

SCIENTIFIC  
COLLECTION  
«INTERCONF»

**№ 2 (29)**

**September, 2020**

THE ISSUE CONTAINS:

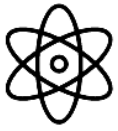
Proceedings of the 6<sup>th</sup>  
International Scientific and  
Practical Conference

**SCIENTIFIC HORIZON IN THE  
CONTEXT OF SOCIAL CRISES**



**TOKYO, JAPAN**

**16-18.09.2020**



**InterConf**  
Scientific Publishing Center

# **SCIENTIFIC COLLECTION «INTERCONF»**

**№ 2 (29) | September, 2020**

## **THE ISSUE CONTAINS:**

Proceedings of the 6th International Scientific and Practical Conference

## **SCIENTIFIC HORIZON IN THE CONTEXT OF SOCIAL CRISES**

TOKYO, JAPAN

**16-18.09.2020**

TOKYO  
2020

UDC 001.1


S 40 *Scientific Collection «InterConf», (29): with the Proceedings of the 6<sup>th</sup> International Scientific and Practical Conference «Scientific Horizon in the Context of Social Crises» (September 16-18, 2020). Tokyo, Japan: Otsuki Press, 2020. 138 p.*

ISBN 978-4-272-00922-0

## EDITOR

**Polina Vuitsik**   
PhD in Economics  
Jagiellonian University, Poland  
@ p.vuitsik.prof@gmail.com

## COORDINATOR

**Mariia Granko**   
Coordination Director in Ukraine  
Scientific Publishing Center InterConf  
@ info@interconf.top


## EDITORIAL BOARD

Mark Alexandr Wagner (DSc. in Psychology)  
University of Vienna, Austria  
@ mw6002832@gmail.com;

Dan Goltsman (Doctoral student)  
Riga Stradiņš University, Republic of Latvia;


Katherine Richard (DSc in Law),  
Hasselt University, Kingdom of Belgium  
@ katherine.richard@protonmail.com;

Richard Brouillet (LL.B.),  
University of Ottawa, Canada;

Stanyslav Novak  (DSc in Engineering)  
University of Warsaw, Poland  
@ novaks657@gmail.com;


Yasser Rahrovani (PhD in Engineering)  
Ivey School of Business, The University of Western  
Ontario, Canada;

Elise Bant (LL.D.),  
The University of Sydney, Australia;

Anna Svoboda  (Doctoral student)  
University of Economics, Czech Republic  
@ annasvobodaprague@yahoo.com;

Dr. Alben Yaneva (DSc. in Sociology and Antropology),  
Manchester School of Architecture, UK;

Vera Gorak (PhD in Economics)  
Karlovarská Krajská Nemocnice, Czech Republic  
@ veragorak.assist@gmail.com;

Dmytro Marchenko  (PhD in Engineering)  
Mykolayiv National Agrarian University  
(MNAU), Ukraine;

Kanako Tanaka (PhD in Engineering),  
Japan Science and Technology Agency, Japan;

George McGrown (PhD in Finance)  
University of Florida, USA  
@ mcgown.geor@gmail.com;

Alexander Schieler (PhD in Sociology),  
Transilvania University of Brasov, Romania

---

If you have any questions or concerns, please contact a coordinator Mariia Granko.

---

**The recommended citation:**

Surname N. (2020). Title of article or abstract. *Scientific Collection «InterConf», (29): with the Proceedings of the 6th International Scientific and Practical Conference «Scientific Horizon in the Context of Social Crises» (September 16-18, 2020) in Tokyo, Japan; pp. 21-27. Available at: [https://interconf.top/...](https://interconf.top/)*



This issue of Scientific Collection «InterConf» contains the International Scientific and Practical Conference. The conference provides an interdisciplinary forum for researchers, practitioners and scholars to present and discuss the most recent innovations and developments in modern science. The aim of conference is to enable academics, researchers, practitioners and college students to publish their research findings, ideas, developments, and innovations.

