МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КОМІТЕТ ВЕРХОВНОЇ РАДИ УКРАЇНИ З ПИТАНЬ СОЦІАЛЬНОЇ ПОЛІТИКИ
ТА ЗАХИСТУ ПРАВ ВЕТЕРАНІВ
ЦЕНТР АДАПТАЦІЇ ДЕРЖАВНОЇ СЛУЖБИ ДО СТАНДАРТІВ
ЄВРОПЕЙСЬКОГО СОЮЗУ

ЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ІВАНА ФРАНКА
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЧЕРНІГІВСЬКА ПОЛІТЕХНІКА»
ІВАНО-ФРАНКІВСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
НАФТИ І ГАЗУ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
МІЖНАРОДНИЙ ЄВРОПЕЙСЬКИЙ УНІВЕРСИТЕТ

за підтримки
ЛЬВІВСЬКОЇ ОБЛАСНОЇ ВІЙСЬКОВОЇ АДМІНІСТРАЦІЇ
ЧЕРНІГІВСЬКОЇ ОБЛАСНОЇ ВІЙСЬКОВОЇ АДМІНІСТРАЦІЇ
ІВАНО-ФРАНКІВСЬКОЇ ОБЛАСНОЇ ВІЙСЬКОВОЇ АДМІНІСТРАЦІЇ
ЛЬВІВСЬКОЇ МІСЬКОЇ РАДИ
ЦЕНТРУ ДОСКОНАЛОСТІ ІМЕНІ ЖАНА МОНЕ ЛНУ ІМЕНІ ІВАНА ФРАНКА
«ЗАХІДНОУКРАЇНСЬКИЙ ДОСЛІДНИЦЬКИЙ ЦЕНТР З ЄВРОПЕЙСЬКИХ СТУДІЙ»

за участі
DTI UNIVERSITY, DUBNICA NAD VAHOM **(SLOVAKIA)**
TECHNICAL UNIVERSITY OF KOŠICE **(SLOVAKIA)**
VARNA FREE UNIVERSITY «CHERNORIZETS HRABAR» **(BULGARIA)**
IVAN PAUL II CATHOLIC UNIVERSITY OF LUBLIN **(POLAND)**
BATUMI NAVIGATION TEACHING UNIVERSITY – RESEARCH CENTER **(GEORGIA)**
SOKHUMI STATE UNIVERSITY **(GEORGIA)**

ЗБІРНИК ТЕЗ
IV МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
«СУЧАСНА ПАРАДИГМА ПУБЛІЧНОГО УПРАВЛІННЯ»

10-12 листопада 2022р.

Друкується згідно з рішенням оргкомітету за рекомендацією Вченої ради факультету управління фінансами та бізнесу Львівського національного університету імені Івана Франка (Протокол №5 від «30» листопада 2022 року).

Сучасна парадигма публічного управління : Збірник тез IV Міжнародної науково-практичної конференції (10-12 листопада 2022р.) / За наук. ред. к.е.н., доцента Стасишина А.В. – Львів : ЛНУ імені Івана Франка, – Львів, 2022. – 988 с.

До збірника увійшли матеріали Четвертої міжнародної науково-практичної конференції «Сучасна парадигма публічного управління», присвяченої актуальним проблемам теорії та практики публічного управління і адміністрування, питанням підвищення якості наукових досліджень та векторам поєднання зусиль вищих закладів освіти, наукових установ, органів влади та місцевого самоврядування, бізнес-структур та громадськості щодо пошуку спільних ефективних підходів до вирішення актуальних проблем забезпечення національної і міжнародної безпеки; досягнення ефективності інституційної та функціональної взаємодії в системі публічного управління в умовах невизначеності, глобальних викликів, ризиків та криз.
Рекомендовано викладачам, аспірантам, здобувачам першого та другого рівнів освіти.

Відповідальність за інформацію, викладену в публікаціях, несуть автори.

Reprinted in accordance with the decision of the organizing Committee on the recommendation of the Academic Council of the faculty of financial management and business.

The modern paradigm of public administration : Thesis of the IV Intern. scientif.-pract. conf. (November 10-12, 2022) / for the Sciences. edited by Ph.D. in Economics, associate Professor Andrii Stasyshyn – Lviv : IFNUL, 2022. – 988 P.

Recommended to teachers, baghelor-, muster- and postgraduate-students

In the book of thessis includes materials of The 4th international scientific-practical conference "The Modern paradigm of Public administration".

