

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ  
НАЦІОНАЛЬНЕ КОСМІЧНЕ АГЕНТСТВО УКРАЇНИ  
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ  
ДП «АНТОНОВ»



# МАТЕРІАЛИ

XII Міжнародної  
науково-технічної конференції  
“АВІА-2015”

28-29 квітня 2015 року

Київ 2015

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ  
НАЦІОНАЛЬНЕ КОСМІЧНЕ АГЕНТСТВО УКРАЇНИ  
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ  
ДП «АНТОНОВ»

# **МАТЕРІАЛИ**

**ХІІ МІЖНАРОДНОЇ  
НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ  
“АВІА-2015”**

**28-29 квітня 2015 року**

**КИЇВ 2015**

## ЗМІСТ

### Секція 1. Методи та засоби технічної та медичної діагностики

<i>М.О. Мельник, В.О. Катан, А.О. Кобернік</i> Аналіз сучасного стану розвитку датчиків, розроблених на базі оптичного волокна	1.1
<i>Г.В. Мартинюк, Н.Б. Марченко, Л.М. Щербак</i> Контроль роботи авіаційних агрегатів та механізмів на основі багатовимірного спектрального зображення вібраційних сигналів	1.5
<i>О.Б. Іванець, О.В. Діхтярук</i> Невизначеність результатів випробувань	1.9
<i>С.В. Ємельянов</i> Особливості використання метода виділення комбінаційних складових, пов'язаних з частотою обертів ротору, у сигналах віброакустичної активності роторних машин і механізмів	1.13
<i>М.А. Назарчук, О.Б. Іванець</i> Розробка системи контролю шкідливих речовин в процесі запуску аерокосмічних апаратів	1.17

### Секція 2. Інформаційна безпека

<i>В.М. Кінзерявий, О.М. Кінзерявий</i> Експериментальне дослідження методу шаблонного приховування даних в структуру векторних зображень	2.1
<i>В.А. Швець, Р.Д. Цигвинцев, Т.В. Мелешко</i> Экспериментальная адаптивная система защиты акустической информации	2.5
<i>К.П. Ануфрієнко, І.С. Грищенко, А.В. Савчин</i> Таксономія методів виявлення уразливостей міжсайтового скриптіngu та SQL-ін'єкції	2.9
<i>Ю.О. Дрейс</i> Модель аналізу і оцінки ризиків захисту персональних даних в державних автоматизованих системах	2.15
<i>В.Г. Кононович, І.В. Кононович, О.Ю. Кунянський</i> Динамічна модель системи інформаційної безпеки консолідованої інформації	2.17
<i>В.А. Швець, В.В. Васянович</i> Устранение недостатка ложного распознавания личности систем контроля и управления доступом	2.21
<i>А.І. Гізун, А.О. Корченко</i> Метод виявлення та ідентифікації інцидентів-потенційних кризових ситуацій	2.26



*Ю.О. Дрейс, к.т.н., доцент  
(Житомирський військовий інститут імені С.П. Корольова,  
Україна, м. Житомир)*

### **Модель аналізу і оцінки ризиків захисту персональних даних в державних автоматизованих системах**

*Розглянуто модель аналізу і оцінки ризиків захисту персональних даних під час їх обробки в державних автоматизованих системах з метою забезпечення їх конфіденційності і підвищення рівня захищеності інформації з обмеженим доступом.*

Посягання на персональні дані українців піднімають проблему відсутності адекватних гарантій захисту персональних даних (ПД). Тому розроблено базову модель аналізу і оцінки ризиків (АОР) захисту ПД в базах персональних даних (для етапу розробки політики безпеки при проектуванні комплексної системи захисту державних інформаційних ресурсів (КСЗІ), що створюється і обробляється прикладним програмним забезпеченням в державних автоматизованих системах (АС), з метою підвищення рівня захищеності персональної інформації, розголошення якої може надати шкоди як самому власнику, суспільству, так і державі у цілому.

Для побудови КСЗІ та інших систем безпеки необхідно проводити АОР. Існуючі засоби оцінки в переважній своїй більшості засновані на статистичних підходах. У багатьох країнах, як на рівні підприємств, так і на державному рівні подібна статистика не ведеться. Це обмежує можливості існуючих засобів, наприклад, щодо використання різних типів вхідних даних для оцінки. Для визначення типів вхідних, внутрішніх та вихідних параметрів, які використовуються для АОР проведено дослідження відповідних існуючих стандартів та методик аналізу і оцінювання ризиків [1] на основі яких розроблено модель аналізу і оцінки ризиків захисту ПД в державних АС.

Типовим порядком [2] не передбачається застосування засобів захисту ПД при її обробці у базах ПД в АС, що суперечить існуючим вимогам нормативно-правового забезпечення щодо умов обробки та захисту державних інформаційних ресурсів або інформації з обмеженим доступом (ІзОД) в системах. За даних обставин було розроблено загальну (базову) модель аналізу і оцінки ризиків захисту ПД у базах ПД (БПД)(на етапі розробки політики безпеки при проектуванні КСЗІ), що створюється і обробляється прикладним програмним забезпеченням в державних АС.

