МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Кафедра прикладної механіки та інженерії матеріалів

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
д.т.н., професор
_____ Оксана МІКОСЯНЧИК
“21” грудня 2023 р.

Кваліфікаційна робота

ВИПУСКНИКА ОСВІТНЬО-КВАЛІФІКАЦІЙНОГО СТУПЕНЯ “МАГІСТР”

Тема: **Система управління інформаційною безпекою в IT компанії**

Виконавець: Богдан МАМАЙ

Керівник: д.т.н., професор Володимир МЕЛЬНИК

Нормоконтролер: Оксана МІКОСЯНЧИК

КИЇВ 2023

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
Аерокосмічний факультет

Кафедра прикладної механіки та інженерії матеріалів

Спеціальність 152. «Метрологія та інформаційно-вимірювальна техніка»
Освітньо-професійна програма «Якість, стандартизація та сертифікація»

ЗАТВЕРДЖУЮ
Завідувач кафедри
д.т.н., професор
_____Оксана МІКОСЯНЧИК
“05” жовтня 2023 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

Богдан МАМАЙ

1. Тема кваліфікаційної роботи «Система управління інформаційною безпекою в ІТ компанії» затверджена **наказом ректора № 2035/ст від 05.10.2023року**
2. Термін виконання роботи: **з 02 жовтня по 31 грудня 2023року**
3. Вихідні дані до роботи: Стандарт 27001:2015, Шкала оцінювання якості аеропортового обслуговування, Показники якості аеропортових послуг для основних авіаперевізників, ваговий коефіцієнт.
4. Зміст пояснювальної записки: Вступ. Розділ 1. Стандарт 27001:2015. Розділ 2. Застосування Стандарту 27001:2015. Розділ 3. Впровадження 27001:2015 в ІТ компанії. Розділ 4. ДСТУ ISO/IEC 14598.

5. Перелік обов'язкового графічного (ілюстративного) матеріалу:
1.Основні розділи стандарту ISO/IEC 27001, 2. Факти про стандарт ISO/IEC 27001, 3. Кроки для застосування стандарту ISO 27001:2015, 4. Впровадження 27001:2015.

6. Календарний план-графік

№ п/п	Завдання	Термін виконання	Відмітка про виконання
1.	Ознайомитися з літературою та сформувати структуру кваліфікаційної роботи.	02.10-09.10 2023	
2.	Написати вступ	10.10-19.10. 2023	
3.	Розробити розділ 1:	20.10-12.11 2023	
4.	Розробити розділ 2:	13.11-23.11 2023	
5.	Розробити розділ 3:	24.11-08.12 2023	
6.	Розробити розділ 4:	09.12-15.12 2023	
7.	Сформулювати висновки по роботі.	16.12-19.12 2023	
8.	Оформити кваліфікаційну роботу та здати на рецензію.	20.12-21.12. 2023	

7. Консультанти з окремих розділів

Розділ	Консультант (посада, П.І.Б.)	Дата, підпис	
		Завдання видав	Завдання прийняв
Охорона навколишнього середовища	Доцент Володимир МЕЛЬНИК	02.10.2023 Володимир МЕЛЬНИК	18.11.2023 Володимир МЕЛЬНИК

Керівник кваліфікаційної роботи _____ (підпис керівника) Володимир Мельник (П.І.Б.)

Завдання прийняв до виконання _____ (підпис випускника) Богдан Мамай (П.І.Б.)

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи «Система управління інформаційною безпекою в ІТ компанії»: сторінок 82, рисунків 4, таблиць 9, використаних джерел 12.

ІНФОРМАЦІЙНА БЕЗПЕКА, ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Об'єкт дослідження - Системи управління інформаційною безпекою (СУІБ) в ІТ компаніях.

Предмет дослідження - Процеси, політики, та методології, які застосовуються в рамках СУІБ, з особливим акцентом на стандарт ISO/IEC 27001:2015 та його практичне впровадження в ІТ компаніях.

Мета дослідження – Аналіз та розробка оптимізованих стратегій для управління інформаційною безпекою в ІТ компаніях, забезпечення відповідності сучасним стандартам безпеки та виявлення можливостей для підвищення ефективності впроваджених систем. Розробка програми з інтерфейсом для розрахунку рівня якості послуг аеропортового комплексу з однаковим ваговим коефіцієнтом.

Методи дослідження – Комбінація якісного та кількісного аналізу, включаючи вивчення нормативних документів та аналіз кращих практик у галузі.

РЕФЕРАТ

Explanatory Note to the Qualification Work "Information Security Management System in IT Companies": 79 pages, 4 figures, 9 tables, 12 sources used.

INFORMATION SECURITY, INFORMATION TECHNOLOGY

Object of Research - Information Security Management Systems (ISMS) in IT companies.

Subject of Research - Processes, policies, and methodologies applied within the ISMS, with a special emphasis on the ISO/IEC 27001:2015 standard and its practical implementation in IT companies.

Purpose of the Research – Analysis and development of optimized strategies for managing information security in IT companies, ensuring compliance with modern security standards, and identifying opportunities for improving the efficiency of implemented systems. Development of a program with an interface for calculating the quality level of airport complex services with an equal weighting factor.

Research Methods – Combination of qualitative and quantitative analysis, including the study of normative documents and analysis of best practices in the field.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ, ТЕРМІНІВ

СУІБ – Система управління інформаційною безпекою

ISO – International Organization for Standardization (міжнародна організація, метою діяльності якої є ратифікація стандартів, розроблених спільними зусиллями делегатів від різних країн)

IEC – International Electrotechnical Commission (Міжнародна електротехнічна комісія)

SWOT – Аналіз широко застосовується у процесі стратегічного планування

ДСТУ – Державний Стандарт України

CEN – Європейський комітет зі стандартизації

ВСТУП

Інформаційні технології в сучасному світі пронизують усі аспекти життя, перетворюючи наш спосіб працювати, спілкуватися та жити. В індустрії інформаційних технологій (IT) відбуваються постійні зміни та розвиток, а це створює неабияку потребу в ефективному управлінні інформаційною безпекою. Інформація стала однією з найцінніших активів підприємств, і її втрата або пошкодження може призвести до серйозних наслідків, включаючи фінансові втрати, порушення конфіденційності та репутаційні ризики. В цьому контексті системи управління інформаційною безпекою набули важливості і стали необхідним компонентом успішної діяльності IT компаній.

Згідно з міжнародними стандартами і нормами, ISO/IEC 27001:2015 визнана як провідний стандарт для систем управління інформаційною безпекою. Цей стандарт надає систематичний підхід до управління ризиками і забезпечення інформаційної безпеки в організаціях. Впровадження стандарту ISO/IEC 27001:2015 стає необхідним для багатьох IT компаній з метою дотримання міжнародних вимог та забезпечення найвищого рівня інформаційної безпеки.

Дослідження систем управління інформаційною безпекою стає актуальним завдяки необхідності адаптації до зростаючих загроз і викликів у цій галузі. IT компанії стикаються з різноманітними загрозами, включаючи кібератаки, витік інформації, внутрішні порушення безпеки і недостатню свідомість співробітників щодо інформаційної безпеки. Створення та ефективне управління системами інформаційної безпеки стає завданням критичної важливості для забезпечення довіри клієнтів, дотримання регуляторних вимог і забезпечення стійкості бізнесу.

Мета даної кваліфікаційної роботи на магістратурі полягає у глибокому

розгляді та аналізі систем управління інформаційною безпекою в IT компаніях, вивченні їх структури, компонентів, методів та рішень, які використовуються для забезпечення інформаційної безпеки. Основною метою є розробка рекомендацій та стратегій для оптимізації системи управління інформаційною безпекою в IT компанії з метою забезпечення її високого рівня захисту та відповідності сучасним стандартам безпеки.

Дослідження передбачає аналіз нормативних вимог, прикладів кращої практики в галузі інформаційної безпеки, технічних засобів та організаційних методів захисту інформації. Впровадження рекомендацій, розроблених в результаті цього дослідження та допоможе IT компаніям ефективніше впоратися з загрозами щоб ті збільшили свою конкурентоспроможність в глобальному IT ринку.

Об'єкт дослідження – **-** Системи управління інформаційною безпекою (СУІБ) в IT компаніях.

Предмет дослідження – Процеси, політики, та методології, які застосовуються в рамках СУІБ, з особливим акцентом на стандарт ISO/IEC 27001:2015 та його практичне впровадження в IT компаніях.

Методи, застосовані в дипломній роботі: Комбінація якісного та кількісного аналізу, включаючи вивчення нормативних документів та аналіз кращих практик у галузі.

Наукова новизна отриманих результатів полягає в: Розробка програмного забезпечення для оцінювання рівня якості послуг аеропортового комплексу.

Практична цінність отриманих результатів полягає в оцінюванні якості послуг аеропортових комплексів за топомогою програмного забезпечення, замінивши дані в програмі можно з легкістю отримати оцінку якості послуг для будь-якого аеропорту. Написану програму можно використовувати не тільки в сфері близькій до аеропортів, але і для порівняння якості мастил, або ж для порівняння якості університетів і тд.

РОЗДІЛ 1

Стандарт 27001:2015

Частина 1.1. Дослідження Стандарту 27001:2015

ISO 27001:2015 є міжнародним стандартом з управління інформаційною безпекою, який містить в собі вимоги до систем управління інформаційною безпекою (СУІБ). Цей стандарт встановлює мінімальні вимоги до СУІБ для захисту конфіденційної, цілісної та доступної інформації в організації.

Застосування стандарту ISO 27001:2015 може допомогти організації зменшити ризики втрати, недоступності або викривлення інформації, забезпечити відповідність вимогам регулюючих органів та покращити довіру клієнтів. Для цього організація повинна реалізувати СУІБ згідно з вимогами стандарту та пройти сертифікацію з управління інформаційною безпекою.

Застосування ISO 27001:2015 може бути корисним для будь-якої організації, яка має важливу інформацію, що потребує захисту, такої як: фінансова інформація, персональні дані, конфіденційна інформація про бізнес-процеси та інші важливі документи. Це може бути вкрай корисним для організацій, що операціонують в регульованих секторах, таких як фінансовий або медичний сектори, там де вимоги до захисту інформації дуже високі.

Розробка стандарту була ініційована відомим британським стандартизаційним органом BSI (British Standards Institution) у 1995 році.

Перші роботи над стандартом розпочалися в 1996 році. Стандарт був заснований на британському стандарті BS 7799-1, який був розроблений для застосування в організаціях у Великобританії. BS 7799-1 включав рекомендації з управління інформаційною безпекою і застосування інформаційних технологій для досягнення цілей безпеки. Перша версія BS 7799-1 була опублікована в 1995 році.

У 1998 році була розроблена друга частина BS 7799, яка містить основні вимоги до системи управління інформаційною безпекою. Ця частина

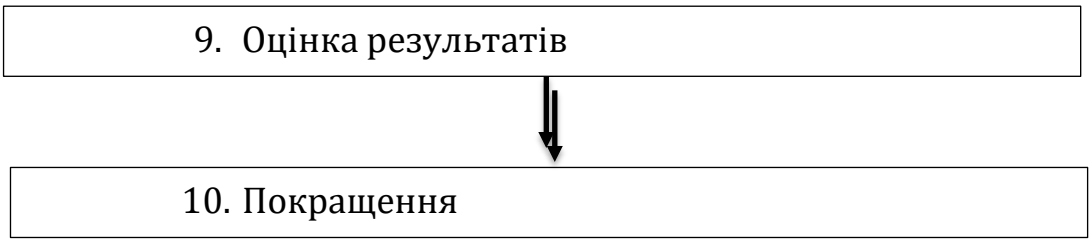
була опублікована під назвою BS 7799-2:1998.

У 2000 році була опублікована нова версія BS 7799-2:2000, яка містить значні зміни порівняно з попередньою версією. Ця версія стала основним підґрунтям для розробки міжнародного стандарту ISO 27001.

У 2005 році був опублікований перший міжнародний стандарт ISO/IEC 27001:2005, який був заснований на BS 7799-2:2000. Пізніше був опублікований новий стандарт ISO/IEC 27001:2015, який замінив попередню версію стандарту. Стандарт ISO 27001 продовжує розвиватися та оновлюватися з метою врахування сучасних технологічних та організаційних викликів.

Стандарт ISO/IEC 27001 містить вимоги до системи управління інформаційною безпекою (СУІБ). Основні розділи стандарту включають:

Таблиця 1



Кожен з цих розділів містить рекомендації та вимоги щодо різних аспектів управління інформаційною безпекою в організації.

Розділ 1 "Предмет та поле застосування стандарту" - у цьому розділі стандарту ISO/IEC 27001:2015 наведено основну інформацію про мету та застосування стандарту, також вказано, що стандарт містить вимоги до системи управління інформаційною безпекою.

Розділ 2 "Нормативні посилання" - у цьому розділі стандарту наведено перелік усіх інших стандартів та документів, до яких можна застосовувати ISO/IEC 27001:2015.

Розділ 3 "Терміни та визначення" - цей розділ стандарту визначає терміни і поняття, які використовуються в ISO/IEC 27001:2015, щоб забезпечити уніфіковане розуміння цих термінів в контексті стандарту. Визначення термінів може бути важливим для розуміння вимог і рекомендацій, що містяться в інших розділах стандарту.

В цілому, перші три розділи стандарту ISO/IEC 27001:2015 надають загальну інформацію про стандарт, вказують на його застосування та нормативні посилання, а також визначають терміни, які використовуються в документі. Однак, більш детальний опис вимог та рекомендацій щодо системи управління інформаційною безпекою містяться в наступних розділах стандарту.

Розділ 4 "Контекст організації" – цей розділ описує, як організація має здійснювати контекстний аналіз для визначення контексту своєї діяльності та ризиків, пов'язаних з інформаційною безпекою.

Розділ 5 "Лідерство" - розділ містить вимоги до керівництва організації з

управління інформаційною безпекою, зокрема щодо забезпечення ресурсів, встановлення політики інформаційної безпеки та залучення персоналу.

Розділ 6 "Планування" – розділ містить вимоги щодо розробки СУІБ, включаючи визначення цілей інформаційної безпеки, ідентифікацію основних ризиків та встановлення контролів безпеки.

Розділ 7 "Підтримка" – даний розділ містить вимоги до забезпечення ресурсів для реалізації СУІБ, зокрема щодо навчання персоналу, управління документацією та управління забезпеченням.

Розділ 8 "Операційна діяльність" – у цьому розділі стандарту ISO/IEC 27001:2015 наведено загальні вимоги щодо забезпечення відповідного захисту інформації та інфраструктури під час її операційної діяльності. Вимоги цього розділу включають в себе контроль доступу до інформації компанії та її інфраструктури, також захист інформації в режимі реального часу, моніторинг та аналіз входів і виходів інформації, розробку та імплементацію усіх процедур для забезпечення відповідного захисту, та документування і зберігання інформації.

Розділ 9 "Оцінка результатів" – у цьому розділі стандарту наведено загальні вимоги щодо процесу оцінки результатів з метою переконатися, що система управління інформаційною безпекою відповідає встановленим вимогам і є ефективною. Вимоги цього розділу включають в себе такі пункти: оцінку ефективності заходів для забезпечення інформаційної безпеки, визначення коригуючих та запобіжних заходів, документування і зберігання інформації, а також процес постійного покращення інформаційної безпеки.

