

**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**

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

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

*Матеріали конференції*



Одеса

21-22 квітня 2022 р.

Стан, досягнення та перспективи інформаційних систем і технологій / Матеріали XXII Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 21-22 квітня 2022 р. - Одеса, Видавництво ОНТУ, 2022 р. – 251 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 ОНТУ

### **Співголови:**

**Поварова Н.М.** – к.т.н., доц., проректор з наукової роботи ОНТУ,  
**Котлик С.В.** – к.т.н., доц., директор ННІКСіТ "Індустрія 4.0" ОНТУ,  
**Даріуш Долива**, д.математичн.наук, уповноважений декана факультету Інформатики УІтаПЗ, м.Лодзь, Польща,  
**Ковалюк Т.В.** - к.т.н., доц., Київський національний університет імені Тараса Шевченка

### **Члени оргкомітету:**

**Плотніков В. М.** – д.т.н., проф., завідувач кафедри ІТтаКБ ОНТУ,  
**Артеменко С.В.** – д.т.н., проф., завідувач кафедри КІ ОНТУ,  
**Хобін В.А.** – д.т.н., проф., завідувач кафедри АТПтаРС ОНТУ,  
**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 та англійською мовами.  
Редактор збірника Котлик С.В.

<b>О.В.</b> (Дніпровський державний технічний університет, Відокремлений структурний підрозділ «Технологічний коледж Дніпровського державного технічного університету»)	
ВИКОРИСТАННЯ КОНЦЕПЦІЇ СИМЕТРІЇ ПРИ ЗНАХОДЖЕННІ ЕКСТРЕМУМУ ФУНКЦІЇ. <b>Сердюк А.В., Сало М.О.</b> (ДВНЗ «Український державний хіміко-технологічний університет)	41
СИСТЕМА МОНІТОРИНГУ ВИРУБКИ ЛІСОВИХ МАСИВІВ УКРАЇНИ, ЩО ПОСТРАЖДАЛИ ВІД ПОЖЕЖ. <b>Тиховський Р.В., Бандурка О.І., Свинчук О.В.</b> (Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»)	43
МАТЕМАТИЧНІ МОДЕЛІ ТА МЕТОДИ ДЛЯ ІДЕНТИФІКАЦІЇ ТА ВИДІЛЕННЯ ОБРАЗІВ. <b>Трухов А. С., Приходько С. Б.</b> (Національний університет кораблебудування імені адмірала Макарова)	44
РОЗРОБКА МАКЕТУ ДОСЛІДЖЕННЯ ПОСЛІДОВНИХ ЛОГІЧНИХ СХЕМ. <b>Шостак М., Жирнова Т.М, Бобрікова І. С.</b> (Одеський національний технологічний університет)	46
ФОРМУВАННЯ МАРШРУТУ З УРАХУВАННЯМ ПАРАМЕТРУ ВИТРАТИ ПАЛИВА. <b>Юрць Т.В., Ткачук В.М.</b> (Прикарпатський національний університет імені Василя Стефаника)	48
<b>Розділ 2: Управління, обробка та захист інформації</b>	50
OVERVIEW OF MODERN CYBER RISKS OF IOT TECHNOLOGIES. <b>Kulia Y.</b> (Kharkiv National University of Radio Electronics)	50
TYPES OF INTERNET FRAUD. <b>Melnik M.V., Kim Ye.R.</b> (Turan University, Kazakhstan)	51
FENWICK TREES AS REPLACEMENT FOR SEGMENT TREES IN THE “RANGE SUM QUERY PROBLEM WITH RANGE UPDATES. <b>R.Masalskyi, I.Mazurok</b> (Odesa I. I. Mechnikov National University)	53
ПРО ОДНУ ЗАДАЧУ ВИЯВЛЕННЯ ІНФОРМАЦІЙНИХ ЗАГРОЗ У КІБЕРПРОСТОРІ. <b>Горборуков В.В., Франчук О.В.</b> (Національний центр "Мала академія наук України")	55
ПРОБЛЕМАТИКА КІБЕРЗЛОЧИНІВ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ. <b>Дмитрук Я.В., Гришанович Т.О.</b> (Волинський національний університет імені Лесі Українки)	57
БАГАТОРІВНЕВИЙ ЗАХИСТ ТЕХНОЛОГІЙ ФУНКЦІОНУВАННЯ ІНТЕЛЕКТУАЛЬНИХ ОБ’ЄКТІВ. <b>Дудикевич В.Б., Микитин Г.В., Галунець М.О., Кутень Р.Б, Васильєв Д.В., Бабенцов Г.</b> (Національний університет «Львівська політехніка»)	58
ТЕХНОЛОГІЇ ВІЗУАЛІЗАЦІЇ ВЕЛИКИХ ДАНИХ. <b>Здолбіцька Н.В., Лавренчук С.В., Ліщина В.О., Ліщина Н.М., Лук’яничук Ю.А.</b> (Луцький національний технічний університет)	60
INFORMATION PROTECTION AND INFORMATION SECURITY. <b>Kapiton A.M., Fedorenko A.</b> (National University «Yuri Kondratyuk Poltava Polytechnic», Scientific lyceum №3 of Poltava city council)	62
ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ORM ТЕХНОЛОГІЙ ПРИ РОБОТІ З РЕЛЯЦІЙНИМИ БАЗАМИ ДАНИХ. <b>Кучерявий І.В. Романюк О.В.</b> (Вінницький національний технічний університет)	64
SPRING SECURITY МОДУЛЬ ЗАХИСТУ JAVA ПРОГРАМ. <b>Майданюк В. П., Марущак А. В.</b> (Вінницький національний технічний університет)	66
УПРАВЛІННЯ ЗАХИСТОМ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ СИСТЕМИ (ІАС) ПРИЙМАЛЬНОЇ КОМІСІЄЮ ОНТУ (ОНАХТ). <b>Мороз А.М., Похлебіна Н.О.</b> (Одеський національний технологічний університет)	68
ШИФРУВАННЯ ДАНИХ ЯК ОДИН З МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ. <b>Попова В.Р., Бобрікова І.С.</b> (Одеський національний технологічний університет)	70
АНАЛІЗ ОСОБЛИВОСТЕЙ ВИКОРИСТАННЯ СУЧАСНИХ СУБД ПРИ РОЗРОБЦІ ВЕБ-ОРІЄНТОВАНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ. <b>Рогачова В.О., Рудніченко М.Д., Шibaєва Н.О.</b> (Державний Університет «Одеська Політехніка»)	72

