невідповідності, аномалії та можливі загрози, беручи до уваги різні параметри для досягнення кращої продуктивності. Особливостями контекстно-залежних алгоритмів є:

1. Виявлення аномалій у роботі ІКС, які можуть свідчити про потенційні загрози, за допомогою статистичних моделей і методів.

2. Динамічну адаптивність до контексту, щоб забезпечити точність виявлення загроз в умовах зміни особливостей роботи системи.

3. Стандартизація критеріїв оцінювання. Оскільки багато критеріїв є неоднозначними, необхідно визначити метрику допустимого відхилення даних від допустимого значення у разі виявлення аномалій.

4. Налаштування роботи контекстно-залежних алгоритмів під специфіку конкретної системи з урахуванням її параметрів та аспектів роботи.

5. Баланс між оптимальними обчислювальними витратами та необхідною точністю та швидкістю обчислень.

6. Використання найбільш ефективних функцій для виявлення аномальної активності в інформаційно-комунікаційній системі.

7. Розробка спеціальних алгоритмів, що дозволяють пояснити причини виявлених аномалій у поведінці системи та спростити процес реагування на них.

Методи машинного навчання широко використовують для виявлення загроз кібербезпеці. Приклади використання ML:

1. Виявлення аномалій у роботі ІКС завдяки побудові моделей, здатних визначати відхилення від встановлених норм і закономірностей. Приклади: One-Class Support Vector Machine (SVM), Isolation Forest.

2. Класифікація загроз на основі навчених моделей, що дає змогу визначити потенційну небезпеку нових даних (нейронні мережі, Random Forest).

3. Аналіз великих даних для більш ефективного виявлення шаблонів загроз (наприклад за допомогою Apache Spark MLlib).

4. Прогнозування кібератак і можливих сценаріїв загроз на основі алгоритмів класифікації (Gradient Boosting, Decision Trees).

5. Використання власної інформації про загрози для навчання особистої моделі запобігання їм.

6. Виявлення кіберзагроз у режимі реального часу завдяки алгоритмам машинного навчання, як-от Online Gradient Descent, дозволяє швидко реагувати та запобігати.

Тож методи машинного навчання дозволяють підвищити ефективність виявлення, усунення та прогнозування кіберзагроз в інформаційно-комунікаційних системах, автоматизувати та прискорити процес прийняття рішень у разі небезпеки [8–9].

3. Особливості контексно-чутливих рекурентних нейронних мереж

Алгоритми ідентифікації загроз в інформаційно-комунікаційних системах використовують методи машинного навчання для виявлення аномалій і відхилень у процесах. Тож рішення можна приймати швидше та в умовах, що динамічно змінюються. Етапи виявлення загроз на основі машинного навчання:

1. Навчання моделі – перше навчання проводять із використанням вихідних наборів даних для створення моделі аналізу даних на основі методів машинного навчання.

2. Додавання функцій, які дозволяють враховувати особливості ІКС, наприклад, активність користувача, тривалість з'єднання тощо.

3. Прийняття рішень за результатами навченої моделі машинного навчання щодо класифікації даних за встановленими критеріями.

4. Оптимізація та вдосконалення моделі на основі отриманих результатів, адаптація стандартних рішень до конкретних умов.

5. Аналіз отриманих результатів та моніторинг ефективності захисту системи на основі навченої моделі дозволяє гнучко вносити корективи в її роботу та підвищувати ефективність.

Підсумовуючи вищесказане, алгоритм розподілу ресурсів на основі машинного навчання дає змогу оптимізувати та автоматизувати процес виявлення кіберзагроз у системах ІКС з урахуванням динамічно змінних умов і параметрів.

Для визначення загроз кібербезпеці від користувачів враховуються різні фактори, які можуть вказувати на можливість атаки, зокрема:

1. Збільшення кількості спроб доступу до ресурсів, особливо, якщо це було незвичним для користувача в минулому.

2. Збільшення обсягу роботи з файлами (читання, запис), особливо, якщо це відбувається в незвичайний час.

3. Передавання інформації, зокрема нестандартного формату або з конфіденційним вмістом, на різні адреси.

4. Помилки авторизації та аутентифікації, зокрема спроби входу в обліковий запис із різних адрес.

5. Незвичайна кількість процесів користувача або зміни їхніх параметрів.

6. Збільшення кількості під'єднань до мережі, під'єднання до сумнівних ресурсів.