©2020 Otsuki Press  
©2020 Authors of the abstracts  
©2020 Scientific Publishing Center InterConf


contact e-mail: [japan@interconf.top](mailto:japan@interconf.top)  
webpage: [www.interconf.top](http://www.interconf.top)

## TABLE OF CONTENTS


## INTERNATIONAL ECONOMICS AND INTERNATIONAL RELATIONS

Зрайло І.І.		ЗОВНІШНЬОЕКОНОМІЧНИЙ ПОТЕНЦІАЛ ЗЕРНО ПРОДУКТОВОГО ПІДКОМПЛЕКСУ АПК УКРАЇНИ: ЧИННИКИ, ФОРМИ ТА ІНСТРУМЕНТИ ЙОГО РЕАЛІЗАЦІЇ	6
Мукумова Н.Н.		ГЛОБАЛЬНЫЕ РЕЙТИНГИ ВУЗОВ	11



## MARKETING, ADVERTISING AND PR

Монтрін І.І.		УПРАВЛІННЯ ЯКІСТЮ ТОВАРІВ ТА ПОСЛУГ В СИСТЕМІ БРЕНД-МЕНЕДЖМЕНТУ НА ПРИКЛАДІ ТОВ «ЕКО»	18
Остроухова Я.Є.			





## FINANCE AND CREDIT

Бурдонос Л.І.		ВПЛИВ КРЕДИТНИХ ОПЕРАЦІЙ НА ФІНАНСОВИЙ СТАН БАНКУ	22
Виноградня В.М.			


## ACCOUNTING AND AUDITING

Косташ Т.В.		УПРАВЛІННЯ РИЗИКАМИ В СИСТЕМІ БУХГАЛТЕРСЬКОГО ОБЛІКУ ПІДПРИЄМСТВА	27
Шара Є.Ю.		ВИЗНАННЯ ТА ОЦІНКА ДОХОДІВ ЗА НАЦІОНАЛЬНИМИ ТА МІЖНАРОДНИМИ СТАНДАРТАМИ	30


## PEDAGOGY AND EDUCATION

Antonenko M.Y.		«ROUND TABLE» AS AN INNOVATIVE COMPONENT OF THE PEDAGOGICAL APPROACH IN THE STUDY OF EARLY POSTOPERATIVE COMPLICATIONS IN PATIENTS AT THE STAGES OF DENTAL IMPLANTATION	35
Vezhnovets T.A.			
Zelinskaya N.A.			
Stolyar V.G.			
Reshetnyk L.L.			
Дудко Н.В.		НАПРЯМИ РОЗВИТКУ ДОДАТКОВОЇ ОСВІТИ ДОРΟΣЛИХ У СВІТІ	42
Курліщук І.І.		ЗАГАЛЬНІ ХАРАКТЕРИСТИКИ СУЧАСНОЇ ІНШОМОВНОЇ ОСВІТИ В УКРАЇНІ	48
Павленко І.Г.			
Сєваст'янова О.А.			
Sidenko Y.		PEDAGOGICAL CONDITIONS FOR THE FORMATION OF COGNITIVE READINESS FOR LEARNING IN SENIOR PRESCHOOLERS WITH AUTISM SPECTRUM DISORDERS	54


## POLITICAL SCIENCE AND PUBLIC ADMINISTRATION

Іваницька О.М.		ДЕРЖАВНЕ УПРАВЛІННЯ ОСВІТОЮ В УМОВАХ ГЛОБАЛЬНИХ СОЦІАЛЬНИХ КРИЗ	57
Ткачова Н.М.			
Казанська О.О.			



**GEOGRAPHY AND LOCAL HISTORY**

Шкурко К.Н. Захарова М.Е.		ЗЕЛЕНІ НАСАДЖЕННЯ ЯК СПОСІБ ФОРМУВАННЯ ЕКОЛОГІЧЕСЬКОГО МИРОВОЗЗРЕННЯ СОВРЕМЕННОЙ МОЛОДЕЖИ	62
------------------------------	---	---	----





**ARTS, CULTURAL STUDIES AND ETHNOGRAPHY**

Данилова Ю.Н. Шамсутдинова Л.Г.		ФИЛОСОФИЯ ЗВУКА И ТИШИНЫ В ЯПОНСКОЙ ТРАДИЦИОННОЙ МУЗЫКЕ	73
------------------------------------	---	---	----