Розділ 10 "Покращення" – у цьому розділі стандарту наведено основні вимоги щодо процесу постійного покращення системи управління інформаційною безпекою. Вимоги цього розділу включають в себе такі процеси: встановлення процесу постійного покращення, визначення потрібних метрик і індикаторів, які дозволяють оцінювати ефективність системи управління інформаційною безпекою, та визначення коригуючих та запобіжних заходів з метою поліпшення системи управління інформаційною

безпекою

Окремо можна виділити такі елементи Стандарту ISO 27001:2015:

1. Вступ - визначає мету стандарту, область застосування, терміни та визначення.
2. Роз'яснювальні матеріали - надають загальну інформацію про стандарт, його розуміння та застосування.
3. Система управління інформаційною безпекою (СУІБ) - це центральний елемент стандарту, який включає в себе політику, процедури та контрольні механізми, необхідні для забезпечення інформаційної безпеки.
4. Планування - включає процеси планування СУІБ, оцінки ризиків та визначення контролів.
5. Підтримка - включає процеси надання ресурсів, навчання та свідчення про виконання вимог СУІБ.
6. Операційна діяльність - включає процеси забезпечення безпеки при обробці інформації та керування доступом до неї.
7. Оцінка результатів - включає процеси вимірювання, моніторингу, оцінки та аналізу ефективності СУІБ.
8. Покращення - включає процеси для забезпечення постійного вдосконалення СУІБ на основі результатів оцінки та аналізу.
9. Завершальні положення - включають інформацію про оцінку відповідності, сертифікацію, перегляд та оновлення стандарту.

Ці елементи узгоджені та інтегровані, щоб забезпечити комплексний підхід до управління інформаційною безпекою, також забезпечити стандартизацію процесів та процедур в цій області, і для зниження ризиків порушення конфіденційності, цілісності та доступності інформації.

Цікаві факти про стандарт ISO/IEC 27001:

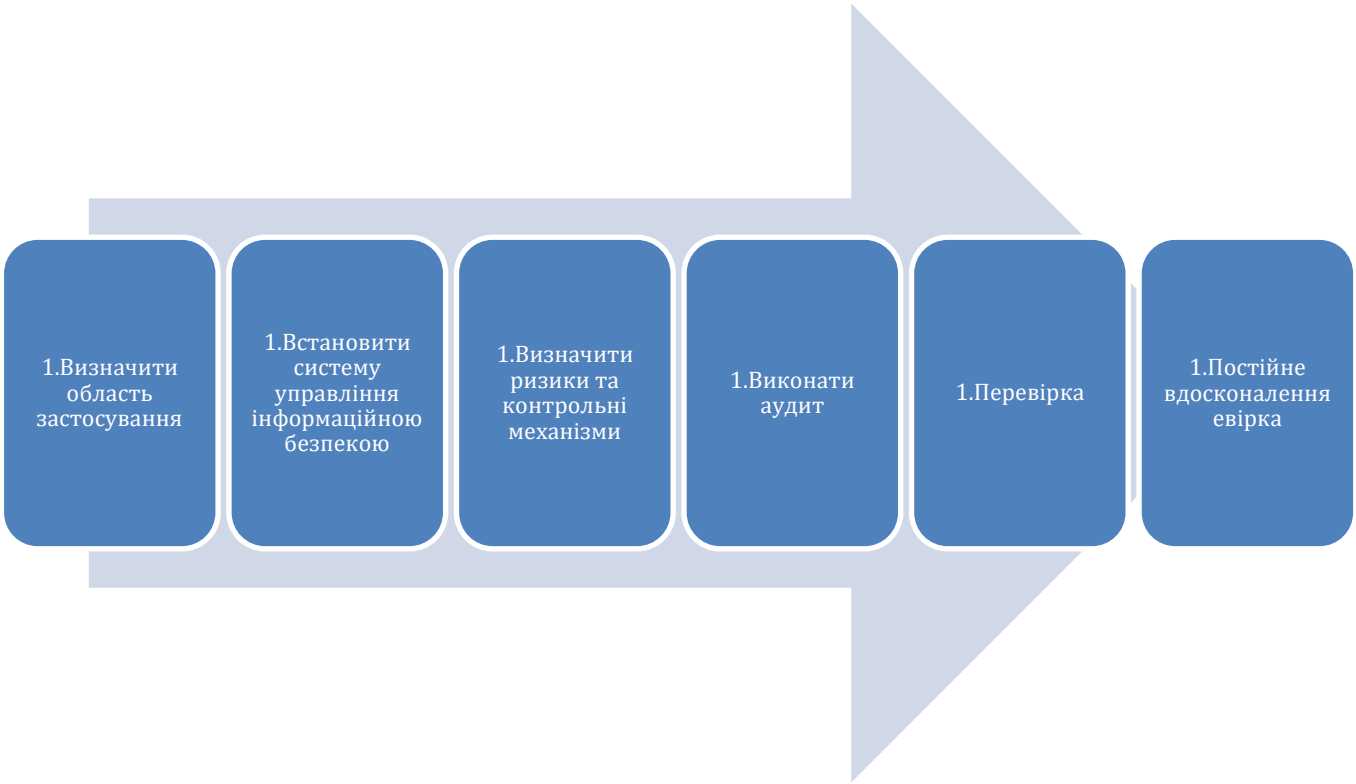
Таблиця 2

•За даними стандартизаційної організації ISO, ISO/IEC 27001 є другим за популярністю стандартом серії ISO, після стандарту ISO 9001 (стандарту управління якістю).	•У 2020 році було зареєстровано понад 44 000 сертифікованих компаній з усього світу, що використовують стандарт ISO/IEC 27001 для забезпечення захисту своєї інформації.Використання стандарту ISO/IEC 27001 є обов'язковим для підприємств та організацій, що отримують контракти з урядовими органами США, військовими установами та іншими організаціями, що працюють зі секретною інформацією.
•Використання стандарту ISO/IEC 27001 може забезпечити значні економічні вигоди, такі як зменшення ризиків, підвищення ефективності, зниження витрат на захист інформації та поліпшення репутації компанії.	•Стандарт ISO/IEC 27001 не обмежується використанням в інформаційних технологіях і може бути застосований в будь-якій сфері діяльності, де необхідно забезпечити захист інформації.

Частина 1.2. Застосування Стандарту 27001:2015

Для застосування стандарту ISO 27001:2015 необхідно виконати такі кроки:

Рисунок 1



1. Визначення області застосування є важливим етапом в процесі впровадження стандарту ISO 27001:2015. Область застосування - це частина організації, яка включає інформаційні ресурси та основні процеси, які підлягають захисту.

При визначенні області застосування необхідно враховувати всі можливі шляхи, за якими інформація може бути вразлива ризикам безпеки. Наприклад, це може бути мережа підприємств, серверні приміщення великих компаній, склади з даними, бази даних, робочі станції, мобільні пристрої та інші ресурси, які містять конфіденційну інформацію.

Для визначення області застосування стандарту ISO 27001

рекомендовано виконати наступні кроки:

- Встановити межі організації: визначити, які просторові, організаційні і технічні межі обмежують діяльність конкретної організації.
- Визначити активи: перелічити всі активи організації, які є важливими для її основної діяльності. До активів можуть відноситись техніка, програмне забезпечення, документи, матеріальні ресурси та ін.
- Визначити загрози: проаналізувати потенційні загрози, які можуть впливати на активи організації. Це можуть бути загрози з боку зловмисників(наприклад: хакери), технічні проблеми, природні катастрофи тощо.
- Оцінити ризики: оцінити ймовірність та наслідки основних можливих загроз для активів організації та визначити рівень ризику кожної загрози окремо а потім сумарно якщо це необхідно.
- Визначити заходи зі зниження ризику: вирішити, які заходи необхідно вжити для зниження ризику до прийнятного рівня. Це можуть бути такі заходи: технічні заходи, організаційні заходи, політики та процедури тощо.
- Визначити відповідальних осіб: визначити, хто відповідає за кожен етап процесу застосування стандарту та контролює виконання заходів.
- Документувати процес: створити основний документ, який відображає область застосування стандарту, включаючи всі етапи процесу та відповідальних осіб за кожний процес.
- Ці кроки допоможуть визначити область застосування стандарту ISO 27001 та виконати інші вимоги стандарту.

2. Встановлення системи управління інформаційною безпекою (СУІБ) є

одним з ключових етапів впровадження стандарту ISO 27001. На цьому етапі потрібно створити процедури, інструкції і політики, та інші документи, необхідні для встановлення і підтримки СУІБ.

Для встановлення СУІБ рекомендується виконати наступні кроки:

- Визначити відповідальну особу або команду для керування СУІБ. Ця команда має бути компетентною в області інформаційної безпеки та мати достатні знання та ресурси для виконання своїх завдань.
- Визначити контекст СУІБ. Для цього потрібно визначити основні межі СУІБ та описати контекст, в якому вона функціонує, включаючи зовнішні і внутрішні фактори, що можуть впливати на її ефективність.
- Виконати інвентаризацію активів інформаційної системи та оцінити всі ризики. Це допоможе зрозуміти, які активи повинні бути захищені та які загрози їм загрожують.
- Розробити політики, процедури та інструкції з інформаційної безпеки. Ці документи мають охоплювати всі аспекти СУІБ, включаючи доступ та захист, зберігання та обробку інформації.
- Встановити систему моніторингу та оцінки СУІБ. Це допоможе переконатися, що СУІБ працює ефективно та забезпечує необхідний рівень захисту інформації організації.
- Навчити персонал з питань інформаційної безпеки який буде взмозі винонувати свої обов ' язки.

3. Один з ключових етапів для імплементації стандарту ISO 27001 - визначення ризиків і контрольних механізмів для їх управління. Цей етап включає такі кроки:

- Оцінка потенційних загроз і вразливостей: Команда повинна зібрати й проаналізувати всі можливі загрози та вразливості, які

можуть вплинути на безпеку інформації в організації. Для цього загалом можна використовувати різноманітні методики, наприклад: SWOT-аналіз, або проводити спеціальні аудити безпеки.

- Визначення ймовірності виникнення ризиків: команда повинна визначити ймовірність того, що кожна загроза може стати реальністю, і яку шкоду це може заподіяти організації в майбутньому. Це можна зробити використовуючи матрицю ймовірностей та впливу.
- Визначення контрольних механізмів: Після того, як були визначені ризики та їх ймовірність, організації необхідно встановити контрольні механізми для їх управління. Контрольні механізми можуть бути різних типів, таких як: технічні (наприклад, захист від вірусів або резервне копіювання даних), організаційні (наприклад, процедури безпеки, ідентифікація та аутентифікація користувачів, обмеження доступу) та фізичні (наприклад, обмеження фізичного доступу до серверних кімнат).
- Визначення рівня прийняття ризику: Організація повинна визначити свій рівень прийняття ризику і встановити, які ризики вона готова приймати, а які - ні.

4. В контексті стандарту ISO/IEC 27001:2015, аудит є одним з найважливіших етапів в процесі впровадження та підтримки системи управління інформаційною безпекою (СУІБ). Аудит передбачає проведення незалежного перегляду усієї діяльності організації, щоб забезпечити відповідність вимогам стандарту.

Виконання аудиту СУІБ може бути внутрішнім та зовнішнім. Внутрішній аудит проводиться організацією самостійно або за допомогою зовнішніх консультантів. Зовнішній аудит проводиться незалежною

організацією або ж сертифікаційним органом з метою визнання відповідності вимогам стандарту.

Аудит має на меті перевірити, чи відповідає СУІБ вимогам стандарту ISO/IEC 27001:2015, а також чи ефективно функціонує СУІБ. Під час аудиту проводяться різні перевірки всіх елементів СУІБ, щоб виявити недоліки та помилки або відхилення від вимог стандарту

Звіт про аудит має містити детальну інформацію про виявлені недоліки або відхилення від вимог стандарту, а також рекомендації щодо усунення цих недоліків та вдосконалення СУІБ в майбутньому.

Виконання аудиту є важливим етапом впровадження та підтримки СУІБ, оскільки дозволяє оцінити ефективність СУІБ та ідентифікувати області для подальшого вдосконалення.

5. Пункт "Перевірка відповідності" є одним з ключових етапів застосування стандарту ISO 27001 і має на меті перевірити відповідність реалізованої системи управління інформаційною безпекою вимогам стандарту.

Перевірка відповідності може бути здійснена як внутрішніми так і зовнішніми аудиторами. Внутрішній аудит зазвичай проводиться командою спеціалістів, яка не має безпосереднього відношення до розробки та реалізації системи управління інформаційною безпекою організації. Зовнішній аудит може бути здійснений незалежним сертифікаційним органом.

Перевірка відповідності включає в себе як оцінку ефективності системи управління інформаційною безпекою так і її відповідності вимогам стандарту ISO 27001. Під час оцінки ефективності можуть бути використані різноманітні методи, такі як перевірка документації, інтерв'ювання персоналу, спостереження за процесами та аналіз результатів аудитування.

На основі отриманих результатів перевірки відповідності можуть бути видані детальні рекомендації щодо подальшого вдосконалення системи управління інформаційною безпекою. Якщо система управління відповідає

вимогам стандарту, то може бути виданий сертифікат, який підтверджує відповідність організації стандарту ISO 27001.

Важливо зазначити, що перевірка відповідності повинна проводитись регулярно, щоб переконатися, що система управління інформаційною безпекою продовжує відповідати вимогам стандарту.

6. Пункт "Постійне вдосконалення" (або "Постійне покращення") є одним з ключових елементів системи управління інформаційною безпекою відповідно до стандарту ISO 27001:2015. Його головною метою є забезпечення постійного покращення ефективності системи управління інформаційною безпекою та її процесів.

Цей пункт містить наступні етапи:

Визначення потреб в покращенні: на даному етапі аналізуються результати виконання цілей та планів, які були встановлені на попередніх етапах, а також збираються дані щодо виявлених проблем, недоліків та можливих вдосконалень.

Визначення можливих покращень: на цьому етапі обговорюються усі можливі варіанти покращення системи управління інформаційною безпекою, які можуть бути реалізовані в організації. Оцінюють користь та ризики від їх застосування.

Вибір оптимального варіанту покращення: на цьому етапі вибирається найбільш ефективний варіант покращення, такий який враховує забезпечення інформаційної безпеки та відповідність до стратегії організації.

Реалізація покращення: на цьому етапі виконуються дії, які необхідні для реалізації вибраного варіанту покращення.

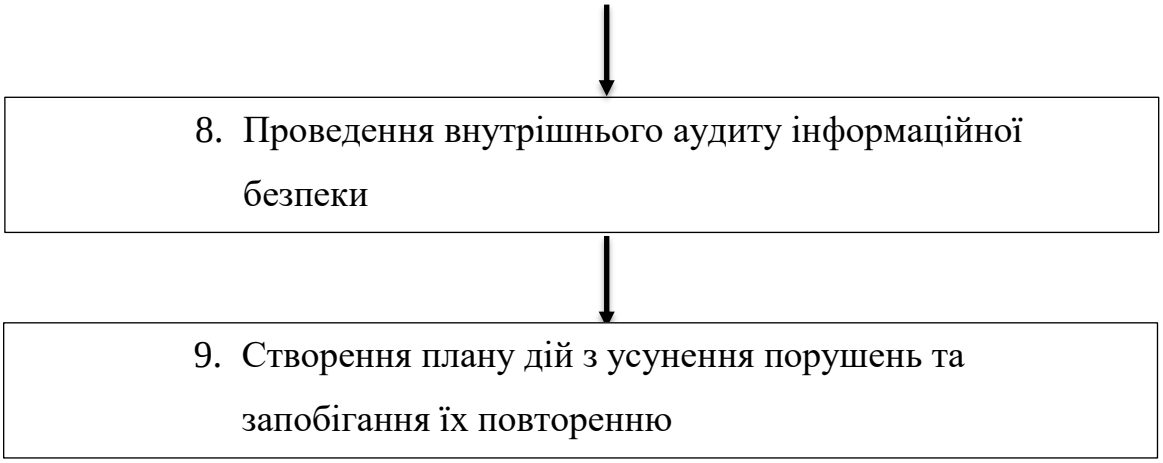
Оцінка ефективності покращеннь: на цьому етапі оцінюється ефективність реалізованих покращень, також визначаються потреби в додаткових змінах та вдосконаленнях.

