

**SCIENTIFIC  
COLLECTION  
INTERCONF**

No **45**  
March, 2021

THE ISSUE CONTAINS:

Proceedings of the 3th  
International Scientific  
and Practical Conference

**SCIENTIFIC COMMUNITY:  
INTERDISCIPLINARY RESEARCH**



HAMBURG, GERMANY  
16-18.03.2021



**InterConf**  
Scientific Publishing Center

# **SCIENTIFIC COLLECTION «INTERCONF»**

**№ 45 | March, 2021**

**THE ISSUE CONTAINS:**

Proceedings of the 3<sup>th</sup> International Scientific and Practical Conference

**SCIENTIFIC COMMUNITY:  
INTERDISCIPLINARY RESEARCH**

HAMBURG, GERMANY

**16-18.03.2021**

HAMBURG  
2021

UDC 001.1

S 40 *Scientific Collection «InterConf», (45): with the Proceedings of the 3<sup>th</sup> International Scientific and Practical Conference «Scientific Community: Interdisciplinary Research» (March 16-18, 2021). Hamburg, Germany: Busse Verlag GmbH, 2021. 551 p.*

ISBN 978-3-512-31217-5

## EDITOR COORDINATOR

**Anna Svoboda** 

Doctoral student  
University of Economics, Czech Republic  
annasvobodaprague@yahoo.com

**Mariia Granko** 

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

## EDITORIAL BOARD

Temur Narbaev  (PhD)

Tashkent Pediatric Medical Institute,  
Republic of Uzbekistan;

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;

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

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

Dmytro Marchenko  (PhD in Engineering)

Mykolayiv National Agrarian University  
(MNAU), Ukraine;

Dr. Albenya 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;

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

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

George McGrown (PhD in Finance)  
University of Florida, USA  
mcgrown.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 styles of citation:

1. Surname N. (2021). Title of article or abstract. *Scientific Collection «InterConf», (45): with the Proceedings of the 3th International Scientific and Practical Conference «Scientific Community: Interdisciplinary Research» (March 16-18, 2021) in Hamburg, Germany; pp. 21-27. Available at: [https://interconf.top/...](https://interconf.top/)*
2. Surname N. (2021). Title of article or abstract. *InterConf, (45), 21-27. Retrieved from [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.

©2021 Busse Verlag GmbH  
©2021 Authors of the abstracts  
©2021 Scientific Publishing Center «InterConf»