**BIOLOGY AND BIOTECHNOLOGY**

Dmytruk I. Bezukh O.		INFLUENCE OF PROTEIN FACTORS IN ACUTE STROKE ON CHANGES IN MUSCLE TONE	79
Podpalova O. Kurovska V. Nozdrenko O. Vygovska O. Soroka V.		CHANGING OF THE MAXIMUM POWER OF THE SKELETAL MUSCLE RESPONSE OF ALCOHOLIC RAT UNDER ELECTRICAL STIMULATION	81


**MEDICINE AND PHARMACY**

Komola Sh.Sh. Sobitov I.Z.		ISSUES OF PREVENTION AND TREATMENT OF IRON DEFICIENCY ANEMIA IN CHILDREN	85
Podluzhnyi S.G. Fushtey I. M Sid' E. V		THE RELATIVE RISK OF LEFT VENTRICULAR REMODELING AMONG PATIENTS WITH PAROXYSMAL ATRIAL FIBRILLATION BY GENE POLYMORPHISMS RENIN-ANGIOTENSIN-ALDOSTERONE SYSTEM	87
Vygovska O. Nozdrenko O. Soroka V. Abramchuk O.		DEVELOPMENT OF MUSCLE FATIGUE IN OBESE RATS	90
Шевченко А.Н. Петрик Н.Д.		ПРОТИВОВОСПАЛИТЕЛЬНАЯ АКТИВНОСТЬ МЕЗЕНХИМАЛЬНЫХ СТЕЛОВЫХ КЛЕТОК ПРИ ХРОНИЧЕСКОМ ВОСПАЛЕНИИ, ВЫЗВАННОМ Л-КАРРАГИНАНОМ У КРЫС. ЛЕЙКОЦИТАРНО-МОНОЦИТАРНОЕ СООТНОШЕНИЕ	95

**NATURE MANAGEMENT, RESOURCE SAVING AND ECOLOGY**

Жиленко Н.В. Бойко Т.О.		СУЧАСНИЙ СТАН ЗЕЛЕНОЇ ЗОНИ ЦЕНТРАЛЬНОЇ САДИБИ ДЕРЖАВНОГО ПІДПРИЄМСТВА «ОЛЕШКІВСЬКЕ ЛІСОМИСЛИВСЬКЕ ГОСПОДАРСТВО»	99
----------------------------	---	---	----


**CHEMISTRY AND MATERIALS SCIENCE**

Чернушенко О.О. Саєвич О.В.		БУДОВА КОМПЛЕКСУ ХРОМУ (III) З АМІНОМАСЛЯНОЮ КИСЛОТОЮ	102
--------------------------------	---	---	-----


### AGROTECHNOLOGIES AND AGRICULTURAL INDUSTRY

Стефанюк С.В.		СТІЙКІСТЬ СОРТІВ ВИНОГРАДУ ДО ХВОРОБ	106
---------------	---	--------------------------------------	-----


### GENERAL ENGINEERING AND MECHANICS

Чмир В.М.		ОЦІНКА ТА АНАЛІЗ ПОКАЗНИКІВ СТІЙКОСТІ АВТОМОБІЛІВ	109
Тітов А.Ю.		ПІДРОЗДІЛІВ ОХОРОНИ КОРДОНУ	


### RADIO ENGINEERING, ELECTRONICS AND ELECTRICAL ENGINEERING

Капустин А.Г.		ИССЛЕДОВАНИЕ СТАТИЧЕСКИХ И ДИНАМИЧЕСКИХ	113
Терещенко К.В.		ХАРАКТЕРИСТИК АВИАЦИОННЫХ БЕСКОНТАКТНЫХ ГЕНЕРАТОРОВ ПОСТОЯННОГО ТОКА	


### INFORMATION AND WEB TECHNOLOGIES

Климова Т.В.		РОЛЬ ВНЕДРЕНИЯ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ	123
Бердо Р.С.		КОМПЛЕКСОВ В УЧЕБНЫЙ ПРОЦЕСС ПРИ ПОДГОТОВКЕ СТУДЕНТОВ СПЕЦИАЛЬНОСТЕЙ «ТУРИЗМ» И «ГОСТИНИЧНО-РЕСТОРАННОЕ ДЕЛО»	

