

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Одеська національна академія харчових технологій
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

XXI Всеукраїнська науково-технічна конференція
молодих вчених, аспірантів та студентів

«СТАН, ДОСЯГНЕННЯ ТА ПЕРСПЕКТИВИ
ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ»

Матеріали конференції



Одеса

22-23 квітня 2021 р.

Стан, досягнення та перспективи інформаційних систем і технологій / Матеріали XXI Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 22-23 квітня 2021 р. - Одеса, Видавництво ОНАХТ, 2021 р. – 229 с.

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

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова - д.т.н., проф., **Єгоров Б.В.**, ректор ОНАХТ.

Співголови:

Поварова Н.М. – к.т.н., доц., проректор з наукової роботи ОНАХТ,
Котлик С.В. – к.т.н., доц., директор ННІКСіТ "Індустрія 4.0" ОНАХТ,
Даріуш Долива, д.математичн.наук, уповноважений декана факультету Інформатики УІтаПЗ, м.Лодзь, Польща,
Ковалюк Т.В. - к.т.н., доц. кафедри АСОІтаУ НТУУ «Київський політехнічний інститут»

Члени оргкомітету:

Плотніков В. М. – д.т.н., проф., завідувач кафедри ІТтаКБ ОНАХТ,
Артеменко С.В. – д.т.н., проф., завідувач кафедри КІ ОНАХТ,
Хобін В.А. – д.т.н., проф., завідувач кафедри АТПтаРС ОНАХТ,
Тарасенко В.П. – д.т.н., проф., завідувач кафедри СКС НТУУ «Київський політехнічний інститут»,
Невлюдов І.Ш. – д.т.н., проф., завідувач кафедри КІТАМ ХНУРЕ,
Мельник А.О. – д.т.н., проф., завідувач кафедри ЕОМ НУ “Львівська політехніка”,
Жуков І.А. – д.т.н., проф., завідувач кафедри КСтаМ НАУ.

Матеріали подано українською, російською та англійською мовами.
Редактор збірника Котлик С.В.

университет информатики и радиоэлектроники, Республика Беларусь)	
THE STATE OF CYBER SECURITY DEVELOPMENT FOR CERTAIN CRITICAL DOMAINS IN THE REPUBLIC OF MOLDOVA. AURELIAN BUZDUGAN (Moldova State University, Republic of Moldova)	38
АНАЛІЗ ШИФРІВ У БЕЗДРОТОВИХ МЕРЕЖАХ. КУЛЯ Ю.Е. (Харківський національний університет радіоелектроніки), ГАВРИЛОВА А.А. (Харківський національний економічний університет імені Семена Кузнеця)	40
ВИКОРИСТАННЯ СИСТЕМИ ДЛЯ РОЗПОДІЛЕНОГО ЗБЕРІГАННЯ ІНФОРМАЦІЇ В АНТИ-ФОРЕНЗИЦІ. МАКАРЕНКО А.О. (Харківський національний економічний університет імені Семена Кузнеця)	42
DDOS-АТАКИ НА ОСВІТНІ ВЕБ-РЕСУРСИ. КОРОЛЕВИЧ Є.М., ПЛОТНИКОВ В.М., ЗІНЧЕНКО І.І. (Одеська національна академія харчових технологій)	44
ОЦІНКА ПРОБЛЕМ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФРАСТРУКТУРІ “РОЗУМНИЙ БУДИНОК”. ЄРЕЩЕНКО О.Д. , (Харківський національний університет імені Семена Кузнеця)	46
ПРО ВРАХУВАННЯ СТАВЛЕННЯ ДО РИЗИКУ В ПРОСТОРОВИХ СИСТЕМАХ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ. КЛЕПАТСЬКА В.В., БУЧИНСЬКА І.В., КУЗНІЧЕНКО С.Д. (Одеський державний екологічний університет)	47
КЛАСИФІКАЦІЯ ЗАГРОЗ ВЕБ-ЗАСТОСУНКІВ. ЛАВРЕНОВ В.А., СІРЕНКО О.І. , (Одеська національна академія харчових технологій)	49
PROOF OF ZERO-KNOWLEDGE IN THE TASKS OF ANONYMIZATION OF FINANCIAL TRANSACTIONS. ПРОКОПОВ Е.К. (Odessa I.I. Mechnikov National University)	51
РОЗРОБКА ПРОГРАМИ ДЛЯ ПЕРЕВІРКИ ТЕКСТІВ НА ОРИГІНАЛЬНІСТЬ. БЕВЗ С.В., БУРБЕЛО С.М., ВОЙТКО В.В., ЗАВАЛЬНЮК Є.К. (Вінницький національний технічний університет)	52
АУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ З ВИКОРИСТАННЯМ АНАЛІЗУ КЛАВІАТУРНОГО ПОЧЕРКУ. КАСІЯНЕНКО Д.В. (Київський національний університет імені Тараса Шевченка)	54
РОЗРОБКА УНІВЕРСАЛЬНОЇ ІНФОРМАЦІЙНОЇ УПРАВЛЯЮЧОЇ СИСТЕМИ ДЛЯ ОРГАНІЗАЦІЇ РОБОТИ СКЛАДУ. КРИВИЙ Є.О., ШВЕЦЬ Н.В. (Одеська національна академія харчових технологій)	56
ВИКОРИСТАННЯ ГРАФІЧНОГО ФРЕЙМВОРКУ LIBGDX ДЛЯ РОЗРОБКИ КРОСПЛАТФОРМНИХ ІГОР. РОМАНЮК О.Н., ВЕРЕНЬКО А.І., МИРГОРОДСЬКИЙ А. В. (Вінницький національний технічний університет)	58
DEVELOPMENT OF MODELS AND ALGORITHMS FOR THREE-FACTOR AUTHENTICATION SYSTEM. DONETS O.V. (V. N. Karazin Kharkiv National University), RADOUTSKA A.K. (Kharkiv National University of Radio Electronics)	60
КОМП'ЮТЕРИЗОВАНИЙ ВІДБІР ОПЕРАТОРІВ БПЛА. МАРУЩАК А.В., ШМАЛЮХ В.А., РОМАНЮК О.Н., КОВАЛЬ Л.Г. (Вінницький національний технічний університет)	61
ПАСИВНИЙ МЕРЕЖЕВИЙ АНАЛІЗ ТА ЗАСОБИ ЙОГО ВДОСКОНАЛЕННЯ. ЖОЛНЕР І.Д., МИРУТЕНКО Л.В., ШЕСТАК Я.В. (Київський національний університет ім. Тараса Шевченка)	63
АНАЛІЗ ХМАРНОЇ ТЕХНОЛОГІЇ GOOGLE DRIVE. РОМАНЮК О.Н., БОРИСОВА К.О., КАТЄЛЬНИКОВ Д.І. (Вінницький національний технічний університет)	65
АНАЛІЗ МЕХАНІЗМІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В ДЕЦЕНТРАЛІЗОВАНИХ СИСТЕМАХ. ТРОЦЬЙ А.О. (Харківський національний економічний університет імені Семена Кузнеця)	67

