

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТАВРІЙСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ В.І. ВЕРНАДСЬКОГО**

Журнал заснований у 1918 році

**ВЧЕНІ ЗАПИСКИ
ТАВРІЙСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
ІМЕНІ В.І. ВЕРНАДСЬКОГО**

Серія: Технічні науки

Том 32 (71) № 1 2021

Частина 1



Видавничий дім
«Гельветика»
2021

Головний редактор:

Кисельов Володимир Борисович – доктор технічних наук, професор, директор Навчально-наукового інституту муніципального управління та міського господарства Таврійського національного університету імені В.І. Вернадського.

Члени редакційної колегії:

Медведєв Микола Георгійович (відповідальний секретар) – доктор технічних наук, професор, завідувач кафедри загальноінженерних дисциплін та теплоенергетики Таврійського національного університету імені В.І. Вернадського;

Бронін Сергій Вадимович – кандидат технічних наук, доцент, доцент кафедри інформаційних систем та технологій Київського національного університету імені Тараса Шевченка;

Домніч Володимир Іванович – кандидат технічних наук, професор, завідувач кафедри автоматизованого управління технологічними процесами Таврійського національного університету імені В.І. Вернадського;

Дехтяр Анатолій Соломонович – доктор технічних наук, професор, професор кафедри архітектурних конструкцій Національної академії образотворчого мистецтва і архітектури;

Дичко Аліна Олегівна – доктор технічних наук, професор, професор кафедри інженерної екології Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»;

Дубко Валерій Олексійович – доктор фізико-математичних наук, професор, професор кафедри вищої математики Київського національного університету технологій та дизайну;

Єремєєв Ігор Семенович – доктор технічних наук, професор, професор кафедри автоматизованого управління технологічними процесами Таврійського національного університету імені В.І. Вернадського;

Лисенко Олександр Іванович – доктор технічних наук, професор, професор кафедри телекомунікацій Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»;

Огородник Станіслав Станіславович – доктор технічних наук, старший науковий співробітник, професор кафедри загальноінженерних дисциплін та теплоенергетики Таврійського національного університету імені В.І. Вернадського;

Сегай Олександр Михайлович – кандидат технічних наук, доцент, доцент кафедри загальноінженерних дисциплін та теплоенергетики Таврійського національного університету імені В.І. Вернадського;

Чумаченко Сергій Миколайович – доктор технічних наук, старший науковий співробітник, завідувач кафедри інформаційних систем Національного університету харчових технологій;

Цомко Олена – доктор філософії по спеціальності «Безпека і управління інформацією», відділення комп'ютерної інженерії, Інститут Міжнародної освіти, Університет Донгсо, Республіка Корея.

Статті у виданні перевірені на наявність плагіату за допомогою програмного забезпечення StrikePlagiarism.com від польської компанії Plagiat.pl.

**Рекомендовано до друку та поширення через мережу Internet
Вченою радою Таврійського національного університету імені В.І. Вернадського
(протокол № 6 від 03.02.2021 року)**

Науковий журнал «Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки» зареєстровано Міністерством юстиції України (Свідоцтво про державну реєстрацію друкованого ЗМІ серія КВ № 22895-12795Р від 11.08.2017 року)

Журнал включено до Переліку наукових фахових видань України (категорія «Б») з технічних наук (спеціальності: 144. Теплоенергетика, 161. Хімічні технології та інженерія, 172. Телекомунікації та радіотехніка) відповідно до Наказу МОН України від 17.03.2020 № 409 (додаток 1), 121. Інженерія програмного забезпечення, 123. Комп'ютерна інженерія, 126. Інформаційні системи та технології, 151. Автоматизація та комп'ютерно-інтегровані технології, 275. Транспортні технології (за видами) відповідно до Наказу МОН України від 02.07.2020 № 886 (додаток 4)

Журнал включено до міжнародної наукометричної бази Index Copernicus International (Республіка Польща)

Сторінка журналу: www.tech.vernadskyjournals.in.ua

ISSN 2663-5941 (Print)

ISSN 2663-595X (Online)

© Таврійський національний університет ім. В.І. Вернадського, 2021

ЗМІСТ

РАДІОТЕХНІКА ТА ТЕЛЕКОМУНІКАЦІЇ

Андрущак В.С., Андрухів Т.В., Максимюк Т.А., Бешлей М.І., Думич С.С. ІНТЕЛЕКТУАЛЬНЕ УПРАВЛІННЯ МАРШРУТИЗАЦІЄЮ В ОПТИЧНИХ ТРАНСПОРТНИХ МЕРЕЖАХ ІЗ ВИКОРИСТАННЯМ ГРАФОВИХ НЕЙРОННИХ МЕРЕЖ.....	1
Лисенко О.І., Романюк В.А., Гуйда О.Г., Дворська С.В., Осинський А.К. КОНЦЕПТУАЛЬНИЙ ПІДХІД ДО ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ ЖИВУЧОСТІ БЕЗПРОВОДОВОЇ СЕНСОРНОЇ МЕРЕЖІ НА ОСНОВІ ВИКОРИСТАННЯ МОБІЛЬНИХ ТЕЛЕКОМУНІКАЦІЙНИХ ПЛАТФОРМ.....	10
Літвінов Є.А., Сайченко І.О. ВИКОРИСТАННЯ ПРОГРАМНО-КОНФІГУРОВАНОГО РАДІО ДЛЯ ДОСЛІДЖЕННЯ ПЕРЕДАННЯ СИГНАЛІВ У ВИДИМОМУ СВІТЛІ.....	17
Ольшевський С.В., Танасійчук Я.В. СИНТЕЗ СТРУКТУРНОЇ СХЕМИ СИСТЕМИ ТЕСТОВОГО ДІАГНОСТУВАННЯ РЕЗОНАТОРНИХ БЛОКІВ МАГНЕТРОНІВ, НАПРАВЛЕНИХ НА РЕГЕНЕРАЦІЮ.....	28