### ARCHITECTURE, CONSTRUCTION AND DESIGN

Хом'як Л.В.		ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ЗД ДРУКУ У РЕСТАВРАЦІЇ.	127
Лукашук Б.Ю.		ЕКО = МАТЕРІАЛИ	

### MILITARY AFFAIRS AND NATIONAL SECURITY

Коломійцев О. В.		АНАЛІЗ КІБЕРНЕТИЧНИХ ЗАГРОЗ	129
Рябуха Ю.М.			
Третяк В.Ф.			
Меленті Є.О.			
Голубничий Д.Ю.			
Третяк Д.В.			

**MILITARY AFFAIRS AND NATIONAL SECURITY**

UDC 323:27

**Коломійцев Олексій Володимирович**

ORCID ID: 0000-0001-8228-8404

Заслужений винахідник України, доктор технічних наук,  
старший науковий співробітник, професор кафедри

Національний технічний університет «Харківський політехнічний університет», Україна

**Рябуха Юрій Миколайович**

ORCID ID: 0000-0001-9821-598x

доктор технічних наук, старший дослідник наукового центру Повітряних Сил  
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Україна

**Третяк Вячеслав Федорович**

ORCID ID: 0000-0003-2599-8834

кандидат технічних наук, доцент, провідний науковий співробітник  
наукового центру Повітряних Сил  
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Україна

**Меленті Євген Олександрович**

ORCID ID: 0000-0003-2955-2469

кандидат технічних наук, завідувач кафедри інституту підготовки  
юридичних кадрів для Служби безпеки України  
Національний юридичний університет імені Ярослава Мудрого, Україна

**Голубничий Дмитро Юрійович**

ORCID ID 0000-0002-6873-7004

кандидат технічних наук, доцент, доцент кафедри Інформаційних систем  
Харківський національний економічний університет імені Семена Кузнеця, Україна

Третяк Дар'я Вячеславівна

ORCID ID: 0000-0002-3476-2666

курсант 2 курсу інституту підготовки юридичних кадрів для Служби безпеки України  
Національний юридичний університет імені Ярослава Мудрого, Україна

## АНАЛІЗ КІБЕРНЕТИЧНИХ ЗАГРОЗ

Розвиток інформаційно-телекомунікаційних мереж та комп'ютеризація військових органів і систем управління, з одного боку, підвищує оперативність прийняття рішень та ефективність управління, а, з іншого, призводить до виникнення загрози інформаційній безпеці у вигляді можливості проведення кібернетичних атак, класифікація яких представлена на рис. 1. Кібернетична атака може бути спрямована на серверне обладнання, на програмне забезпечення або на ПЕОМ [1-4].

Атака на серверне обладнання може бути реалізована наступними шляхами:

- взлом механізму автентифікації серверів;
- несанкціоноване використання прав авторизації;
- відмова в обслуговуванні клієнтів (DoS, DDoS);
- використання сервісів серверів не за призначенням;
- виконання зловмисного коду.

Здійснити взламування автентифікації серверу можливо декількома способами. Найпоширеніший спосіб – перебір паролів (Brute-Force атака), для чого використовуються спеціальні програми, що перебирають паролі шляхом комбінування букв, цифр та спеціальних символів. Якщо на сервері передбачена система відновлення паролів, це дає змогу особі, що атакує, змінити старий пароль на свій і таким чином отримати повний доступ до серверу.

Також можливий варіант, що системний адміністратор не досить компетентний і недостатньо налаштував автентифікацію. Це дає змогу зловмиснику легко отримати доступ до серверу, не використовуючи спеціальне програмне забезпечення для взлому.



