

**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.

## ЗМІСТ

<b>Розділ 1.</b>		
<b>Математичне і комп'ютерне моделювання складних процесів</b>		
СУЧАСНІ ТЕНДЕНЦІЇ В КЛАСТЕРНОМУ АНАЛІЗІ ПРИ ОБРОБЦІ МУЛЬТИМОДАЛЬНИХ ДАНИХ. <b>БОЙКО Н.І.</b> (Національний університет «Львівська політехніка»)		11
ЗАБЕЗПЕЧЕННЯ ВЛАСТИВОСТІ ФУНКЦІОНАЛЬНОЇ СТІЙКОСТІ ТЕХНОЛОГІЧНИХ ПРОЦЕСІВ ІЗ ВИКОРИСТАННЯМ НЕЙРОННИХ МЕРЕЖ. <b>СОБЧУК В.В., ОЛІМПІЄВА Ю.І.</b> (Державний університет телекомунікацій)		13
ТАБЛИЧНА РЕАЛІЗАЦІЯ МОДУЛЬНИХ ОПЕРАЦІЙ ОБЧИСЛЮВАЛЬНОГО ПРИСТРОЮ АВТОМАТИЗОВАНОЇ СИСТЕМИ КОНТРОЛЮ ТА ОБЛІКУ ЕЛЕКТРОЕНЕРГІЇ. <b>ЗВЄЗДІН В.М., ЯНКО А.С.,</b> (Національний університет «Полтавська політехніка імені Юрія Кондратюка»)		15
ГЕНЕРАТОР ТЕСТІВ. <b>РОМАНИШИН Д.М., КУЛІКОВ В.М.</b> (Інститут спеціального зв'язку та захисту інформації НТУУ «КПІ ім. Ігоря Сікорського»)		17
РОЗРОБКА ДОДАТКУ ДЛЯ ІМІТАЦІЇ ТА РОЗРАХУНКУ ПОЛЬОТУ ДРОНУ. <b>ОСТАПЧУК Н.О., РОЖКО В.В., ШЕВЧУК Я.І.</b> (Обласний науковий ліцей в м. Рівне Рівненської обласної ради)		19
ОБҐРУНТУВАННЯ ПАРАМЕТРІВ ПРИВОДУ ЩОКОВОЇ ДРОБАРКИ З ПРОСТИМ РУХОМ ЩОКИ. <b>МАНЬКОВСЬКА К.О., ПАНЧЕНКО О.В.</b> (Національний технічний університет «Дніпровська політехніка»)		21
СУЧАСНІ ТЕХНОЛОГІЇ 3D СКАНУВАННЯ. <b>ВОСТРЕЦОВ М.І., САХАРОВА С.В., БАРАБАШ Т.М.</b> (Одеська національна академія харчових технологій)		23
ЗАСТОСУВАННЯ AUTOMATED MARKET MAKER ДЛЯ ВПРОВАДЖЕННЯ РИНКУ ОПЛАТИ СЕРВІСІВ В ДЕЦЕНТРАЛІЗОВАНИХ МЕРЕЖАХ. <b>ВОЛКОВ К.С., МАЗУРОК І.Є., ЛЕОНЧИК Є.Ю.</b> (Одеський національний університет імені І. І. Мечникова)		25
МЕТОДИКА ОЦІНКИ ЧАСУ ОБРОБКИ ЗАПИТІВ СЕРВЕРАМИ ГЕТЕРОГЕННИХ РОЗПОДІЛЕНИХ БАЗ ДАНИХ. <b>КОРНАГА Я.І., БАРАБАШ А.О.</b> (Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»)		26
МОДЕЛІ ТА ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ДЛЯ ІДЕНТИФІКАЦІЇ ТА ОПТИМІЗАЦІЇ СИСТЕМИ СТАБІЛІЗАЦІЇ РІВНЯ ВОДИ В ПАРОГЕНЕРАТОРІ ПГВ-1000. <b>СЕВЕРИН В.П., НІКУЛІНА О.М., КОЦЮБА Н.В.</b> (Національний технічний університет «Харківський політехнічний інститут»)		28
ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ ДВОЕТАПНОГО КОНСЕНСУСУ НА ОСНОВІ ПРОТОКОЛУ TENDERMINТ. <b>ВОРОХТА А.Ю., ВОЛКОВ К.С., МАЗУРОК І.Є., ЛЕОНЧИК Є.Ю., СТРАХОВ Є.М.</b> (Одеський національний університет імені І.І.Мечникова)		30
ДИНАМІЧНА СТРАТЕГІЯ БАЛАНСУВАННЯ НАВАНТАЖЕННЯ. <b>ЗАВЕРТАЙЛО К.С.</b> (Інститут проблем математичних машин і систем)		32
<b>Розділ 2.</b>		
<b>Управління, обробка та захист інформації</b>		
ЗАХИСТ ОСОБИСТИХ ДАНИХ ЗА ТЕХНОЛОГІЄЮ БЛОКЧЕЙН. <b>ПОПОВА В.Р., БОБРИКОВА І.С.</b> (Одеська національна академія харчових технологій)		34
ВЛИЯНИЕ COVID-19 НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ РЕСПУБЛИКИ БЕЛАРУСЬ. <b>КУПРЕЙЧИК А.С., СМІРНОВА Н.А.</b> (Белорусский государственный		36