ІНФОРМАТИКА, ОБЧИСЛЮВАЛЬНА ТЕХНІКА ТА АВТОМАТИЗАЦІЯ

Алієв Н.А. THE CALCULATING METHOD OF NGN ACCESS NODE CHARACTERISTICS WHEN SERVICING VOICE AND DATA TRAFFIC.....	33
Баган Т.Г., Бунь В.П., Ремінна А.А. СИНТЕЗ СИСТЕМИ АВТОМАТИЧНОГО КЕРУВАННЯ ТЕМПЕРАТУРИ ПАРИ ПРЯМОТОЧНОГО КОТЛОАГРЕГАТУ З ВИКОРИСТАННЯМ НЕЙРОКОНТРОЛЕРА.....	38
Бараненко Р.В. КІБЕРАТАКИ ЯК ОДНА З ФОРМ КІБЕРТЕРОРИЗМУ.....	45
Виганяйло С.М., В'юнєнко О.Б. ТЕНДЕНЦІЇ РОЗВИТКУ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У БІЗНЕС-АНАЛІТИЦІ.....	51
Войтко В.В., Бевз С.В., Бурбело С.М., Ставицький П.В. АНАЛІЗ ЗАСОБІВ ДЛЯ ПРОГРАМНОЇ РЕАЛІЗАЦІЇ СИСТЕМИ СИНТЕЗУ ТА АНАЛІЗУ МУЗИЧНИХ ЗВУКІВ.....	56
Зіноватна С.Л., Комлева О.О., Улізко Г.В., Писаренко К.О. УПРАВЛІННЯ ВИМОГАМИ ДО ТЕКСТОВОГО РЕДАКТОРА З МОЖЛИВІСТЮ ДОДАВАННЯ АУДІОНОТАТОК.....	61
Івченко Р.А., Купін А.І. ДОСЛІДЖЕННЯ МЕТОДІВ БАГАТОКРИТЕРІАЛЬНОЇ ОПТИМІЗАЦІЇ ДЛЯ ВИБОРУ ОБЛАДНАННЯ АБО ДЕТАЛЕЙ НА ВИРОБНИЦТВІ.....	67
Качурівський В.О., Качурівська Г.М. ПОБУДОВА АНІМАЦІЙНИХ ДІАГРАМ ЗАСОБАМИ CANVAS API.....	73
Киричек Г.Г., Гаркуша В.Ю. ВІРТУАЛІЗАЦІЯ ХОСТІВ НА ОСНОВІ PROXMOX VE В УМОВАХ НАДЛИШКОВОГО ВИКОРИСТАННЯ РЕСУРСІВ.....	78
Коломоєць Г.П. АВТОМАТИЗАЦІЯ ПЕРЕВІРКИ ДОДАТКІВ ДО ДИПЛОМІВ ПРО ВИЩУ ОСВІТУ.....	85
Кравець А.М., Сімоненко В.П. МЕТОД ЗНАХОДЖЕННЯ ІСТОРИЧНИХ ПАМ'ЯТОК НА ЗОБРАЖЕННІ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЙ КОМП'ЮТЕРНОГО ЗОРУ.....	93

Левкін Д.А., Бережна Н.Г., Макаров О.А., Кутья О.В. МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ТЕХНІЧНИХ СИСТЕМ.....	98
Логвін А.О. ТИПИ ГЕНЕРАТИВНИХ НЕЙРОННИХ МЕРЕЖ.....	103
Логінова Н.І., Янковський О.Г., Лобода Ю.Г., Толокнов А.А. ПРОГРАМНА РЕАЛІЗАЦІЯ ЗАДАЧІ АВТОМАТИЗОВАНОГО ФОРМУВАННЯ РОЗПОДІЛУ НАВЧАЛЬНОГО НАВАНТАЖЕННЯ НАУКОВО-ПЕДАГОГІЧНИХ ПРАЦІВНИКІВ КАФЕДРИ.....	110
Мануляк І.З., Мельничук С.І. ЗАСТОСУВАННЯ МЕТОДІВ ПОПЕРЕДНЬОГО ОПРАЦЮВАННЯ СИГНАЛІВ ЗІ ЗБЕРЕЖЕННЯМ ІНФОРМАЦІЙНОЇ ПРОДУКТИВНОСТІ ДЖЕРЕЛ ДАНИХ.....	117
Марченко Н.Б., Монченко О.В., Мартинюк Г.В. БАГАТОРІВНЕВІ СИСТЕМИ МОНІТОРИНГУ ТА ДІАГНОСТИКИ ЯК КОНСТРУКТИВНИЙ РОЗВИТОК ІНТЕЛЕКТУАЛЬНИХ ІНФОРМАЦІЙНИХ СИСТЕМ.....	123
Movchan K.O., Oleshchenko L.M. CLUSTERING OF INTERNET USERS SEARCH QUERIES USING GRAPH THEORY.....	128
Озерова Д.С., Пелих С.М. ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ АВТОМАТИЧНОЇ СИСТЕМИ РЕГУЛЮВАННЯ РІВНЯ ВОДИ У ГРУПІ ПІДГРІВАЧІВ ВИСОКОГО ТИСКУ.....	134
Осадчий С.І., Березюк І.А., Мельніченко М.М. МАКСИМІЗАЦІЯ ТОЧНОСТІ СТАБІЛІЗАЦІЇ КУТОВОГО ПОЛОЖЕННЯ ПОСАДОЧНОЇ ПЛАТФОРМИ.....	140
Плохотнюк М.О., Пелих С.М. РОЗРОБКА ФУНКЦІОНАЛЬНОЇ СХЕМИ АВТОМАТИЗАЦІЇ ГРУПИ ПІДГРІВАЧІВ НИЗЬКОГО ТИСКУ АТОМНОЇ ЕЛЕКТРОСТАНЦІЇ.....	146
Чанышев Р.И. УСЛОВИЯ ОБЕСПЕЧЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ И БЕЗОПАСНОСТИ ДАНЫХ ПОЛЬЗОВАТЕЛЯ ПРИ РАБОТЕ С ПРОВАЙДЕРАМИ ОБЛАЧНЫХ СЕРВИСОВ.....	151
Шаров С.В., Лубко Д.В., Шарова Т.М. ОСОБЛИВОСТІ РОЗРОБКИ ЕЛЕКТРОННОГО ПІДРУЧНИКА З УКРАЇНСЬКОЇ ЛІТЕРАТУРИ.....	159
Шкарупило В.В., Чемерис О.А., Душеба В.В., Кудерметов Р.К., Польська О.В. МОДЕЛЬНО-ОРІЄНТОВАНИЙ ПІДХІД ДО КОНТРОЛЮ ПОКАЗНИКІВ НЕФУНКЦІОНАЛЬНИХ ХАРАКТЕРИСТИК ПІД ЧАС ПРОЄКТУВАННЯ.....	166
ВІДОМОСТІ ПРО АВТОРІВ.....	172

CONTENTS

RADIO ENGINEERING AND TELECOMMUNICATIONS

Andrushchak V.S., Andrukhiv T.V., Maksymiuk T.A., Beshlei M.I., Dumych S.S. INTELLIGENT ROUTING MANAGEMENT IN OPTICAL TRANSPORT NETWORK USING GRAPH NEURAL NETWORK.....	1
Lysenko O.I., Romaniuk V.A., Guida O.G, Dvorskaya S.V., Osinskiy A.K. CONCEPTUAL APPROACH TO SURVIVABILITY FUNCTIONAL WIRELESS SENSOR NETWORKS THROUGH THE USE OF MOBILE TELECOMMUNICATION PLATFORM.....	10
Litvinov Ye.A., Saichenko I.O. USING SOFTWARE DEFINED RADIO TO STUDY SIGNAL TRANSMISSION IN VISIBLE LIGHT.....	17
Olszewski S.V., Tanasiichuk Ya.V. INVESTIGATION OF THE INFLUENCE OF THE DEFECT IN THE MAGNETRON RESONATORY SYSTEM ON THE PARAMETERS OF IT'S MICROWAVE FIELD.....	28

