ДОДАТОК А СЛАЙДИ ПРЕЗЕНТАЦІЇ

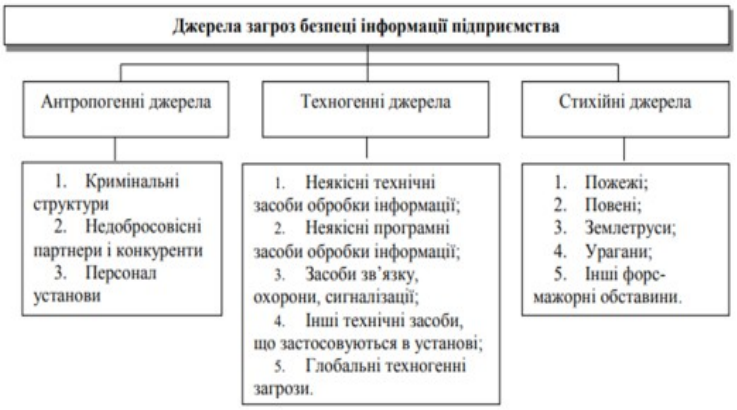
«Розрахунок ризиків інформаційної безпеки інфокомунікаційного підприємства»

Кваліфікаційна робота магістерки групи ІМІм-20-1

Спесівцевої Анастасії Сергіївни

Завдання на кваліфікаційну роботу

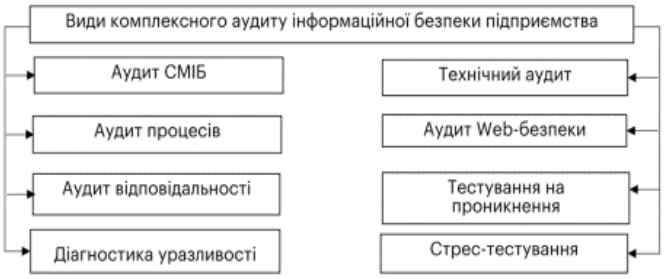
- *Визначити й оцінити ризики інформаційній безпеці для типової розподіленої мережі інфокомунікаційного підприємства.*
- *Головний акцент при забезпеченні інформаційної безпеки в інфокомунікаційній мережі, що досліджується, зробити на мінімізацію збитків від загроз, спрямованих на порушення цілісності й доступності програмно-апаратного комплексу інфокомунікаційної системи, а не на конфіденційність інфокомунікаційних ресурсів, які обробляються з їхньою допомогою.*
- *Розрахувати інформаційні ризики інформаційній безпеці, заснованій на виділенні цінних активів підприємства; ступеню потенційних збитків при реалізації загроз на такі активи; ймовірність реалізації загроз для даної інфокомунікаційної мережі підприємства.*



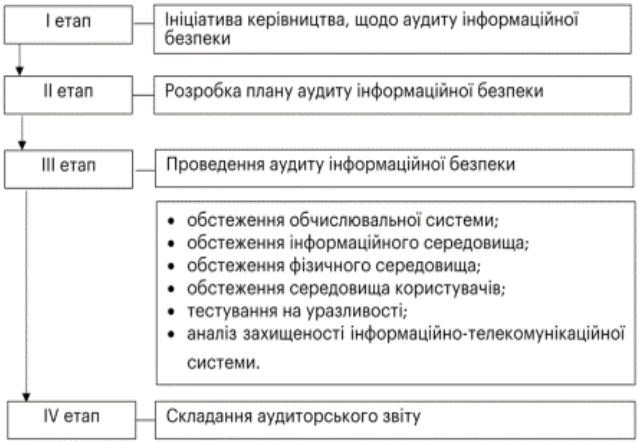
Головні елементи організації ІБ на підприємстві

N п/п	Елемент інформаційної безпеки	Захисні заходи
1	Виявлення вразливостей	Перелік інформаційних ресурсів, що підлягають захисту
2	Виявлення інформаційних ризиків	Визначення всіх можливих загроз для кожного ресурсу ІКМ
3	Оцінювання рівня загроз	Побудова шкали рівнів інформаційних ризиків для кожного ресурсу ІКМ на випадок кібератаки
4	Контроль управління доступом до інформаційних ресурсів	Сегментування ІКМ підприємства за категоріями доступу до конфіденційної інформації
5	Протидія інформаційним загрозам	Розробка СЗІ, що унеможливлює НСД до інформаційних ресурсів, які обробляють конфіденційну інформацію
6	Впровадження нових СЗІ	Сертифікація та контроль за дотриманням політики безпеки
7	Усунення наслідків кібератак і кіберзагроз	Швидке реагування на НСД до конфіденційної інформації, що обробляється в ІКМ з метою мінімізації завданої шкоди

