Міністерство освіти і науки України
Одеський національний технологічний університет
Вінницький національний технічний університет
Інститут комп`ютерної інженерії, автоматизації, робототехніки та програмування ім.П.Н.Платонова

ПРОГРАМА

ІІІ ВСЕУКРАЇНСЬКОЇ
НАУКОВО – ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ
МОЛОДИХ ВЧЕНИХ, АСПІРАНТІВ
ТА СТУДЕНТІВ

«КОМП'ЮТЕРНІ ІГРИ І МУЛЬТИМЕДІА ЯК ІННОВАЦІЙНИЙ ПІДХІД ДО КОМУНІКАЦІЇ - 2023»

28-29 вересня 2023 р.
ОДЕСА

ПРЕЗИДІЯ ТА ОРГКОМІТЕТ КОНФЕРЕНЦІЇ

ГОЛОВА ПРЕЗИДІЇ

Єгоров Б.В., Президент ОНТУ, академік НААН України, д.т.н., професор

ЧЛЕНИ ПРЕЗИДІЇ

Іванченкова Л.В., Ректор Одеського національного технологічного університету, д.е.н., професор

Поварова Н.М., проректор з наукової роботи, к.т.н., доцент

ГОЛОВА ОРГКОМІТЕТУ

Котлик С.В., директор навчально-наукового інституту комп`ютерної інженерії, автоматизації, робототехніки та програмування ОНТУ, к.т.н., доц.

ЗАСТУПНИК ГОЛОВИ ОРГКОМІТЕТУ

Сергій Шестопалов, к.т.н., доц., каф. Комп'ютерної інженерії, ОНТУ

ЧЛЕНИ ОРГКОМІТЕТУ

Олексій Ізвалов, регіональний координатор Global Game Jam в Східній Європі, ETI ім.Ельворті,

Сергій Артеменко, зав.каф. Комп'ютерної інженерії, ОНТУ,

Михайло Кисленко, Unity Developer, DALS Games,

Олександр Романюк, зав.каф. Програмного забезпечення, ВНТУ,

Ольга Чолишкіна, директор Інституту комп'ютерно-інформаційних технологій і дизайну, МАУП,

Олександр Терьошин, Unity 3d developer, BlueGoji,

Павло Івасюк, Senior Snapchat JS Developer, BeVisioned,

Петро Горват, зав.каф. Комп'ютерних систем і мереж, ДВНЗ "Ужгородський національний університет".

УДК 004.01/08

Комп'ютерні ігри та мультимедіа як інноваційний підхід до комунікації - 2023 / Матеріали III Всеукраїнської науково-технічної конференції молодих вчених, аспірантів і студентів, Одеса, 28-29 жовтня 2023 р**.** - Одеса, Видавництво ОНТУ, 2023 р. – 270 с.

Збірник включає матеріали доповідей учасників конференції, які об'єднані за тематичними напрямками конференції.

Збірник буде корисним як для фахівців і працівників фірм, зайнятих в області розробки та просування комп'ютерних ігор, так і для викладачів, магістрів і студентів вищих навчальних закладів, які навчаються за напрямами і спеціальностями програмного забезпечення, комп'ютерних наук, комп'ютерної інженерії, прикладної математики та обробки інформації, буде корисним професіоналам у сферах гейміфікації, кіберспорту, стрімінгу, віртуальної реальності, доповненої реальності, штучного інтелекту, машинного навчання, геймдізайну, саунддізайну.

Результати досліджень у збірнику представляють собою своєрідний зріз сучасного стану справ в перерахованих галузях знань, який може допомогти як фахівцям, так і студентам університетів скласти загальну картину розвитку комп'ютерних ігор ы мультимедіа та пов'язаних з ними питань.

Наукові праці згруповані за напрямками роботи конференції та наведені в алфавітному порядку прізвищ авторів.

Матеріали (тези доповідей) друкуються в авторській редакції. Відповідальність за якість та зміст публікацій несе автор.

Матеріали подано українською та англійською мовами.

Редактор збірника Котлик С.В.