## **ПРОБЛЕМАТИКА КІБЕРЗЛОЧИНІВ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ**

ДМИТРУК Я. В. (*dmytruk.yana2018@vnu.edu.ua*)

ГРИШАНОВИЧ Т. О. (*hryshanovych.tatiana@vnu.edu.ua*)

Волинський національний університет імені Лесі Українки

*У роботі описано поняття та класифікацію кіберзлочинів відповідно до нормативно-правових документів України та інших держав. Окреслено основні проблеми, з якими доводиться зіштовхуватись правоохоронцям у сфері кіберзахисту, а також наведено можливі шляхи протидії таки видам правопорушень.*

Злочини у сфері інформаційної діяльності не є новими для України, проте вони досі залишаються актуальними внаслідок неефективного регулювання питання кіберзлочинів та недостатньою грамотністю інтернет-користувачів. Актуальність теми пов'язана з поширенням кіберзлочинів та неможливістю ефективно їм протистояти. Варто згадати інформаційну війну на тлі повномасштабного російського вторгнення: велика кількість підроблених медіа-файлів та надходження конфіденційних даних у відкритий доступ.

Перш за все варто визначитися з термінологією. Згідно з законом України «Про основні засади забезпечення кібербезпеки України» пунктом 8 частиною 1 статті 1 «кіберзлочин (комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України» [2]. Тобто, це дія чи бездіяльність, яка має місце в кіберпросторі, або з його використанням і є карною, тобто покарання безпосередньо передбачено певним нормативно-правовим актом (далі – НПА) України чи іншої країни, за умови що цей НПА був ратифікований Україною, а також це діяння створює небезпеку у суспільстві.