Види аудиту ІБ інфокомунікаційного підприємства



Етапи аудиту ІБ інфокомунікаційного підприємства



Таблиця 2.1 – Порівняння методологій оцінювання інформаційні ризиків

Критерії	CRAMM	CORAS	Risk Watch	OCTAVE	Oracle Crystal Ball
Загальні характеристики					
Розрахованість на організацію різного розміру і сфери діяльності	+	+	+	+	+
Автоматизація «What-if»	-	?	+	-	+
Зручність сприйняття графіків і звітів	-	+	-	+	+
Простота використання	-	+	-	+	+
Безкоштовне використання	-	+	-	+	-
Підтримка	+	+	+	+	+
Кількісна оцінка	+	+	+	-	?
Якісна оцінка	+	+	-	+	?
Українська локалізація	-	?	+	?	-
Підвищення інформативності співробітника	-	-	-	+	?
Придатність до регулярного використання	+	-	?	+	?
Використання незалежної оцінки	+	+	?	-	+

Критерії	CRAMM	CORAS	Risk Watch	OCTAVE	Oracle Crystal Ball
Вхідні дані					
Ресурси	+	+	+	+	+
Тип інформаційної системи	+	?	+	+	-
Цінність ресурсів	+	+	+	+	?
Загрози	+	+	+	+	+
Уразливості системи	+	+	+	+	+
Вибір контрзаходів	+	?	+	-	-
Базові вимоги в сфері безпеки	-	?	+	-	-
Втрати	-	?	+	-	-
Заходи захисту	+	-	+	+	-
Частота виникнення загроз	-	?	+	-	-
Мережеве обладнання	-	?	-	+	-
Види інформації	-	?	-	?	-
Групи користувачів	-	?	-	-	-
Засоби захисту	-	?	-	+	-

Шкала цінності активів

Ідентифікатор	Актив підприємства		Конфіденційність	Цілісність	Доступність	Цінність актива
A	Основні активи інформації	Інформація необхідна для реалізації назначення чи бізнес організації	2	4	4	**4**
B.		Інформація особистого характеру, яка визначена особливим образом, відповідним національним законам про недоторканість приватного життя	3	1	1	**3**
C.		Стратегічна інформація, необхідна для досягнення цілей організації	2	2	1	**2**
D.			3	2	2	**3**
E.	Апаратно-програмний комплекс		-	3	4	**4**
F.	Носії інформації		-	1	2	**2**
G.	Мережа		-	3	4	**4**
H.	Працівники		-	1	1	**1**
I.	Місце функціонування організації		-	1	1	**1**

Класифікація загроз інформаційній безпеці

Найменування загрози	Характер загрози (прояв)	Збиток
ОРГАНІЗАЦІЙНО-УПРАВЛІНСЬКА		
Відсутність нормативів і правил, що регламентують політику у сфері інформаційної безпеки	Необґрунтоване визначення рівня інформаційного захисту	Фатальний
Відсутність документації, що регламентує рівень таємності інформації, доступ до неї посадових осіб	Існуюча можливість розголошення комерційної таємниці	Сильний
Відсутність положень, посадових інструкцій відносно процедур обмеженого доступу до інформації	Неефективне управління інформаційними ресурсами	Сильний
Відсутність процедур адміністративного контролю над програмно-апаратними засобами	Неефективне управління інформаційними ресурсами	Помірний
ВИРОБНИЧО-ПРОЦЕСНА (процеси обробки й видачі інформації)		
Відсутність профілів захисту	Відсутність чітко сформульованої і зрозумілої співробітниками політики безпеки	Сильний
Несанкціонований доступ до інформації та інформаційних продуктів	Зловживання	Сильний
Відсутність процедур ідентифікації користувачів	Несанкціонований вхід в інформаційну систему	Помірний
Несанкціонована модифікація, обробка, передача інформації та інформаційних продуктів (у т. ч. з віддалених терміналів у комп'ютерних мережах)	Шахрайство. Обдурювання. Витік інформації в процесі передачі по каналах зв'язку (втрата інформацією конфіденційності, порушення доступу, втрата цілісності та модифікація авторизованої інформації)	Сильний
Відсутність процедур аутентифікації	Доступ до авторизованої інформації	Слабкий
Відсутність процедур адміністрування паролів	Порушення якісних властивостей профілів захисту	Помірний
Відсутність процедур захисту файлів	Доступ до авторизованої інформації	Слабкий