Частина 1.3. Впровадження 27001:2015 в IT компанії

Для впровадження стандарту ISO 27001:2015 в IT компанії необхідно виконати наступні кроки:

Таблиця 3

1. Створення проектної групи
2. Оцінка потреб в інформаційній безпеці
3. Розроблення та затвердження політики інформаційної безпеки
4. Розроблення програми управління інформаційною безпекою
5. Виконання аудиту наявної інфраструктури та визначення необхідних заходів для відповідності вимогам
6. Розроблення та впровадження процедур забезпечення безпеки
7. Запровадження системи моніторингу та аналізу подій для виявлення порушень інформаційної безпеки



1. Створення проектної групи зі спеціалістів в галузі інформаційної безпеки, яка буде включати в себе керівника проекту, керівника процесу інформаційної безпеки, системного адміністратора, менеджера зі зв'язків з громадськістю, представника відділу юридичного супроводу, аналітика з оцінки ризиків та інших спеціалістів залежно від розміру компанії.

Створення проектної групи є важливим етапом впровадження стандарту ISO 27001:2015 в будь-якій компанії, оскільки забезпечує ефективне керівництво та координацію процесу впровадження стандарту.

Проектна група складається зі спеціалістів з різних областей, що дозволяє враховувати різні аспекти інформаційної безпеки і максимально точно відобразити реальний стан речей компанії. Керівник проекту забезпечує організацію та керівництво всім процесом, в той час коли керівник процесу інформаційної безпеки відповідає за розробку та впровадження політики інформаційної безпеки. Системний адміністратор має забезпечувати технічну підтримку та відповідати за налаштування систем безпеки. Менеджер зі зв'язків з громадськістю відповідає за зв'язок з громадськістю та розробку спільних з нею проектів. Представник відділу юридичного супроводу відповідає за відповідність роботи компанії всім законодавчим вимогам і правилам. Аналітик з оцінки ризиків відповідає за оцінку ризиків та розробку стратегії мінімізації цих ризиків. Інші спеціалісти в проектній групі

виконують різноманітні завдання залежно від розміру компанії і потреб впровадження стандарту.

Створення проектної групи дозволяє підготувати всі необхідні процедури та документацію, визначити відповідальних за їх виконання та забезпечити якісне впровадження стандарту.

2. Оцінка потреб в інформаційній безпеці шляхом визначення рівня критичності активів і оцінки ризиків, що пов'язані з цими активами.

Етап оцінки потреб в інформаційній безпеці полягає в визначенні критичних активів, які важливі для діяльності компанії, а також в оцінці ризиків, пов'язаних з цими активами. Це важливий етап, оскільки він дозволяє компанії зосередитися на захисті найважливіших активів та ризиків, які можуть негативно вплинути на діяльність компанії.

На цьому етапі зазвичай формується список критичних активів, які включають інформаційні ресурси, документацію, обладнання та інші матеріальні та нематеріальні активи компанії. Для кожного активу визначається його значимість для діяльності компанії та можливі наслідки його порушення.

Після цього проводиться оцінка ризиків, пов'язаних з кожним активом. Ризики можуть виникати з різних джерел, включаючи зовнішні загрози (наприклад, хакерські атаки) та внутрішні загрози (наприклад, недбале ставлення до безпеки з боку співробітників). Для кожного ризику визначається його ймовірність та потенційні наслідки.

На основі всієї цієї інформації формується план заходів з підвищення безпеки інформаційних активів конкретної компанії. Саме цей план може включати технічні та організаційні заходи, такі як, розробку і впровадження нових процедур, налаштування мережевої інфраструктури, впровадження криптографічних засобів захисту, підвищення рівня свідомості та кваліфікації персоналу тощо.

3. Розроблення та затвердження політики інформаційної безпеки, яка включає в себе загальні принципи, вимоги до захисту інформації та процедури, які необхідно дотримуватись.

Розроблення та затвердження політики інформаційної безпеки це важливий етап впровадження стандарту ISO 27001:2015. На цьому етапі відбувається створення документу, який встановлює загальні принципи і вимоги щодо захисту інформації в організації.

Для розроблення політики інформаційної безпеки необхідно враховувати рівень ризику, який приймає організація, також правові вимоги, які стосуються збереження та захисту інформації.

Основні етапи розроблення політики інформаційної безпеки:

- Формування команди. Необхідно створити команду зі спеціалістів з інформаційної безпеки, щоб забезпечити широку експертизу та відповідальність за розробку політики.
- Оцінка ризиків. Команда повинна провести оцінку ризиків, пов'язаних з активами організації, що вимагає захисту.
- Розробка політики. На основі результатів оцінки ризиків команда повинна розробити загальні принципи та вимоги до захисту інформації та процедури, які необхідно дотримуватись. Політика повинна включати в себе вимоги до захисту активів, процедури з контролю доступу, процедури з управління інцидентами, процедури з резервного копіювання і т.д.
- Затвердження політики. Після розробки політики вона повинна бути затверджена керівництвом організації, а також розіслана всім співробітникам, які мають стосунок до інформації організації.
- Розгортання політики. Команда повинна розгорнути політику на всіх рівнях організації, надати доступ до неї всім співробітникам, навчити їх її дотримуватися і забезпечити контроль за її дотриманням.

- Після розгортання політики інформаційної безпеки необхідно забезпечити постійне її вдосконалення та оновлення. Це можна зробити шляхом проведення регулярних аудитів та оцінок ризиків, щоб виявляти нові загрози та вразливості, які потрібно включити до політики.

4. Розроблення програми управління інформаційною безпекою, що містить в собі опис процесів та процедур, вимог до персоналу, вимоги до обладнання та програмного забезпечення, а також план заходів щодо управління інформаційною безпекою.

Розроблення програми управління інформаційною безпекою є одним з ключових етапів впровадження стандарту ISO 27001:2015 в компанії. На цьому етапі формується план дій щодо забезпечення інформаційної безпеки компанії, зокрема, визначаються процеси та процедури, необхідні для забезпечення захисту інформації, вимоги до персоналу, обладнання та програмного забезпечення, а також план заходів щодо управління інформаційною безпекою.

Основні етапи плану заходів щодо управління інформаційною безпекою можуть включати:

- Розроблення та затвердження політики інформаційної безпеки.
- Визначення потреб у захисті інформації та оцінка ризиків.
- Розроблення та затвердження програми управління інформаційною безпекою, включаючи опис процесів та процедур, вимог до персоналу, обладнання та програмного забезпечення.
- Впровадження заходів щодо захисту інформації, включаючи налагодження системи моніторингу та аналізу подій, контроль доступу, захист мережевого з'єднання та інших заходів.
- Забезпечення безпеки під час розробки та використання програмного забезпечення та інших технічних засобів.

- Забезпечення безпеки під час виконання робіт з обробки та зберігання інформації.
- Забезпечення безпеки під час взаємодії з постачальниками та партнерами.
- Проведення внутрішнього та зовнішнього аудиту інформаційної безпеки.
- Постійне вдосконалення системи управління інформаційною безпекою та її адаптація до змін у вимогах та умовах діяльності компанії.

5. Виконання аудиту наявної інфраструктури та визначення необхідних заходів для відповідності вимогам стандарту ISO 27001:2015.

Цей етап передбачає проведення аналізу існуючої інфраструктури компанії з точки зору вимог стандарту ISO 27001:2015. Цей стандарт визначає міжнародні стандарти в галузі управління інформаційною безпекою.

Аудит наявної інфраструктури полягає у зборі, оцінці та аналізі інформації про наявні процеси, системи, мережі та програмне забезпечення компанії. Цей аналіз допомагає виявити можливі ризики і вразливості, які можуть впливати на безпеку інформації в компанії.

Після аудиту наявної інфраструктури, необхідно визначити необхідні заходи для відповідності вимогам стандарту ISO 27001:2015. Ці заходи можуть включати в себе вдосконалення процесів управління інформаційною безпекою, встановлення нових систем та програмного забезпечення, підвищення кваліфікації персоналу, та інші.

Метою цього етапу є забезпечення відповідності компанії до вимог стандарту ISO 27001:2015 і зниження ризику порушення безпеки інформації. Це може допомогти компанії збільшити довіру клієнтів та партнерів, також зменшити можливість штрафних санкцій за порушення безпеки інформації, та збільшити загальну ефективність бізнесу.

6. Розроблення та впровадження основних процедур забезпечення безпеки, які включають в себе процедури резервного копіювання, контролю доступу, захисту від вторгнень, розгляду інцидентів та контролю інформації.

Цей етап включає в себе розроблення та впровадження процедур, що забезпечують захист всіх важливих активів компанії від неправомірного доступу до них, також втрати або пошкодження.

Одна з найважливіших процедур забезпечення безпеки - це процедура резервного копіювання. Вона включає регулярні створення резервних копій важливої інформації компанії, щоб забезпечити можливість відновлення даних у випадку їх втрати або пошкодження. Це може бути здійснено за допомогою спеціальних програм для резервного копіювання або засобів зовнішнього зберігання даних(жорстких дисків або серверів).

Контроль доступу - це ще одна з важливих процедура забезпечення безпеки, вона полягає у контролі доступу до важливих активів компанії. Це може включати регулярне оновлення паролів, використання двофакторної автентифікації, налаштування прав доступу та багато інших методів забезпечення безпеки доступу.

Процедури захисту від вторгнень мають на меті запобігти несанкціонованому доступу до важливих активів компанії, а також виявити й усунути вторгнення, які все ж таки стались. Це може включати налаштування брандмауера, антивірусного програмного забезпечення та інших інструментів захисту.

Контроль інформації - це процедура забезпечення безпеки, що має на меті забезпечити конфіденційність, цілісність та доступність інформації. Це може включати застосування криптографії і тд.

7. Запровадження системи моніторингу та аналізу подій для виявлення порушень інформаційної безпеки є одним з ключових етапів впровадження стандарту ISO 27001:2015 в продуктовій компанії.

Цей етап передбачає запровадження системи моніторингу, яка дозволяє виявляти та відслідковувати події, що пов'язані з інформаційною безпекою, та аналізувати їх для подальшого виявлення можливих порушень.

Система моніторингу та аналізу подій має бути розроблена таким чином, щоб вона змогла виявляти підозрілі активності та інциденти, що можуть стати загрозою для інформаційної безпеки компанії. Для цього можуть використовуватися різноманітні інструменти моніторингу, такі як системи логування, моніторинг мережевої активності, системи виявлення вторгнень тощо.

Крім того, система моніторингу повинна мати можливість збирати та аналізувати дані, щоб виявляти та аналізувати потенційні загрози. Це дозволить компанії оперативно реагувати на виявлені інциденти та вживати заходи для їх запобігання в майбутньому.

Крім системи моніторингу та аналізу подій, на цьому етапі можуть бути встановлені додаткові заходи, такі як автоматизовані процедури реагування на інциденти чи системи повідомлення про інциденти, та інші механізми для ефективного управління інформаційною безпекою.

8. Проведення внутрішнього аудиту інформаційної безпеки.

Це процес внутрішньої перевірки дієвості та ефективності системи управління інформаційною безпекою відповідно до встановлених вимог стандарту ISO 27001:2015.

Під час внутрішнього аудиту експерти з інформаційної безпеки проводять оцінку рівня відповідності встановленим політикам, процедурам та вимогам, що стосуються інформаційної безпеки. Це оцінювання проводиться шляхом перевірки документації та контрольних точок або інших засобів контролю.

Після проведення аудиту, внутрішні аудитори повідомлять керівництву про будь-які відхилення, виявлені під час аудиту. Це дозволяє керівництву компанії розробити план заходів щодо виправлення виявлених недоліків та

підвищення ефективності системи управління інформаційною безпекою. Крім того, внутрішній аудит також допомагає виявляти компанії потенційні ризики та проблеми, що можуть виникнути в майбутньому, що дозволяє вчасно приймати відповідні заходи щодо їх запобігання.

9. Створення плану дій з усунення порушень та запобігання їх повторенню, а також плану розвитку системи управління інформаційною безпекою на майбутнє.

Цей етап передбачає створення документів, які допоможуть як продуктовій так і будь-якій іншій компанії виконувати задачі з управління інформаційною безпекою. Першим кроком на цьому етапі є підготовка плану дій з усунення порушень, який включає в себе опис порушень, які виявили під час внутрішнього аудиту, а також конкретні дії, які необхідно вжити для усунення порушень.

Другим кроком є підготовка плану запобігання повторення порушень, який містить опис процедур та процесів, що повинні бути впроваджені, щоб запобігти повторенню порушень у майбутньому. Це можуть бути, наприклад, процедури моніторингу, процедури резервного копіювання, процедури захисту від вторгнень та інші.

Окремою частиною плану є план розвитку системи управління інформаційною безпекою на майбутнє. Цей план містить стратегічні цілі та плани дій компанії на майбутнє з метою забезпечення високого рівня інформаційної безпеки. План повинен включати в себе ініціативи щодо розвитку процедур, технологій, інфраструктури, навчання персоналу та інших засобів, що допоможуть підвищити рівень інформаційної безпеки в майбутньому.

Усі ці плани повинні бути підтримувані та оновлюватися регулярно, щоб забезпечити ефективність системи управління.

Висновки до розділу 1:

Висновок з аналізу стандарту ISO 27001:2015 зосереджується на його значущості та впливі на управління інформаційною безпекою в організаціях. Цей міжнародний стандарт встановлює вимоги до систем управління інформаційною безпекою (СУІБ), що є ключовим для забезпечення конфіденційності, цілісності та доступності важливої корпоративної інформації. Він виник як розвиток британського стандарту BS 7799-1, згодом трансформувавшись у повноцінний міжнародний стандарт, який актуалізує практики і процедури управління інформаційною безпекою. ISO 27001:2015 став невід'ємною частиною регуляторного ландшафту, особливо в регульованих секторах, де вимоги до захисту інформації є особливо сувворими. Цей стандарт допомагає організаціям не тільки мінімізувати ризики втрати, недоступності або викривлення інформації, але й підвищує довіру клієнтів та партнерів до організації. Впровадження ISO 27001:2015 сприяє стандартизації процесів та покращує загальну структуру управління інформаційною безпекою. Він охоплює такі аспекти, як планування, підтримка, операційна діяльність, оцінка результатів та постійне покращення, тим самим забезпечуючи комплексний та систематичний підхід до забезпечення інформаційної безпеки. У підсумку, ISO 27001:2015 відіграє критичну роль у формуванні ефективної стратегії інформаційної безпеки організації, що є невід'ємним аспектом сучасного управлінського процесу в організаціях різних розмірів та профілів.

На момент написання цієї роботи набула дійсності більш нова версія документу - ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою.(за наказом від 17.08.2023 № 210 Про прийняття національних стандартів, зміни до національного стандарту та скасування національних стандартів)

Розділ 2

Безпека Інформаційних Систем у Авіації

Сучасна авіація відіграє найважливішу роль у світовій економіці та сприяє глобальному зв'язку. Цей розвинений сектор використовує інформаційні технології та інфраструктуру, щоб забезпечити безпеку, ефективність та комфорт подорожей. Проте, разом із зростанням цифрової трансформації з'являються нові виклики у сфері кібербезпеки. Цей подовжений реферат досліджує значення безпеки інформаційних систем у галузі авіації, визначає загрози та пропонує стратегії для забезпечення їхньої безпеки.

Частина 2.1. Загрози кібербезпеці в авіації

2.1.1. Кібератаки на авіаційні системи

Авіаційні системи на сьогоднішній день стали надзвичайно інтегрованими та залежними від інформаційних технологій. Ця інтеграція і залежність створюють неабиякі виклики та загрози у вигляді кібератак. Наведемо детальний аналіз цього аспекту:

Типи кібератак:

- Деніал-сервіс атаки (Distributed Denial of Service, DDoS): Вони полягають у переповненні авіаційних серверів запитами, що призводить до перебоїв у роботі та відмов у наданні послуг компанії.
- Внутрішні атаки: Співробітники авіакомпаній або аеропортів можуть бути використані для здійснення кібератак зсередини системи.
- Фішинг та соціальна інженерія: Зловмисники можуть намагатися отримати доступ до систем шляхом обману персоналу аеропортів або авіакомпаній. Можливі надсилання фейкових листів.

- Кібершпигунство та крадіжка інформації: Зловмисники можуть намагатися викрасти конфіденційну інформацію про авіаційні системи, розклади польотів, пасажирів і т. д.