Наприклад, в наукових дослідженнях, штучний інтелект може допомогти виявити нові матеріали, спрогнозувати кліматичні зміни або визначити потенційні області для розвитку нових технологій.

Перспективи розвитку штучного інтелекту надзвичайно широкі і обіцяючі. Штучний інтелект вже змінює багато галузей індустрії та суспільства, і цей тренд очікується продовжити розвиватися в майбутньому.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Шестопалов С. В., Григорюк С. В. Ігровий штучний інтелект в іграх жанру RPG // Інформаційні технології і автоматизація–2020 : зб. доп. XIII Міжнар. наук.-практ. конф., Одеса, 22–23 жовт. 2020 р., Одеса. 2020. С. 300–303.
2. Warpefelt H. Verhagen H. "A model of non-player character believability" (2017), pp. 1-13.
3. Як IT-індустрія розвиває інші галузі економіки у 2022 році [Електронний ресурс] – Режим доступу: https://finance.ua/ua/goodtoknow/jak-it-industrija-rozvyvae-inshi-galuzi-ekonomiky.
4. Henderson R. Cockburn M. Stern S. “The impact of artificial intelligence innovation”. IEEE Transactions on Engineering and Technology, (2018), pp. 1-40.

УДК 007:004.056.5]004.77(043.2)

ПРОБЛЕМИ БЕЗПЕКИ ТА КОНФІДЕНЦІЙНОСТІ ІНТЕРНЕТУ РЕЧЕЙ

УСЕНКО М. П. (mpu.mailbx@gmail.com)
БАНДОРІНА Л.М. (bandorina7@gmail.com)
Український державний університет науки і технологій

Огляд проблем безпеки та конфіденційності у світі Інтернету речей (IoT). Розглядається важливість забезпечення безпеки у сфері IoT та необхідність враховувати як технічні, так і людські аспекти у цьому контексті.

Актуальність проблеми. В даний час все складніше знайти пристрої, які не мають можливості підключення до інтернету, бо деякі виробники орієнтуються виключно на продукти, що підключаються. Із кожним днем ми все більше починаємо залежати від пристроїв IoT, що допомагають нам з вирішення повсякденних завдань.

Поняття IoT, або Інтернет речей (Internet of Things), включає наступні складові:

– пристрої, підключені до інтернету і об’єднані в мережу;
– додатки, технології та стандарти, які дозволяють фізичним об’єктам підключатися до мережі інтернет, збирати та обробляти інформацію, приймати і передавати дані, інтегруватися в комп’ютерну мережу;
– окремі мережі, які працюють за різними стандартами та розв’язують свої власні задачі, в яких взаємодія людей з пристроями і взаємодія пристроїв між собою дозволяє автоматично реагувати на зовнішні зміни і навіть приймати рішення без участі користувача.

Ключова ідея, як зазначають вчені Б. Ю. Жураковський і І.О. Зенів [1] – з’єднати між собою всі об’єкти, які можна з’єднати, підключити їх до мережі для збирання даних і прийняття рішень на їх основі. У такому середовищі створюються якісно інші, ніж сьогодні, умови для бізнесу, для охорони здоров’я, для забезпечення екологічної безпеки, трансформуються особисті та соціальні аспекти життя [1].

Беручи до уваги те, що абсолютну безпеку пристроїв гарантувати не можна, сьогодні досить важливим питанням є забезпечення їх захисту. Зростаючий рівень підключеності [2] створює нову проблему – вразливість пристроїв інтернету-речей та несанкціонований доступ до них [3]. Наприклад, ми звісно зможемо вимкнути інтернет холодильника після кібератаки, але зовсім не так просто буде вимкнути інтернет-з'єднання електролічильника, системи керування світлофорами або імплантованого кардіостимулятора. Загроза конфіденційності може критися також у нешкідливих комбінаціях потоків IoT-даних, бо об’єднавши та зіставивши кілька потоків даних можна отримати набагато чіткіший цифровий портрет людини чи організації. Ще одна вразливість

криється в прихованому зборі даних про користувача IoT-пристроєм. Ця схема збору даних отримує все більше розповсюдження у сфері побутових пристроїв, таких як «розумні колонки», «розумні телевізори» та ігрові приставки. У таких пристроїв є функція розпізнавання зображення та голосу і тому вони мають можливість безперервно переглядати або слухати те, що відбувається навколо і активно передавати ці дані до різноманітних хмарних сервісів для подальшої обробки, і в цьому процесі іноді задіяні треті сторони. Тому забезпечення безпеки пристроїв та послуг IoT стає важливим та критичним завданням. Залежність від цих пристроїв зростає, а їх робота може мати глобальний вплив на наше повсякденне життя.