7. Зміна налаштувань безпеки та антивірусного програмного забезпечення.

8. Зміни обсягу використання користувачем обчислювальних ресурсів системи.

Для ідентифікації загроз безпеці інформаційно-комунікаційних систем необхідно враховувати не одну ознаку, а їхню сукупність.

Використання рекурентних нейронних мереж дозволяє ідентифікувати шаблони в даних і обробляти їх відповідно до певного контексту. Такий підхід зручно використовувати у разі вирішення загроз кібербезпеці. Також основні особливості RNN при їхньому використанні для захисту даних:

1. Послідовність обробки, яка дає змогу порівнювати їх і відзначати динаміку змін.

2. Виявлення аномалій у даних як відхилення поведінки системи від її звичного стану.

3. Легкість виявлення змін параметрів і характеристик у часі.

4. Узагальнення та аналіз виявлених змін у поведінці ІКС та усунення загроз.

5. Завдяки застосуванню LSTM у рекурентних нейронних мережах можна моделювати довгострокові залежності на основі довгострокових спостережень, визначати частину інформації, яку доречно обробити зараз, і відкидати надлишок.

6. Адаптивність до динамічних змін, різноманітних особливостей і станів системи [10–11].

Контекстно-чутливий алгоритм на основі рекурентних нейронних мереж (CCM-RNN) було запропоновано в роботі для моніторингу кібербезпеки (рис. 1). Модифікований алгоритм має кілька етапів:

1. Підготовка даних. Визначення обсягу даних і нормалізація для більш зручної подальшої обробки.

2. Визначення особливостей, які будуть враховуватися під час навчання, що можуть свідчити про можливі загрози.

3. Навчання моделі RNN на основі різних обсягів даних і функцій для виявлення аномалій у поведінці користувачів і висування гіпотез про можливі загрози.

4. Візуалізація результатів навчання;

5. Корекція результатів для підвищення ефективності алгоритму. Для обчислення CCM-RNN слід враховувати такі залежності:

1. Обчислення кроку прямого зв'язку RNN (RNN Feedforward Step):

$$h_t = \sigma\left(W_{ih} x_t b_{ih} + W_{hh} h_{t-1} + b_{hh}\right), \tag{1}$$

$$y_t = \sigma\left(W_{hy} h_t + b_{hy}\right), \tag{2}$$

де x_t – вхідний вектор на кроці часу t; h_t – прихований стан на кроці часу t; y_t – вихідний вектор на кроці часу t; W_{ih}, W_{hh}, W_{hy} – вагові матриці; b_{ih}, b_{hh}, b_{hy} – коефіцієнти зміщення; ih – коефіцієнти (input-hidden) представляють ваги між вхідним шаром і прихованим шаром (чим вище значення коефіцієнта, тим більший вплив відповідного входу на активацію прихованих нейронів); hh – коефіцієнти (hidden-hidden) представляють вагові коефіцієнти між прихованим шаром і ним самим на попередньому кроці часу, визначаючи, як попередні стани прихованих нейронів впливають на поточний стан прихованих нейронів; hy – коефіцієнти (hidden-output) представляють вагові коефіцієнти між прихованим шаром і вихідним шаром (чим вище значення коефіцієнта, тим більший вплив відповідного прихованого нейрона на вихідний сигнал); σ – функція активації.

Рис. 1. Контекстно-чутливий алгоритм моніторингу кібербезпеки на основі рекурентних нейронних мереж

2. Функція втрати:

$$L(y, y') = -\frac{1}{N}\sum_{i=1}^{N}\left(\left(y_i \log\left(y'\right)\right) + \left(1 - y_i\right)\left(1 - y_i'\right)\right), \quad (3)$$

де y і y' – істинний і прогнозований вектори міток; N – кількість прикладів у навчальному наборі.

Доцільність і передумови алгоритму CCM-RNN порівняно з існуючими алгоритмами визначають певними його особливостями, як-от:

1. Боротьба зі складними кіберзагрозами. CCM-RNN дозволяє ефективно та динамічно адаптуватися до різних умов, працювати з різними контекстами атак.

2. Чутливість до контексту та можливість його адаптації в різних сценаріях.

3. CCM-RNN найкраще демонструє свої переваги в складних системах із великою кількістю пристроїв, взаємодій між ними, аномалій для аналізу даних.

4. Економічна ефективність CCM-RNN за рахунок оптимізації обробки великих даних.