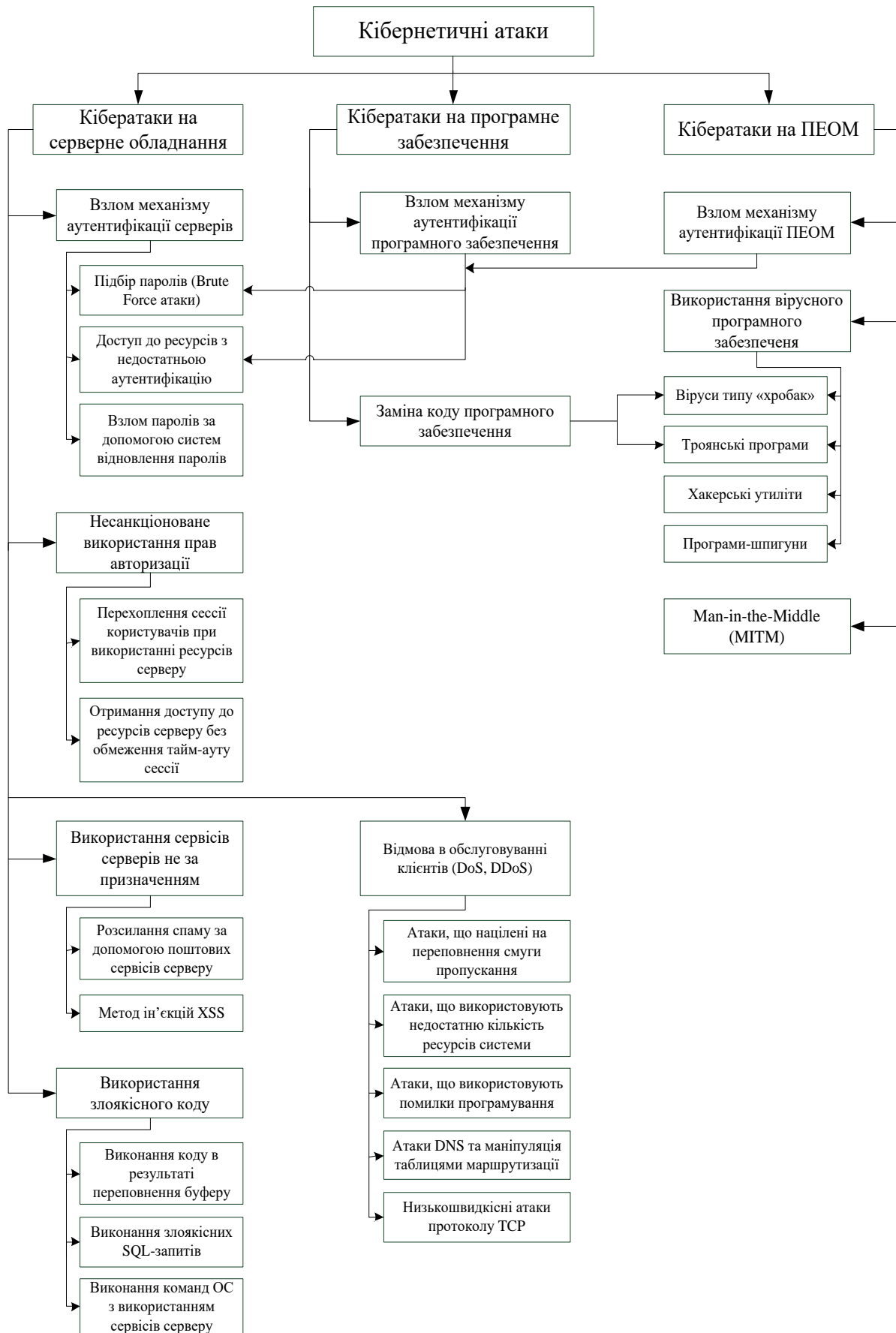


Рис. 1. Класифікація кібернетичних атак

Зловмисник може не санкціоновано отримати і використати право авторизації. Це можливо шляхом перехоплення сесії користувача, що використовує ресурси серверу. Для цього використовуються спеціальні програми моніторингу – сніфери, що перехоплюють пакети, які циркулюють у мережі. Перехопивши пакет від користувача, який намагається авторизуватися у системі, зловмисник отримує доступ до серверу від його імені. Якщо політика безпеки на сервері налаштована не досить коректно, і тайм-аут сесії необмежений, зловмиснику не треба буде повторно авторизуватися після закінчення тайм-ауту сесії, що робить процес несанкціонованого отримання інформації більш швидким і менш помітним для систем виявлення вторгнень.