Методи для вирішення проблеми. Усунення вразливостей: пристрої інтернету речей, будучи підключеними до мережі, стають потенційними точками входу, та можуть бути легко зламані, що й робить їх потенціальною платформою для атаки [4], тому важливо, щоб вони були добре захищені, для запобігання їх злому. Згодом кіберзлочинці можуть використовувати ці вже зламані пристрої для злому інших компонентів системи, що вже будуть містити або надавати доступ до конфіденційних даних. Насправді, будь-який мережевий пристрій може стати інструментом атаки на інший елемент системи. Наприклад, вразлива система опалення, вентиляції та кондиціонування повітря може використовуватися для доступу до мережі магазину, де хакери можуть отримати доступ до POS-терміналів та фінансових даних, включаючи імена клієнтів та інформацію про кредитні картки, що може призвести до витоку особистих даних та інших злочинів. З огляду на це, забезпечення кібербезпеки перебуває у пріоритеті.

Однак зниження ймовірності хакерського злому та його наслідків цілком під силу кожній організації. Цього можна досягти через сегментацію мережі, зміцнення заходів безпеки та регулярну переоцінку методів і процедур кібербезпеки [5], враховуючи загрози, що завжди змінюються.

Усунення людського фактору: сучасні інструменти, технології та функції мають стратегічне значення для забезпечення безпеки у сфері кіберпростору, але вони виявляються неефективними, коли йдеться про найслабшу складову цієї системи: людський фактор. Саме тому організації повинні наголошувати на встановленні і суворому дотриманні стандартів і політик, а також на впровадженні норм і правил безпеки. Це мають бути рекомендації щодо підключення персональних пристроїв, таких як смартфони та точки бездротового доступу, до мережі організації. Коли компанія має детальне знання про те, яке обладнання та пристрої використовуються в їхній мережі, вони можуть створити правила та процедури для захисту цієї мережі та всіх підключених пристроїв. Це також дозволяє переконатися, що пристрої забезпечують відповідний рівень захисту та можуть бути оновлені або посилені за потреби за допомогою ПЗ. Після введення відповідних правил у дію, організаціям також слід призначити відповідальну особу, яка дотримуватиметься IT-політики та буде взаємодіяти з інтегратором, щоб переконатися, що пристрої налаштовані відповідно до поточних приписів. Наприклад, однією з політик може бути вимога про обов'язкове використання шифрування в локальній мережі клієнта для всіх пристроїв, встановлених у мережі (наприклад, відеореєстратори, робочі станції або системи відеоспостереження), що допомагає знизити ризик кібератак.

Відповідно до цієї політики, будь-яка IP-камера, встановлена в мережі, повинна мати шифрування, а програмне забезпечення для відеоспостереження повинно мати відповідно функціональність для декодування зашифрованих повідомлень з цих камер. Також користувачі повинні приділяти увагу своїм смартфонам та дотримуватись правил, які забезпечують захист мережі організації. Всі ці аспекти відіграють фундаментальну роль у боротьбі з людським фактором у сфері кібербезпеки.