4. Дослідження та моделювання контекстно-чутливого алгоритму моніторингу кібербезпеки на основі рекурентних нейронних мереж

Для роботи контекстно-залежного алгоритму для навчання моделі використовувалися різні вхідні ознаки, які визначали ненормальність даних у певному контексті: тривалість сеансу, кількість і частота з'єднань, кількість доступних для читання даних, тощо. Кількість ознак (властивостей, features) визначають як 1, 5 і 10 для кращого порівняння їхнього впливу на результат. Дані використано з відкритих джерел і нормалізовано перед обробкою, щоб адекватно представити їх як вхідні параметри моделі навчання (під нормалізацією мається на увазі їхнє приведення до одного масштабу або діапазону значень). Алгоритм використовує шар LSTM з 50 юнітами, під час компіляції моделі використовувався оптимізатор Адама. Кількість епох навчання встановлено як десять. Такі параметри є загальним вибором і забезпечують баланс між точністю та ефективністю для багатьох наборів даних і моделей. Модель навчання для алгоритму CCM-RNN реалізована на мові Python, результати її роботи представлені графічно.

Вплив ознак на роботу може сильно залежати від кількості та характеристик вхідних даних. Хоча збільшення кількості ознак може підвищити точність, зрештою може статися перенавчання, що погіршить результат. Крім того, збільшення кількості ознак впливає на тривалість обчислень (рис. 2).

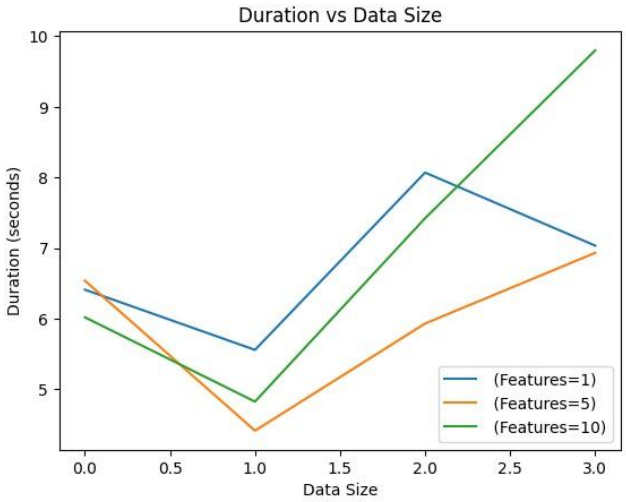

Рис. 2. Залежність тривалості обчислень алгоритму CCM-RNN від розміру матриці даних

У контексті кібербезпеки необхідно знайти баланс між надмірною кількістю непотрібних функцій і браком необхідних даних для навчання. Таку задачу можна розв'язати за допомогою контекстно-залежного алгоритму, аналізуючи результати з різною кількістю ознак. Вплив кількості врахованих ознак на точність виявлення аномалії алгоритмом CCM-RNN показано на рис. 3.

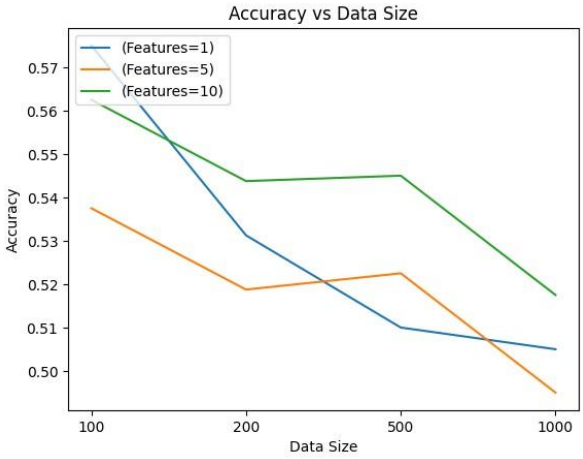

Рис. 3. Залежність точності обчислення алгоритму CCM-RNN від розміру матриці даних

Відповідно до результатів дослідження, наведених на рис. 2, використання більшої кількості ознак зменшує тривалість навчання, хоча тимчасові зміни в цій динаміці також можливі. Також цікавими є результати порівняння точності розрахунків (рис. 3), згідно з якими точність розрахунків загрози залишається досить високою у разі використання 10-ти ознак. На рис. 4 також наведено результати дослідження залежності точності обчислень від кількості епох навчання.