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

## TABLE OF CONTENTS





**PART I**

<b>REGIONAL ECONOMY</b>			
Kondybayeva S. Yessirkepova D.		ASSESSMENT OF INVESTMENT RISKS IN THE REAL ECONOMY OF KAZAKHSTAN	9
Пустовойт О.В.		РОЗВИТОК НАУКОВИХ ПІДХОДІВ ДОСЛІДЖЕННЯ ЕКСПОРТНОЇ КОНКУРЕНТОСПРОМОЖНОСТІ	14
<b>INTERNATIONAL ECONOMICS AND INTERNATIONAL RELATIONS</b>			
Antoci N.		FREE ECONOMIC ZONES AND THEIR ROLE IN THE SYSTEM OF INTERNATIONAL ECONOMIC RELATIONS	23
Ishik O.K.M.		DIRECTIONS OF AZERBAIJAN'S ENERGY POLICY	29
<b>MANAGEMENT</b>			
Khankishiev F.K.		IMPROVING THE TAX SYSTEM APPLIED TO INDIVIDUAL ENTREPRENEURSHIP IN THE REPUBLIC OF AZERBAIJAN	33
Ізюмцева Н.В. Олійник В.В.		ПОСТАНОВКА ЗАВДАНЬ ПРИ РЕОРГАНІЗАЦІЇ ПІДПРИЄМСТВА	41
<b>MARKETING, ADVERTISING AND PR</b>			
Нepochatenko A.V.		CRM-SYSTEM AS A TOOL OF BUSINESS MANAGEMENT STRATEGY	46
<b>FINANCE AND CREDIT</b>			
Поплюйко А.М. Голосна О.В.		НОВЕ ЗАКОНОДАВСТВО ПРО ФІНАНСОВИЙ ЛІЗИНГ: ЧАС ОНОВЛЕННЯ	51
<b>PEDAGOGY AND EDUCATION</b>			
Dusbayeva N.N.		IMPROVING THE QUALITY OF EDUCATION IN UZBEKISTAN	59
Fayzullayeva A.S.		MODERN INNOVATIVE METHODS OF TEACHING ENGLISH	63
Fayzullayeva B.B. Qadirova L.I.		IMPROVING PEDAGOGICAL COMPETENCE THROUGH E-LEARNING RESOURCES	68
Koretska V.O.		THEORETICAL APPROACHES TO DEFINING THE PHENOMENON OF GENDER IN SCIENTIFIC THEORIES	75
Kurkina O.O.		THE HIGH SCHOOL STUDENTS' RESPONSIBLE PARENTING FORMATION IN EDUCATIONAL INSTITUTIONS OF UKRAINE	80
Kuychiyeva Z.I.		DIE THEORIE DER RELEVANZ VON ERNST AUGUST GUTT	83
Madiyeva G.A.		THE ROLE OF WARM UP ACTIVITIES IN TEACHING ENGLISH	88
Shodiyev M.B.		THE IMPORTANCE OF STUDYING THE REGIONAL DICTIONARIES OF ENGLISH LANGUAGE	93
Абдрахманова С. Майгельдиева Ш.М		РАЗВИТИЕ ПОЗНАВАТЕЛЬНОГО ИНТЕРЕСА УЧАЩИХСЯ НАЧАЛЬНЫХ КЛАССОВ НА ОСНОВЕ МУЛЬТИПЛИКАЦИОННЫХ СРЕДСТВ	98
Ишматова Ш.А.		ФОРМИРОВАНИЕ КОММУНИКАТИВНЫХ И ОБЩЕКУЛЬТУРНЫХ КОМПЕТЕНЦИЙ УЧАЩИХСЯ НА УРОКЕ РУССКОГО ЯЗЫКА	104
Липай Е.В.		ВОПРОСЫ ОРГАНИЗАЦИИ ИССЛЕДОВАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ УЧАЩИХСЯ ПРИ ОБУЧЕНИИ АНГЛИЙСКОМУ ЯЗЫКУ	110






## SCIENTIFIC COMMUNITY: INTERDISCIPLINARY RESEARCH



### GENERAL ENGINEERING AND MECHANICS

Kholkhodjajev B.A. Mamirov U.F.		APPLICATION OF THE OPERATIONAL REGULARIZATION METHOD FOR RESTORING THE INPUT SIGNALS OF DYNAMIC SYSTEMS BASED ON VARIATION INEQUALITIES	466
Mamirov U.F.		FORMAL DESCRIPTION OF ALGORITHMS FOR CONTROLLING SYSTEMS UNDER CONDITIONS OF MODEL UNCERTAINTY	470
Rustamov S.A.A.		DAS WIRKUNGSPRINZIP UND DIE THEORETISCHEN AUSLEGUNGEN EINER NEUEN AUSFÜHRUNG DES LENKGETRIEBES	474
Швачка А.В.		МЕТОД ДИАГНОСТИКИ СОСТОЯНИЯ РЕЗИНОТРОСОВЫХ КАНАТОВ В ЛИФТАХ ПО ЗНАЧЕНИЯМ ИХ ЭЛЕКТРИЧЕСКИХ СОПРОТИВЛЕНИЙ	482