УДК [004.383.2:004.738.5:378]:004.056.5

DDOS-АТАКИ НА ОСВІТНІ ВЕБ-РЕСУРСИ

КОРОЛЕВИЧ Є.М.

Наукові керівники: д.т.н., зав. кафедри ІТКБ ПЛОТНІКОВ В. М.,

директор НТБ ЗІНЧЕНКО І. І.

Одеська національна академія харчових технологій

На даний момент більшість компаній зберігає інформацію в електронному форматі на серверах. Таке зберігання даних технологій має як переваги так, і недоліки. Одним з головних недоліків це кібератаки, адже, щороку їх кількість на веб-ресурси збільшується.

Сучасне зловмисне програмне забезпечення являє собою складну багатофункційну програмну систему та комплекс, який побудований з використанням ефективних методів створення програмних засобів та методів поширення зловмисного коду [1]. Зловмисники найчастіше використовують, для зараження жертв, декілька типів шкідливих програм одночасно[2].

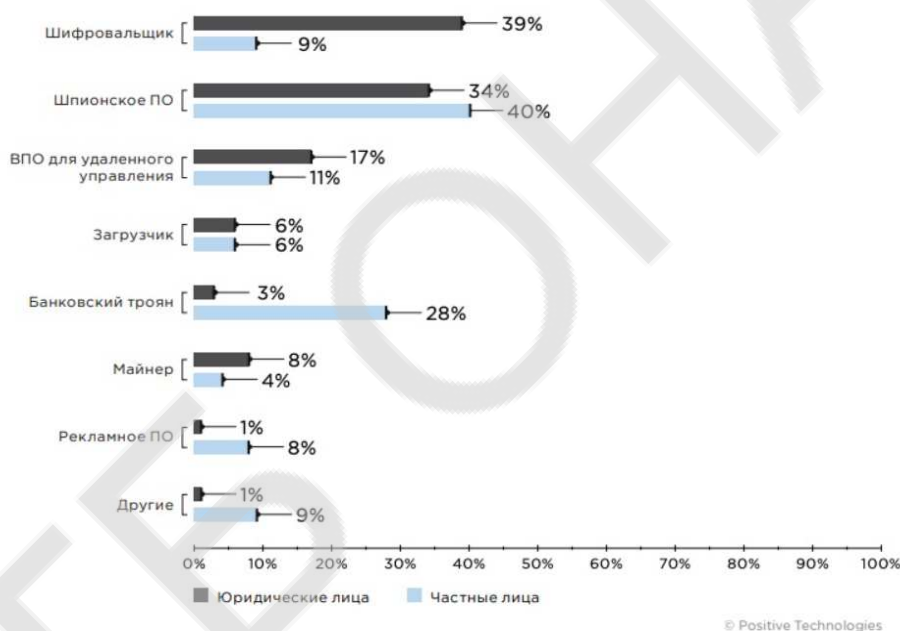


Рис. 1 «Доля атак з використанням зловмисного програмного забезпечення»

Сучасні атаки, які завдають великого збитку компаніям, вважаються віддаленні мережеві атаки, серед яких найбільш небезпечною є Distributed Denial of Service (DDoS-атака)[3]. DDoS-атака – «розподілена відмова в обслуговуванні» (англ. – Distributed Denial-of-service attack) – спрямована на обчислювальну систему, з метою створення таких умов, за яких користувачі системи не можуть отримати доступ до деяких ресурсів або сервісів [4].