INFORMATICS, COMPUTER ENGINEERING AND AUTOMATION

Aliev H.A. THE CALCULATING METHOD OF <i>NGN</i> ACCESS NODE CHARACTERISTICS WHEN SERVICING VOICE AND DATA TRAFFIC.....	33
Bahan T.H., Boun V.P., Reminna A.A. DESIGN OF AUTOMATIC CONTROL SYSTEM OF DIRECT-FLOW BOILER STEAM TEMPERATURE USING A NEUROCONTROLLER.....	38
Baranenko R.V. CYBER ATTACKS AS A FORM OF CYBER TERRORISM.....	45
Vyhaniailo S.M., Viunenko O.B. TENDENCY OF DEVELOPMENT OF INFORMATION TECHNOLOGY IN BIZNES ANALYTIC.....	51
Voitko V.V., Bevz S.V., Burbelo S.M., Stavytskyi P.V. ANALYSIS OF TOOLS FOR SOFTWARE IMPLEMENTATION OF SYNTHESIS SYSTEM AND ANALYSIS OF MUSICAL SOUNDS.....	56
Zinovatna S.L., Komleva O.O., Ulizko H.V., Pysarenko K.O. MANAGEMENT OF REQUIREMENTS FOR THE TEXT EDITOR WITH THE POSSIBILITY OF ADDING AUDIO NOTES.....	61
Ivchenko R.A., Kupin A.I. RESEARCH OF MULTICRITERIA OPTIMIZATION METHODS FOR SELECTION OF EQUIPMENT OR PARTS IN PRODUCTION.....	67
Kachurivskii V.O., Kachurivska H.M. CONSTRUCTION OF ANIMATION DIAGRAMS BY CANVAS API.....	73
Kirichek G.G., Harkusha V.Yu. HOSTS VIRTUALIZATION ON BASED PROXMOX VE IN CONDITIONS EXCESSIVE USE OF RESOURCES.....	78
Kolomoiets H.P. AUTOMATION OF HIGHER EDUCATION DIPLOMAS SUPPLEMENTS VERIFICATION.....	85
Kravets A.M., Simonenko V.P. LANDMARKS RECOGNITION METHOD USING COMPUTER VISION TECHNOLOGIES.....	93
Levkin D.A., Berezhnaja N.H., Makarov O.A., Kutiya O.V. MATHEMATICAL MODELING OF TECHNICAL SYSTEMS.....	98

Бараненко Р.В.

Уманський національний університет садівництва

КІБЕРАТАКИ ЯК ОДНА З ФОРМ КІБЕРТЕРОРИЗМУ

У статті зосереджено увагу на питаннях протидії кібератакам як актам кібертероризму в контексті забезпечення національної та міжнародної системи кібербезпеки. Зроблено акцент, що проникнення до інформаційної сфери та її використання кримінальними, у тому числі й терористичними, елементами породило явища, які називаються кіберзлочинністю й кібертероризмом.

Наголошується, що кібертерорист може становити небезпеку для значно більшої кількості людей, безпосередньо не беручи участі в терористичному акті, а перебуваючи в безпечному для себе місці.

Наведено визначення заходів забезпечення кібернетичної безпеки держави в кіберпросторі, аналіз змісту кібертероризму, його складників і методів реалізації актів кібертероризму.

Наведено перелік цілей, для реалізації яких терористичні організації широко використовують Інтернет і новітні інформаційні технології.

За своїми можливостями акти кібертероризму розподілено на три рівні.

Особливий акцент зроблено на тому, що однією з найяскравіших форм кібертероризму є проведення кібератак. Наведено поняття кібератак типу «убивчий ланцюжок» (Kill Chain) та етапів її реалізації. Проаналізовано кожен з етапів. Оскільки особливою формою кібератаки, яка фокусується на перериванні мережного сервісу, є DoS-атака, то розглянуто схеми таких атак, класифікаційні ознаки кібератак і варіанти організації DDoS-атак: ботнет, флешмоб і HTTP-флуд.

Зазважено, що особливою проблемою для фахівців з кібербезпеки є визначення комп'ютера користувача мережі, з якого здійснено кібератаку.

У підсумку наведено перелік факторів, які рекомендовано враховувати для протидії кібератакам.

Ключові слова: кібератака, кібербезпека, кіберпростір, кібертероризм, протидія кібератакам.

Постановка проблеми. Швидкий розвиток інформаційних і телекомунікаційних технологій сягає з кожним днем усе нових і нових рівнів, про що вказує їх активне впровадження до всіх без винятку сфер життєдіяльності людини. Інформаційні мережі, мережа Інтернет, хмарні сервіси дають змогу обмінюватися інформацією за лічені секунди, крім цього, упровадження комп'ютерних систем управління стало причиною автоматизації різноманітних виробничих та інших процесів.

Становлення інформаційного суспільства не лише дає змогу зводити більш ефективно й успішно суспільство, а й надає нових імпульсів традиційним загрозам безпеці держави і створює принципово нові складнощі для системи національної безпеки. У таких умовах особливого значення набуває пошук нових можливостей гарантування безпеки держави з огляду на формування нового поля протиборства – кіберпростору.

Проникнення до інформаційної сфери та її використання кримінальними, у тому числі й терористичними, елементами породило явища, які називаються кіберзлочинністю і кібертероризмом.

Комп'ютерна техніка використовуються в різних сферах суспільного життя, від бібліотек до

атомних електростанцій і військових об'єктів. Якщо терорист, який використовує у своїх цілях звичайне озброєння, небезпечний для десятків або сотень людей, то кібертерорист може становити небезпеку для значно більшої кількості людей, безпосередньо не беручи участі в терористичному акті, а перебуваючи в безпечному для себе місці. Зважаючи на той факт, що проти України вже сьомий рік ведеться гібридна війна з боку Російської Федерації, для нашої держави є дуже важливим забезпечення безпеки комп'ютерної техніки й телекомунікаційних мереж у сферах, які критично впливають на життєзабезпечення українського народу. Такий стан справ дає підстави стверджувати, що відсутність надійної системи кібернетичної безпеки (стан захищеності кіберпростору загалом або окремих об'єктів його інфраструктури та засобів їх взаємодії від ризику стороннього кібернетичного впливу) може призвести до втрати політичної незалежності будь-якої держави світу, тобто до фактичного програшу нею війни невійськовими засобами та підпорядкування її національних інтересів інтересам іншої (протиборчої) сторони [1].

