Міністерство освіти і науки України
Державна наукова установа "Інститут модернізації змісту освіти"
Центральноукраїнський національний технічний університет

Комп'ютерна інженерія і кібербезпека: досягнення та інновації

Матеріали II Всеукраїнської науково-практичної конференції здобувачів вищої освіти й молодих учених

м. Кропивницький, 25–27 листопада 2020 р.

Кропивницький ЦНТУ 2020

УДК 004
ББК 32.97
К63

К63 **Комп'ютерна інженерія і кібербезпека : досягнення та інновації :** матеріали II Всеукр. наук.-практ. конф. здобувачів вищої освіти й молодих учених, м. Кропивницький, 25–27 листоп. 2020 р. / М-во освіти і науки України, Держ. наук. установа "Інститут модернізації змісту освіти", Центральноукр. нац. техн. ун-т ; [відп. за вип. О. П. Доренський]. — Кропивницький: ЦНТУ, 2020. — 147 с.

Збірник містить тези доповідей учасників II Всеукраїнської науково-практичної конференції здобувачів вищої освіти й молодих учених "Комп'ютерна інженерія і кібербезпека: досягнення та інновації", яка відбулася 25–27 листопада 2020 року в онлайновому форматі на базі Центральноукраїнського національного технічного університету, місто Кропивницький. Праці учасників конференції присвячені актуальним питанням інформаційних систем і технологій, інженерії програмного забезпечення, комп'ютерних систем штучного інтелекту, мережевих IT, інформаційної безпеки національного сегмента кіберпростору, боротьби з кіберзлочинністю, захисту програм та даних в комп'ютерних системах і мережах.

Видання призначене для здобувачів вищої освіти за IT-спеціальностями у ЗВО України, науковців, викладачів, фахівців галузі інформаційних технологій, а також буде корисним всім, хто цікавиться сучасними досягненнями та інноваціями у сферах комп'ютерної інженерії й кібернетичної безпеки.

УДК 004
ББК 32.97
К63

Рекомендовано до друку Науково-технічною радою Центральноукраїнського національного технічного університету (протокол № 10 від 24 листопада 2020 р.)

Відповідальний за випуск: канд. техн. наук Доренський О. П.

Тексти матеріалів, тез доповідей друкуються у авторській редакції, мовою оригіналу. За достовірність наведених у публікаціях даних, назв, імен, цитат та іншої інформації відповідальність несуть автори.

Адреса організаційного комітету конференції
Центральноукраїнський національний технічний університет
Кафедра кібербезпеки та програмного забезпечення
просп. Університетський, 8, м. Кропивницький, 25006
(0522) 55-10-49, 39-04-49; cnts-conference@ukr.net; www.kntu.kr.ua

МЕРЕЖНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Басов Б. В. Програмна частина системи розумного будинку із голосовим керуванням.....90

Бельфер Р. Е., Савенко О. С. Архітектура однорангової багаторівневої мережі Layered Peer-to-Peer (LP2P).....92

Бердадін В. К., Бурячченко К. О. Дослідження системи керування розподіленою СХД за допомогою специфікації NVMe over Fabrics.....93

Беліков Д. Ю. Віддалений доступ до комп'ютера.....95

Головатий В. І., Бурячченко К. О. Дослідження системи моніторингу мережі підприємства на основі комутаторів Nexus 9000.....97

Марченко Л. В., Бурячченко К. О. Дослідження системи відеоспостереження на основі бездротових камер і каналів LTE.....99

Селіванов Т. В. Дослідження застосування віртуальних виділених серверів при розробці та обслуговуванні веб-додатків.....101

Сиволяр Є. В. Дослідження системи управління інфраструктурою на основі рішень SD-WAN.....102

Юхимчак О. О. Дослідження системи керування технологічними процесами за рахунок використання технологій Industrial Internet Reference Architecture.....104

ІНФОРМАЦІЙНА БЕЗПЕКА НАЦІОНАЛЬНОГО СЕГМЕНТА КІБЕРПРОСТОРУ ТА БОРОТЬБА З КІБЕРЗЛОЧИННІСТЮ

Kolodiazhnyi I. A Software of Tor and VPN Blocking Implementation.....106

Гафіяк А. М., Гончарова Г. С., Кукоба С. Засади правового забезпечення кібербезпеки.....107