### INFORMATION AND WEB TECHNOLOGIES

Quliyev N.A. Shamilov Z. A. Akbarova S.H.		THE ROLE OF HASHING ALGORITHMS IN FILE SECURITY	484
Тумочко О.І. Pavlenko M. Larin V. Timochko O.O. Kolmykov M.		METHOD REPRESENTATION OF THE DIFFERENTIAL-REPRESENTED SERVICE DATA FOR COMPUTER SYSTEMS OF SPECIAL PURPOSES	491
Артикова М.А. Патуллоев Н.М.		К ВОПРОСУ ВЫБОРА ИНСТРУМЕНТА ДЛЯ РАЗРАБОТКИ МОБИЛЬНОГО ПРИЛОЖЕНИЯ	498


### ARCHITECTURE, CONSTRUCTION AND DESIGN

Кириченко Є.Р. Мерилова І.О.		ТРАНСПОРТНІ ПРОБЛЕМИ ТА МЕТОДИ ЇХ ВИРІШЕННЯ	505
Унайбаев Б.Б. Унайбаев Б.Ж. Дюсембаева Б.Е. Медетова К.О. Ичева Ю.Б.		ИЗЫСКАНИЯ НА ТЕРРИТОРИЯХ, СЛОЖЕННЫХ ЗАСОЛЕННЫМИ ПЫЛЕВАТО-ГЛИНИСТЫМИ ГРУНТАМИ	509

### PHYSICAL EDUCATION AND SPORTS

Берданов А.О.		ФОРМИРОВАНИЕ ЗДОРОВОГО ОБРАЗА ЖИЗНИ – КАК АКТУАЛЬНАЯ ПРОБЛЕМА ЧЕЛОВЕЧЕСТВА. ЗДОРОВЬЕСБЕРЕГАЮЩИЕ ТЕХНОЛОГИИ	517
Коваленко Є.В. Житник А.О.		НЕОБХІДНІСТЬ ЗАСТОСУВАННЯ АЕРОБІКИ НА ЗАНЯТТЯХ З ФІЗИЧНОГО ВИХОВАННЯ В ЗАКЛАДАХ ВИЩОЇ ОСВІТИ	522
Синьков Д.В. Машков И.Ю. Шемкутова Е.Ю.		МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ ДИСТАНЦИОННОГО ОБУЧЕНИЯ В ВУЗЕ ПО ДИСЦИПЛИНЕ «ФИЗИЧЕСКАЯ КУЛЬТУРА»	529

### MILITARY AFFAIRS AND NATIONAL SECURITY

Голубничий Д.Ю. Северінов О.В. Коломійцев О.В. Місюра О.М. Третьак В.Ф. Власов А.В. Крук Б.М.		АНАЛІЗ СУЧАСНИХ ЗАГРОЗ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ЗА СКЛАДОВИМИ ЗАГРОЗ: КІБЕРБЕЗПЕКИ, ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА БЕЗПЕКИ ІНФОРМАЦІЇ	541
---	---	---	-----

## MILITARY AFFAIRS AND NATIONAL SECURITY

**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

**Сєверінов Олександр Васильович**

ORCID ID: 0000-0002-6327-6405

кандидат технічних наук, доцент  
доцент кафедри безпеки інформаційних технологій  
Харківський національний університет радіоелектроніки, Україна

**Коломійцев Олексій Володимирович**

ORCID ID: 0000-0001-8228-8404

Заслужений винахідник України, доктор технічних наук, старший науковий співробітник, професор кафедри Національного технічного університету "Харківський політехнічний університет", Україна

**Місюра Олег Миколайович**

кандидат технічних наук, старший науковий співробітник, заступник начальника 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, науковий співробітник наукового центру Повітряних Сил Харківський національний університет Повітряних Сил імені Івана Кожедуба, Україна

**Власов Андрій Володимирович**

ORCID ID: 0000-0001-6080-237

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

Крук Богдан Миронович

ORCID ID: 0000-0002-0937-8777

Харківський національний університет Повітряних Сил  
імені Івана Кожедуба, Україна

## АНАЛІЗ СУЧАСНИХ ЗАГРОЗ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ЗА СКЛАДОВИМИ ЗАГРОЗ: КІБЕРБЕЗПЕКИ, ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА БЕЗПЕКИ ІНФОРМАЦІЇ

Незважаючи на широке застосування різних криптографічних алгоритмів на різних рівнях захисту комп'ютерних мереж, вона схильна до різних загроз, загальна класифікація яких приведена у трьох сферах безпеки на рис. 1.