Наслідки кібератак:

- Порушення безпеки польотів: Кібератаки можуть призвести до втрати керування над повітряними суднами, зміни маршрутів польотів, або навіть аварій.
- Втрата даних: Крадіжка або пошкодження даних, таких як рейсові розклади, дані про пасажирів або багаж, може призвести до серйозних проблем в роботі авіакомпаній.
- Порушення громадської безпеки: Атаки на системи, відповідальні за повітряний рух, можуть створити загрозу для громадської безпеки.

2.1.2. Соціальна інженерія та фішинг

Фішинг - це атака, при якій зловмисники відправляють підроблені повідомлення або листи, які видаватимуться за легітимні повідомлення від авіакомпаній або аеропортів. Метою таких атак може бути отримання особистої інформації, такої як паролі або номери кредитних карт:

Електронна пошта фішингу: Зловмисники відправляють підроблені листи, які видаватимуться за авіакомпанії або аеропорти, і просять одержувачів надати конфіденційну інформацію.

Фішингові веб-сайти: Зловмисники створюють фішингові веб-сайти, які схожі на офіційні веб-сайти авіакомпаній або аеропортів, і намагаються отримати дані від користувачів

Спам і фішинг на соціальних мережах: Зловмисники можуть використовувати соціальні мережі для поширення підроблених повідомлень і лурить користувачів надавати особисту інформацію.

Заходи захисту:

- Для захисту від соціальної інженерії та фішингу необхідно проводити свідому роботу серед персоналу:
- Навчання персоналу: Освіта і тренування співробітників щодо впізнавання підроблених повідомлень та правил безпеки.
- Моніторинг комунікацій: Спостереження за електронною поштою та іншими формами комунікації для виявлення підозрілих активностей
- Використання антивірусних програм та фільтрів для електронної пошти: Це допомагає виявляти підроблені повідомлення та блокувати їх.
- Перевірка легітимності веб-сайтів: Перш ніж надавати конфіденційну інформацію, переконайтеся, що веб-сайт, на якому ви вводите дані, є легітимним.
- Зміцнення кібербезпеки на рівні авіаційних систем: Застосування сучасних технологій та заходів захисту для запобігання атакам.

2.1.3. Загрози від держав та терористичних організацій

У сучасному світі авіаційні системи стали об'єктом підвищеної уваги для держав та терористичних організацій, оскільки авіація є стратегічно важливим сектором. Розглянемо детально загрози, які виникають від держав і терористичних організацій:

Загрози від держав:

- Кібершпигунство: Ворожі держави можуть намагатися здійснювати кібершпигунство з метою здобуття конфіденційної інформації про авіаційні системи, такої як розклади польотів або технічні характеристики.

- Кібератаки: Держави можуть використовувати кібератаки для завдання шкоди авіаційним системам і порушення нормального функціонування аеропортів або авіакомпаній
- Шпигунство в реальному світі: Державні агенти можуть намагатися отримати доступ до авіаційних приміщень, або використовувати таємні агенти, щоб здійснювати фізичне шпигунство.

Загрози від терористичних організацій:

- Кібертероризм: Терористичні організації можуть намагатися здійснювати кібератаки на авіаційні системи з метою створення хаосу та небезпеки для громадської безпеки.
- Використання безпілотників: Терористи можуть намагатися використовувати безпілотники для атак на повітряні судна або інфраструктуру аеропортів.
- Саботаж: Терористи можуть спрямовувати зусилля на саботаж інфраструктури аеропортів або повітряних суден.

Заходи захисту:

- Захист від кібератак: Застосування сучасних засобів кіберзахисту, мережевих брандмауерів та інших технічних рішень для запобігання кібератакам.
- Фізичний захист: Зміцнення фізичного захисту аеропортів та авіаційних інфраструктур від потенційних загроз.
- Розвідка та контррозвідка: Проведення діяльності з розвідки та контррозвідки для виявлення потенційних загроз інфраструктурі авіації.
- Співпраця з правоохоронними органами: Запровадження систем співпраці з правоохоронними органами для реагування на загрози від держав та терористичних організацій.

Частина 2.2. **Важливість безпеки інформаційних систем в авіації**

2.2.1. Забезпечення безпеки польотів

Забезпечення безпеки польотів в авіації - це один із найважливіших аспектів, оскільки від цього залежить безпека пасажирів, екіпажу і наземного персоналу. Цей розділ детально розглядає заходи та процедури, що вживаються для забезпечення безпеки польотів в авіаційній галузі.

Сертифікація інфраструктури і повітряних суден:

- Сертифікація літаків: Перед тим як літаки можуть експлуатуватися для пасажирських або вантажних польотів, вони повинні успішно пройти сертифікацію, що включає тестування та оцінку їхньої безпеки.

  Стандарти для сертифікації літаків:

1. Стандарт EASA (Європейське агентство з авіаційної безпеки): Європейська авіаційна організація встановлює стандарти та регуляції для сертифікації літаків в Європейському Союзі.
2. Стандарт FAA (Федеральне авіаційне управління, США): FAA встановлює стандарти та правила для сертифікації літаків, які експлуатуються в Сполучених Штатах.
3. ICAO (Міжнародна організація цивільної авіації): ICAO розробляє міжнародні стандарти для безпеки авіації, які дотримуються багатьма країнами.

- Сертифікація аеропортів: Аеропорти також повинні бути сертифіковані для забезпечення безпеки пасажирів і повітряних суден.

Стандарти для сертифікації аеропортів:

Стандарти ICAO (Міжнародна організація цивільної авіації): ICAO встановлює міжнародні стандарти та рекомендації для аеропортів, включаючи безпеку, ефективність та інші аспекти.

Стандарти ЕКАС (Європейська координаційна організація з безпеки авіації): ЕКАС встановлює стандарти безпеки для аеропортів, які розташовані в країнах-членах Європейського Союзу.

Пілотаж і підготовка екіпажу:

- Тренування пілотів: Пілоти проходять інтенсивну підготовку та тренування, включаючи симулятори, щоб вони могли ефективно реагувати на різні надзвичайні ситуації.
- Тренування екіпажу кабіни: Членам екіпажу кабіни надається навчання з пасажирської безпеки та процедур в надзвичайних ситуаціях.

Технічна безпека повітряних суден:

- Регулярні обліки та обслуговування: Літаки проходять регулярні обліки і технічне обслуговування, щоб впевнитися в їхній безпеці та працездатності.
- Безпека пального та двигунів: Пальне та двигуни піддаються особливому контролю, оскільки вони впливають на безпеку польоту.

Безпека пасажирів та багажу:

- Сканування та контроль пасажирів: Пасажири та їхні ручні багажі піддаються обов'язковому скануванню та перевірці на предмет заборонених предметів.
- Системи безпеки кабіни: Кабіни пасажирів обладнані системами безпеки для запобігання конфліктам та забезпечення безпеки під час польоту.

Надзвичайні ситуації та процедури:

- Евакуаційні плани та навчання: Аеропорти та авіакомпанії мають навчати пасажирів процедурам евакуації у надзвичайних ситуаціях.
- Керування надзвичайними ситуаціями: Авіакомпанії мають визначити процедури керування надзвичайними ситуаціями та реагування на них.

Моніторинг і безпека повітряного простору:

- Радари та системи слідкування: Повітряний простір стежиться за допомогою радарів та систем слідкування для уникнення зіткнень та контролю руху повітряного судна.

Міжнародні стандарти та регулювання:

- Міжнародна організація цивільної авіації (МОНТ)*: МОНТ встановлює міжнародні стандарти та рекомендації щодо безпеки в авіації, які дотримуються країнами-членами.

2.2.2. Збереження даних та конфіденційності

Збереження даних та забезпечення конфіденційності є критичними аспектами в сфері авіації, оскільки авіаційні системи залежать від обробки величезної кількості інформації, включаючи особисті дані пасажирів та конфіденційну інформацію про безпеку польотів. Ось докладніше про заходи та процедури, пов'язані з цим аспектом:

Захист даних пасажирів:

- Обмеження доступу: Обмеження доступу до особистих даних пасажирів та конфіденційної інформації лише авторизованим користувачам та персоналу.
- Шифрування: Використання шифрування для захисту даних пасажирів під час їх передачі та збереження.
- Аудит та моніторинг: Проведення аудиту та постійного моніторингу доступу до даних для виявлення незвautorизованої діяльності.

Захист інформації про безпеку польотів:

- Класифікація інформації: Класифікація інформації про безпеку польотів на рівні доступу та застосування відповідних заходів безпеки.

- Захист від кіберзагроз: Захист інформації про безпеку від потенційних кіберзагроз та кібератак.
- Безпека комунікацій: Захист безпеки комунікацій між авіаційними системами та контролем повітряного руху.

Захист інфраструктури авіаційних систем:

- Фізичний захист: Фізичний захист інфраструктури авіаційних систем від несанкціонованого доступу та загроз.
- Мережевий захист: Застосування заходів захисту мереж та серверів авіаційних систем.

Навчання та освіта персоналу:

- Співробітники освіти: Навчання та освіта персоналу щодо стандартів безпеки даних та конфіденційності.
- Соціальна інженерія: Навчання персоналу розпізнавати соціальну інженерію та фішингові атаки.

Аудит та оцінка:

- Регулярний аудит безпеки даних: Проведення регулярних аудитів для перевірки дотримання стандартів безпеки даних.
- Оцінка ризиків безпеки: Оцінка ризиків та розробка стратегій зменшення цих ризиків.

Частина 2.3. Стратегії для забезпечення безпеки інформаційних систем в авіації

2.3.1. Кіберзахист інфраструктури

Кіберзахист інфраструктури в авіаційній галузі є критично важливим завданням, оскільки авіаційні системи стають все більше цифровими та

піддаються кіберзагрозам. Цей розділ детально розглядає заходи та процедури, які вживаються для захисту інфраструктури авіаційних систем від кіберзагроз.

Ідентифікація та аналіз загроз:

- Аналіз потенційних загроз: Аналіз потенційних кіберзагроз та визначення їх впливу на авіаційні системи.
- Виявлення вразливостей: Виявлення вразливостей інфраструктури, які можуть бути використані кіберзлочинцями.

Заходи захисту інфраструктури:

- Захист мереж: Встановлення мережевих брандмауерів, інтрафейсних фільтрів та інших технічних заходів для запобігання несанкціонованому доступу.
- Шифрування даних: Використання сучасних методів шифрування для захисту даних, що передаються в мережах.

Моніторинг і виявлення інцидентів:

- Системи моніторингу: Впровадження систем моніторингу мереж та систем для виявлення аномальних активностей.
- Реагування на інциденти: Розробка процедур реагування на кіберінциденти та швидкого виправлення вразливостей.

Навчання та свідомість персоналу:

- Тренування персоналу: Тренування персоналу щодо кіберзагроз та безпеки мереж та систем.
- Свідомість про кібербезпеку: Створення свідомості про кібербезпеку серед співробітників та користувачів інфраструктури.

Резервне копіювання та відновлення:

- Резервне копіювання даних: Регулярне створення резервних копій важливих даних та систем.

- Плани відновлення: Розробка планів відновлення в разі кіберінциденту або втрати даних.

Міжнародні стандарти та регуляції:

- ICAO (Міжнародна організація цивільної авіації): Дотримання міжнародних стандартів та рекомендацій ICAO щодо кіберзахисту в авіації.
- Регуляторні органи: Співпраця з регуляторними органами та владними установами для забезпечення дотримання вимог щодо кібербезпеки.

Висновки до розділу 2:

Розділ зосереджується на важливості забезпечення безпеки інформаційних систем в сучасному авіаційному секторі. У розділі розглядаються різноманітні види загроз, такі як: кібератаки, соціальна інженерія, фішинг, кібершпигунство, та їх потенційний вплив на безпеку польотів, втрату даних та загрозу громадській безпеці. Також аналізуються стратегії захисту, включаючи: навчання персоналу, моніторинг комунікацій, використання антивірусних програм та зміцнення кібербезпеки на рівні авіаційних систем. Особливу увагу приділено загрозам від держав та терористичних організацій, які розглядають авіаційні системи як стратегічно важливі об'єкти. Розгляд даної теми підкреслює значення комплексного підходу до кіберзахисту, включаючи сертифікацію інфраструктури та повітряних суден, контроль безпеки повітряного простору та збереження даних. Заключно, автори наголошують на важливості кібербезпеки як невід'ємної складової ефективної та безпечної роботи авіаційної галузі.

Розділ 3

Розробка програмного забезпечення для оцінювання рівня якості послуг аеропортового комплексу

Частина 3.1. Теоретичні відомості

Мета діяльності будь-якого аеропорту це надання якісних та своєчасних послуг як авіаційного, так і неавіаційного характеру.

Для оцінювання рівня якості послуг використовуються кількісні та якісні показники якості. Кількісні показники — це час виконання технологічних операцій або необхідна площа приміщення, відсоток справності обладнання тощо. Якісні показники визначає споживач (пасажир) за визначеною шкалою (Таблиця 4).

Таблиця 4

Шкала оцінювання якості аеропортового обслуговування

Оцінка(бали)	Характеристика рівня якості послуги
0	Послуги немає
1	Послуга надається вперше, якість незадовільна
2	Послуга надається, якість надання задовільна, тенденція до погіршення
3	Послуга надається, якість надання задовільна, тенденція до поліпшення
4	Послуга надається, якість надання добра
5	Послуга надається на найвищому рівні

Основні групи показників рівня якості послуг аеропортів вказані в Таблиці 5.

Таблиця 5

Показники якості аеропортових послуг для основних авіаперевізників

№ з/п	Назва показника якості
1	Можливість виконання послуг з наземного обслуговування (НО) власними силами
1.1	Прийання-випуск ПС

1.2	Внутрішнє прибирання ПС
1.3	Оброблення вантажу
1.4	Бортхарчування
1.5	Паливне забезпечення
2	Аеродромне забезпечення
2.1	Стан покриття рулильних доріжок, місць стоянки
2.2	Наявність відповідної розмітки, маркування
2.3	Організація робіт на місцях стоянки. Наявність стаціонарних джерел електроживлення, місць стоянки, обладнаних централізованою системою заправки, засобів пожежогасіння, буксирування, наземного обладнання
3	Орнітологічне забезпечення
3.1	Статистика про зіткнення ПС з тваринами і птахами на аеродромі та в районі аеродрому через несприятливі орнітологічніобставини
3.2	Заходи щодо поліпшення орнітологічної обстановки
4	Наземне обслуговування ПС
4.1	Наявність технологічних графіків обслуговування
4.2	Наявність і достатність персоналу, спецтранспорту, обладнання для НО ПС, заправки, обслуговування пасажирів, оброблення багажу, евакуації ПС
4.3	Наявність джерел електроживлення необхідної потужності
4.4	Якість обслуговування пасажирів та обробки багажу
4.5	Дотримання часу обслуговування ПС на стоянці за розкладом. Здатність аеропорту в критичних ситуаціях зберегти і / або скоротити час обороту ПС
4.6	Статистика пошкоджень ПС під час наземного обслуговування
4.7	Організація системи роботи з трансферним багажем
4.8	Наявність системи управління ризиками
5	Аеропортове обслуговування

5.1	Реєстрація пасажирів
5.2	Центрування ПС

5.3	Стан аеровокзального комплексу
5.4	Відповідність заявленої пропускної здатності (зали очікування, стійки реєстрації, прикордонний контроль тощо) реальній
5.5	Можливість використання власної системи реєстрації пасажирів
5.6	Наявність автоматизованої системи пошуку багажу
5.7	Обслуговування спеціальних категорій пасажирів
5.8	Якість обслуговування пасажирів в аеровокзалі
5.9	Якість оброблення багажу, у тому числі траснферного
5.10	Організація роботи на привокзальній площі
6	Організація оброблення вантажу та пошти
6.1	Наявність техніки для перонного оброблення великовагових вантажів, що перевозяться пасажирськими неконтейнернимі типами ПС
6.2	Наявність системи управління ризиками
6.3	Надання NOTOC (SpecialLoadNotificationtoCaptain) на спеціальні вантажі (як на небезпечні, так і безпечні вантажі)
6.4	Готовність обслуговуючих компаній до ліквідації наслідків інцидентів, спричинених небезпечними вантажами
6.5	Наявність каналу SITATEX для інформаційного супроводу вантажних перевезень
6.6	Наявність у персоналу допусків на оброблення небезпечних вантажів відповідно до сертифікатів на аеропортову діяльність
6.7	Організація надання звітів про інциденти, спричинені небезпечними вантажами і про виявлення незадекларованих або неправильно задекларованих небезпечних вантажів
6.8	Організація виявлення незадекларованих небезпечних вантажів