Інколи зловмиснику не потрібен доступ до серверу, його метою є виведення останнього з працездатного стану для того, щоб користувачі не могли використовувати його ресурси. Для цього застосовуються DDoS-атаки. Будь-яка DDoS-атака направлена на виведення мережі з працездатного стану шляхом використання тими, хто атакує, усіх її наявних ресурсів. Внаслідок цього легітимні користувачі мережі не обслуговуються. Атака може бути реалізована як з одного комп'ютера, так і з декількох. Така атака називається DDoS (Distributed Denial of Service – розподілена атака типу "відмова в обслуговуванні").

Досить часто метою зловмисника є не сам сервер, а деякі його клієнти. В такому разі можуть бути використані поштові сервіси серверу для розсилання спаму. Або застосована XSS-ін'єкція (XSS – CrossSiteScripting – між сайтовий скриптинг), що впроваджується у веб-сторінку, яка видається сервером. Внаслідок цього усі комп'ютери, що завантажили дану сторінку будуть інфіковані.

Для взлому серверу може бути використаний спеціальний зловмисний код. Як правило це SQL-ін'єкція – один з найпоширеніших способів взлому сайтів та програм, що використовують бази даних. Вона дозволяє зловмиснику виконати довільний запит до бази даних, отримати можливість читання та запису локальних файлів, а також виконання довільних команд. Також можливе

застосування програм, при виконанні яких переповнюється буфер, і сервер перестає повноцінно функціонувати.

Кібернетична атака на комп'ютери може бути реалізована наступними шляхами:

- взлом механізму автентифікації комп'ютерів (ідентичний взлому механізму автентифікації серверу);
- використання вірусного програмного забезпечення;
- Man-in-the-Middle (MITM).

Найбільш розповсюдженим видом атак на комп'ютери є атаки з використанням вірусного програмного забезпечення, тобто такого яке здатне створювати копії самого себе та впроваджувати його в код інших програм, системні області пам'яті, завантажуючі сектори з метою порушення роботи програмно-апаратних комплексів, видалення файлів, блокування роботи користувачів, а також приведення до непрацездатного стану апаратних комплексів комп'ютера. Розрізняють наступні види вірусів: віруси типу «хробак» (робить копії самого себе, що призводить до зменшення ресурсів для корисних програм), троянські програми (застосовуються для крадіжки інформації з комп'ютера, що був заражений), програми шпигуни (збирають інформацію про дії та поведінку користувача, а також адреси і паролі), хакерські утиліти (застосовуються для отримання несанкціонованого доступу до комп'ютера).

Сутність атаки Man-in-the-Middle (людина посередині) полягає в прослуховуванні каналу зв'язку та перехопленні повідомлень, що по ньому передаються, або зміна цих повідомлень таким чином, що ні особа, яка передає повідомлення, ні особа, яка його приймає, не здогадуються про це.

Атака на програмне забезпечення може бути реалізована наступними шляхами:

- взлом механізму автентифікації програмного забезпечення;
- заміна коду програмного забезпечення.

Взлом механізму автентифікації програмного забезпечення виконується тими ж методами, що і взлом механізму автентифікації серверу.

Заміна коду програмного забезпечення виконується за допомогою комп'ютерних вірусів, розглянутих вище.

Існує велика кількість загроз інформаційній безпеці інформаційно-телекомунікаційної мережі, більшість з яких націлена на отримання несанкціонованого доступу до конфіденційної інформації або порушення її цілісності. Реалізація таких атак потребує від зловмисника глибоких знань структури інформаційно-телекомунікаційної мережі, особливостей функціонування протоколів, що в ній застосовуються, наявності в системі недоліків в політиці безпеки та в організації її експлуатації обслуговуючим персоналом і легітимними користувачами. Але у більшості випадків метою зловмисника є виведення інформаційно-телекомунікаційної мережі з працездатного стану, що призведе до відмови в обслуговуванні її легітимних користувачів. Ця мета досягається значно простіше, ніж вказані вище цілі атак. Для цього використовуються розподілені атаки типу «відмова в обслуговуванні» або DDoS-атаки.