Грищук О. М. Особливості вибору ключа шифрування для криптосистеми Фредгольма.....109

Золотухін Б. Є. Проблеми безпеки при використанні веб-сервісів в Інтернет-покупках.....111

Мороз А. С. Компоненти інформаційної безпеки.....112

Радій Д. О. Аспекти проблеми інформаційної безпеки України.....113

Федюк Я. В. Інформаційна безпека національного сегмента кіберпростору та боротьба з кіберзлочинністю.....114

Хлапонін Ю. І., Драгунов П. І. Кібербезпека в Україні та стратегія протидії кіберзлочинності.....115

УДК 330.341.1:004

А. М. Гафінк[1], Г. С. Гончарова[2], С. Кухоба[2]
[1]*Національний університет «Полтавська політехніка імені Юрія Кондратюка»*
[2]*Науковий ліцей №3 Полтавської міської ради*

Засади правового забезпечення кіберзахисту

Доцільно зауважити, в контексті нашого дослідження, що величтю XXI століття став кіберпростір, який є двигуном зростання економіки, поширення інформації, новою сферою державного співробітництва і суверенітету, соціального управління. Згадуючи, що Кремнієва Долина починалась з «ідеї гуманних технологій», підкреслимо, що сьогодні, в час розвитку інформаційно-комунікаційних технологій, у життя втілено прекрасні ідеї: безперервний обмін інформацією, онлайн навчання й безліч прекрасних можливостей для ефективного особистісного розвитку. Коли та за яких умов виникла загроза? Вона з'явилася з новими можливостями. Від ери новин перейшли до ери дезінформації, теорій змовоірів, фейків, поляризації суспільства, підтасовки виборів, культурних революцій. Суспільство стало більш вразливим до кіберзагроз. Чи захищені ті, хто проводить безліч часу в віртуальному світі, чи захищені люди, банки, компанії, політичні партії, державні відомства і держави від кібератак, від негативних наслідків, до яких сьогодні призвело користування новітніми технологіями? Сьогодні тема безпеки в кіберпросторі є найбільш затребуваною суспільством, оскільки це стосується кожного, хто стикається зі світом інформаційних технологій. Проблема досить актуальна, що доведено в документальному фільмі 2020 року режисера Джеффа Орловскі «Соціальна дилема». Колишні співробітники Google, Instagram, Twitter, YouTube, Tik Tok, Snapchat і Facebook (FB) розповідають про те, як соціальні мережі маніпулюють користувачами. Трістан Гарріс, фахівець з етичного дизайну Google стверджує, що у людей виробляється залежність. Він доводить, що 50 молодих розробників (від 20 до 30 років) ухвалюють рішення, яке потім впливає на 2 мільярди людей. Для цього постійно оновлюються алгоритми, які допомагають сайтам передбачати інтереси користувачів, щоб продавати більше реклами. Дослідники обґрунтовують, як на глобальному рівні використовуються соціальні мережі, щоб дестабілізувати обстановку в країнах, поширювати неправдиву інформацію. Крім цього, Тім Кендел, який відповідає за монетизацію у FB, називає соцмережі машинами для виробництва грошей. Дивлячись грошей є вплив на вчинки представників інформаційного простору, на мислення суспільства. Зі слів авторів, можна зробити висновок, що «продається майбутнє людей. Їх увага, час і життя, а платформами соціальних мереж заробляються трильйони доларів» [1, 2, 3].

Справжня дилема для суспільства - це вплив платформ на свідомість людей, а особливо молоді. Хто їх захистить від шкідливого впливу, де контроль, регулювання в перегляді YouTube та інших ресурсів? На перший погляд невинні кліки в інтернеті, такі як лайки, насправді діють на самооцінку людей, викликають дисфункції психіки. Психологи наводять статистику, що сьогодні стрибок у депресивній тривожності, депресій, самогубствах за останні роки зростає. Не менш важливим є захист від тотального стеження, хакерських атак, вірусів, підробки даних, впливу на роботу й продуктивність співробітників, використовування інформації проти людини, забезпечення конфіденційності та доступності даних, ресурсів, а саме необхідно захистити дані на етапі їх обробки та зберігання. Наразі зростає потреба в особистій кібербезпеці, тому що чим далі, тим більше ми "зростаємось" із нашими гаджетами. У 2016 році в Одесі на

конференції Black Sea Summit презентували вперше в Україні вживлений людині чіп у руку, яким вона могла оплачувати рахунки, як банківською карткою. З 2018 року чіпи, які би замінювали ключі, карти, ідентифікаційні дані, імплантували в інших країнах. Apple заснували тенденцію на FaceID, завдяки якій вже можна розплачуватися на касі та ідентифікувати людину просто за обличчям [2, 4, 5].