Політика ЄС щодо України: сучасні виклики та реалії

EU policy towards Ukraine: modern challenges and realities

Список використаних джерел
1. Бакуменко В. Д., Кравченко С. О. Методологія системних досліджень в державному управлінні: навч. посіб. Київ: ВПЦ АМУ, 2011. 116 с.
2. Бутник О.О., Немирівська О.Я. Особливості публічного управління в умовах світової пандемії. *Право та державне управління*. 2020. № 2. С. 142.
3. Васильєв О. С. Концептуалізація поняття «державна політика»: сучасне розуміння. Державне будівництво. 2014. № 1. URL: http://nbuv.gov.ua/UJRN/DeBu_2014_1_7 (дата звернення: 11.10.2022).
4. Дєгтяр О.А. Державне регулювання розвитку соціальної сфери: концептуальні засади та практика: монографія. Харків: С.А.М., 2014. 508 с.

Солдатенко А.О., здобувачка вищої освіти,
Науковий керівник: д.держ.упр., доцент **Антонова О.Р.,**
Льотна академія Національного авіаційного університету,
Україна

КІБЕРБЕЗПЕКА У СФЕРІ ПОВІТРЯНОГО ТРАНСПОРТУ: ПРОБЛЕМИ І НАПРЯМИ УДОСКОНАЛЕННЯ

Незважаючи на те, що правова основа у сфері національної безпеки України урегульована на міжнародному і конституційному рівнях та гарантована спеціальним Законом України «Про національну безпеку України» (стаття 2) [1], непоодинокими є випадки порушення основоположних принципів цих нормативно-правових актів.

Вперше Україна зазнала кібератаки на комп'ютерні системи та центральний сервер аеропортів «Бориспіль» і «Харків» у червні 2017 року, що призвело до відмови в обслуговуванні літаків і затримок рейсів. Через кілька місяців, у жовтні 2017 року, вильоти рейсів з аеропорту Одеса були затримані через злом комп'ютерної мережі аеропорту, що призвело до втрати конфіденційності інформації [2; с. 26].

Інциденти кібератак в аеропортах світу також мають місце, зокрема:

2006 рік – Інтернет-атака на центри контролю повітряного руху США;

2008 рік – зараження бортового комп'ютера рейса Spanair 5022 шкідливим програмним забезпеченням, що призвело до катастрофи;

2009 рік – втручання в систему GPSСША, що використовується для заходу на посадку повітряного судна (далі – ПС);

2013 рік – втручання в інформаційну систему аеропортів Туреччинпи, що призвело до призупинення паспортного контролю;

2013 рік – втручання в комп'ютерні мережі 75 аеропортів США;

2014 рік – втрата керування ПС при дистанційному підключенні до автопілоту та зникнення ПС рейсу MH370 Малазійских авіаліній з радарів(одна з ключових версій катастрофи);

2014 рік – масштабні атаки на комп'ютерні авіаційні системи Пакистану, Саудовскої Аравії, Південної Кореї та США;

2015 рік. – поширення шкідливого програмного забезпечення в комп'ютерні системи аеропорту США, що призвело до призупинення польотів;

2015 рік. – несанкціоноване втручання в комп'ютерну системи аеропорту Польської авіакомпанії LOT, що призвело до збоїв при обслуговуванні ПС та втраті конфіденційної інформації;

2016 рік – проникнення до комп'ютерної системи та зараження комп'ютерів аеропорту Талліну шкідливим програмним забезпеченням, що призвело до втрати конфіденційної інформації;

2017 рік – втручання в комп'ютерну систему внутрішніх авіаліній США, що призвело до вимушеної посадки ПС та збоїв в роботі Авіаційної бортової системи адресації і передачі повідомлень (ACARS);

2018 рік. – збої в комп'ютерній системі організації Eurocontrol, що призвело до порушення цілісності системи обміні даних та затримки більш 15000 рейсів в Європі. [3, с.28]

До тепер складають загрозу робота автоматизованих функціональних систем і комплексів електроніки, точки доступу через

Інтернет (за допомогою постачальника програмного забезпечення до свого оператора або постачальника) і точки, де програмована інформація передається від оператора (диспетчерський центр аеропорту вздовж маршруту спостереження).

Також, під час розповсюдження програмного забезпечення для авіоніки FS літака небезпека полягає у підробці та пошкоджені критичного програмного забезпечення, призначеного для оновлення програмного забезпечення літака. Під терміном «маніпулювання та пошкодження критичного програмного забезпечення» слід розуміти навмисне несанкціоноване використання оригінального програмного забезпечення або впровадження підробленого програмного забезпечення [4, с. 272].

Проблема полягає у складності вчасного виявлення втручання в програмне забезпечення, фальсифікації адміністративних повідомлень операційної системи (далі – ОС) (тобто команд завантаження, запитів і відповідних відповідей) . Цей тип програмної атаки може призвести, для прикладу, до загальної відмови в обслуговуванні та спричинити необґрунтовані затримки рейсів літаків і поставити під загрозу авіаційну безпеку в цілому [5, с.39-41].