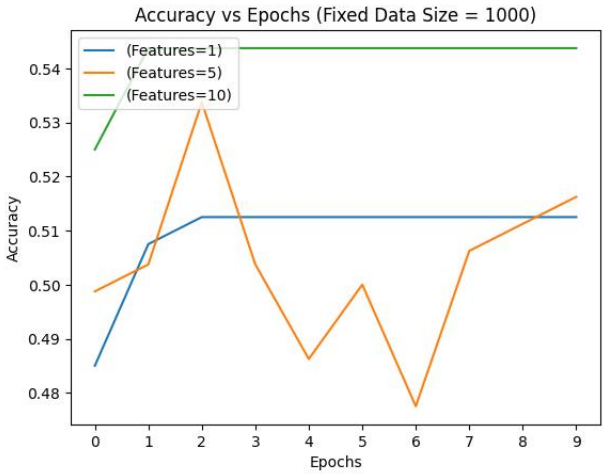

Рис. 4. Залежність точності розрахунку алгоритму CCM-RNN від кількості епох навчання

Згідно з рис. 4, аналіз загроз на основі 10-ти вхідних ознак дає найкращий результат. Узагальнюючи результати дослідження, запропонований алгоритм дозволяє визначити найбільш ефективні параметри навчання моделі виявлення кіберзагроз. У цьому випадку найвища точність та швидкість обчислень зафіксована при використанні для обчислень 10-ти ознак, що відповідні певним аномаліям у роботі системи ІКС (тривалість та частота під'єднань користувачів, обсяг переданих даних, кількість помилок при авторизації тощо). Модифікований алгоритм є адаптивним до використання різної кількості ознак, гнучким у реалізації та відкриває перспективи для подальших досліджень. Отже, запропонований модифікований алгоритм CCM-RNN є ефективним для використання в системах ІКС, оскільки дозволяє враховувати різні параметри їхньої роботи при виявленні кіберзагроз, швидко та точно надавати результат.

Висновки

У роботі досліджено алгоритми виявлення кіберзагроз у сучасних інформаційно-комунікаційних системах та визначено основні типи таких загроз. Проаналізовано основні аспекти забезпечення кібербезпеки. Встановлено доцільність використання RNN і LTSN для боротьби із загрозами завдяки їхній гнучкості та точності виявлення аномалій.

Запропоновано модифікований контекстно-чутливий алгоритм моніторингу кібербезпеки на основі рекурентних нейронних мереж, який дає змогу враховувати особливості поведінки користувачів, що можуть вказувати на можливі кіберзагрози. Досліджено роботу алгоритму на основі різних обсягів інформації та ознак. Продемонстровано вплив зміни кількості ознак на точність виявлення аномалії для різних обсягів даних. Експериментально визначено оптимальну кількість параметрів для найкращої швидкості та точності обчислень – 10 вхідних ознак. Встановлено ефективність алгоритму до виявлення кіберзагроз та перспективи його використання в різних сценаріях функціонування інформаційно-комунікаційних систем.

Список використаних літературних джерел

[1] *Y. Fang, Y. Zhang and C. Huang, "CyberEyes: Cybersecurity Entity Recognition Model Based on Graph Convolutional Network," in The Computer Journal, vol. 64, no. 8, pp. 1215-1225, Oct. 2020, doi: 10.1093/comjnl/bxaa141.*

[2] *R. Sabillon, J. Serra-Ruiz, V. Cavaller and J. Cano, "A Comprehensive Cybersecurity Audit Model to Improve Cybersecurity Assurance: The CyberSecurity Audit Model (CSAM)," 2017 International Conference on Information Systems and Computer Science (INCISCOS), Quito, Ecuador, 2017, pp. 253-259, doi: 10.1109/INCISCOS.2017.20.*

[3] *A. Atapour-Abarghouei, A. S. McGough and D. S. Wall, "Resolving the cybersecurity Data Sharing Paradox to scale up cybersecurity via a co-production approach towards data sharing," 2020 IEEE International Conference on Big Data (Big Data), Atlanta, GA, USA, 2020, pp. 3867-3876, doi: 10.1109/BigData50022.2020.9378014.*

[4] *N. Shingari, S. Verma, B. Mago and M. S. Javeid, "A review of cybersecurity challenges and recommendations in the healthcare sector," 2023 International Conference on Business Analytics for Technology and Security (ICBATS), Dubai, United Arab Emirates, 2023, pp. 1-8, doi: 10.1109/ICBATS57792.2023.10111096.*