Протидія економічним злочинам, злочинам проти екосистем, ядерних об'єктів, антимонопольна безпека, захист від крадіжок інтелектуальної власності, шпіонажу -- один з етапів кібербезпеки. Ряд судових позовів вказує на недосконалість захисту в цій сфері. Google вже кілька разів була оштрафована Європейською комісією за порушення антимонопольного законодавства на загальну суму 8,2 млрд євро. У 2014 році компанія «Лабораторія Касперського» спільно з Європолом та Інтерполом розкрила групу Carbanak, яка протягом багатьох років виводила кошти з банків через банкомати або онлайн-банкінг (позов до федерального суду в штаті Каліфорнія США від 2 червня 2020). Google звинуватили в незаконному вторгненні в приватне життя мільйонів користувачів, шляхом відстеження їх дій у випадках, коли вікна браузерів відкривалися в режимі інкогніто. Компанію звинувачують, що вона дізнавалась про хобі користувачів, коханих, звички та інтимні речі, які вони шукають в інтернеті [2, 5].

Україна, як і більшість країн світу не уникла участі у інформаційній війні, яка характеризується спонуканням до хаосу через соціальні мережі, розповсюдженнямрізномантітних політичних, економічних та соціальних фейків відносно діяльності урядових структур, з використанням мобільних кібератак. Загроза національній безпеці країни потребує створення Стратегії кібербезпеки країни, особливо, з огляду на сучасний політичний стан держави. Указом Президента України від 15 березня 2016 року було прийнято Закон України «Про основні засади забезпечення кібербезпеки України». На жаль, дія цього Закону не поширюється на послуги, пов'язані зі змістом інформації, що передається, зберігається в соціальних мережах, у мережі Інтернет. 09 травня 2018 року набрала чинності Директива Європейського парламенту і Ради (ЄС) №2016/1148, під назвою «Безпека мереж та інформації» (Network and Information Security). Нормативно правове забезпечення кібербезпеки – складний процес, але це складова успішного бізнесу, захисту особистості і в цілому цивілізації. Світова спільнота найближчим має звернути увагу на удосконалення правового забезпечення кібербезпеки і належної відповідальності за вчинення інформаційних кіберзлочинів проти людства. Світ має стати розумнішим і кращим, чого має прагнути людство.

Список використаних джерел

1. *Алгоритм должен быть разрушен: Netflix выпустил фильм о влиянии соцсетей на человечество [Електронний ресурс]. Режим доступу: https://ms.detector.media/trends/post/25581/2020-09-25-algoritm-dolzhen-byt-razrushen-netflix-vypustil-film-o-vliyanii-sotssetei-na-chelovechestvo/.*
2. *Espreso.tv. News [Електронний ресурс]. Режим доступу: https://espreso.tv/news/2020/06/05/nimechchyna_maye_dokazy_prychetnosti_rf_do_masshtabnoyi_kiberataky_na_bundestag_media.*
3. *Ukranews.com [Електронний ресурс]. Режим доступу: https://ukranews.com/ua/news/706732-nimechchyna-dovela-prychetnist-rosiyi-v-kiberatatsi-na-bundestag.*
4. *Суспільне. Новини. [Електронний ресурс]. Режим доступу: https://suspilne.media/61873-vsesvitnij-den-zapobigannia-samogubstvam-navinciatno-poshreni-mifi-pro-suicid/.*
5. *Відшкодування збитків за порушення конкуренції: національні та світові тенденції private enforcement [Електронний ресурс]. Режим доступу: https://yur-gazeta.com/publications/practice/antimonopolne-konkurentne-pravo/vidshkoduvannya-zbitkiv-za-porushennya-konkurenciyi-nacionalni-ta-svitovi-tendenciyi-private-enforce.html.*