У зв'язку з цим постає питання визначення самого поняття «кібертероризм» і його змісту,

аналіз його складників і методів реалізації актів кібертероризму; розробки рекомендацій і заходів протидії кібертероризму.

Аналіз останніх досліджень і публікацій.

Окремі аспекти протидії кібертероризму й забезпечення кібернетичної безпеки держави розглядали В.Л. Бурячок, В.М. Бутузов, В.Д. Гавловський, В.О. Голубєв, І.В. Діордіца, О.Д. Довгань, Д.В. Дубов, Н.В. Коваленко, В.В. Марков, В.А. Ліпкан, В.В. Носов, О.В. Манжай, М.А. Ожеван, М.А. Погорєцький, К.В. Тітуніна, В.Г. Хлань, В.О. Хорошко, В.П. Шеломенцев; зарубіжні науковці: Л. Вентц, Д. Деннінг, Ф. Крамер, М. Лібіцькі, Дж. Ліпман, Дж. Льюїс, Дж. Най, Г. Раттрей, Д. Фахренкурт, Дж. Шелдон та інші.

Проте низка важливих питань у сфері протидії кібертероризму залишилася без достатньої уваги дослідників.

Постановка завдання. Метою роботи є визначення заходів забезпечення кібернетичної безпеки держави в кіберпросторі, аналіз змісту кібертероризму, його складників і методів реалізації актів кібертероризму; розробка рекомендацій і заходів протидії кібертероризму.

Об'єктом дослідження є система протидії кібертероризму як сукупність явищ і процесів. Предметом дослідження є характеристика методів і засобів реалізації кібератак як актів кібертероризму та механізмів їх протидії.

Виклад основного матеріалу дослідження.

Кібертероризм – це багатогранний феномен, зумовлений багато в чому безконтрольним використанням глобальних мереж, недостатньою увагою з боку держави, громадянського суспільства і спецслужб до цього сегменту інформаційного простору, що виявляється в атаках на комп'ютери, комп'ютерні програми й мережі або розміщену в них інформацію, з метою створення атмосфери страху та безвиході в суспільстві в ім'я досягнення цілей та інтересів суб'єктів терористичної діяльності, що вимагає об'єднання зусиль світової спільноти для ефективної протидії йому [2, с. 15].

Відомо, що терористичні організації широко користуються Інтернетом і новітніми інформаційними технологіями для реалізації таких цілей:

- налагодження конфіденційного зв'язку (наприклад, через чати онлайн-ігор або кодовані повідомлення);
- планування атак за допомогою таких сервісів, як Google Maps або Earth;
- координація атак за допомогою VoIP-телефонії та інших інформаційних технологій, що забезпечують анонімність і конфіденційність;

- визначення потенційних цілей (наприклад, використання соціальних мереж для визначення «прибуткових» жертв з метою отримання викупу за їх викрадення);

- підвищення обізнаності у сфері військової тактики і створення вибухових пристроїв;

- фінансування терористичної діяльності через анонімні онлайн-пожертвування з усього світу, що здійснюються за допомогою електронних платіжних систем;

- залучення нових членів і поширення терористичної ідеології завдяки створенню високоякісних медіа-ресурсів та активній вербувальній роботі у соціальних мережах [3, с. 340].

Групою Monterey визначено три рівні кібертерору за своїми можливостями:

- простий неструктурований: можливість проводити основні атаки проти окремих систем, що використовують інструменти, створені кимось іншим. Організація має невеликий цільовий аналіз, управління й контроль;

- просунуто-структурований: можливість проводити більш складні атаки проти декількох систем або мереж і, можливо, модифікувати або створювати базові інструменти злову. Організація має елементарний об'єкт аналізу, управління й контролю;

- комплексно-координований: можливість до скоординованих атак, здатних викликати масове руйнування інтегрованих гетерогенних систем захисту (у тому числі криптографічних). Можливість створювати складні інструменти злову. Організація має дуже ефективний цільовий аналіз, управління й контроль [4].

Науковці І.В. Владленова, Е.А. Кальницький розрізняють різні прийоми кібертероризму в кіберпросторі:

- нанесення шкоди окремим фізичним елементам інформаційного простору, наприклад, руйнування мереж електроживлення, здійснення перешкод;

- використання спеціальних програм, що стиmulюють руйнування апаратних засобів;

- крадіжка або знищення інформаційного, програмного й технічного ресурсів, що мають суспільну значимість, шляхом подолання систем захисту, упровадження вірусів тощо;

- вплив на програмне забезпечення та інформацію з метою їх спотворення або модифікації в інформаційних системах і системах управління;

- розкриття й загроза опублікування або самоопублікування закритої інформації про функціонування інформаційної інфраструктури держави,

суспільно значущих і військових інформаційних систем, коди шифрування, принципи роботи систем шифрування;

– захоплення каналів ЗМІ з метою поширення дезінформації, чуток, демонстрації потужності терористичної організації та оголошення своїх вимог тощо [5].

Сьогодні вже ні для кого не є секретом, що особливий інтерес для терористів становлять саме державні інформаційні системи, об'єктами їх діяльності стають важливі елементи державної інфраструктури, наприклад, системи управління та функціонування атомних об'єктів, електростанцій, залізні дороги, аеропорти тощо [6, с. 57].

Однією з найяскравіших форм кібертероризму є проведення кібератак. Наприклад, тільки в листопаді та грудні 2016 року Україна піддавалася кібератакам 6500 разів. Крім інформаційної пропаганди й викрадення важливої інформації, російські кібервійська добралися й до електрики в столиці України. 17 грудня 2016 року в Києві ненадовго вимкнулося світло. Після проведеного розслідування підприємство «Укренерго» заявило, що ця атака пов'язана з іншими: зломом системи «Укрзалізниця», Міністерства фінансів і Пенсійного фонду України. Це не перше втручання до українських енергосистем. У грудні 2015 року без світла ненадовго залишилися 230 тисяч киян. Фахівці з кібербезпеки з Information Systems Securit Partners (ISSP), які проводили розслідування для «Укренерго», пов'язують ці два зломи. Наслідки цих атак вдалося легко усунути. Експерти висловили припущення, що ці атаки проводилися лише з метою демонстрації своїх можливостей. Україна перетворилася на тестовий полігон для російських хакерів. BugDrop – ще одна кібератака, яка відбулася в Україні в лютому 2017 року. Ініціатори цього злому досі невідомі. Кібератаку виявила міжнародна компанія у сфері безпеки CyberX, яка на своєму сайті опублікувала офіційне розслідування [7].