Оскільки в кіберпросторі існує можливість здійснення різних злочинів, що вимагають наявності різних навичок і знань, то і кіберзлочинців ділять на різні групи, тому що вони мають різні особисті характеристики.

З огляду на специфіку кіберзлочину, кіберзлочинець визначається як висококваліфікований фахівець у галузі інформаційних технологій, який проникає в інформаційну систему з метою порушення її цілісності або використання інформації в корисливих неправомірних цілях.

У результаті аналізу наукової літератури встановлено сім основних типів кіберзлочинців, а саме:

1. Скрипткіді (англ, *scriptkiddies'*) - особи, що користуються скриптами або програмами, розробленими іншими, для атаки комп'ютерних систем і мереж, не розуміючи механізму їхньої дії. Зазвичай здатні лише атакувати дуже слабо захищені мережеві системи.

2. Спамери (англ, *scammers*) - ті, хто за допомогою спаму (масової розсилки кореспонденції рекламного чи іншого характеру людям, які не висловили бажання її одержувати) вчиняє шахрайство (поширення порнографії, комп'ютерних вірусів, виманювання коштів, виведення поштової системи з ладу (відмова сервісу) тощо).
3. Групи хакерів (англ, *hacker groups*) - зазвичай працюють анонімно і створюють інструменти для злому в кіберпросторі. Вони часто зламують комп'ютери без кримінальних мотивів, а іноді їх наймають компанії, щоб перевірити власну систему захисту.
4. Фішери (англ, *phishers*) - шахраї, що мають на меті виманювання в довірливих або неуважних користувачів мережі персональних даних клієнтів онлайн-аукціонів, сервісів із переказу або обміну валюти, інтернет-магазинів, карткових рахунків. Фішери використовують усілякі пастки, які найчастіше змушують користувачів самостійно розкрити конфіденційні дані, наприклад, надсилають електронні листи із пропозиціями підтвердити реєстрацію облікового запису, що містять посилання на веб-сайт в Інтернеті, зовнішній вигляд якого цілком копіює дизайн відомих ресурсів.
5. Політичні/релігійні/комерційні групи кіберзлочинців. Вони зазвичай не зацікавлені у фінансовій вигоді, розробляють шкідливі програми для політичних цілей. Наприклад вірус Стакснет (англ. *Stuxnet*). Є припущення, що саме цей вірус - спеціалізована розробка ізраїльських спецслужб, спрямована проти ядерного проекту Ірану.
6. Інсайдери (англ, *insiders*). Вони можуть становити лише 20% загрози, але завдають збитків на цілих 80%. Такі кіберзлочинці вважаються найвищим ризиком у кіберпросторі. Що ще гірше, як впливає з назви, вони часто перебувають у межах організації, де працюють.
7. Прояви стійкої загрози (англ. *Advanced persistent threat* (APT)). Йдеться про цілеспрямовані напади, що проводяться надзвичайно організованими групами, члени яких мають доступ до великих обчислювальних ресурсів і

володіють глибокими технічними знаннями.

Також є класифікація Кузнецова А., згідно з якою кіберзлочинців можна розділити на три категорії:

- до першої групи належать особи, відмінною рисою яких є стійке поєднання професіоналізму в області комп'ютерної техніки і програмування з елементами своєрідного фанатизму і винахідливості. Вони сприймають засоби комп'ютерної техніки як виклик своїм творчим і професійним знанням, умінням і навичкам;

- друга група складається з осіб, які страждають на новий різновид психічних захворювань - інформаційну, або комп'ютерну залежність;

- до третьої групи входять професійні «комп'ютерні» злочинці з яскраво вираженими корисливими мотивами.

Так, Батурін М.Ю. виділяє: корисливих злочинців; осіб які вчинили комп'ютерні злочини через недбалість; шпигунів-хакерів (зломщиків); кракерів (комп'ютерних хуліганів).