[5] *C. Easttom, "SecML: A Proposed Modeling Language for CyberSecurity," 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 2019, pp. 1015-1021, doi: 10.1109/UEMCON47517.2019.8993105.*

[6] *David Ward; Paul Wooderson, "Introduction to Automotive Cybersecurity," in Automotive Cybersecurity: An Introduction to ISO/SAE 21434 , SAE, 2021, pp.1-6.*

[7] *V. Gonzalez, O. Perez and R. Romero, "Cybersecurity in ECE Curriculum, an Expanded Collaboration Program to Disseminate Real Security Experiences in Cyber-Physical Systems," 2023 IEEE Frontiers in Education Conference (FIE), College Station, TX, USA, 2023, pp. 1-4, doi: 10.1109/FIE58773.2023.10343280.*

[8] *L. Oliveira et al., "Assessing Cybersecurity Hygiene and Cyber Threats Awareness in the Campus - A Case Study of Higher Education Institutions in Portugal and Poland," 2023 IEEE International Conference on Cyber Security and Resilience (CSR), Venice, Italy, 2023, pp. 168-173, doi: 10.1109/CSR57506.2023.10224910.*

[9] *S. Peng, A. Zhou, S. Liao and L. Liu, "A Threat Actions Extraction Method Based on The Conditional Co-occurrence Degree," 2020 7th International Conference on Information Science and Control Engineering (ICISCE), Changsha, China, 2020, pp. 1633-1637, doi: 10.1109/ICISCE50968.2020.00323.*

[10] *C. Onwubiko and K. Ouazzane, "SOTER: A Playbook for Cybersecurity Incident Management," in IEEE Transactions on Engineering Management, vol. 69, no. 6, pp. 3771-3791, Dec. 2022, doi: 10.1109/TEM.2020.2979832.*

[11] *J. Wang, D. Brylow and D. Perouli, "Implementing Cybersecurity into the Wisconsin K-12 Classroom," 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), Milwaukee, WI, USA, 2019, pp. 312-317, doi: 10.1109/COMPSAC.2019.10225.*

INVESTIGATION OF A CONTEXT-SENSITIVE CYBER SECURITY MONITORING ALGORITHM BASED ON RECURRENT NEURAL NETWORKS

M. Klymash, A. Senyk, Yu. Pyrih, V. Mrak

Lviv Polytechnic National University, S. Bandery Str., 12, 79013, Lviv, Ukraine

The most common problems faced by modern information and communication systems (ICS) in the context of combating cyber threats were examined in the paper. The importance of ensuring the reliable operation of ICS, and protecting their users' private data from unauthorized interception or destruction was emphasized. The main principles of effective protection of ICS systems against possible interference in their work were defined. The classification of cyber threats and their impact on the functioning of information systems was presented. Features of the use of modern information technologies were determined, such as machine learning (ML), and recurrent neural networks (RNN) for increasing the effectiveness of detecting and preventing such threats, speeding up the process of calculating large volumes of information about various aspects of the work of information and communication systems. The parameters of the analysis of ICS behavior, which indicate the presence of problems in cyber security, were studied. The features and advantages of deploying RNN in ICS were analyzed, which makes it possible to simplify the tasks of cyber defense. A modified context-sensitive algorithm for cyber security monitoring (CCM-RNN) was proposed, which is based on RNN and allows taking into account the dynamics of system changes in the established context, for example, the type or volume of traffic from users, etc. The method of selecting the most effective parameters and properties of ICS for detecting cyber threats was improved. The results of the study of the effectiveness of the use of the modified CCM-RNN algorithm demonstrated its broad capabilities for fast and accurate detection of anomalies in the operation of ICs that may threaten their cyber security. By changing the number of properties of the CCM-RNN algorithm, which correspond to the characteristics of various aspects of the IC, it is possible to achieve the maximum accuracy of cyber threat detection. The modified algorithm also allows for the reduction of the duration of calculations during analysis. Based on the research results, a conclusion was made about the feasibility of using the proposed modified CCM-RNN algorithm for the ability to detect cyber security threats in ICS by flexibly adjusting the number and type of learning parameters of neural networks. In this way, the accuracy and duration of calculations were optimized, as well as the peculiarities and contexts of information and communication systems were taken into account.

Keywords: *cyber security, recurrent neural networks, monitoring algorithms, information and communication systems.*