**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**Одеський національний технологічний університет**
**Університет Інформатики і прикладних знань, м.Лодзь, Польща**
**Національний технічний університет України «Київський політехнічний інститут»**
**Навчально-науковий інститут комп'ютерних систем і технологій «Індустрія 4.0» ім. П.М. Платонова**

**XXIII Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів**

# «СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

***Матеріали конференції***

Одеса

**20-21 квітня 2023 р.**

Стан, досягнення та перспективи інформаційних систем і технологій / Матеріали XXIII Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 20-21 квітня 2023 р**.** - Одеса, Видавництво ОНТУ, 2023 р. – 449 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 IT, так і для викладачів, магістрів і студентів вищих навчальних закладів, які навчаються за напрямами і спеціальностями програмного забезпечення, обчислювальної техніки і автоматизованих систем, прикладної математики та обробки інформації, буде корисним професіоналам з комп'ютерного моделювання та розробки комп'ютерних ігор.

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 інформаційних технологій 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.

| | |
|---|---|
| 7. Порівняльний аналіз сучасних шляхів діагностики складних технічних виробничих систем. **Лактіонов О.** (Національний університет «Полтавська політехніка) | 93 |
| 8. Optimization of paths, taking into account the significance of intermediate points. **Мазурок І.Є., Веремйов К.В.** (Одеський національний університет ім. Мечникова) | 95 |
| 9. Методика навчання фахівців із інформаційної безпеки соціальної інженерії з використанням OSINT і мови SIEVE. **Миронов І. В., Болтач С. В.** (Одеський національний технологічний університет) | 97 |
| 10. Дослідження факторів впливу на безпеку мобільних застосунків на прикладі клієнтської частини кіберфізичної системи розумної парковки. **Павлова О.О., Авсієвич В.Р., Кузьмін А.А.** (Хмельницький національний університет ) | 98 |
| 11. Парсинг тексту: використання потужностей NLP задля підвищення точності отримуваних даних. **Пелович Д. В., Смиш О. Р.** (Національний університет «Києво-Могилянська академія») | 100 |
| 12. Захист підприємств від кібератак на корпоративні мережі. **Петрук Д. С.** (Волинський національни університет імені Лесі Українки) | 102 |
| 13. Використання мобільних застосунків у роботі з документацією ТОВ "Аграна Фрут Україна". **Погоріла Ю. В.** (Донецький національний університет імені Василя Стуса) | 103 |
| 14. Технологія HDR у моніторах. **Романюк О. Н., Захарчук М. Д., Романюк О.В., Коробейнікова Т. І.** (Вінницький національний технічний університет, Національний університет «Львівська політехніка») | 105 |
| 15. Проєктування інформаційної системи управління сегрегаційним комплексом збору відходів оперативної поліграфії. **Сторожук Д.І.** (Українська академія друкарства) | 107 |
| 16. Дослідження методів перетворення повідомлень у бортових автомобільних системах. **Чайковський О.Р., Селіванова А.В.** (Одеський національний технологічний університет) | 109 |
| 17. Процес безпечної передачі інформації у мобільному додатку “Студент ЧДТУ” з Використанням Spring Security на основі JWT. **Куницька С.Ю., Архіпов М.О., Чоповенко В.М.** (Черкаський державний технологічний університет) | 110 |
| 18. Захист даних та вихідних файлів від несанкціонованого доступу та копіювання комп’ютерних відеоігор. **Шаповал В.В.** (Київський національний університет імені Тараса Шевченка) | 112 |
| 19. Програмне забезпечення для забезпечення безпеки резервного архівування даних у хмарних системах. **Шевчук Р.П., Заріцький О.І.** (Західноукраїнський національний університет) | 114 |
| 20. Вплив війни в Україні на кібербезпеку. **Шередега Р.О., Бутенко Т.А.** (Харківський державний біотехнологічний університет ) | 116 |
| 21. Дослідження застосування стандартів PAPERLESS у закладах вищої освіти. **Чіклікчі О.С., Лукашенко Д.О., Ольшевська О.В.** (Одеський національний технологічний університет) | 117 |
| 22. 3-D візуалізація авторадіограмм радіоактивних частинок. **Новіков А.М.** (Інститут проблем безпеки атомних електростанцій Національної академії наук України) | 119 |
| **Розділ 3: Нові інформаційні технології в освіті** | 121 |
| 1. Development of a methodology for evaluating the efficiency of ship operator model. **Nosov P.S., Masonkova M.M., Diahyleva P.S., Solovey O.S.** (Херсонська державна морська академія) | 121 |
| 2. Optimization of management processes for maritime transport personnel qualification. **Nosov P.S., Ponomaryova V.P., Diahyleva O.S., Ben A.P.** (Херсонська державна морська академія) | 123 |
| 3. Using SolidWorks in modern education and science. **Rudyk O.Yu., Baranov I.I., Gereta M.M., Dytynyuk V.O., Fedoryshyn S.I.** (Хмельницький національний університет) | 125 |