Вехов В.Б., Лопатіна Т.М. і Побегайло А.Е. ділять осіб, які вчинили комп'ютерні злочини, на три групи: «фанатики» - особи, відмінною рисою яких є стійке поєднання професіоналізму в області комп'ютерної техніки і програмування з елементами фанатизму (хакери); «Психічно хворі» - особи, які страждають на такі психічними захворюваннями, як інформаційна хвороба або комп'ютерна фобія; «Профі» - професійні комп'ютерні злочинці з яскраво вираженими корисливими цілями.

На думку Дворецького М.Ю. і Копирюліна А.Н., комп'ютерних злочинців можна розділити на наступні групи: порушники правил користування електронно-обчислювальних машин (ЕОМ); «Білі комірці» (або респектабельні злочинці); комп'ютерні шпигуни; хакери.

Дремлюга Р.І. дає таку класифікацію: «Інтернет-шахрай»; «Інтернет-зломщик» (хакер); розробник Інтернет-вірусів. Аналізуючи таке розмаїття видів кіберзлочинців, можна виявити одну особливість: майже всі вчені так чи інакше окремо виділяють дві самостійні групи кіберзлочинців: хакерів і корисливих

злочинців. Якщо врахувати, що ці дві групи один одного не виключають, то серед корисливих кіберзлочинців можна зустріти як хакерів, так і звичайних шахраїв. Також серед хакерів можна зустріти як корисливих хакерів, так і навпаки, некорисливих (наприклад, рухомих хуліганськими спонуканнями).

Слід зазначити, що сучасна кіберзлочинність характеризується використанням новітніх технологій, сучасних апаратних і програмним забезпеченням; організованістю, міжрегіональними та міжнародними зв'язками; використанням інформаційних ресурсів, які територіально розташовані в різних країнах. Подальшої криміналізації кіберпростору сприяє ряд характерних особливостей "віртуального" середовища: транснаціональність Інтернету (відсутність кордонів, митниць, територіальна роз'єднаність груп людей); уявна анонімність користувачів (імена в мережі використовуються псевдоніми (ніки)) значна кількість користувачів, до яких легко можна довести свої ідеї, організувати їх для проведення будь-якої акції, формувати громадську думку, навмисно дезінформувати, проводити збір інформації; законодавча неврегульованість цього середовища.

#### Список джерел:

1. Борисенко О. А., Бережна О. В., Новгородцев А. І., Сердюк В. В. & Яковлев М. М. (2019) "Система передачі та відображення інформації із захистом числових даних", Системи обробки інформації, вип. 2, с. 103 – 108.
2. Коломійцев, О., Третьяк, В., Закіров, З., Кукобко, С., Калачова, В., & Мартовицький, В. (2020). Оптимізація завантаження файлів сховища даних в o1ar-файли на основі рангового підходу. InterConf, (25), 108-117. вилучено із <https://ojs.ukrlogos.in.ua/index.php/interconf/article/view/4300>.
3. Кучернюк П. В., (2018) "Методи і технології захисту комп'ютерних мереж (фізичний та каналний рівні)", Мікросистеми, Електроніка та Акустика, т. 22, № 6(101), с. 64 – 70
4. Коломійцев, О., Рябуха, Ю., Калачова, В., & Третьяк, В. (2020). Аналіз методів і процедур шкального оцінювання в задачах прийняття рішень при проектуванні і супроводженні розподілених автоматизованих інформаційних систем. InterConf, (15). вилучено із <https://ojs.ukrlogos.in.ua/index.php/interconf/article/view/2309>.

**SCIENTIFIC EDITION**

BN 979-1-293101-09



9 791293 101093

**SCIENTIFIC COLLECTION «INTERCONF»**

**№ 2 (29) | September, 2020**

**The issue contains:**

Proceedings of the 6th International Scientific  
and Practical Conference

**SCIENTIFIC HORIZON IN THE CONTEXT  
OF SOCIAL CRISES**

TOKYO, JAPAN

16-18.09.2020

---

**Contacts of the editorial office:**

Scientific Publishing Center «InterConf»

E-mail: [info@interconf.top](mailto:info@interconf.top)

URL: <https://www.interconf.top>



**InterConf**

Scientific Publishing Center