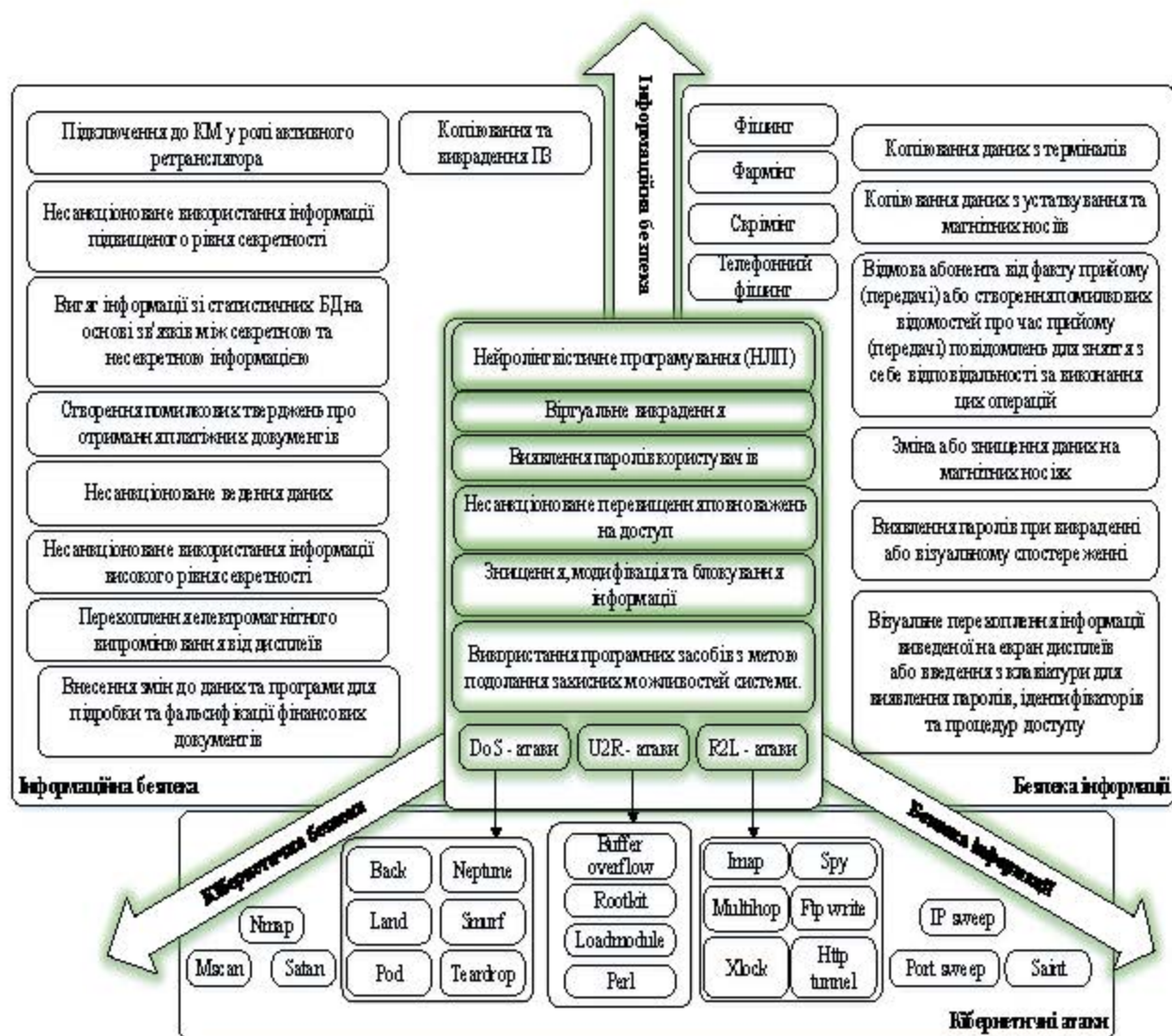


Рис. 1. Загальна класифікація загроз КМ



Загрози КМ – потенційно можливі або реальні дії зловмисників або конкурентів, здатні завдати системі матеріальної чи моральної шкоди [1-2]. У загальному вигляді реалізацію загрози можна представити у наступному вигляді (рисунок 2).