Підбір відповідних технологій: для інтеграторів, які прагнуть забезпечити високий рівень кібербезпеки, початковий етап полягає у виборі відповідних продуктів, здатних гарантувати захист клієнтів. У питаннях придбання рішень для кінцевих користувачів слід акцентувати увагу на пристроях, що пропонують функції, які задовольняють безпекові потреби конкретного клієнта. Це може включати опції шифрування, IP-фільтрацію для обмеження доступу до пристроїв, використання програмного забезпечення з цифровим підписом або забезпечення безпечного завантаження. Однак необхідно зазначити, що встановлення та розгортання пристроїв не повинні означати всебічне включення всіх доступних функцій безпеки з надією, що вони працюватимуть належним чином. Оскільки IoT заснований на основі того, що пристрої можуть обмінюватися

даними один з одним, тому важливо, щоб ці зв'язки були добре організовані, а інформацію, яку вони передають, було захищено від сторонніх. Не всі методи шифрування однаково надійні. Якщо пристрій забезпечує шифрування даних, це шифрування має також застосовуватися і на сервері, до якого цей пристрій підключено. Кожен користувач повинен налаштувати свої пристрої з урахуванням певних параметрів. Деякі виробники надають посібники, які докладно описують заходи щодо безпеки пристроїв, і це корисний ресурс як для інтеграторів, так і для кінцевих користувачів. Тим не менш, важливо наголосити, що це не може повністю замінити необхідність розробки суворої безпекової політики. При виборі продуктів також важливо враховувати репутацію виробників, які дотримуються сучасних методів кібербезпеки, включаючи надійне шифрування та інші додаткові заходи безпеки, що забезпечують високий рівень захисту.

З урахуванням різноманітності доступних сьогодні мережевих пристроїв, включаючи компоненти "розумного будинку" та інші елементи IoT, можливості застосування таких мереж обмежені лише уявою.

Висновок. Не зважаючи на те, що пристрої IoT з’явилися достатньо давно та отримали широке поширення, питання їх безпеки і до сих пір стоїть гостро навіть сьогодні. Одними з основних проблем при використанні IoT пристроїв є слабкий рівень їхньої захищеності, зумовлений прагненням виробника залишатися конкурентоспроможним знижуючи рівень витрат, недостатній рівень підтримки з боку виробників та необізнаність або ігнорування користувачами правил безпеки. Однак, приділяючи належну увагу питанням безпеки при використанні пристроїв інтернету речей, користуюсь одним або декількома наведеними методами можна убезпечити себе від можливих загроз.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Технології інтернету речей. Навчальний посібник [Електронний ресурс]: навч. посіб. для студ. спеціальності 126 «Інформаційні системи та технології», спеціалізація «Інформаційне забезпечення робототехнічних систем» / Б. Ю. Жураковський, І.О. Зенів; Київ : КПІ ім. Ігоря Сікорського, 2021. 271 с. URL: https://ela.kpi.ua/bitstream/123456789/42078/1/Zhurakovskyi_B_Zeniv_Tehnologii_internet_rechey.pdf (Доступ 18.09.2023)
2. State of IoT 2023: Number of connected IoT devices growing 16% to 16.7 billion globally URL: https://iot-analytics.com/number-connected-iot-devices/ (Доступ 18.09.2023)
3. Homeowner's Blood ‘Ran Cold' as Smart Cameras, Thermostat Hacked, He Says URL: https://www.nbcchicago.com/news/national-international/my-blood-ran-cold-as-smart-cameras-thermostat-hacked-homeowner-says/6523/ (Доступ 18.09.2023)
4. Avast Smart Home Security Report 2019 URL: https://cdn2.hubspot.net/hubfs/486579/avast_smart_home_report_feb_2019.pdf (Доступ 18.09.2023)
5. The Importance of End-to-End IoT Security URL: https://ts2.space/en/the-importance-of-end-to-end-iot-security/ (Доступ 18.09.2023)

УДК 004.8

ПРОГНОЗУВАННЯ КОНВЕРСІЇ ПО КАРТИНЦІ ТОВАРУ

ХАЙНАС О.Ю. (alexander.haynas@gmail.com)
Національний Університет «Львівська Політехніка»

У сучасному світі електронної комерції та інтернет-маркетингу, прогнозування конверсії по картинці товару стає все більш актуальним та необхідним дослідженням. Визначення основних факторів, які впливають на успішність продажу товарів, допомагає компаніям виробляти та презентувати свою продукцію таким чином, щоб забезпечити максимальну конверсію. Дане дослідження може бути використано в таких сферах, як роздрібна торгівля, маркетинг, дизайн продуктів та веб-аналітика.