Інтегроване представлення параметрів ризику з відображенням на сферу захисту ПД здійснюється у вигляді конкретного кортежу. Кортеж параметрів ризику захисту ПД в АС можна представити у наступному вигляді:

$$\langle A, B, C, D, E, F, G, H, I \rangle,$$

де *A* – характеристика ПД (ідентифікація їх складу та змісту); *B* – характеристика середовища обробки БПД в АС; *C* – мета обробки ПД; *D* – аудит застосованих механізмів безпеки; *E* – характеристика існуючих функціональних послуг; *F* –

ідентифікація загроз захисту ПД при обробці БПД в АС;  $G$  – величина можливого збитку від витоку ПД (чи БПД в АС);  $H$  – АОР захисту ПД;  $I$  – керування ризиком та досягнення необхідного рівня гарантій захисту ПД.

Дана модель має стандартну типову структуру і реалізується виконанням 6 етапів (рис.1), в яких визначено набір базових параметрів для АОР захисту ПД у БПД, що обробляються в державних АС.

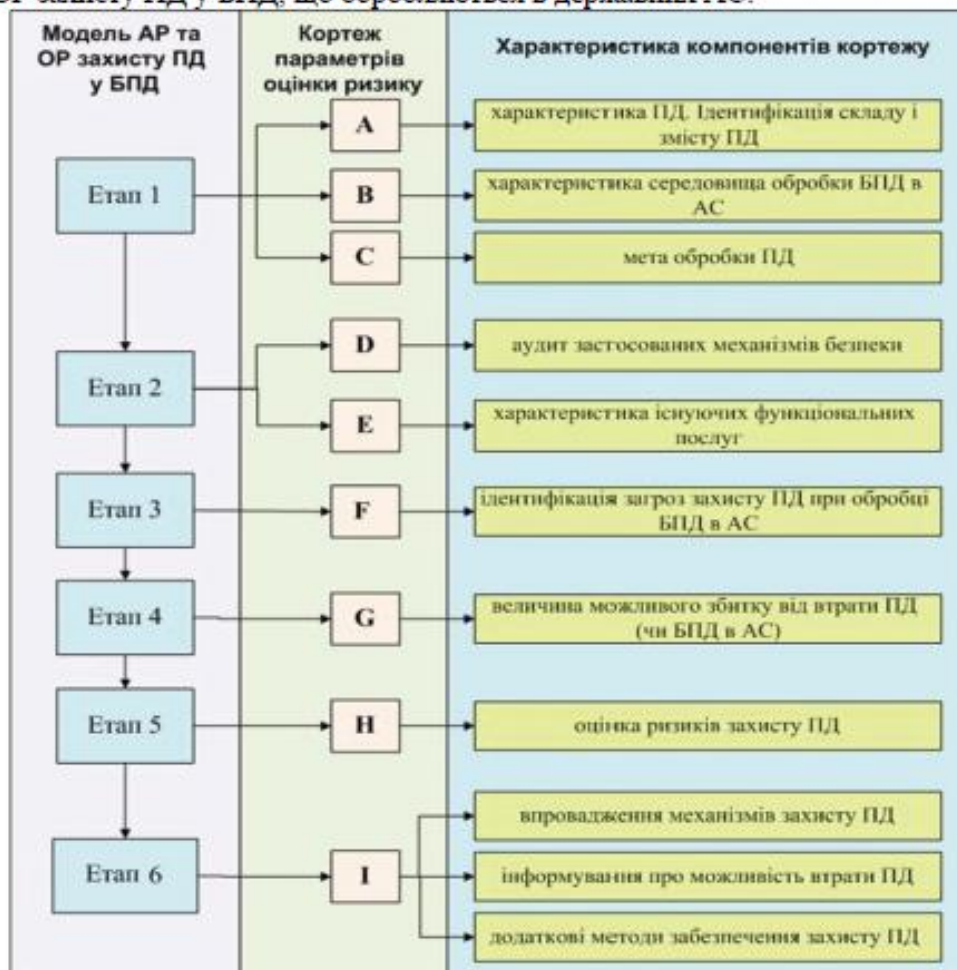


Рисунок 1 – Базова модель аналізу і оцінки ризиків захисту ПД в державних АС

**Висновки.** Так як ІзОД в АС повинні оброблятися із застосуванням КСЗІ і наразі відсутня встановлена методика оцінювання ризиків загроз до ПД в державних АС, то розроблена модель має місце на розвиток і застосування.

#### Список літератури

6. Анализ и оценивание рисков информационной безопасности: монография / [Корченко А.Г., Архипов А.Е., Казмирчук С.В.]. – К.: ООО «Лазурит-Полиграф», 2013. – 275с.

7. Про затвердження документів у сфері захисту персональних даних / Уповноважений ВР з прав людини; Наказ, Порядок, Форма типового документа [...] від 08.01.2014 № 1/02-14.