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

## **ВЛИЯНИЕ COVID-19 НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ РЕСПУБЛИКИ БЕЛАРУСЬ**

КУПРЕЙЧИК А.С., студентка (*rfnz5014@gmail.com*),  
СМИРНОВА Н.А., научный руководитель (*sn@unica.by*)

Белорусский государственный университет информатики и радиоэлектроники

*Пандемии относятся к числу социальных катастроф, сеющих панику, стрессовые и посттравматические стрессовые психологические травмы, массовую агрессию и прочие нарушения поведенческих реакций общества. Сила данных реакций связана с информационным влиянием на человека в период, когда в его психике оказывается постоянное, не поддающееся рациональному контролю, воздействие. Хотя угрозы пандемии еще не отступили, уже пришло время анализа реакций, возникших в социуме в период COVID-19.*

Пандемия превратила Интернет в «золотую жилу» - часто единственный путь выживания, обеспечение продуктами, организации работы и образования. Данная ситуация поспособствовала росту количества новых способов мошенничества с использованием Интернет-технологий. Мошенничество всегда растет в периоды кризиса, и не важно с чем они связаны, так как в такие периоды в обществе начинается паника и уровень внимательности, к получаемой информации, снижается [1].

Фишинг, один из самых распространённых видов мошенничества в сети, – это вид интернет-атаки, цель которой получение доступа к конфиденциальным данным пользователей [2]. Особую тревожность вызывают факты активизации виртуальных мошенников во время пандемии коронавируса, когда мошенники используют тему коронавируса как «приманку» и просят переходить по ссылке в письмах, якобы отправленных из банка. В этих письмах может оказаться «сайт-ловушка». Цель таких рассылок – узнать пароли, логины, данные карты за счёт подделки сообщений от доверенного источника. Фишинговые страницы похожи на оригинальные страницы сайта банков, вследствие чего люди становятся жертвами преступников. Другими последствиями киберпреступности в период карантина стала организация большого количества сбоев в работе информационных ресурсов. Финансовые угрозы нарушения целостности данных были связаны с переходом многих предприятий на удаленный режим работы без соблюдения необходимых мер безопасности. Помимо проблем для государственных структур и бизнеса в части нарушения целостности или хищения конфиденциальных данных, внедрение хакеров вызывало, например, сбои в процессе дистанционного образования и научной работы.

Новое исследование Anti-Phishing Working Group (APWG) показало, что уровень фишинговых атак на сайты финансовых учреждений, веб-почты и сайты SaaS. рос до 2020 года, удваиваясь в течение года. Приблизительно 70% всех доменных имен в мире, зарегистрированных в злонамеренных целях, принадлежат китайскими преступниками для использования против различных брендов и предприятий. Число выявленных и заблокированных в глобальной сети за девять месяцев 2020 года фишинговых сайтов превысило показатель прошлого года [3].