Проте найбільш вразливою виявилася масштабна хвиля кібератак у червні 2017 року. 27 червня в Україні вірус-вимагач «Petya.A» зупинив роботу платіжних терміналів у «Київському метрополітені» й призвів до масових збоїв в українських торговельних мережах, енергокомпаніях, ЗМІ, банках, поштових сервісах. За дві доби до Національної поліції звернулися понад 1,5 тис. юридичних і фізичних осіб як жертв зазначеної кібератаки. При цьому тільки 178 із них написали офіційні заяви, з яких 152 заяви – від представників приватного сектору, 26 – від державних структур [8].

Відомим українським дослідником з питань кібербезпеки професором В.Л. Бурячком сформульоване таке визначення поняття «кібератака» – це сукупність узгоджених щодо мети, змісту й часу дій або заходів, так званих кіберакцій, спрямованих на певний об'єкт впливу з метою порушення конфіденційності, цілісності, доступності, спостережуваності або авторства інформації, що циркулює в ньому, з урахуванням її уразливості, а також порушення роботи ІТ-систем і мереж зазначеного об'єкта [9].

Кібератаки можуть бути таргетованими, тобто спрямованими проти конкретної цілі з прихованням слідів активності на всіх її етапах. Таргетована (цільова) кібератака (від англ. target) є безперервним тривалим процесом несанкціонованої активності кіберзлочинів в умовах конкретного об'єкта критичної інфраструктури, покликаним здолати конкретні механізми забезпечення безпеки й завдати конкретного збитку (фізичного, інформаційного, морального тощо). Цей процес віддалено керований у реальному часі організованою професійною групою кіберпорушників, озброєних потужними апаратно-програмними засобами. Інструментарієм таргетованих кібератак є засоби АРТ (Advanced Persistent Threat – атакуюча безперервна загроза) – комбінація спеціальних утиліт віддаленого доступу, шкідливого програмного забезпечення, механізмів використання вразливостей «нульового дня», а також інших компонентів, спеціально розроблених для реалізації конкретної атаки [10, с. 79].

У кібербезпеці існує поняття «убивчий ланцюжок» (Kill Chain), яке позначає етапи кібератаки на інформаційні системи – об'єкти атаки.

До компрометації об'єкта атаки передують такі етапи:

– *розвідка* – збір інформації про об'єкт атаки за допомогою відкритих джерел;

– *озброєння* – створення шкідливого ПЗ та експлоїтів для відправки до об'єкта атаки;

– *доставка* – відправка до об'єкта атаки експлоїтів і шкідливого ПЗ електронною поштою, з використанням web-сайтів тощо.

Під час компрометації об'єкта атаки виконуються такі 2 етапи:

– *реалізація (зараження)* – виконання експлоїтів;

– *установлення* – на об'єкт атаки встановлюється шкідливе ПЗ та бекдори.

Після компрометації об'єкта атаки вже можлива реалізація таких етапів:

– керування й контроль – віддалене керування об'єктом атаки, що здійснюється за допомогою командного сервера або каналу;

– виконання дій – зловмисник здійснює шкідливі дії, наприклад, викрадає інформацію, шифрує файли, перехоплює керування, виконує підміну даних, виводить пристрої системи з ладу або проводить додаткові атаки на інші пристрої в мережі, знову реалізуючи етапи «убивчого ланцюжка».

Щоб захиститися від «убивчого ланцюжка», засоби мережного захисту створюються для протистояння кібератаці на кожному етапі цього ланцюжка. При побудові системи захисту організації від подібних кібератак, на думку фахівців компанії Lockheed Martin, потрібно відповісти на такі питання:

Що є індикаторами атаки на кожному етапі «убивчого ланцюжка»?

Які інструменти безпеки необхідні для виявлення індикаторів атаки на кожному з етапів?

Чи є проблеми з виявлення атаки в системі кібербезпеки організації?

Особливою формою кібератаки, яка фокусується на перериванні мережного сервісу, є DoS-атака, що досягається відправленням зловмисниками великих обсягів трафіку або даних через цільову мережу, поки мережа не перевантажується («відмова в обслуговуванні»). Як правило, DoS-атака здійснюється одним комп'ютером або одним центральним розташуванням комп'ютерів. Популярна категорія DoS-атак – розподілена атака на відмову в обслуговуванні (DDoS), що відрізняється від звичайної DoS атаки кількістю комп'ютерів, що беруть у ній участь. Ці комп'ютери працюють разом за допомогою Інтернету для передачі трафіку до цільової мережі [11, с. 153].

В.А. Світличний виділяє такі атаки на відмову залежно від схеми атаки, тобто шляхів, якими здійснюється доставка шкідливого трафіку від атакуючого комп'ютера до атакованої інформаційної системи:

– пряма, під час якої пересилка трафіку здійснюється безпосередньо з одного або багатьох хостів;

– віддзеркалена, під час якої пересилка трафіку здійснюється через третіх осіб;

– прихована, під час якої зловмисний трафік ховається в «законному» трафіку [12, с. 89].

В.Л. Бурячок, В.Б. Толубко та інші наводять такі класифікаційні ознаки кібератак:

1. За метою впливу на об'єкт атаки розрізняють спрямований, наприклад, на порушення ціліс-

ності або конфіденційності інформації, її захищеності від несанкціонованого доступу, а також на порушення живучості системи та надійності її функціонування.

2. За принципом впливу на об'єкт атаки:

– використання прихованих каналів (шляхів передавання інформації, що дають змогу двом процесам обмінюватися нею у спосіб, який порушує політику безпеки);

– застосування прав суб'єкта системи (користувача, процесу) до об'єкта (файлів даних, каналів зв'язку тощо).

3. За характером впливу на об'єкт атаки:

– активний вплив (користувач виконує деякі дії, що виходять за рамки його обов'язків і порушують наявну політику безпеки, наприклад, розкриття пароля);

– пасивний вплив (користувач прослуховує лінії зв'язку між двома вузлами мережі).

4. За способом впливу на об'єкт атаки, зокрема на систему дозволів (захоплення привілеїв), а також безпосередній доступ до даних, програм, служб, каналів зв'язку з використанням привілеїв.

5. За засобами впливу на об'єкт атаки, що передбачають використання або стандартного програмного забезпечення, або спеціально розроблених програм.

6. За об'єктом атаки: напад може здійснюватися на систему загалом; на дані та програми, що містяться на зовнішніх (дисківоди, мережні пристрої, термінали) або внутрішніх (оперативна пам'ять, процесор) пристроях системи, а також у каналах передавання даних; на процеси й підпроцеси системи за участю користувачів. Метою таких атак є або прямий вплив на роботу процесу (його припинення, зміна привілеїв і характеристик), або зворотний вплив (використання зловмисником привілеїв, характеристик тощо іншого процесу у своїх цілях).

7. За станом об'єкта: безпосередньо під час атаки інформація в ньому може зберігатися, передаватися або оброблятися.