Важливе значення для регламентації міжнародного співробітництва держав-членів ІКАО у вирішенні проблем кібербезпеки цивільної авіації має резолюція А39-19, прийнята у 2016 році в ході 39-ї сесії Асамблеї ІКАО. У цьому документі закріплено основні напрями протидії кіберзагрозам, серед яких такі: визначення кола обов'язків національних органів з боротьби з кіберзагрозами; заохочення координації дій між державами-членами; визначення юридичних наслідків дій, які ставлять під загрозу безпеку польотів повітряних суден, шляхом використання кібервразливих місць; сприяння розробці та втіленню міжнародних стандартів, стратегій та передової практики у сфері захисту застосовуваних для цілей цивільної авіації критично важливих систем інформації та зв'язку від актів втручання, які можуть загрожувати безпеці польотів цивільної авіації [6, с. 99].

У резолюції А40-11 Асамблеї ІКАО передбачено додаткові кроки із забезпечення кібербезпеки цивільної авіації, зокрема:

- враховувати потенційне використання не за призначенням дистанційно пілотованих авіаційних систем і застосовувати відповідні заходи безпеки з метою запобігання їх використання в актах незаконного втручання;

- розширити використання механізмів обміну інформацією, зокрема застосування системи попередньої інформації про пасажирів (API) і даних записів реєстрації пасажира (PNR), які надаються авіакомпаніями для підвищення рівня авіаційної безпеки й скорочення ризику для пасажирів, за одночасного забезпечення недоторканності приватного життя і громадянських свобод [7, с. 61].

Враховуючи актуальність зазначених вище напрямів, відповідним державним і приватним структурам необхідно застосовувати і удосконалювати загальні (універсальні)рекомендації щодо захисту інформації та інформаційних систем під час впровадження міжсистемного обміну інформацією в усіх сегментах авіаційної сфери [8]. При цьому варто синергувати зусилля ООН, держав-членів ІКАО, у тому числі Україна, та інших міжнародних авіаційних організацій для розробки універсальних стандартів, які б забезпечили ефективну боротьбу з кіберзагрозами у сфері повітряного транспорту.

Список використаних джерел

1. Про національну безпеку України: Закон України від 15.06.2022 р. № 2469-VIII. Ст. 2. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення : 19.10.2022).

2. Ільєнко С., Ільєнко А., Кваша С. Сучасний стан забезпечення кібернетичної безпеки цивільної авіації України та світу. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2020. – С. 24-36. URL: https://doi.org/10.28925/2663-4023.2020.9.2436 (дата звернення : 19.10.2022).

3. Лісовська Ю.П. Кібербезпека: ризики та заходи: навч. посібник. — К.: Видавничий дім «Кондор», 2019. — 272 с. URL: http://dcmaup.com.ua/assets/files/kiberbezpeka.pdf (дата звернення : 19.10.2022).

4. Антонова О. Р. Органи прокуратури та судової влади у реалізації механізму конституційно-правового регулювання шлюбу і сім'ї. Журнал східноєвропейського права. Київ. 2018. № 51. С. 59–66.
5. Григоров О. М. Міжнародно-правові стандарти кібербезпеки цивільної авіації / О. М. Григоров // Актуальні проблеми держави і права : зб. наук. пр. Вип. 91 / редкол.: Г. І. Чанишева (голов. ред.) та ін. – Одеса : Гельветика, 2021. – С. 38-43. URL:http://dspace.onua.edu.ua/handle/ (дата звернення : 19.10.2022).
6. Решение проблем кибербезопасности в гражданской авиации. Резолюции Ассамблеи. АССАМБЛЕЯ – 39-я СЕССИЯ, г. Монреаль, 27 сентября – 6 октября 2016 г. A 39/19. С. 99–101. ICAO .URL: https://www.icao.int/Meetings/a39/Documents/Resolutions/ (дата звернення : 19.10.2022).
7. Сводное заявление о постоянной политике ИКАО в области авиационной безопасности. Резолюции Ассамблеи. Ассамблея – 40я сессия, г. Монреаль, 24 сентября – 4 октября 2019 г. A40-11.С.53–69.ICAO.URL:https://www.icao.int/Meetings/a40/Documents/ (дата звернення : 19.10.2022).
8. Антонова О. Р. Роль держави у забезпеченні безпеки та захисту прав людини і громадянина в умовах воєнного стану. Державна Служба України: сучасні виклики та перспективи повоєнної трансформації: зб. тез щоріч. міжнар. круглого столу (Київ, 17 черв. 2022 р.), Київ. 2022, с. 109-111.

Співак С.Є., здобувач вищої освіти,
Науковий керівник: д.держ.упр., доцент **Антонова О.Р.,**
Льотна академія Національного авіаційного університету,
Україна

КІБЕРБЕЗПЕКА УКРАЇНИ: БЕЗПЕЧНИЙ КІБЕРПРОСТІР АВІАЦІЙНОЇ ГАЛУЗІ

У 2016-2017 році Україна вперше пережила потужні кібератаки, коли на деякий час була заблокована робота об'єктів критичної транспортної інфраструктури та багатьох інших