Проблематика киберпреступности в период пандемии освещалась в СМИ, а также через социальные сети, что, в связи с мобильностью доведения информации о возможных угрозах, снизило риски и денежные потери населения. Несмотря на это, ряд информационных ресурсов подвергся DDoS-атакам, с них происходило массовое хищение персональных данных граждан, функционирование ресурсов приостанавливалось из-за создававшихся злоумышленниками сбоев в их работе.

Удавалось мошенничеству, как правило, при наличии уязвимостей у информационного ресурса, а также благодаря неосведомленности, доверию и невнимательности граждан в моменты наибольшей психической уязвимости. Прежде всего, были подвержены мошенничеству граждане, находящиеся в особо сложной жизненной ситуации, а также сотрудники в режиме удаленной работы, оперирующие данными организаций, не

предназначенними для обнародования. Интернет-мошенничество особенную опасность представляло для населения с низкой финансовой, правовой и компьютерной грамотностью. Если речь идет о мошенничестве по отношению к гражданам, то кроме неосведомленности, оно апеллирует к сильным эмоциям и жизненным приоритетам потребителей: к сочувствию, тревоге за жизнь близких, к фобиям и страхам [4].

Распространение информации о борьбе с мошенниками, помимо указанных выше каналов, шло через печатную прессу, радио, телевидение, видеозкраны в общественных пространствах, объявления в общественном транспорте.

Применявшиеся меры профилактики мошенничества были связаны с усилением защиты информационных ресурсов с целью предотвращения их взлома, а также с информированием населения о приемах распознавания и о порядке реагирования на действия мошенников для исключения утечки персональных данных и финансовых потерь.

На мой взгляд, одной из причин подобного уровня мошенничества является недостаточное образовательное сопровождение. В связи с этим следует сформировать систему образования соответствующим навыкам в информационном пространстве:

1) сегодня навыки пользования информационными технологиями в общих чертах преподаются в рамках информатики, но изучения вопросов информационной безопасности не имеется, в связи с чем следует ввести в школах специальную дисциплину касательно понятия и сущности сети Интернет, данная дисциплина также должна предусматривать обучение навыкам первичного пользования и поведения в виртуальном пространстве [5];

2) в системе высшего образования подготовка технических кадров в области информационной безопасности осуществляется в Белорусском государственном технологическом университете, Белорусском государственном университете, Белорусском государственном университете информатики и радиоэлектроники, Витебском государственном университете имени П. М. Машерова, Гродненском государственном университете имени Янки Купалы, Полоцком государственном университете, при этом современная тенденция в области кадровой политики требует подготовки специалистов в междисциплинарном русле;

3) следует создать программу повышения квалификации и переподготовки кадров, осуществляющих оперативно-розыскные мероприятия, дознание или следствие по преступлениям, связанным с информационной безопасностью, в правоохранительных органах.

В целом проблема доверия в сети Интернет является комплексной. В этой части необходимо формировать Интернет-культуру со стороны пользователей виртуального пространства путем проведения курсов и ознакомительных уроков, брошюр и иных материалов.

#### **Список использованных источников:**

1. Н.В. Кузина, «Информационная безопасность в условиях пандемии: методы стабилизации состояния социума в электронных СМИ и Интернете» *Бюллетень науки и практики*, №9, С. 356-394, 2020 [Электронный ресурс]. Доступно: <https://doi.org/10.33619/2414-2948/58/37>. Дата доступа: 27.03.2021

2. Национальный правовой Интернет-портал, 2021 [Online]. – Available: <https://pravo.by>. Accessed on: March 20, 2021

3. APWG, 2021 [Online]. – Available: <https://apwg.org>. Accessed on: March 27, 2021

4. Onliner, 2021 [Online]. – Accessed on: <https://www.onliner.by>. Accessed on: March 25, 2021

5. А. Расулев, «Информационная безопасность в условиях пандемии коронавируса» *Вестник юридических наук*, №1, С. 224-228, 2020 [Электронный ресурс]. Доступно: <https://tsul.uz/files/pdf/vestnik2020.pdf>. Дата доступа: 25.03.2021

**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.