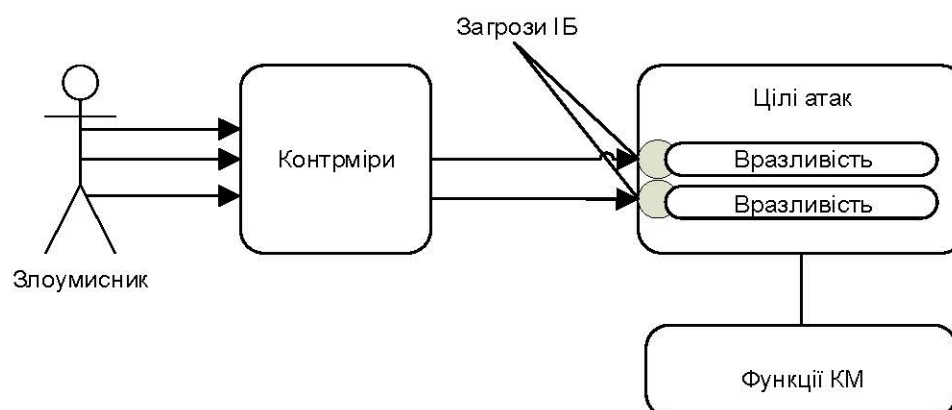


Рис. 1. Схема реалізації загрози ІБ на КМ

За походженням джерел загрози поділяються на внутрішні та зовнішні. Як перші, так і другі за спрямованістю та характером впливу на діяльність КМ можуть бути економічними, фізичними, інтелектуальними.

Економічні загрози: корупція, шахрайство, несумлінна конкуренція, використання неефективних технологій виробництва. Реалізація таких загроз веде до заподіяння збитків або упущення вигоди.

Фізичні загрози: крадіжки, грабежі майна і коштів, поломки, виведення з ладу обладнання, неефективна його експлуатація. При реалізації таких загроз завдаються збитки, пов'язані з втратою своєї власності і необхідністю нести додаткові витрати на відновлення засобів виробництва та інших матеріальних засобів.

Інтелектуальні загрози: розголошення або неправомірне використання інформації, дискредитація власника системи на ринку послуг, різного роду соціальні конфлікти. Наслідки реалізації: збитки, погіршення іміджу, соціальна чи психологічна напруженість.

Проаналізувавши рисунок 1, можна зробити висновок, що існуючі загрози набули ознак гібридності. Прояви ознак гібридності внаслідок



одночасного впливу загроз інформаційній безпеці, кібернетичній безпеці та безпеці інформації на інформаційні ресурси призвели до виникнення явища синергізму, негативні прояви якого потребують кардинального перегляду концепцій побудови діючих систем безпеки [5]. Для протидії гібридним загрозам потрібна співпраця державних інституцій та бізнесу, медіа та IT-сектору.

Окрему увагу слід приділити кіберзагрозам, оскільки вони набувають більшої розповсюдженості через використання в КМ проколів Internet. Значно зростає кількість кіберзлочинності, а також обчислювальні можливості зловмисників, спостерігається подальше вдосконалення відомих кібератак і поява нових. Основна класифікація кібератак представлена у вигляді схеми на рисунку 3.