6.9	Внутрішнє прибирання ПС (своєчасність і якість послуги)
7	Забезпечення ПММ
7.1	Виробничі потужності паливо-заправного комплексу (ПЗК)
7.2	Дисципліна поставок авіапалива
7.3	Якість поставленого авіапалива
7.4	Якість лабораторного аналізу в ПЗК
7.5	Якість надання послуги із заправлення
8	Підтримання льотної придатності
8.1	Наявність лінійних станцій технічного обслуговування (ЛСТО)

8.2	Можливість створення власних ЛСТО
8.3	Наявність можливості надання технічної допомоги перевізникам (on-call)
8.4	Якість надаваних послуг, можливість усунення зауважень екіпажу
9	Організація взаєморозрахунків
9.1	Умови взаєморозрахунків
9.2	Упровадження електронного документообігу – електронний обмін фінансовими документами
9.3	Стимулювання польотів перевізника. Наявність маркетингових програм (знижок у наземному обслуговуванні)
9.4	Організація обслуговування уфорс-мажорних ситуаціях
10	Забезпечення запасними аеродромами
10.1	Наявність зручних запасних аеродромів
10.2	Організація наземного і аеропортового обслуговування на запасних аеродромах
10.3	Обслуговування пасажирів у форс-мажорних ситуаціях
10.4	Аварійно-рятувальне забезпечення
11	Нормативне регулювання у галузі надання послуг

11.1	Порушення вимог нормативних документів з аеропортового і наземного обслуговування ПС

Для розробки програмного забезпечення та розрахунків було взято та заповнено декілька групових показників якості(Таблиця 3):

Таблиця 6

№ з/п	Назва показника якості	Результат оцінювання		
		Аеропорт 1	Аеропорт 2	Аеропорт 3
1	Можливість виконання послуг зназемного обслуговування (НО) власними силами			
1.1.	Приймання-випуск ПС	3	3	3
1.2.	Внутрішнє прибирання ПС	3	4	3
1.3.	Оброблення вантажу	3	3	3
1.4.	Бортхарчування	3	5	3
1.5.	Паливне забезпечення	4	3	2
2	Аеродромне забезпечення			
2.1.	Стан покриття рулильних доріжок, місць стоянки	3	3	3
2.2.	Наявність відповідної розмітки,маркування	3	1	3
2.3.	Організація робіт на місцях стоянки. Наявність стаціонарних джерел електроживлення, місць стоянки, обладнаних централізованою системою заправки, засобів пожежогасіння, буксирування, наземного обладнання	4	3	5
3	Орнітологічне забезпечення			

3.1.	Статистика про зіткнення ПС з тваринами і птахами на аеродромі та в районі аеродрому через несприятливі орнітологічні обставини	3	5	3
3.2.	Заходи щодо поліпшення орнітологічної обстановки	3	3	3
4	Наземне обслуговування ПС	3,125	3,25	3,25
4.1.	Наявність технологічних графіків обслуговування	3	3	3
4.2.	Наявність і достатність персоналу, спецтранспорту, обладнання для НО ПС, заправки, обслуговування пасажирів, оброблення багажу,евакуації ПС	3	3	3
4.3.	Наявність джерел електроживлення необхідноїпотужності	3	3	3
4.4.	Якість обслуговування пасажирів та оброблення багажу	3	5	3
4.5.	Дотримання часу обслуговування ПС на стоянці за розкладом. Здатність аеропорту в критичних ситуаціях зберегти і / або скоротити час обороту ПС	3	3	3
4.6.	Статистика пошкоджень ПС під час наземного обслуговування	4	3	5
4.7.	Організація системи роботи ztрансферним багажем	3	3	3
4.8.	Наявність системи управління ризиками	3	3	3

5	Орнітологічне забезпечення			
5.1.	Наявність лінійних станцій технічного обслуговування(JTCTO)	3	2	3
5.2.	Можливість створення власних ЛСТО	3	4	4
5.3.	Наявність можливості надання технічної допомоги перевізникам (on-call)	4	4	3
5.4.	Якість надаваних послуг	4	3	5

Для кількісної оцінки якості аеропортів було взято формулу:

Формула 1

$$Q = \sum_{i=1}^{n} \sum_{k=1}^{m} v_{ik} * P_{ik}$$

де *vік* - ваговий коефіцієнт цього показника, що відображає його важливість;

Pік - показники, які забезпечують якість послуг аеропорту (кожний з вказаних показників оцінюється за 5-бальною шкалою);

n – кількість параметрів;

m – кількість показників у кожному параметрі.

Комплекс показників рівня якості послуг аеропортів за 5 параметрами і 25 показниками зформовано у вигляді матриці (Малюнок 2).

Рисунок 2

$$P := \begin{pmatrix} P_{11} & P_{12} & P_{13} & P_{14} & P_{15} \\ P_{21} & P_{22} & P_{23} & P_{24} & P_{25} \\ P_{31} & P_{32} & P_{33} & P_{34} & P_{35} \\ P_{41} & P_{42} & P_{43} & P_{44} & P_{45} \\ P_{51} & P_{52} & P_{53} & P_{54} & P_{55} \end{pmatrix}$$

V – ваговий коефіцієнт взято від 1 до 5. (Таблиця 7)

Таблиця 7

Виговий коєфіцієнт	Вагомість
1	Надзвичайно важливо
2	Дуже важливо
3	Важливо
4	З помірною важливістю
5	Мало важливо

Частина 3.2. Розробка програми (Код програми)

```
public class MatrixCalculationGUI {
public static void main(String[] args) {

        int[][] matrixP = {
                {3, 3, 3, 3, 4, 0, 0, 0},
                {3, 3, 4, 0, 0, 0, 0, 0},
                {3, 3, 0, 0, 0, 0, 0, 0},
                {3, 3, 3, 3, 3, 4, 3, 3},
                {3, 3, 4, 4, 0, 0, 0, 0}
        };

        int[][] matrixV = {
                {1, 2, 3, 4, 0, 0, 0, 0},
                {1, 1, 5, 0, 0, 0, 0, 0},
                {2, 3, 0, 0, 0, 0, 0, 0},
                {1, 1, 0, 5, 0, 3, 4, 1},
                {1, 1, 3, 2, 0, 0, 0, 0}
        };

        int[][] matrixT = {
                {3, 4, 3, 5, 3, 0, 0, 0},
                {3, 1, 3, 0, 0, 0, 0, 0},
                {5, 3, 0, 0, 0, 0, 0, 0},
                {3, 3, 3, 3, 3, 3, 3, 3},
                {2, 4, 4, 3, 0, 0, 0, 0}
        };

        int[][] matrixK = {
                {1, 2, 3, 4, 0, 0, 0, 0},
                {1, 1, 5, 0, 0, 0, 0, 0},
                {2, 3, 0, 0, 0, 0, 0, 0},
                {1, 1, 0, 5, 0, 3, 4, 1},
                {1, 1, 3, 2, 0, 0, 0, 0}
        };

        int[][] matrixR = {
                {3, 3, 3, 3, 2, 0, 0, 0},
                {3, 3, 5, 0, 0, 0, 0, 0},
                {3, 3, 0, 0, 0, 0, 0, 0},
                {3, 3, 3, 3, 3, 5, 3, 3},
                {3, 4, 3, 5, 0, 0, 0, 0}
        };
```

```
        int[][] matrixS = {
                {1, 2, 3, 4, 0, 0, 0, 0},
                {1, 1, 5, 0, 0, 0, 0, 0},
                {2, 3, 0, 0, 0, 0, 0, 0},
                {1, 1, 0, 5, 0, 3, 4, 1},
                {1, 1, 3, 2, 0, 0, 0, 0}
        };

    String[] matrixNames = {
            "Можливість виконання послуг з наземного обслуговування (НО)
власними силами",
            "Аеродромне забезпечення",
            "Орнітологічне забезпечення",
            "Наземне обслуговування ПС",
            "Забезпечення ПММ"
    };

    int[][][] matricesP = {matrixP, matrixT, matrixR};
    int[][][] matricesV = {matrixV, matrixK, matrixS};
    int[] totalSums = new int[matricesP.length];

    for (int k = 0; k < matricesP.length; k++) {
        int[][] currentMatrixP = matricesP[k];
        int[][] currentMatrixV = matricesV[k];

        int numRowsP = currentMatrixP.length;
        int numRowsV = currentMatrixV.length;
        int[] rowSums = new int[numRowsP];

        if (numRowsP != numRowsV) {
            System.out.println("Матриці мають різну кількість рядків,
множення неможливе.");
            return;
        }

        int totalSum = 0;

        for (int i = 0; i < numRowsP; i++) {
            int rowSum = 0;
            for (int j = 0; j < currentMatrixP[i].length; j++) {
                rowSum += currentMatrixP[i][j] * currentMatrixV[i][j];
            }
            System.out.println(matrixNames[i] + ": " + rowSum);
            rowSums[i] = rowSum;
            totalSum += rowSum;
        }

        totalSums[k] = totalSum;
        System.out.println("Кількісне значення рівня якості послуг аеропорту
" + (k + 1) + ": " + totalSum);
        System.out.println();
    }

    int maxSum1 = totalSums[0];
    int minSum1 = totalSums[0];
    int middleSum1 = totalSums[0];
    int maxSumIndex = 0;
    int minSumIndex = 0;
    int middleSumIndex = 0;

    for (int i = 1; i < totalSums.length; i++) {
        int sum = totalSums[i];
        if (sum > maxSum1) {
            maxSum1 = sum;
```

```
            maxSumIndex = i;
        }
        if (sum < minSum1) {
            minSum1 = sum;
            minSumIndex = i;
        }
    }

    for (int i = 0; i < totalSums.length; i++) {
        int sum = totalSums[i];
        if (sum < maxSum1 && sum > minSum1) {
            middleSum1 = sum;
            middleSumIndex = i;
        }
    }

    System.out.println("Найбільший кількісний показник якості послуг
: " + maxSum1 + " (Належить аеропорту " + (maxSumIndex + 1) + ")");
    System.out.println("Середній кількісний показник якості послуг
: " + middleSum1 + " (Належить аеропорту " + (middleSumIndex + 1) + ")");
    System.out.println("Найменший кількісний показник якості послуг
: " + minSum1 + " (Належить аеропорту " + (minSumIndex + 1) + ")");
}
}
```

У цій програмі описано:

1. matrixP, matrixT, matrixR - комплекс показників рівня якості послуг аеропортів 1,2,3 відповідно.
2. matrixP, matrixT, matrixR - ваговий коефіцієнт у вигляді матриці для кожного показника рівня якості послуг.
3. За Формулою 1, проведено розрахунки кількісних показників. Де значеня P_{ik} взяте з матриць: matrixP, matrixT, matrixR, а значення *vік* з матриць: matrixP, matrixT, matrixR відповідно.
4. Після запуску данної програми ми маємо результат де розраховано кількісне значення рівня якості послуг для кожного аеропорту окремо, а потім порівняно 3 аеропорти (Таблиця 8).

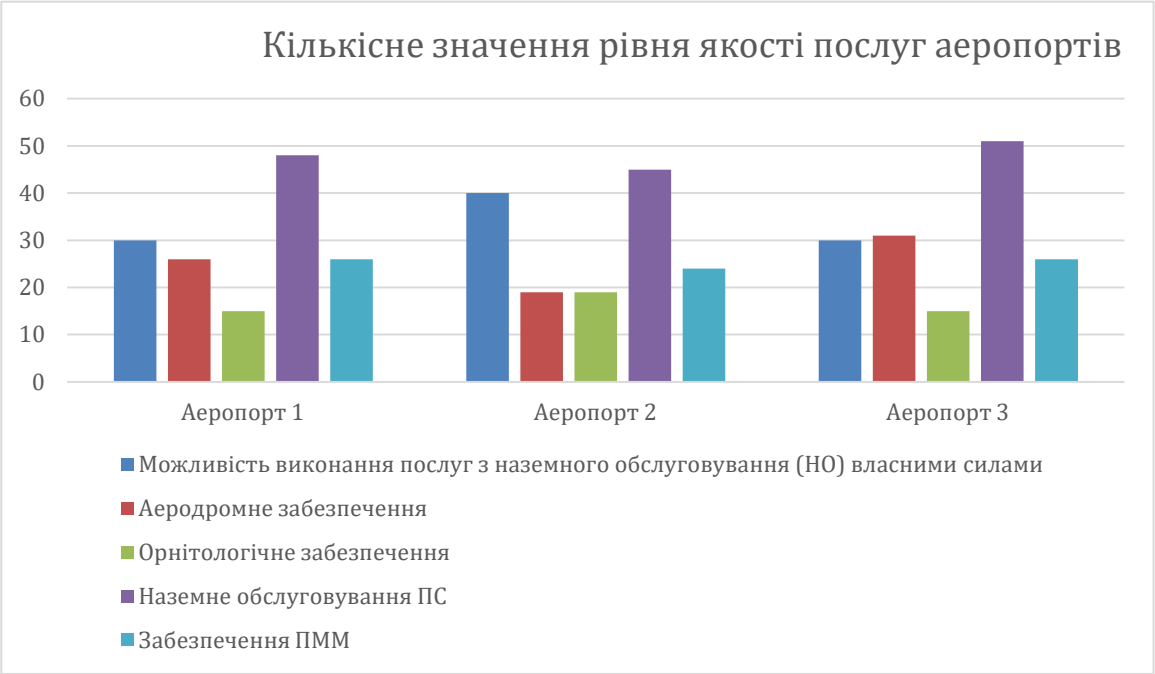
Таблиця 8

Можливість виконання послуг з наземного обслуговування (НО) власними силами: 30
Аеродромне забезпечення: 26
Орнітологічне забезпечення: 15
Наземне обслуговування ПС: 48
Забезпечення ПММ: 26

Кількісне значення рівня якості послуг аеропорту 1: 145
Можливість виконання послуг з наземного обслуговування (НО) власними силами: 40 Аеродромне забезпечення: 19 Орнітологічне забезпечення: 19 Наземне обслуговування ПС: 45 Забезпечення ПММ: 24 Кількісне значення рівня якості послуг аеропорту 2: 147
Можливість виконання послуг з наземного обслуговування (НО) власними силами: 30 Аеродромне забезпечення: 31 Орнітологічне забезпечення: 15 Наземне обслуговування ПС: 51 Забезпечення ПММ: 26 Кількісне значення рівня якості послуг аеропорту 3: 153
Порівняння: Найбільший кількісний показник якості послуг: 153 (Належить аеропорту 3) Середній кількісний показник якості послуг: 147 (Належить аеропорту 2) Найменший кількісний показник якості послуг: 145 (Належить аеропорту 1)

З отриманих данних можна побудувати діаграму з даними показників якості трьох аеропортів (Таблиця 9).

Таблиця 9



Висновки до розділу 3:

1. Дану програму в даномму випадку було використано рівні якості послуг аеропортового комплексу з однаковим ваговим коефіцієнтом, цю програму також можна використовувати в будь-якій сфері (наприклад в трибології – порівняння мастил).
2. Ця робота зосереджувалася на аналізі данних 3 різних аеропортів, на основі зібраних даних та аналізу встановлено, що є Аеропорт 1 з найнижчим кількісним показником якості – 145. З огляду на ці результати, рекомендується вжити наступні кроки щодо аеропорту з найнижчим показником:
    - Детальний аналіз проблеми
    - Розробка плану поліпшення
    - Імплементація та моніторинг
3. У підсумку, ця робота показує, що кількісний показник якості є цінним інструментом для визначення областей для поліпшень та для відстеження ефективності впроваджених змін.