Усі кіберзлочини можна поділити на декілька груп, керуючись такими НПА як Конвенція про кіберзлочинність [1]:

- правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем;
- правопорушення, пов'язані з комп'ютерами (шахрайство та підробка);
- правопорушення, пов'язані зі змістом (протиправна інформація);
- правопорушення, пов'язані з порушенням авторських та суміжних прав.

Основними проблемами, з якими доводиться зіштовхуватись правоохоронним органам, є:

- наївність користувачів: надання особистої інформації у загальний доступ, активні відповіді на спам-листи і їх подальше поширення, віра у різноманітні фейки;
- відсутність політики оплати додатків, що робить поширеним піратство;
- використання простих паролів;
- відсутність або не використання двох факторної автентифікації;
- можливість повної анонімізації у мережі.

Ефективними способами протидії злочинам в інтернеті можуть бути:

- вдосконалення наявної правової системи – збільшення відповідальності за кіберзлочини;
- вдосконалення системи контролю за дотриманням правил поведіння у кіберпросторі;
- покращення захисту конфіденційної та секретної інформації в інтернеті;
- впровадження новітніх технологій у сфері кібербезпеки та кіберзахисту;
- впровадження загальних стандартів у сфері кібербезпеки;
- тісніший зв'язок та взаємодія ІТ-фахівців з різних сфер та країн.

Підсумовуючи все вищезазначене, можна дійти висновку, що перш за все користувачам потрібно самостійно турбуватися про свою безпеку, не переходити за підозрілими посиланнями та не завантажувати сторонні програми, законодавчому апарату потрібно запровадити новітню систему відповідальності за кіберзлочини, Україні - налагоджувати зв'язки з іншими державами у сфері кібербезпеки та заохочувати свої компанії розробляти застосунки, які будуть орієнтовані на національний ринок.

### СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Конвенція про кіберзлочинність. [Online]. Available: [https://zkon.rada.gov.ua/laws/show/994\\_575#Text](https://zkon.rada.gov.ua/laws/show/994_575#Text)
2. Про основні засади забезпечення кібербезпеки України. [Online]. Available: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>

УДК 004.056

### БАГАТОРІВНЕВИЙ ЗАХИСТ ТЕХНОЛОГІЙ ФУНКЦІОНУВАННЯ ІНТЕЛЕКТУАЛЬНИХ ОБ'ЄКТІВ

ДУДИКЕВИЧ В.Б. (vdudykev@polynet.lviv.ua), МИКИТИН Г.В. (cosmos-zirka@ukr.net),  
ГАЛУНЕЦЬ М.О. (skyzhero50@gmail.com), КУТЕНЬ Р.Б. (roman.b.kuten@lpnu.ua),  
ВАСИЛЬЄВ Д.В. (dmytro.vasyliiev.mkb.2020@lpnu.ua),  
БАБЕНЦОВ Г.А. (justgeorge888@gmail.com)  
Національний університет "Львівська політехніка"

*Запропонована універсальна модель багаторівневого захисту технологій функціонування інтелектуальних об'єктів на основі концепції "об'єкт – загроза – захист".*

**Актуальність комплексної системи безпеки інтелектуальних об'єктів.** В Україні тривають процеси інтелектуалізації об'єктів інфраструктури суспільства, основним інструментарієм безпечного функціонування яких є: давачі (Д), автоматизовані системи (АС), комунікаційні системи (КС) [1]. Постановка проблеми: з метою забезпечення цілісного захисту інформації ефективним є створення комплексної системи безпеки (КСБ) інтелектуального об'єкта (ІО) на основі системного підходу та моделі багаторівневого захисту інформації, яка функціонує на рівні контурів, що перекривають одні й ті ж канали несанкціонованого доступу (НСД) до інформаційно-комунікаційних технологій функціонування інтелектуального об'єкта.

**Модель багаторівневого захисту технологій функціонування інтелектуального об'єкта.** На рис. 1 представлена модель багаторівневого захисту інформації в технологіях функціонування ІО – давачах, автоматизованих системах та комунікаційних системах.

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

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

Одеса

21-22 квітня 2022 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.