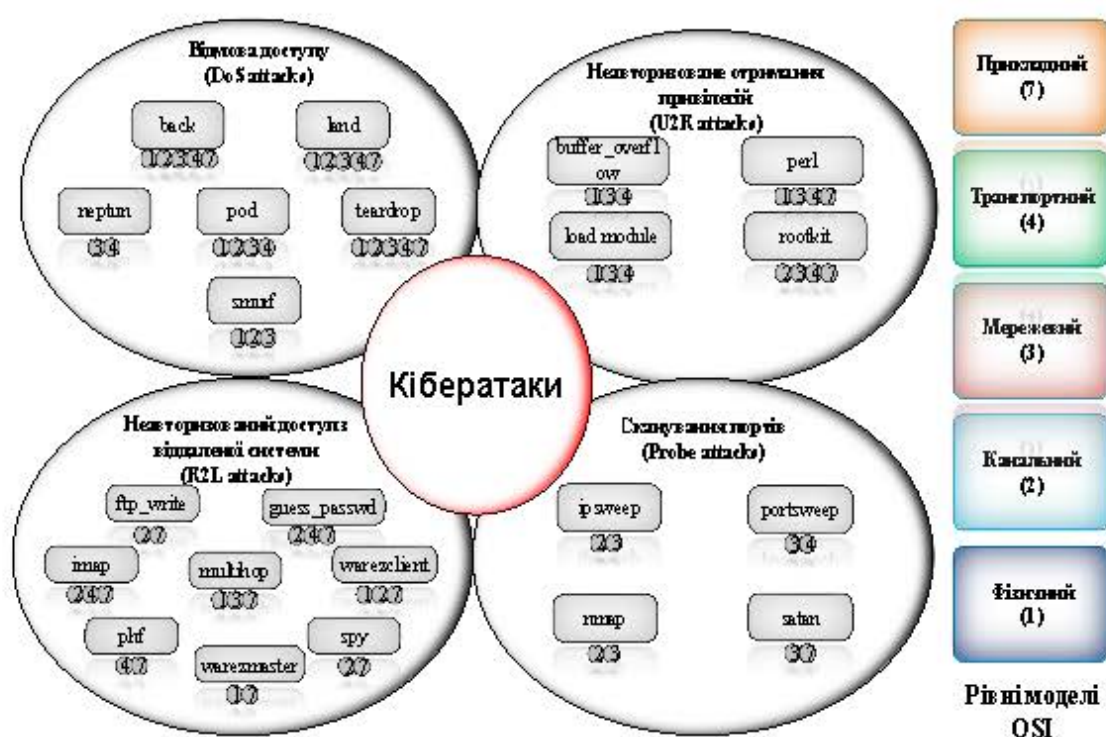


Рис. 2. Класифікація кібератак

Перелік атак, які застосовуються для проведення вторгнень поділяються на 4 категорії, кожна з яких містить множину типів атак, що реалізують мету вторгнення. В свою чергу, кожен тип атаки несе загрозу мережі на відповідних рівнях мережевої моделі OSI (open systems interconnection) та виконує свою

функцію, щодо здійснення деструктивного впливу на мережу [1-5]. До вказаних категорій атак відносять:

DoS атаки (Denial of Service) – це мережеві атаки на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, спрямовані на виникнення ситуацій, коли відбувається відмова в обслуговуванні. Атаки характеризуються заповненням системи великою кількістю з'єднань, зловживанням ресурсами системи, появою помилок, пов'язаних зі зміною параметрів конфігурації системи, що призводить до перенавантаження та блокування сервера комп'ютерної системи.

Якщо атака відбувається одночасно з великої кількості IP-адрес, то її називають розподіленою (Distributed Denial of Service – DDoS).

U2R атаки – зловмисник здійснює доступ до облікового запису звичайного користувача і, використовуючи уразливість системи, отримує несанкціонований доступ до кореневого каталогу.

R2L атаки, що характеризуються отриманням доступу незареєстрованого користувача до мережі з боку віддаленої станції.

Probe-атаки – полягають в скануванні мережевих портів з метою отримання конфіденційної інформації.

Вказані типи атак за своєю функцією можуть впливати на: управління передачею даних, обмін пакетами, організацію з'єднань, міжмережевий обмін, енергетичні характеристики засобів зв'язку, доступ до кодування, управління інформацією та інше. Виходячи з цього, вплив атак можна розподілити за рівнями мережевої моделі OSI (табл. 1.)