Розділ 4
Охорона навколишнього середовища в Авіації

Авіація є невід'ємною частиною сучасного світу і має значний вплив на навколишнє середовище. Повітряний транспорт забезпечує глобальну мобільність та зручність подорожей, але разом із цим він також призводить до викидів забруднюючих речовин та інших негативних впливів на навколишнє середовище. Охорона природи та навколишнього середовища стають все важливішими завданнями для авіації. У цьому рефераті розглянемо вплив авіації на навколишнє середовище та стратегії зменшення цього впливу.

Частина 4.1. Викиди та їх вплив

1.1 Викиди шкідливих речовин

Авіаційні двигуни спалюють пальне, що призводить до викиду різних шкідливих речовин у атмосферу. Серед них вуглеводні, оксиди азоту, сірку та інші забруднюючі речовини. Ці викиди мають поганий вплив на якість повітря та сприяють погіршенню клімату.

Основні Забруднювачі та Їх Вплив

- Вуглеводні (HC): Складаються з різних органічних сполук. Деякі з них, наприклад, метан, є потужними парниковими газами.
- Оксиди Азоту (NOx): Включають різні сполуки азоту та кисню, такі як NO і NO2. Ці гази сприяють утворенню озону в нижніх шарах атмосфери, викликаючи проблеми з якістю повітря і впливаючи на здоров'я людей.
- Сірка (S) та Сполуки: Хоча сучасне авіаційне паливо містить низький вміст сірки, її сполуки все ще можуть утворюватися при високих температурах спалювання і спричиняти кислотні дощі.

Вплив на Клімат:

Викиди від авіації, особливо CO2 і NOx, мають прямий та непрямий вплив на клімат. CO2 є довготривалим парниковим газом, що сприяє глобальному потеплінню. NOx у свою чергу впливає на концентрацію озону та метану в атмосфері, що також веде до зміни клімату.

1.2 Ефект парникового газу

Авіаційна індустрія вносить вагомий вклад у викиди парникових газів. Особливо це стосується CO2, який випускається при спалюванні авіаційного пального. Хоча відсоток викидів CO2 від авіації в загальному обсязі емісій парникових газів не є надзвичайно великим, він має тенденцію до зростання через постійне збільшення обсягів повітряного транспортування.

Викиди високолітних літаків мають особливо велике значення, оскільки вони впливають на верхні шари атмосфери. На цій висоті, парникові гази, а також водяні пари, які утворюються в результаті роботи авіаційних двигунів, можуть довше зберігатися та більш інтенсивно впливати на клімат.

Для боротьби з викидами парникових газів у авіації, впроваджуються різні стратегії. Серед них - вдосконалення ефективності палива, використання альтернативних видів палива, таких як біопаливо, та розробка більш ефективних авіаційних технологій.

Частина 2: Стратегії зменшення впливу авіації

2.1 Використання біопалива

Один зі способів зменшення впливу авіації на навколишнє середовище - це використання біопалива. Воно може бути виготовлене з відновлюваних

джерел, таких як біомаса або водорості, і має менший викид шкідливих речовин. Відомо що виробництво біопалива дорожче ніж звичайного, як мінімум через складність виробництва та недостатність інфраструктури для цього. З розвиткому часу, відкривається все більше компаній які можуть виробляти біопаливо, це може спричинини конкурченцію на ринку, а з цим ціни на біопаливо будуть ставати меншими.

Використання біопалива це в першу чергу – зниження вуглецевого сліду, так як фосильні палива випускають більше вуглекислого газу.

Найпопулярнішим видом біопалива є біоетанол, який виробляється переважно з кукурудзи та цукрової тростини. Цей вид біопалива використовується в багатьох країнах як альтернатива або доповнення до традиційного бензину, часто у вигляді бензинових сумішей. Біоетанол вважається екологічно чистішим, оскільки він виробляється з відновлюваних ресурсів. На таблиці (Малюнок 3) можна спостерігати, що загальна тенденція виробництва спирту в тому числі й біоетанолу зростає.

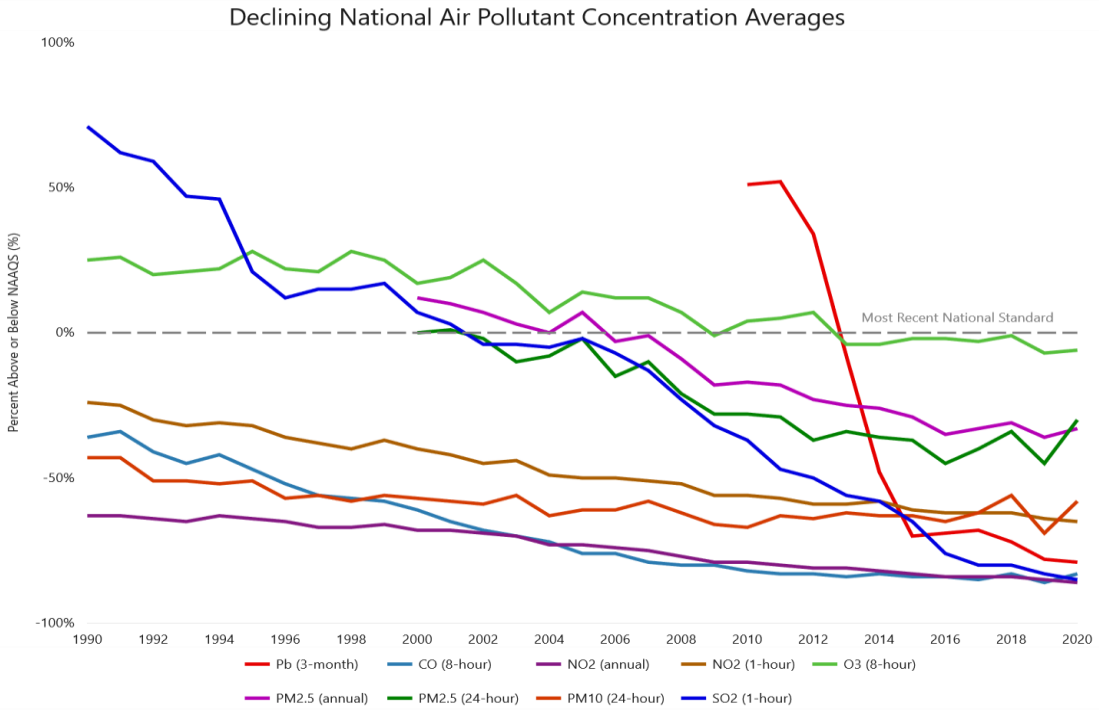
Рисунок 3

Виробництво спирту в світі, по країнам (в млн. галонів)								
Країна	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**2021**
США	14313	14807	15413	15936	16091	15778	13941	15015
Бразилія	6190	7093	6840	6730	8060	8860	8100	7430
ЄС	1445	1387	1190	1250	1300	1350	1280	1350
Китай	635	813	730	850	810	1010	930	860
Канада	510	436	460	460	460	497	429	434
Інші країни	1490	1147	1417	1544	1819	1835	1790	2181
Світ	**24583**	**25683**	**26050**	**26770**	**28540**	**29330**	**26470**	**27270**

2.2 Вдосконалення технологій

Сучасні авіаційні технології постійно вдосконалюються для зменшення викидів. Використання більш ефективних двигунів та аеродинамічних розрахунків дозволяє зменшити споживання пального та викиди забруднюючих речовин.

Рисунок 4



На цьому графіку (Малюнок 4) ми можемо побачити показники викидів з 1990 року по 2020 рік. Наприклад, викиди оксиду вуглецю (CO) знизилися на 70%, аміаку (NH_3) - на 8%, оксидів азоту (NO_x) - на 68%, прямого твердого частинкового забруднення 2.5 мікронів (PM 2.5) - на 38%, прямого твердого частинкового забруднення 10 мікронів (PM_{10}) - на 31%, двоокису сірки (SO_2) - на 92% та летких органічних сполук (VOC) - на 48%. Крім того, з 1990 по 2017 рік викиди токсичних повітряних забруднювачів знизилися на цілих 74%, що було забезпечено за рахунок впровадження як федеральних так і штатних регуляцій щодо стаціонарних та пересувних джерел забруднення, а також технологічних досягнень американських інноваторів

2.3 Зменшення числа рейсів

Один зі способів зменшити вплив авіації на навколишнє середовище - це зменшити кількість надлишкових рейсів. Ефективне планування маршрутів та зменшення надмірної активності можуть допомогти зменшити викиди.

2.4 Розвиток альтернативних видів транспорту

Розвиток альтернативних видів транспорту є ключовим елементом в стратегії зменшення викидів забруднюючих речовин від авіаційного транспорту. Збільшення ефективності та доступності інших видів транспорту, таких як залізниця та водний транспорт, може зменшити необхідність у користуванні авіацією для деяких маршрутів.

Роль Залізничного та Водного Транспорту:

Залізничний Транспорт: Залізниця є одним із найбільш екологічно чистих видів транспорту, особливо коли вона працює на електричній тязі. Висока швидкість та ефективність залізничного транспорту роблять його конкурентоспроможним вибором для середніх та довгих дистанцій.

Водний Транспорт: Хоча водний транспорт не є швидким, він може бути ефективним для перевезення великих вантажів, що може зменшити навантаження на авіаційний та автомобільний транспорт.

Інновації та Технологічний Прогрес

Інновації у галузі транспортних технологій, такі як розвиток високошвидкісних залізниць та покращення ефективності судноплавства, відіграють важливу роль у зменшенні залежності від авіації. Такі проекти як гіперлуп та електричні пороми також відкривають нові можливості для екологічно чистішого та ефективнішого пересування.

Переваги та Виклики

Розвиток альтернативних видів транспорту може зменшити загальний викид вуглекислого газу та інших парникових газів. Водночас, існують виклики, такі як високі витрати на інфраструктуру, необхідність узгодження

транспортних систем, та потреба в інвестиціях для розвитку нових технологій.

Розвиток альтернативних видів транспорту є важливою частиною глобальних зусиль із зменшення впливу транспорту на навколишнє середовище. Це не лише зменшує залежність від авіаційного транспорту, але й сприяє створенню більш сталої та ефективної транспортної інфраструктури.

Частина 3: Міжнародні стандарти та регулювання

Міжнародні організації, такі як Міжнародна організація цивільної авіації (МАУ), розробляють стандарти та рекомендації для зменшення впливу авіації на навколишнє середовище. Регулювальні органи встановлюють ліміти на викиди та стандарти безпеки, що спрямовані на зменшення негативного впливу.

В контексті охорони навколишнього середовища в авіації, міжнародні стандарти та регулювання відіграють ключову роль у зменшенні негативного впливу авіаційної індустрії на природу. Міжнародні організації, такі як Міжнародна організація цивільної авіації (ICAO) та Європейське агентство з безпеки польотів (EASA), розробляють стандарти, рекомендації та регуляції, спрямовані на мінімізацію впливу авіаційної галузі на довкілля.

Основні напрямки регулювання включають обмеження викидів шкідливих речовин, зокрема парникових газів, регулювання використання біопалива, впровадження новітніх технологій для зменшення викидів, а також розвиток альтернативних видів транспорту, що можуть замінити авіаційні перевезення на деяких маршрутах.

Регуляції та стандарти, розроблені цими організаціями, охоплюють широкий спектр аспектів – від технічних характеристик літаків та їх двигунів до

операційних процедур, які забезпечують ефективність польотів та зменшують надмірне навантаження на атмосферу.

З огляду на глобальний характер авіаційної індустрії, міжнародні стандарти та регулювання є важливими інструментами у забезпеченні єдиного підходу до охорони навколишнього середовища. Вони дозволяють синхронізувати зусилля різних країн та компаній для досягнення спільної мети – зменшення впливу авіації на довкілля.

Висновок до розділу 4:

Охорона навколишнього середовища в авіації стає все більш важливою проблемою. Незважаючи на вигоди, які надає авіація, необхідно приділяти належну увагу зменшенню її негативного впливу на природу. Використання біопалива, вдосконалення технологій, зменшення кількості надлишкових рейсів та дотримання міжнародних стандартів можуть сприяти збереженню навколишнього середовища для майбутніх поколінь.

ВИСНОВКИ

Кваліфікаційна робота "Система управління інформаційною безпекою в ІТ компанії" здійснює всебічний аналіз важливості, викликів та стратегій впровадження систем управління інформаційною безпекою в ІТ сфері. Основна увага зосереджена на стандарті ISO/IEC 27001:2015, його ключових положеннях та методах адаптації до специфіки ІТ компаній. Робота розкриває роль СУІБ у захисті від кіберзагроз, а також важливість нормативної та законодавчої відповідності.

Проаналізовано, як СУІБ сприяє зниженню ризиків втрати, недоступності або викривлення інформації, в той час як забезпечує високий рівень довіри клієнтів та партнерів. Наголошено на необхідності комплексного підходу до управління інформаційною безпекою, включаючи регулярний моніторинг, аудити та оновлення системи для відповідності сучасним викликам та змінам у галузі.

Ключовою рекомендацією є впровадження наступних кроків: визначення області застосування СУІБ, ідентифікація та оцінка ризиків, реалізація відповідних заходів безпеки, постійний моніторинг та вдосконалення системи. Висвітлено важливість інтеграції СУІБ з загальною стратегією компанії, що включає навчання співробітників, ефективне управління ресурсами та розвиток корпоративної культури, заснованої на принципах інформаційної безпеки.

Окрім зосередження на важливості СУІБ та її інтеграції в загальну структуру ІТ компанії, значну увагу у цій кваліфікаційній роботі приділено розробці конкретної програми управління інформаційною безпекою. Важливим аспектом є розробка програмного забезпечення, що може автоматизувати та оптимізувати процеси оцінки ризиків, моніторингу безпеки та відповідності нормативам. Така програма може включати модулі для ідентифікації та аналізу ризиків, контролю заходів безпеки, ведення

документації та звітності, а також інструменти для регулярного аудиту та оцінки ефективності впроваджених процедур.

Розробка такої програми передбачає тісну співпрацю між ІТ фахівцями, фахівцями з інформаційної безпеки та керівництвом компанії. Це дозволить забезпечити, що програма не лише відповідає технічним вимогам, але й ефективно інтегрується в бізнес-процеси, сприяючи підвищенню загальної безпеки та продуктивності організації.

Таким чином, розробка програми управління інформаційною безпекою є критично важливим елементом у підвищенні рівня захисту інформаційних активів ІТ компанії. Це не лише допомагає уникнути потенційних кіберзагроз, але й забезпечує зростання довіри з боку клієнтів та партнерів, що є невід'ємною частиною успіху в сучасному цифровому світі.

У підсумку, робота підкреслює, що успішне впровадження та управління СУІБ є ключовим фактором у забезпеченні стабільності, безпеки та конкурентоспроможності ІТ компаній у сучасному цифровому світі.

СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

1. Петренко, А. І., & Литвинова, С. І. (2017). “Сучасні методи та засоби захисту інформації в інформаційних системах.” Київ: Наукова думка.
2. ISO/IEC 27001:2015. “Information technology — Security techniques — Information security management systems — Requirements.” International Organization for Standardization.
3. Calder, A. & Watkins, S. (2016). “IT Governance: An International Guide to Data Security and ISO27001/ISO27002.” Kogan Page.
4. Кравчук, В. А. (2018). “Основи кібербезпеки.” Львів: Видавництво Національного університету "Львівська політехніка".
5. Krutz, R. L., & Vines, R. D. (2010). “The CISSP Prep Guide: Mastering the Ten Domains of Computer Security.” Wiley.
6. Swanson, M., & Guttman, B. (1996). “Generally Accepted Principles and Practices for Securing Information Technology Systems.” National Institute of Standards and Technology.
7. Кравчук, В. А. (2018). “Основи кібербезпеки.” Львів: Видавництво Національного університету "Львівська політехніка
8. Мельник, О. М., & Кузьмін, О. Є. (2019). “Інформаційна безпека в системах управління.” Харків: ХНУ імені В. Н. Каразіна.
9. Clarke, R. & Kumar, R. (2019). “Cyber-Security Threats in Aviation: A Management Perspective.” Aeronautics and Aerospace Open Access Journal.
10. Федоров, М. І., & Кузьмін, О. В. (2018). “Проблеми кібербезпеки в сучасній авіації.” Журнал "Авіаційна техніка".
11. Strohmeier, M., Lenders, V., & Martinovic, I. (2017). “On the Security of the Automatic Dependent Surveillance-Broadcast Protocol.” IEEE Communications Surveys & Tutorials.