8. За використовуваною системою захисту; за кількістю атакуювальників; за джерелами атак; за розміщенням атакуючого об'єкта стосовно атакованого; за наявністю зв'язку з атакованим об'єктом; за рівнем еталонної моделі OSI об'єкта, на який здійснюється вплив. При цьому помилки системи захисту інформації можуть бути зумовлені, наприклад, помилками адміністративного управління, помилками в алгоритмах програм, а також у зв'язках між ними, помилками кодування тощо [13, с. 45–46].

У більшості випадків результат DDoS-атаки – це непрацюючий або повільно працюючий веб-сервер, але останнім часом DDoS-атаки орієнтовані не тільки на веб-сервери. Основними цілями сучасних DDoS-атак усе частіше стають інтернет-канал і міжмережний екран [14, с. 22].

Є два варіанти організації DDoS-атак:

– ботнет – зараження певного числа комп'ютерів програмами, які в певний момент починають здійснювати запити до атакованого сервера;

– флешмоб – домовленість великого числа користувачів інтернету почати здійснювати певні типи запитів до атакованого сервера [15, с. 53].

Ще однією особливістю сучасних DDoS-атак є атаки типу HTTP-флуд. Вони починаються, коли атакуючий направляє велику кількість HTTP GET/POST запитів, підриваючи ресурси сервера. При цьому, хоча HTTP-атаки залишаються найбільш розповсюдженими, SSL-шифровані атаки залишаються небезпечними, оскільки їм важко протидіяти. Зловмисники використовують цю функцію зашифрованих повідомлень як засіб обходу рішень безпеки (анти-DoS/DDoS, брандмауера й IPS/IDS), які, урешті, не фіксують атаку [14, с. 22].

Додатковою проблемою для фахівців з кібербезпеки є визначення комп'ютера користувача мережі, з якого здійснено кібератаку. Погрішність ідентифікації, заснованої на IP-адресі (до недавнього часу облік був основним методом ідентифікації), складається з погрішностей передачі й погрішностей користування комп'ютером. Так, наприклад, при роботі користувачів через проху-сервер уся підмережа, яка за ним ховається, у більшості випадків матиме єдину IP-адресу. З іншого боку, працюючи через комутоване з'єднання, користувач при кожному підключенні отримуватиме від провайдера нову IP-адресу тощо [16, с. 151].

Завдання ідентифікації пристрою зазвичай вирішується за допомогою унікальних кодів,

таких як MAC або IP-адреса в мережах Ethernet або IMEI в мережах GSM. Проте використання унікального коду дає відповідь лише на питання, це той самий пристрій чи ні, але не повідомляє точний тип пристрою та спосіб його використання конкретним користувачем [16, с. 152].

Висновки. Кібератаки на інформаційні системи держустанов, організацій та об'єкти критичної інфраструктури як акти кібертероризму становлять значну загрозу як для системи міжнародної кібербезпеки, так і для української національної безпеки як її невід'ємного складника, наносячи непоправну шкоду нормальній життєдіяльності українського суспільства особливо в умовах ведення гібридної війни з Російською Федерацією. Засоби сучасного інформаційного суспільства дають змогу кібертерористам легко пропагувати свої ідеї, розширювати лави своїх учасників і досягати своєї мети, використовуючи кіберпростір.

Тому для виявлення слідів кібератак і як заходи їх протидії рекомендуємо враховувати такі фактори, запропоновані в дослідженні Н.С. Козак:

1) контроль цілісності програм, файлів даних та інших інформаційних ресурсів, які підлягають захисту;

2) аналіз діяльності користувачів і процесів, а також мережного трафіку в комп'ютерній мережі, над якою здійснюється контроль;

3) контроль фізичних форм нападу на елементи інформаційної системи, у тому числі й на відчужувані джерела збереження інформації;

4) аналіз дій адміністраторів з перевірки попередніх інцидентів [17].

Звісно, що жодні превентивні заходи не дають 100% захисту інформаційної системи – об'єкта атаки від руйнівного впливу кібератак. Проте їх запровадження до чинної системи кіберзахисту об'єкта атаки дасть змогу зменшити нанесену кібертерористами шкоду.

Список літератури:

1. Бурячок В.Л. Кібернетична безпека – головний фактор сталого розвитку сучасного інформаційного суспільства. *Сучасна спеціальна техніка*. 2011. № 3 (26). С. 104–114.
2. Молодчая Е.Н. Политика противодействия кибертероризму в современной России: политологический аспект : автореф. дисс. ... канд. полит. наук : 23.00.02. Москва, 2011. 30 с.
3. Ткачук Н. Кібертероризм як новий виклик національній безпеці. *Протидія терористичній діяльності: міжнародний досвід і його актуальність для України* : матеріали Міжнар. наук.-практ. конф. (30 вересня 2016 року). Київ : Національна академія прокуратури України, 2016. С. 340–342.
4. Dorothy E. Denning (May 23, 2000). "Cyberterrorism". cs.georgetown.edu. Archived from the original on March 10, 2014. Retrieved June 19, 2016.
5. Владленова І.В., Кальницький Е.А. Кіберзлочинність як виклик інформаційному суспільству. *Гілея: науковий вісник* : збірник наукових праць. 2013. Вип. 77. С. 142–146.

6. Бойченко О.В., Ончурова О.О. Кібертероризм у складі сучасних проблем національної безпеки. *Фортеця права*. 2010. № 2. С. 57.
7. Всесвітній огляд економічних злочинів. Кіберзлочини в центрі уваги. URL: http://www.pwc.com/ua/en/services/forensic/assets/gecs_2011_report_ukraine_ukr.pdf.
8. Питання місяців: стало відомо, хто допоможе Україні у протистоянні кібератакам. URL: <https://www.obozrevatel.com/ukr/crime/61395-pitannya-misyatsiv-stalo-vidomo-hto-dopomozhe-ukraini-v-vidobrazhenni-kiberatak.htm>.
9. Бурячок В.Л. Основи формування державної системи кібернетичної безпеки : монографія. Київ : НАУ, 2013. 432 с.
10. Козюра В.Д., Хорошко В.О. Як протистояти реальним кіберзагрозам об'єктам критичної інфраструктури України. *Кібербезпека в Україні: правові та організаційні питання* : матеріали Всеукр. наук.-практ. конф., м. Одеса, 17 листопада 2017 р. Одеса : ОДУВС, 2017. С. 79–80.
11. Бараненко Р.В., Задорожна А.Ю. Аналіз методів протидії кібератакам. *Юридичний бюлетень*. 2018. № 6. С. 148–161.
12. Світличний В.А. Дослідження атак на відмову в обслуговуванні інформаційно-телекомунікаційних систем. *Кібербезпека в Україні: правові та організаційні питання* : матеріали Всеукр. наук.-практ. конф., м. Одеса, 30 листопада 2018 р. Одеса : ОДУВС, 2018. С. 88–89.
13. Інформаційна та кібербезпека: соціотехнічний аспект : підручник / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. Київ : ДУТ, 2015. 288 с.
14. Гнусов Ю.В., Кійков В.М. Сучасні тенденції розвитку DDoS-атак. *Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності* : матеріали Міжнар. наук.-практ. конф., м. Харків, 12 листоп. 2014 р. / МВС України, Харків. нац. ун-т внутр. справ. Харків : Права людини, 2014. 200 с.
15. Торяник В.В., Чмирь А.Ю. Актуальність проблеми атаки на відмову в обслуговуванні. *Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності* : матеріали Міжнар. наук.-практ. конф., м. Харків, 12 листоп. 2014 р. / МВС України, Харків. нац. ун-т внутр. справ. Харків : Права людини, 2014. 200 с.
16. Світличний В.А., Петров К.Е. Від ідентифікації комп'ютера до ідентифікації користувача у мережі Інтернет. *Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності* : матеріали Міжнар. наук.-практ. конф., м. Харків, 12 листоп. 2014 р. / МВС України, Харків. нац. ун-т внутр. справ. Харків : Права людини, 2014. 200 с.
17. Козак Н.С. Криміналістичні прийоми, способи і засоби виявлення, розкриття та розслідування комп'ютерних злочинів : дис. ... канд. юрид. наук : 12.00.09. Ірпінь, 2011. 229 с.