Таким чином, проведений аналіз підтверджує пропорційне зростання кібератак з еволюційним зростанням обчислювальної техніки і комп'ютерною грамотністю зловмисників в останні десятиліття.

Розвиток комп'ютерних мереж та комп'ютеризація 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. 4.

Вплив атак на рівнях мережевої моделі OSI

Категорія атак	Типи атак	Рівні мережевої моделі OSI				
		Прикладний	Транспортний	Мережевий	Канальний	Фізичний
DoS	back	+	+	+	+	+
	land	+	+	+	+	+
	neptune		+	+		
	pod		+	+	+	+
	smurf			+	+	+
	teardrop	+	+	+	+	+
U2R	buffer overflow		+	+		+
	loadmodule		+	+		+
	perl	+	+	+		+
	rootkit	+	+	+	+	
R2L	ftp write	+			+	
	guess_passwd	+	+		+	
	imap	+	+		+	
	multihop	+		+		+
	phf	+	+			
	spy	+			+	
	warezclient	+			+	+
	warezmaster	+				+
	ipsweep			+	+	
Probe	nmap			+	+	
	portsweep		+	+		
	satan	+		+		
	guess_passwd	+	+		+	

Кібернетична атака може бути спрямована на серверне обладнання, на програмне забезпечення або на хост.

Атака на серверне обладнання може бути реалізована наступними шляхами: зламування механізму автентифікації серверів; несанкціоноване використання прав авторизації; відмова в обслуговуванні клієнтів (DoS, DDoS); використання сервісів серверів не за призначенням; виконання злочинного коду.

Здійснити зламування 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.