**УДК 004.9**

# ВПЛИВ ВІЙНИ В УКРАЇНІ НА КІБЕРБЕЗПЕКУ

**ШЕРЕДЕГА Р.О., БУТЕНКО Т.А.**
(ruslan.sheredega@gmail.com)
Харківський державний біотехнологічний університет

*Розглянуті питання збільшення активності кіберзагроз з початком повномасштабного вторгнення через різні канали доступу до користувачів в Україні та за кордоном; кроки української влади для захисту від кібератак та рекомендації щодо забезпечення захисту своїх інформаційних ресурсів.*

З початком Україна неодноразово ставала ціллю кіберзлочинців. У січні-квітні 2022 року загальна кількість виявлених загроз зросла на 20% порівняно з останніми чотирма місяцями 2021 року. Зокрема збільшилась кількість шпигунських програм та кібератак, які поширюються через електронну пошту.

Кількість загроз, які поширювалися через електронні листи, у перші місяці 2022 року збільшилася на 37%. Це найбільше зростання цього виду загроз із 2020 року. Така динаміка пов'язана з відновленням діяльності ботнета Emotet, який масово розсилав користувачам спам-повідомлення зі шкідливими вкладеннями. Крім звичайних тем електронних листів, таких як платежі, замовлення та доставки, з початку року росла кількість шкідливих повідомлень на тему подорожей. Також повернення Emotet вплинуло на зростання кількості завантажувачів на 121%.

Кількість загроз для викрадення інформації зросла на 12%. При цьому найбільше зростання було у підкатегоріях шпигунського та шкідливого банківського програмного забезпечення. Зокрема кількість шпигунських програм у цей період зросла на близько 18%.

Попри незначний ріст кількості загроз для Android, на цій операційній системі найпоширенішими теж залишалися шпигунські програми. Активність таких програм, які можуть отримати доступ до різних функцій смартфона, зокрема здійснювати запис аудіо та відео, збільшилась на 170%. Зростання їх виявлення свідчить про пошук зловмисників способів заробітку на особистих або навіть корпоративних даних на пристроях Android. Щодо операційної системи macOS, то майже половина всіх виявлених зразків становили потенційні небажані додатки.

Одразу після вторгнення росії в Україну шахраї вирішили скористатися бажанням людей зі всього світу підтримати українців, зокрема зловмисники під цим приводом виманювали кошти у користувачів. Вже 24 лютого спеціалісти виявили значне зростання спам-повідомлень та перші шахрайські домени, які використовували тему війни.

У середньому телеметрія компанії ESET щоденно виявляла 4,8 мільйонів вебзагроз та 370 тисяч шкідливих URL-адрес у всьому світі. При цьому кількість заблокованих фішингових URL-адрес зросла майже на 30%. Найвищий рівень виявлення припав на 07 березня, збільшившись утричі за середній щоденний показник з початку 2022 року.

Крім цього, за даними компанії ESET приблизно третина фішингових URL-адрес, виявлених у січні-квітні 2022, маскувалися під фінансові організації. Зловмисники використовували фальшиві сторінки для входу у Facebook та WhatsApp також як приманку.