Baranenko R.V. CYBER ATTACKS AS A FORM OF CYBER TERRORISM

The article focuses on the issues of countering cyber attacks as acts of cyber terrorism in the context of ensuring the national and international cyber security system. The emphasis is made that the penetration into the information sphere and its use by criminal, including terrorist elements, has given rise to phenomena called cybercrime and cyber terrorism.

It is noted that a cyber terrorist can pose a danger to a significantly larger number of people, not directly participating in a terrorist act, but being in a safe place for himself.

The paper provides definitions of measures to ensure the cyber security of the state in cyberspace, analysis of the content of cyber terrorism, its components and methods of implementing acts of cyber terrorism.

A list of goals for the realization of which terrorist organizations widely use the Internet and the latest information technologies are given.

According to their capabilities, acts of cyber terrorism are divided into three levels.

Particular emphasis is placed on the fact that one of the most prominent forms of cyber terrorism is the conduct of cyber attacks. The concepts of cyber attacks such as "Kill Chain" and the stages of its implementation are given. Each of the stages is analyzed. Since a special form of cyber attack, which focuses on interrupting a network service, is a DoS attack, the paper considers schemes of such attacks, classification signs of cyber attacks and options for organizing DDoS attacks: botnet, flash mob, and HTTP flood.

It was noted that a special problem for cyber security specialists is the identification of the computer of the network user from which the cyber attack was carried out.

As a result, a list of factors that are recommended to be taken into account in countering cyber attacks is provided.

Key words: *cyber attack, cyber security, cyberspace, cyber terrorism, countering cyber attacks.*

Відомості про авторів

Алієв Хайдар – PhD, Азербайджанський технічний університет

Андрухів Т.В. – кандидат технічних наук, директор Львівської філії (керуючої філії Західного макрорегіону) ПАТ «Укртелеком»

Андрущак В.С. – аспірант кафедри телекомунікацій Національного університету «Львівська політехніка»

Баган Т.Г. – кандидат технічних наук, доцент, доцент кафедри автоматизації теплоенергетичних процесів Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»

Бараненко Р.В. – кандидат технічних наук, доцент, доцент кафедри інформаційних технологій Уманського національного університету садівництва

Бевз С.В. – кандидат технічних наук, доцент, доцент кафедри електричних станцій і систем Вінницького національного технічного університету

Бережна Н.Г. – кандидат технічних наук, доцент кафедри транспортних технологій і логістики Харківського національного технічного університету сільського господарства імені Петра Василенка

Березюк І.А. – кандидат технічних наук, доцент, Центральноукраїнський національний технічний університет

Бешлей М.І. – кандидат технічних наук, докторант кафедри телекомунікацій Національного університету «Львівська політехніка»

Бунь В.П. – кандидат технічних наук, доцент, доцент кафедри автоматизації теплоенергетичних процесів Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»

Бурбело С.М. – кандидат технічних наук, доцент кафедри програмного забезпечення Вінницького національного технічного університету

В'юненко О.Б. – кандидат економічних наук, доцент, доцент кафедри кібернетики та інформатики Сумського національного аграрного університету

Виганяйло С.М. – кандидат економічних наук, доцент кафедри соціально-економічних наук Сумської філії Харківського національного університету внутрішніх справ

Войтко В.В. – кандидат технічних наук, доцент, доцент кафедри програмного забезпечення Вінницького національного технічного університету

Гаркуша В.Ю. – магістр факультету комп'ютерних наук та технологій Національного університету «Запорізька політехніка»

Гуйда О.Г. – старший викладач кафедри загальноінженерних дисциплін та теплоенергетики Таврійського національного університету імені В.І. Вернадського

Дворська С.В. – навчальний майстер кафедри телекомунікацій Інституту телекомунікаційних систем Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»

Думич С. С. – кандидат технічних наук, доцент кафедри телекомунікацій Національного університету «Львівська політехніка»

Душеба В.В. – кандидат технічних наук, доцент, в.о. завідувача відділу математичного та комп'ютерного моделювання Інституту проблем моделювання в енергетиці імені Г.Є. Пухова Національної академії наук України

Зіноватна С.Л. – кандидат технічних наук, доцент, кафедра системного програмного забезпечення Одеського національного політехнічного університету

Івченко Р.А. – аспірант кафедри «Автоматизації, комп'ютерних наук і технологій» Криворізького національного університету

Качурівська Г.М. – кандидат фізико-математичних наук, доцент, доцент кафедри інформаційних технологій та вищої математики Відокремленого підрозділу Національного університету біоресурсів і природокористування України «Бережанський агротехнічний інститут»

Качурівський В.О. – інженер, кандидат педагогічних наук, доцент, доцент кафедри інформаційних технологій та вищої математики Відокремленого підрозділу Національного університету біоресурсів і природокористування України «Бережанський агротехнічний інститут»

Киричек Г.Г. – кандидат технічних наук, доцент, доцент кафедри комп'ютерних систем та мереж Національного університету «Запорізька політехніка»

Коломоєць Г.П. – кандидат фізико-математичних наук, доцент, доцент кафедри програмного забезпечення автоматизованих систем Інженерного навчально-наукового інституту Запорізького національного університету

Комлева О.О. – кафедра системного програмного забезпечення Одеського національного політехнічного університету

Кравець А.М. – магістрант кафедри обчислювальної техніки Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»