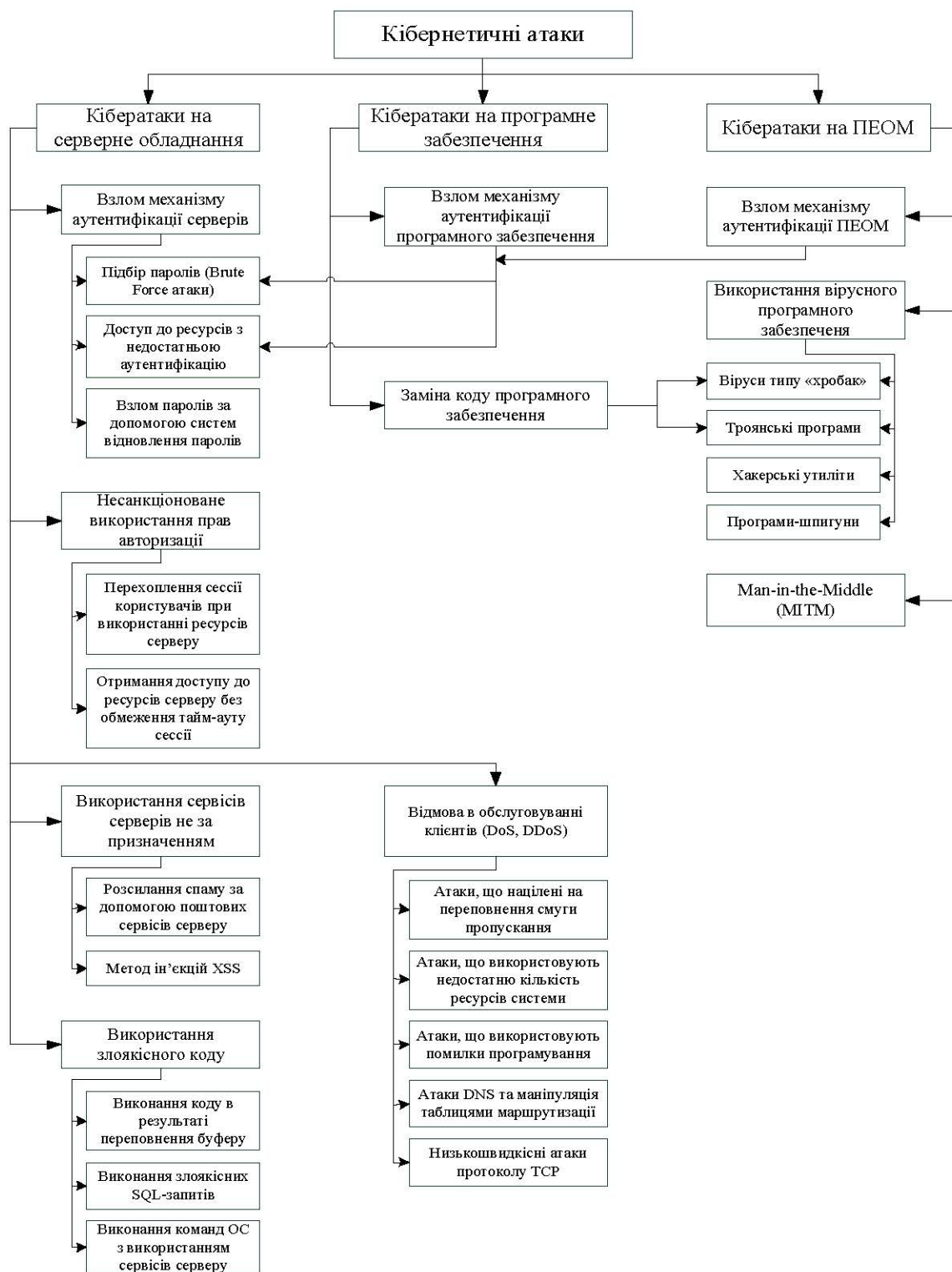


Рис. 4. Класифікація кібернетичних атак

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 зламування.

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 Denialof 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 зламування серверу може бути використаний спеціальний злоякісний код. Як правило це SQL-ін'єкція – один з найпоширеніших способів зламування 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: зламування механізму автентифікації комп'ютерів (ідентичний зламуванню 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: зламування механізму автентифікації програмного забезпечення; - заміна коду програмного забезпечення.

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.

**Список джерел:**

1. Информационная безопасность: учеб, пособие / В. И. Лойко, В. Н. Лаптев, Г. А. Аршинов, С. В. Лаптев. - Краснодар:КубГАУ, 2020. - 332 с.
2. Информационная политика и безопасность: учебное пособие / авторсоставитель Безродный В.П. - Донецк: ДонНУ, 2020. - 175 с.
3. Третяк, В., & Пашнева, А.(2017) Оптимізація структури сховища даних у вузлах інфокомунікаційної мережі хмарного середовища. Системи управління, навігації та зв'язку. № . 4 (44). – С. 122-128.
4. Третяк, В., Голубничий, Д., Коломійцев, О., Мегельбей, Г., Возний, О., & Філіпенков, О. (2020). Математична модель рангового підходу. Збірник наукових праць ЛОГОС, 116-122. <https://doi.org/10.36074/25.12.2020.v1.40>
5. Балашов П. А. Оцінка ризиків інформаційної безпеки на основі нечіткої логіки / П.А. Балашов, Р.И. Кислой, В.П. Безгузиков // Безпека комп'ютерних систем. Конфидент. – № 5, 2013. – С. 56-59.

**SCIENTIFIC EDITION**

BN 978-3-512312-17



9 783512 312175

**SCIENTIFIC COLLECTION «INTERCONF»**

**№ 45 | March, 2021**

**The issue contains:**

Proceedings of the 3<sup>th</sup> International  
Scientific and Practical Conference

**SCIENTIFIC COMMUNITY:  
INTERDISCIPLINARY RESEARC**

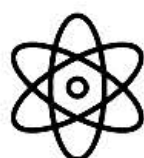
HAMBURG, GERMANY  
16-18.03.2021

Published online: March 25, 2021  
Printed: April 4, 2021. Circulation: 200 copies.

---

**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