12. Білинський, Ю. І., & Петров, В. О. (2020). “Кіберзахист авіаційних інформаційних систем.” Науковий вісник Національного авіаційного університету.

Додатки

Додаток А ОЦІНКА ЕФЕКТИВНОСТІ МАСЛЯНОЇ ДІЇ ОЛИВ З КАРБОНОФТОРИДНИМИ ПРИСАДКАМИ ПРИ НЕСТАЦІОНАРНИХ РЕЖИМАХ ТЕРТТЯ

УДК 621.831.004.55

В. Б. МЕЛЬНИК, Р. Г. МНАЦАКАНОВ, Д. В. ЛЕУСЕНКО, Б. М. МАМАЙ

Національний авіаційний університет, Україна

ОЦІНКА ЕФЕКТИВНОСТІ МАСЛЯНОЇ ДІЇ ОЛИВ З КАРБОНОФТОРИДНИМИ ПРИСАДКАМИ ПРИ НЕСТАЦІОНАРНИХ РЕЖИМАХ ТЕРТТЯ

Викладено результати дослідження впливу карбонофторидних присадок на мастильну дію авіаційних олив ВНІІНП-50-1-4у, ІПМ-10; МС-8п, індустріальних олив І-20А, ІГП-18 та автомобільної оливи М-10$Г_2$К при нестаціонарних режимах тертя. Введення присадки КФ у мастильні середовища значно зменшує, а в окремих випадках повністю усуває тимчасове погіршання мастильної дії при нестаціонарних режимах за рахунок високих адсорбційних властивостей та хімічної активності карбонофторидів За допомогою розробленої програми визначено області найбільш ефективного використання олив з КФ-присадками за інтегрованим показником ефективності масляної дії.

Ключові слова: *ефективність масляної дії, карбонофторидні присадки, оливи, нестаціонарний режим тертя, тимчасове погіршення мастильної дії (ТПМД), товщина мастильного шару,інтегрований показник.*

Постановка проблеми. Нестаціонарні режими роботи значно впливають на працездатність і економічність пар тертя. Загальновідомо, що нестаціонарні режими викликають найбільше зношування [1;2], проте здатність мастильних середовищ протистояти цьому поки що не оцінюється,

невідомо навіть чи пов'язано збільшення зносу з властивостями мастильного середовища, чи можна вибором мастильних середовищ його зменшити.

Як встановлено проведеними дослідженнями, однією з основних причин підвищеного зносу при нестаціонарному режимі є тимчасове погіршення мастильної дії (ТПМД), викликане зміною граничних процесів, що протікають - руйнуванням спочатку сформованих фізично адсорбованих і формуванням більш стійких хемосорбційних шарів [3; 4]. Подібний ефект зменшення кількості адсорбованого на поверхні матеріалу за нестаціонарних умов встановлений дослідженнями з фізико-хімії твердого тіла [5; 6].

Експерименти показали, що зростання за нестаціонарних умов тертя інтенсивності зношування корелює з інтенсивністю ТПМД. Небезпека ТПМД (у деяких випадках може призвести до пошкодження вузла тертя) визначається видом нестаціонарності, показниками режиму роботи та найбільшою мірою властивостями мастильних середовищ.

Розроблено метод оцінювання ТПМД за результатами вимірювання товщини мастильного шару. Метод заснований на тому, що змащувальні властивості рідких середовищ при нестаціонарних умовах визначаються ступенем тимчасового зменшення товщини мастильного шару і тривалістю цього зменшення [7].

Великий вплив на ТПМД, крім вуглеводневого складу олив, надають присадки. Присадки можуть як згладжувати ТПМД, так і посилювати його. Тому правильний підбір присадок для олив, що працюють у нестаціонарних умовах, має винятково важливе значення.

Особливу увагу останнім часом викликають фторвуглецеві сполуки (карбонофторид, фторований вуглець, фторграфіт, полімонофторид вуглецю) як ефективні присадки до мастильних середовищ, здатні модифікувати поверхні пар тертя з метою підвищення їх антифрикційних та протизносних властивостей. Відповідно до сучасних уявлень [8; 9; 10; 11] частинки карбонофторидів (КФ) утворюються в результаті хімічної реакції графіту і

вільного фтору при температурі 420 °С, мають кристалічну структуру, що утворюється рівноважними шарами атомів вуглецю і фтору, який розташований між вуглецевими шарами і пов'язаний з атомами вуглецю ковалентними зв'язками. Відстань між атомами вуглецю С - С становить 1,41-1,47Å, міжшарову відстань - 5,7 - 11,2Å, граничне насичення фтором (у масових частках) досягає 66,6%, температура розкладання Тразл = 583 ... 753 °К, щільність ρ = 2,35…2,68·103 кг/м3. Оптимальні за розмірами частинки порядку 10 ... 100 шарів, а в стані поставки частинки більше 50 ... 100 мкм, при цьому КФ, що поставляється хімічно інертний, так як, енергія зв'язку С-F дуже висока (500 кДж / моль), внаслідок чого частинки пасивуються при приєднання частинок середовища та газів. У зоні тертя відбувається диспергування КФ із утворенням активних радикалів здатних вступити у міцний хімічний зв'язок з атомами металу на поверхні тертя.

Модифікація поверхонь тертя за допомогою КФ-присадок має ряд переваг у порівнянні з відомими:

– при взаємодії з металами (CFx)n забезпечує утворення зв'язків металевого типу, що зміцнює матеріал поверхневого шару;

– модифікований (CFx)n шар матеріалу має велику термостійкість у порівнянні з модифікацією іншими матеріалами, у тому числі органічними;

– при терті протікають активні трибохімічні реакції за участю фтору, який пригнічує дію кисню.

Методика дослідження. Дослідження впливу КФ-присадок на мастильну дію масляних середовищ при нестаціонарних режимах тертя виконувалося в умовах лінійного локального контакту при коченні з просковзанням циліндричних зразків на модернізованій машині тертя СМЦ-1, що дозволяє багаторазово проводити запуск, роботу з постійною частотою та гальмування за заданими параметрами - навантаження, швидкості та часу кожного циклу [12].

Умови випробувань моделювали умови зачеплення зубів зубчастих передач. Під час випробувань реєструвалися: – частота обертання; пусковий і встановлений момент тертя; товщина мастильного шару після виходу на частоту обертання, що встановилася (сумарна товщина гідродинамічної та граничної складових мастильного шару); товщина мастильного шару на стоянці (товщина твердоподібних самогенеруючих органічних плівок СОП) [13]; температура середовища.

Випробовувалися такі мастильні середовища:

- авіаційні оливи ВНІІНП-50-1-4у; ІПМ-10; МС-8п;

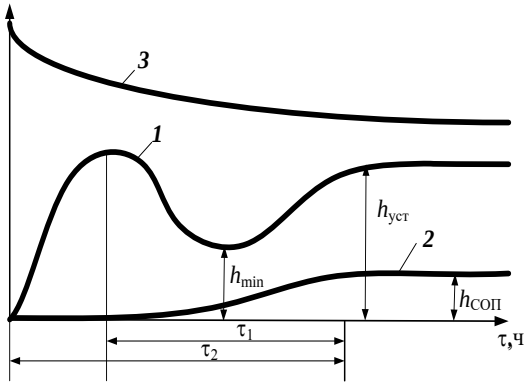
- індустріальні оливи І-20А; ІДП-18;

- автомобільне масло М-10$Г_2$К.

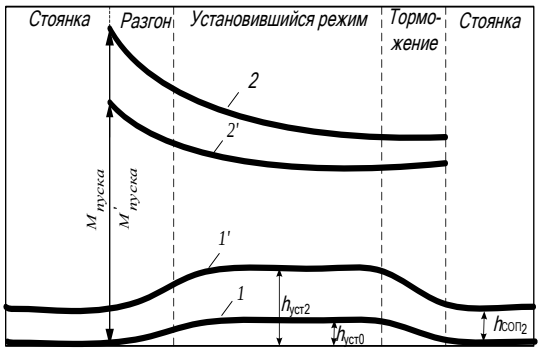
Мастильні середовища випробовувалися в однаковому нестаціонарному режимі (пуски-зупинки), без присадок та з присадками карбонофторидів (ТУ 6:-02-2-859-85) у концентрації: 0,125; 0,25; 0,5; 1% (масових часток). Обсяг випробуваного середовища – 100 мл.

Умови випробувань: контактна напруга – 700 МПа, прослизання – 20 %, сумарна швидкість кочення – 4,23 м/с, матеріал роликів – ст. 40Х, твердість HRC 30 - 32, шорсткість Ra - 0,3 мкм. Режим нестаціонарності: розгін до заданої швидкості (4,23 м/с) протягом 3 с, робота з постійною швидкістю – 10 с, гальмування – 3 с, стоянка – 5 с. Цикли розгін - встановлений режим - гальмування - стоянка слідують один за одним без перерви протягом 2 год.

На Мал. 1 показані типові криві зміни сумарної товщини мастильного шару (крива 1), товщини самогенеруючої органічної плівки (крива 2) та моменту тертя (крива 3) за нестаціонарних умов за весь час експерименту. На Мал. 2 представлені осцилограми зміни цих параметрів за один цикл на початку експерименту і після припрацювання.



Мал. 1. Типові криві зміни в часі сумарної товщини мастильного шару (1), товщини самогенеруючої органічної плівки (2) та моменту тертя (3) за нестаціонарних умов [18]



Мал. 2. Осцилограми зміни моменту тертя (2), та сумарної товщини мастильного шару (1) 1,2 - олива без КФ-присадок; $1^1 2^1$ - олива з КФ-присадками [18]

Як основні критерії оцінки ефективності мастильної дії при нестаціонарних умовах тертя запропоновані:

τ_1 - тривалість зменшення товщини мастильного шару при ТПМД;

h_{min} - мінімальна товщина мастильного шару при ТПМД;

$h_{уст}$ - товщина мастильного шару, що встановилася після приробітку;

$h_{соп}$ – товщина твердоподібних СОП;

τ_2 – час до стабілізації параметрів тертя (час припрацювання);

f_n – коефіцієнт тертя при запуску;

f_1 – коефіцієнт тертя, що встановився;

ΔТ – збільшення температури мастильного середовища; І - знос.

Результати дослідження наведено в таблиці 1.

Таблиця 1.

Вплив концентрації КФ-присадок на основні показники мастильної дії при нестаціонарних режимах тертя [18]

Масло	Концентрация КФ, %	Основні показники мастильної дії									Інтегрований показник ефективності масляної дії ***Q***
		τ_1, мин.	τ_2, мин.	h_{min}, мкм.	$h_{уст.}$, мкм.	$h_{соп.}$, мкм.	$f_п$	$f_{уст.}$	ΔT, °С	И, мкм.	
ВНИИ НП 50-1-4у	0	55	90	0,7	0,95	0,3	0,38	0,22	22	2,5	169
	0,1	45	90	0,65	0,85	0,12	0,38	0,22	20	2,8	157
	0,25	30	35	0,8	0,9	0,15	0,33	0,17	12	0,75	77
	0,5	30	50	0,85	0,95	0,475	0,31	0,18	14	0,47	94
	1	40	100	0,9	1	0,25	0,37	0,23	15	0,65	156
ПМ-10	0	20	70	1,2	1,25	0,41	0,41	0,26	16	0,69	108
	0,1	30	40	0,8	0,9	0,45	0,34	0,15	12	0,8	82
	0,25	50	60	0,7	0,9	0,56	0,38	0,21	11	0,75	121
	0,5	20	30	0,85	0,9	0,65	0,34	0,19	16	1,74	67
	1	30	85	0,8	0,85	0,45	0,34	0,19	13	1,1	129
МС-8п	0	5	20	1,05	1,4	0,71	0,36	0,23	21	1,28	49
	0,1	50	60	0,85	1,1	0,64	0,34	0,21	22	1,2	134
	0,25	20	30	0,9	1,15	0,64	0,33	0,2	20	0,75	71
	0,5	10	30	0,9	1,2	0,62	0,32	0,2	21	1	63
	1	10	30	0,75	1,2	0,51	0,32	0,2	18	0,9	59
И-20А	0	90	90	0,4	1	0,25	0,32	0,19	21	1,44	203
	0,1	20	85	0,9	1	0,07	0,32	0,19	16	0,34	122
	0,25	50	85	0,9	0,95	0,25	0,34	0,2	15	1	151
	0,5	45	55	0,25	0,55	0,08	0,36	0,2	17	0,4	117
	1	20	20	0,25	0,6	0,08	0,33	0,2	15	1,31	56
ИГП-18	0	10	110	0,8	1	0,1	0,32	0,2	17	0,65	138
	0,1	15	80	0,55	0,65	0,05	0,32	0,2	23	0,7	118
	0,25	-	5	0,65	0,65	0,45	0,32	0,2	21	0,85	26
	0,5	15	30	0,65	0,75	0,05	0,33	0,17	21	0,6	66
	1	-	10	0,65	0,6	0,05	0,31	0,2	22	0,75	32
М-10Г К	0	25	50	0,45	0,55	0,05	0,33	0,17	23	0,4	98
	0,1	20	50	0,65	0,95	0,28	0,34	0,15	18	0,42	88
	0,25	20	40	1	1,05	0,15	0,31	0,17	21	0,43	83
	0,5	20	85	0,9	1,1	0,125	0,35	0,19	22	0,56	123
	1	20	40	0,85	1,05	0,08	0,341	0.18	22	0,44	83

Розрахунок кількісного показника ефективності мастильної дії олив з карбонофторидними присадками при нестаціонарних режимах тертя проводився за Формулою (1):

Формула (1)

$$Q = \sum_{i=1}^{n} \sum_{k=1}^{m} v_{ik} * P_{ik}$$

де *vік* - ваговий коефіцієнт показника, що відображає його важливість;

Рік – одиничні показники, які забезпечують якість (кожний з вказаних показників оцінюється за 5-бальною шкалою);

n – кількість груп показників;

m – кількість одиничних показників у кожній групі.

Комплекс показників ефективності мастильної дії 6 олив карбонофторидними присадками 5 різних концентрацій при нестаціонарних режимах тертя за 9 групами показників якості і 45 одиничними показниками зформовано у вигляді матриці.

$$P := \begin{pmatrix} P_{11} & P_{12} & P_{13} & P_{14} & P_{15} & P_{16} & P_{17} & P_{18} & P_{19} \\ P_{21} & P_{22} & P_{23} & P_{24} & P_{25} & P_{26} & P_{27} & P_{28} & P_{29} \\ P_{31} & P_{32} & P_{33} & P_{34} & P_{35} & P_{36} & P_{37} & P_{38} & P_{39} \\ P_{41} & P_{42} & P_{43} & P_{44} & P_{45} & P_{46} & P_{47} & P_{48} & P_{49} \\ P_{51} & P_{52} & P_{53} & P_{54} & P_{55} & P_{56} & P_{57} & P_{58} & P_{59} \end{pmatrix}$$

Мал 3. Матриця показників якості

V – ваговий коефіцієнт взято від 1 до 5. (Таблиця 2)

Таблиця 2.