Кудерметов Р.К. – кандидат технічних наук, доцент, завідувач кафедри комп'ютерних систем та мереж Національного університету «Запорізька політехніка»

Купін А.І. – доктор технічних наук, професор, професор кафедри «Комп'ютерних систем та мереж» Криворізького національного університету

Кутья О.В. – старший викладач кафедри транспортних технологій і логістики Харківського національного технічного університету сільського господарства імені Петра Василенка

Левкін Д.А. – кандидат технічних наук, старший викладач кафедри вищої математики Харківського національного технічного університету сільського господарства імені Петра Василенка

Лисенко О.О. – доктор технічних наук, професор, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»

Літвінов Є.А. – магістрант інституту телекомунікаційних систем Національного технічного університету України «Київського політехнічного інституту імені Ігоря Сікорського»

Лобода Ю.Г. – кандидат педагогічних наук, доцент, доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія»

Логвін А.О. – аспірант кафедри електронних обчислювальних машин факультету комп'ютерної інженерії та управління Харківського національного університету радіоелектроніки

Логінова Н.І. – кандидат педагогічних наук, доцент, завідувач кафедри інформаційних технологій Національного університету «Одеська юридична академія»

Лубко Д.В. – кандидат технічних наук, доцент, доцент кафедри комп'ютерних наук Таврійського державного агротехнологічного університету імені Дмитра Моторного

Макаров О.А. – кандидат фізико-математичних наук, доцент кафедри прикладної математики Харківського національного університету імені В.Н. Каразіна

Максимюк Т.А. – кандидат технічних наук, докторант кафедри телекомунікацій Національного університету «Львівська політехніка»

Мануляк І.З. – кандидат технічних наук, доцент кафедри комп'ютерних систем та мереж Івано-Франківського національного технічного університету нафти і газу

Мартинюк Г.В. – кандидат технічних наук, доцент кафедри засобів захисту інформації Національного авіаційного університету

Марченко Н.Б. – кандидат технічних наук, доцент, доцент кафедри комп'ютеризованих систем управління Національного авіаційного університету

Мельничук С.І. – доктор технічних наук, завідувач кафедри комп'ютерних систем та мереж Івано-Франківського національного технічного університету нафти і газу

Мельніченко М.М. – аспірант Центральноукраїнського національного технічного університету

Мовчан К.О. – старший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби Безпеки України

Монченко О.В. – кандидат технічних наук, доцент, доцент кафедри біокібернетики та аерокосмічної медицини Національного авіаційного університету

Озерова Д.С. – студентка кафедри комп'ютерних технологій автоматизації Одеського національного політехнічного університету

Олещенко Л.М. – кандидат технічних наук, доцент кафедри програмного забезпечення комп'ютерних систем Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»

Ольшевський С.В. – доктор технічних наук, доцент, доцент кафедри радіотехніки та радіоелектронних систем Київського національного університету імені Тараса Шевченка

Осадчий С.І. – доктор технічних наук, професор Центральноукраїнського національного технічного університету

Осинський А.К. – науковий магістр кафедри телекомунікацій Інституту телекомунікаційних систем Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»

Пелих С.М. – професор кафедри комп'ютерних технологій автоматизації Одеського національного політехнічного університету

Писаренко К.О. – кандидат технічних наук, доцент кафедри системного програмного забезпечення Одеського національного політехнічного університету

Плохотнюк М.О. – студент 6 курсу групи ТК-1514, кафедри комп'ютерних технологій автоматизації Одеського національного політехнічного університету

Польська О.В. – старший викладач кафедри комп'ютерних систем та мереж Національного університету «Запорізька політехніка»

Ремінна А.А. – магістр кафедри автоматизації теплоенергетичних процесів Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»

Романюк В.А. – доктор технічних наук, професор, заступник начальника інституту з навчальної та наукової роботи Військового інституту телекомунікацій та інформатизації Національного технічного університету України «Київський політехнічний інститут»

Сайченко І.О. – аспірант інституту телекомунікаційних систем Національного технічного університету України «Київського політехнічного інституту імені Ігоря Сікорського»

Сімоненко В.П. – професор кафедри обчислювальної техніки Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»

Ставицький П.В. – аспірант кафедри програмного забезпечення Вінницького національного технічного університету

Танасійчук Я.В. – аспірант кафедри радіотехніки та радіоелектронних систем Київського національного університету імені Тараса Шевченка

Толокнов А.А. – асистент кафедри інформаційних технологій Національного університету «Одеська юридична академія»

Улізко Г.В. – інженер 1 категорії кафедри кібербезпеки та програмного забезпечення Одеського національного політехнічного університету

Чанишев Р.І. – кандидат юридичних наук, доцент, доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія»

Чемерис О.А. – доктор технічних наук, старший науковий співробітник, заступник директора з наукової роботи Інституту проблем моделювання в енергетиці імені Г.Є. Пухова Національної академії наук України

Шаров С.В. – кандидат педагогічних наук, доцент, доцент кафедри комп'ютерних наук Таврійського державного агротехнологічного університету імені Дмитра Моторного

Шарова Т.М. – кандидат філологічних наук, доцент, доцент кафедри української і зарубіжної літератури Мелітопольського державного педагогічного університету імені Богдана Хмельницького

Шкарупило В.В. – кандидат технічних наук, доцент, докторант Інституту проблем моделювання в енергетиці імені Г.Є. Пухова Національної академії наук України

Янковський О.Г. – кандидат технічних наук, доцент, доцент кафедри інформаційних технологій Національного університету «Одеська юридична академія»

НОТАТКИ

Науковий журнал

**ВЧЕНІ ЗАПИСКИ
ТАВРІЙСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
ІМЕНІ В.І. ВЕРНАДСЬКОГО**

Серія: Технічні науки

Том 32 (71) № 1 2021

Частина 1

Коректура • *Н. Пирог*

Комп'ютерна верстка • *Н. Кузнєцова*

Адреса редакції:

Таврійський національний університет імені В.І. Вернадського

м. Київ, вул. Джона Маккейна, 33

Електронна пошта: editor@tech.vernadskyjournals.in.ua

Сторінка журналу: www.tech.vernadskyjournals.in.ua

Формат 60×84/8. Гарнітура Times New Roman.

Папір офсетний. Цифровий друк. Обл.-вид. арк. 15,20. Ум. друк. арк. 21,16. Зам. № 0321/81

Підписано до друку 04.02.2021. Наклад 150 прим.

Видавництво і друкарня – Видавничий дім «Гельветика»

03150, м. Київ, вул. Велика Васильківська 74, оф. 7

Телефон +38 (048) 709 38 69,

+38 (095) 934 48 28, +38 (097) 723 06 08

E-mail: mailbox@helvetica.com.ua

Свідоцтво суб'єкта видавничої справи

ДК № 6424 від 04.10.2018 р.