Раніше за спостереженням аналітиків ESET, хакери використовували LinkedIn і WhatsApp під час атак на оборонну галузь країн Європи.

Війна в Україні також значно вплинула на поширення загроз у світі. Зокрема ця тема активно використовувалася у спам-повідомленнях та на шкідливих сайтах. Зокрема з 23 лютого під час атак на українські організації зловмисники використали ряд шкідливих

програм для знищення даних, а також унікальну загрозу Industroyer, націлену на енергетичний сектор.

Щоб не стати жертвою різних видів кіберзагроз, варто дотримуватись базових правил кібербезпеки, зокрема використовувати надійні паролі та двофакторну аутентифікацію, подбати про безпеку мобільного пристрою, а також забезпечити надійний захист ноутбука.

Українська влада встановила більш досконале апаратне і програмне забезпечення і прийняла законодавство, щоб надати своїм регулюючим органам більше повноважень і гнучкості для захисту даних, які вони зберігають про громадян. Однак це не створило герметичну архітектуру і деякі атаки пройшли успішно. росія посилила свої фішингові атаки через соціальні мережі та використала вкрадені акаунти, щоб мати змогу орієнтуватися на окремих осіб всередині уряду. Але обмеження доступу до кількості користувачів, які мали фізичні маркери як другий фактор аутентифікації, допомогло уникнути катастрофи.

**СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:**

1. Рейтинг Інтернет-загроз: IT-фахівці проаналізували вплив війни в Україні на кібербезпеку [Електронний ресурс] – Режим доступу: https://www.unian.ua/techno/reyting-internet-zagroz-it-fahivci-proanalizuvali-vpliv-viyni-v-ukrajini-na-kiberbezbeku-11852508.html.

**2.** Impact of Ukraine-Russia war: Cybersecurity has improved for all [Електронний ресурс] – Режим доступу: https://www.washingtonpost.com/technology/2023/02/25/ukraine-war-cyber-security/.

**УДК 004.912:[657.37:378.4]**

## ДОСЛІДЖЕННЯ ЗАСТОСУВАННЯ СТАНДАРТІВ PAPERLESS У ЗАКЛАДАХ ВИЩОЇ ОСВІТИ

**ЧІКЛІКЧІ О.С., ЛУКАШЕНКО Д.О., ОЛЬШЕВСЬКА О.В.**
Одеський національний технологічний університет

Наш світ неухильно стає цифровим, а суспільством поступово переходить до paperless (безпаперової) ери. Насьогодні, кожна людина має можливість перевірити електронну пошту з будь-якого пристрою, керувати банківськими рахунками та рахунками кредитних карток в Інтернеті та навіть надсилати запрошення цифровим способом.

Оскільки ці зміни відбуваються в широких масштабах, можливість переходу на електронну документацію має унікальний вплив на окремі сфери. Зрештою, це економить гроші, час та зменшує вплив на навколишнє середовище. Одним з таких ринків, який стає безпаперовим через переваги, які він пропонує, є освіта, а також компанії, які обслуговують академічні кола.

Оскільки заклади освіти переходять на безпаперові документи, їм потрібні життєздатні, надійні електронні версії найважливіших документів, включаючи дипломи, сертифікати, стенограми, листи про вступ та документи про фінансову допомогу. Конфіденційний характер цих документів створює проблеми для IT-відділів, щоб підтримувати надійну та безпечну мережу, а також дотримуватися всіх правил конфіденційності даних. Зокрема, освітній простір все частіше шукає шляхи захисту цих електронних документів, адже як можна гарантувати, що електронні версії цих важливих документів настільки ж надійні, як і паперові версії, які вони замінюють.

Багато закладів вищої освіти (ЗВО) дійшли висновку, що підтримка економічно вигідного бек-офісу є важливою стратегією стабілізації плати за навчання та операційних витрат. Одним із способів зменшити витрати - зменшити залежність від паперових документів. Паперові операції коштують дорого, а для зберігання паперових документів