Ваговий коєфіцієнт

Ваговий коєфіцієнт	Вагомість
1	Надзвичайно важливо
2	Дуже важливо
3	Важливо
4	З помірною важливістю
5	Мало важливо

Розробка програми

В цій програмі описано:

1. MatrixA1, MatrixA2, MatrixA3, MatrixA4, MatrixA5, MatrixA6 – основні оціночні показники мастильної дії згідно Таблиці 1, де:

- матриця MatrixA1 заповнена данними оливи ВНИИ НП 50-1-4у
- матриця MatrixA2 заповнена данними оливи ІПМ-10
- матриця MatrixA3 заповнена данними оливи МС-8п
- матриця MatrixA4 заповнена данними оливи І-20А

- матриця MatrixA5 заповнена данними оливи ІГП-18
- матриця MatrixA6 заповнена данними оливи М-10$Г_2$ К

2. MatrixA1_1, MatrixA2_2, MatrixA3_3, MatrixA4_4, MatrixA5_5, MatrixA6_6 – ваговий коефіцієнт, який в нашому випадку заданий як одиниця і однаковий для всіх показників.

3. За Формулою 1, проведено розрахунки кількісних показників кожного коефіцієнту концентрації присадки (0%, 0.1%, 0.25%, 0.5%, 1%). Де значеня P_{ik} взяте з матриць: MatrixA1, MatrixA2, MatrixA3, MatrixA4, MatrixA5, MatrixA6, а значення vik з матриць: MatrixA1_1, MatrixA2_2, MatrixA3_3, MatrixA4_4, MatrixA5_5, MatrixA6_6 відповідно.

4. Після опрацювання результатів дослідження за цією програмою ми отримуємо інтегрований показник ефективності масляної дії Q (Таблиця 1).

Результати дослідження. Аналіз результатів випробувань шести марок масел, наведених у таблиці, показує, що ефективність впливу КФ-присадок на мастильну дію при нестаціонарних умовах тертя залежить від базового мастильного середовища і концентрації присадки, що вводиться.

Так, наприклад, високоякісні авіаційні масла МС-8п і ІПМ-10, що володіють гарною мастильною дією на встановленому режимі, добре працювали і при нестаціонарних умовах: при ТПМД товщина мастильного шару не зменшувалася нижче 1мкм і протягом усього експерименту інтенсивно утворювалися СОП (товщина СОП 0,71 і 041 мкм відповідно).

Застосування КФ-присадок у цих оліях неефективне, а при деяких концентраціях може призвести до погіршення основних показників дії мастила.

Введення в мастильний матеріал присадки КФ призводить, під впливом тих же умов контакту, до утворення фази FeF в поверхневому шарі металу і хемосорбованих шарів CF_2 і CF_3 на поверхнях тертя. Експерименти показали, що ці хемосорбовані плівки, як і СОП, мають високі протизносні

характеристики [13; 17].

З шести випробуваних мастил найбільш інтенсивно утворювали СОП авіаційні масла МС-8П,

ІПМ-10, ВНДІ НП-50-1-4У (товщина СОП - 0,71; 0,41; 0,3 мкм відповідно). Ці масла при нестаціонарному режимі тертя показали найменшу величину ТПМД (мінімальна товщина шару – 1,05; 1,0; 0,7 мкм). Індустріальні олії І-20А, ІГП-18 та автомобільна олія М-10$Г_2$К значно гірше утворювали СОП (товщина відповідно – 0,25; 0,1 та 0,05 мкм).

Введення присадок КФ у випробувані за даних режимах авіаційні оливи не призвело до відчутного поліпшення мастильної дії. При введенні цих присадок навіть у малій концентрації в оливі І-20А, ИГП-18, М-10Г2К змащувальна дія покращувалася. Наприклад, якщо масова частка присадки КФ становить 0,125% маслі М-10$Г_2$К товщина твердоподібної плівки зростає в 3 рази, а мінімальна товщина шару при ТПМД збільшується з 0,45 до 0,65 мкм.

Висновки: За розробленими критеріями оцінено ефективність мастильної дії шести марок масел з КФ-присадками при нестаціонарних режимах тертя. Ефективність застосування КФ-присадок залежить від властивостей базової олії та їх концентрації. Для випробуваних масел різного складу та призначення оптимальна масова частка присадки становила 0,25 – 0,5 %.У зв'язку з тим, що компоненти масел можуть конкурувати з КФ-присадками та перешкоджати утворенню ними твердоподібних плівок, доцільно застосовувати КФ-присадки в умовах слабкого утворення СОП.

Введення присадки КФ у мастильні середовища значно зменшує, а в окремих випадках повністю усуває ТПМД при нестаціонарних режимах за рахунок високих адсорбційних властивостей та хімічної активності карбонофторидів. Розроблена програма оцінки ефективності масляної дії олив з карбонофторидними присадками при нестаціонарних режимах терття за інтегрованим показником ефективності масляної дії Q є дієвим

інструментом для визначення областей для поліпшень та для відстеження ефективності масляної дії олив з присадками при нестаціонарних режимах терття

Список літератури

1. *Канарчук Е. А., Канарчук В. Е.* Влияние режимов работы на износ двигателей внутреннего сгорания. К.: Наук. думка, 1970. – 312 с.

2. *Калиновский М., Недель Р*. Пусковой износ двигателей // Автомоб. пром-ть США. – Т.128, №4. – 1963. – С. 2 – 4.

3. *Райко М. В., Мнацаканов Р. Г., Дмитриченко Н. Ф., Мельник В. Б.* Смазочное действие и изнашивание в условиях часто повторяющихся пусков // Механизация и электрификация сельского хозяйства». – К., Урожай, 1985. – Вып. 61. – С. 78 – 82.

4. *Райко М. В., Мнацаканов Р. Г., Мельник В. Б*. Повышение работоспособности узлов трения с локальным контактом при неустановившихся режимах работы путем оптимизации процессов смазочного действия. // Всесоюз. науч.-техн. конф. «Обеспечение надежности узлов трения машин»: Тезисы докл. (Ворошиловград, 1988), – Ворошиловград: Ворошиловоград-ский машиностроительный ин-т – 71 с.

5. *Адам Н. К.* Физика и химия поверхностей. ОГИЗ, – М.: Гостехиздат, 1947. – 552 с.

6. *Моррисон* С. Химическая физика поверхности твердого тела: М.: Мир, 1980. – 488 с.

7. *А. с. СССР №1536263*. Способ оценки смазывающих свойств смазочных материалов для пары трения / Р. Г. Мнацаканов, М. В. Райко, В. Б. Мельник и др. – Заявл. 29.02.88; Опубл. 15.01.90, БИ№2. – 4 с.

8. *Fusaro R. L., Sliney H. E.* Graphite fluoride (CFx)n a new solid lubricant. ASLE Transactions, 1970. V.13. – P. 56 – 65.

9. *Gisser H., Petronio M., Shapiro A*, Graphite fluoride as a solid lubricant. Lubrication Enginering, 1972. V.28. – №5. – P. 161 – 164.

10. *Повышение* долговечности узлов трения путем применения карбонофторидов. / Н. Д. Кузнецов, Д. Г. Громаковский, Л. И. Куксенова, и др. // Вестн. машиностроения, 1987. – №8. – С. 13 – 16.

11. *Мельник В. Б., Громаковский Д. Г., Білякович О. М.* Механізм мастильної дії карбонофторидних присадок // Міжнар. НТК «Вдосконалення конструктивних та експлуатаційних параметрів автомобілів і машин», (Київ, 1995): Тези доп. – К.: Транспортна академія України – 95 с.

12. *Райко М. В., Мнацаканов Р. Г., Дмитриченко Н. Ф.* Установка для исследования процесов трения, изнашивания и смазки при запуске и остановке // Совершенствование ремонта авиацион-ной техники. – К.: КИИГА, 1983. – С. 37 – 39.

13. *А. с. СССР №1718031.* Способ оценки смазывающих свойств масел / В. Б. Мельник, М. В. Райко, В. В. Тыркаев – Заявл. 05.02.90; Опубл. 07.03.92, БИ №9. – 3 с.

14. *Райко М. В.* Смазка зубчатых передач. – К.: Техніка, 1970. – 196 с.

15.Райко М. В. Исследование смазочного действия нефтяных масел в условиях работы зубчатых передач: Дис. ... д-ра техн. наук: 05.02.04. – К., КИИГА, 1974. – 369 с.

16. *Кадомский В. П.* Исследование смазочных слоев и твердо-пластичных пленок, образующихся в контакте деталей при качении со скольжением: Дис. ... канд. техн. наук: 05.02.04. – К., КИИГА, 1971. – 140 с.

17. *Atkinson I. B., Waghoxne R. M.* The Tribochemistry of Graphite Fluoride Studied Using XPS, Wear, 37, –1978. – P. 123 – 128.

18. Мельник В.Б. Смазочное действие масел с карбонофторидными присадками при нестационарных режимах трения /В.Б.Мельник, Р.Г.Мнацаканов, В.П.Федына // Проблеми терття та зношування. – 2007. - №47. С. 249-258.

Стаття надійшла до редакції 23.08.2023.

Мельник Володимир Борисович – канд. техн. наук, доцент, доцент кафедри прикладної механіки та інженерії матеріалів, Національного авіаційного університету, м. Київ Україна, nau12@ukr.net. https://orcid.org/0000-0003-4379-654X.

Мнацаканов Рудольф Георгійович – д. техн.наук, професор, професор кафедри підтримання льотної придатності повітряних суден, Національний авіаційний університет, пр. Любомира Гузара, 1, м.Київ,Україна, 03058, тел.:+38 044 406 76 70; Email: mnatsakanov@ukr.net https://orcid.org/0000-0001-5035-2432.

Леусенко Дар'я Володимирівна – аспірантка кафедри прикладної механіки та інженерії матеріалів, Національного авіаційного університету, м. Київ, nau12@ukr.net. https://orcid.org/0000-0001-8024-6104.

Мамай Богдан Миколайович – здобувач вищої освіти освінього ступеня магістр за спеціальністю 152 «Метрологія та інформаційно-вимірювальна техніка», освітньо-професійна програма «Якість, стандартизація та сертифікація» Національний авіаційний університет, пр. Любомира Гузара, 1, м.Київ,Україна, 03058, Email: b909mamay@gmail.com.

V. B. MELNYK, R. G. MNATSKANOV, D. V. LEUSENKO, B. M. MAMAI

EVALUATION OF THE EFFICIENCY OF THE LUBRICATION OF OILS WITH CARBONFLUORIDE ADDITIVES IN NON-STATIONARY FRICTION REGIMES

The results of the study of the effect of carbonofluoride additives on the lubricating effect of aviation oils VNIINP-50-1-4u, IPM-10 are presented; MS-8p, industrial oils I-20A, IGP-18 and automotive oil
M-10G2K in non-stationary friction modes. The introduction of KF additives into lubricating media significantly reduces, and in some cases completely eliminates, the temporary deterioration of the lubricating effect in non-stationary modes due to the high adsorption properties and chemical activity of carbonofluorides. Actions**Key words:** effectiveness of oil action, carbonofluoride additives, oils, non-stationary mode of friction, temporary deterioration of lubricating action (TPMD), thickness of the lubricating layer, integrated indicator.

References

1. Kanarchuk E. A., Kanarchuk V. E. Influence of work modes on wear of internal combustion engines. K.: Science. dumka, 1970. - 312 p.
2. Kalinovsky M., Nedel R. Starting wear of engines // Avtomob. industry of the USA. - Vol. 128, No. 4. - 1963. - P. 2 - 4.
3. Raiko M.V., Mnatsakanov R.G., Dmytrychenko N.F., Melnyk V.B. Lubricating action and wear in the conditions of frequently repeated starts // Mechanization and electrification of agriculture". - K., Urozhai, 1985. - Vol. 61. – P. 78 – 82.
4. Raiko M.V., Mnatsakanov R.G., Melnyk V.B. Increasing the performance of friction units with local contact under unstable operating modes by optimizing the processes of lubrication action. // All Union. scientific and technical conf. "Ensuring the reliability of friction units of machines": Theses add. (Voroshilovgrad, 1988), - Voroshilovgrad: Voroshilovgrad-sky mashinostroitelnyy in-t - 71 p.
5. Adam N.K. Physics and chemistry of surfaces. OGIZ, - M.: Gostekhizdat, 1947.

- 552 p.
6. Morrison S. Chemical physics of the surface of a solid body: Moscow: Mir, 1980. – 488 p.
7. A. p. USSR No. 1536263. A method of assessing the lubricating properties of lubricants for friction pairs / R. G. Mnatsakanov, M. V. Raiko, V. B. Melnyk, etc. - Appl. 29.02.88; Publ. 15.01.90, BI#2. - 4 s.
8. Fusaro R. L., Sliney H. E. Graphite fluoride (CFx)n a new solid lubricant. ASLE Transactions, 1970. V.13. - R. 56 - 65.
9. Gisser H., Petronio M., Shapiro A, Graphite fluoride as a solid lubricant. Lubrication Engineering, 1972. V.28. – #5. – P. 161 – 164.
10. .Increasing the durability of friction nodes by applying carbon fluorides. / N. D. Kuznetsov, D. G. Gromakovsky, L. I. Kuksenova, and others // Vestn. machine engineering, 1987. - No. 8. – P. 13 – 16.
11. Melnyk V.B., Gromakovsky D.G., Bilyakovich O.M. The mechanism of the lubricating effect of carbonofluoride additives // Interna. NTK "Improvement of structural and operational parameters of cars and machines", (Kyiv, 1995): Abstracts of add. - K.: Transport Academy of Ukraine - 95 p.
12. Raiko M.V., Mnatsakanov R.G., Dmytrychenko N.F. Installation for the study of friction, wear and lubrication processes during startup and shutdown // Improvement of aircraft repair. - K.: KIIGA, 1983. - P. 37 - 39.
13. A. p. USSR No. 1718031. A method of evaluating the lubricating properties of oils / V.B. Melnyk, M.V. Raiko, V.V. Tyrkaev - Appl. 05.02.90; Publ. 03/07/92, BI #9. - 3 s.
14. Raiko M.V. Lubrication of gears. - K.: Technika, 1970. - 196 p.
15. Rayko M. V. Lubricating action of petroleum oils in the conditions of gear work: Diss. ... Dr. Tech. Sciences: 05.02.04. - K., KIIGA, 1974. - 369 p.
16. Kadomskii V.P. Investigation of lubricating layers and hard-plastic films formed in the contact of parts during rolling with sliding: Diss. ... candidate technical Sciences: 05.02.04. - K., KIIGA, 1971. - 140 p.
17. Atkinson I. B., Waghoxne R. M. The Tribochemistry of Graphite Fluoride Studied Using XPS, Wear, 37, -1978. - R. 123 - 128.
18. Melnyk V.B. Lubricating effect of oils with carbonofluoride additives in non-stationary modes of friction / V. B. Melnyk, R. G. Mnatsakanov, V. P. Fedyna // Problems of friction and wear. – 2007. - No. 47. P. 249-258.
Melnyk Volodymyr Borysovych - candidate. technical of Sciences, Associate Professor, Associate Professor of the Department of Applied Mechanics and Materials Engineering, National Aviation University, Kyiv, Ukraine, nau12@ukr.net. https://orcid.org/0000-0003-4379-654X.
Mnatsakanov Rudolph Georgiyovych - Doctor of Technical Sciences, Professor, Professor of the Department of Aircraft Airworthiness Maintenance, National Aviation University, 1 Lubomyra Huzara Ave., Kyiv, Ukraine, 03058, phone: +38 044 406 76 70; Email: mnatsakanov@ukr.net https://orcid.org/0000-0001-5035-2432.
Darya Volodymyrivna Leusenko is a graduate student at the Department of Applied Mechanics and Materials Engineering, National Aviation University,

Kyiv, nau12@ukr.net. https://orcid.org/0000-0001-8024-6104.
Mamai Bohdan Mykolayovych - graduate of higher education with a master's degree in the specialty 152 "Metrology and information and measurement technology", educational and professional program "Quality, standardization and certification" National Aviation University, 1 Lubomyra Huzar Ave., Kyiv, Ukraine, 03058, Email: b909mamay@gmail.com.