Оскільки персональні ресурси користувачів мережі зазвичай не мають належного захисту та потужності, щоб протидіяти DDoS-атаці, тому у більшості ситуацій, в яких DDoS-атака здійснюється на особистість, вебсайт людини або ж власне персональний комп'ютер, причинами можуть бути особиста неприязнь зловмисника, розвага або ж використання особистості в якості тренувальної мішені [5].

Окремо можна говорити про використання комп'ютерів користувачів як засобу реалізації DDoS-атаки, перетворення ресурсів користувачів в так звані «зомбі-комп'ютери».

Зазвичай, «зомбування» здійснюється за допомогою троянської програми, що встановлює необхідне зловмиснику фонове завдання. В середньому, інтенсивність DDoS-атаки, що відповідає даному сценарію, складає 100 Мбіт/с. Це еквівалентно, наприклад, тому, що на сайт зайшли 1000 користувачів і вони кожену секунду оновлюють сторінку [5].

Захист від DDoS-атак розділений на три напрямки: запобігання, виявлення та реакція на атаку.

Основною метою запобігання атаці є припинення атак до нанесення нею збитків. Для цього використовують наступні типи, а саме виконують фільтрацію вхідного/вихідного трафіку та на рівні маршрутизаторів, використовують протоколи перевірки адрес джерела.

Методи виявлення атаки спрямовані на контроль та дослідження системи в якій виникають нетипові події. Є такі типи як відстеження активної взаємодії, вкладені поля, на основі хеша, сигнатурні та статистичні.

Методи реакції на атаку в яких жертва реагує на атаку після виявлення. Використовують наступні види StopIt, SIFF, TVA.

У цих методах відповідальність на виявлення і боротьбу з нападом лежить на самій жертві.

Отже, захист інформації відіграє надзвичайно важливу роль, як в забезпеченні безпеки даних підприємств, так і приватних даних користувачів. Також для автоматизації роботи фахівця з кібербезпеки можна використовувати сканери вразливості, основним завданням яких є можливість сканувати мережу для швидкого виявлення вірусу або підозрілих процесів та їх усунення.

Використання сучасних технологій для зберігання даних є зручним способом але вимагає певного комплексу засобів для захисту, але розробка в даному напрямку є дуже перспективною. Отже в майбутньому захист інформації буде ставати більш надійним.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Створене посилання: Савенко О. Теорія та практика створення розподілених систем виявлення зловмисного програмного забезпечення в локальних комп'ютерних мережах : дис. на здобуття наук. ступеня доктор технічних наук : 05.13.05 : захищена 25.10.2019 : затв. NaN.NaN.NaN / Савенко Олег . - Львів. - 27 с. Транслітерація: Savenko O. Teoriya ta praktika stvorennya rozpodilениkh sistem viyavlennya zlovmisnoho prohramnoho zabezpechennya v lokal`nikh komp`yuternikh merezhakh : dis. na zdobuttya nauk. stupenya doktor tekhnichnikh nauk : 05.13.05 : zakhishchena 25.10.2019 : zatv. NaN.NaN.NaN / Savenko Oleh . - L`viv. - 27 s.
2. Створене посилання: <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q2/> // Positive Technologies [Веб-сайт]. - URL: <https://www.ptsecurity.com/> (дата звернення: 08.03.2021). Транслітерація: <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q2/> // Positive Technologies [Veb-sayt]. - URL: <https://www.ptsecurity.com/> (data zvernennya: 08.03.2021).
3. DDoS-атаки: реальна небезпека віртуального світу [Електронний ресурс]. – Режим доступу: <http://zillya.ua/ddos-ataki-realna-nebezpeka-virtualnogo-svitu>.
4. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с.: ил.
5. Створене посилання: ІЄРАРХІЯ ФАКТОРІВ ТИПОВИХ СЦЕНАРІЇВ РЕАЛІЗАЦІЇ DDOS-АТАК - Київ. - 18 с. - (МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ В ЕКОНОМІЦІ). Транслітерація: ІYеRARKhIYа ФАКТОРИV ТИПОВИkh STSEHARIYiV REALIZATSIYi DDOS-АТАК - Kiyiv. - 18 s. - (МАТЕМАТИChNE MODELyVANNYа V EKONOMITSI).

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

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

Одеса

22-23 квітня 2021 р.

Збірник включає доповіді учасників конференції. Тези доповідей публікуються у вигляді, в якому вони були подані авторами.

Відповідальність за зміст і форму подачі матеріалу несуть автори статей.

Редакційна колегія: Котлик С.В., Корнієнко Ю.К.

Комп'ютерний набір і верстка: Соколова О.П.

Відповідальний за випуск: Котлик С.В.