Класифікація загроз інформаційній безпеці

Найменування загрози	Характер загрози (прояв)	Збиток
ЗАБЕЗПЕЧУВАЛЬНА		
Використання неліцензійного програмного забезпечення (системного та прикладного)	Укладання некоректних договорів	Фатальний
Несанкціоноване підключення до джерела інформації і використання інформації, що відноситься до комерційної таємниці	Доступ до винятково конфіденційної інформації (без її коректування), сканування	Сильний
Незаконна модифікація програмного забезпечення – системного та прикладного – протягом життєвого циклу інформаційної системи	Троянські коні. Логічні закладки. Програмні віруси.	Сильний
Використання «сумнівних» джерел інформації у процесах прийняття управлінських рішень	Укладення некоректних договорів із відповідними організаціями	Помірний
Відсутність регламентованих процедур тестування наявного програмного забезпечення	Відсутність чіткої організації експлуатації наявного програмного забезпечення	Сильний

Найнебезпечніші ризики

- I- загроза тривалого утримання обчислювальних ресурсів користувачами;
- II - загроза завантаження нештатної операційної системи;
- III -загроза приведення системи в стан" відмова в про слугування;
- IV - "загроза програмного виведення з ладу коштів зберігання, обробки або введення/виведення/передачі інформації;
- V - загроза втрати обчислювальних ресурсів;
- VI - загроза втрати носіїв інформації;
- VII - загроза фізичного виведення з ладу засобів збереження, обробки або введення/виводу/передачі інформації;
- VIII - загроза форматування носіїв інформації;
- IX - загроза розкрадання засобів зберігання, обробки;
- X - загроза неправомірного шифрування інформації;
- XI - загроза поширення «поштових хробаків» ;
- XII - загроза фізичного старіння апаратних компонентів
- XIII- загроза надлишкового видалення оперативної пам'яті;
- XIV - загроза зміни компонентів системи;
- XV - загроза використання інформація про ідентифікацію /
- автентифікації, визначеної за замовчуванням;
- XVI - загроза використання вразливостей протоколів мережево /локального обміну даними;
- XVII - загроза дослідження механізмів роботи програми;
- XVIII - загроза несанкціонованого видалення конфіденційної
- інформації;
- XIX - загроза перезавантаження апаратних і програмно-апаратних засобів обчислюваної техніки;
- XX - загроза пошкодження системного реєстру;
- XXI - загроза підвищення привілеїв;
- XXII загроза подолання фізичного захисту;
- XXIII - загроза впровадження шкідливого коду через рекламу, сервіси і контент;
- XXIV - загроза маскування дій шкідливого коду.

Визначення ступені вразливості активів

Загрози ІБ	Цінні активи організації								
	A.	B.	C.	D.	E.	F.	G.	H.	I.
I	-	-	-	-	2	-	-	-	-
II	1	1	1	1	3	-	-	-	-
III	-	-	-	-	2	-	2	-	-
IV	-	-	-	-	3	-	-	-	-
V	2	2	2	2	1	-	-	-	-
VI	-	-	-	-	-	-	1	-	-
VII	1	1	1	1	1	-	1	-	-
VIII	3	3	3	3	-	-	-	-	-
IX	-	-	-	-	2	-	-	-	-
X	2	2	2	2	2	-	-	-	-
XI	-	-	-	-	2	-	-	-	-
XII	1	1	1	1	3	3	-	-	-
XIII	-	-	-	-	3	-	3	-	-
XIV	3	3	3	3	2	2	-	-	-
XV	1	1	1	1	3	3	3	-	-
XVI	3	3	3	3	-	2	-	-	-
XVII	-	-	-	-	1	1	-	-	-
XVIII	1	1	1	1	-	1	-	-	-
XIX	1	1	1	1	2	2	-	-	-
XX	2	2	2	2	-	-	-	-	-
XXI	-	-	-	-	-	-	2	-	-
XXII	-	-	-	-	1	-	1	-	-
XXIII	2	2	2	2	-	-	2	-	-
XXIV	-	-	-	-	1	-	1	-	-

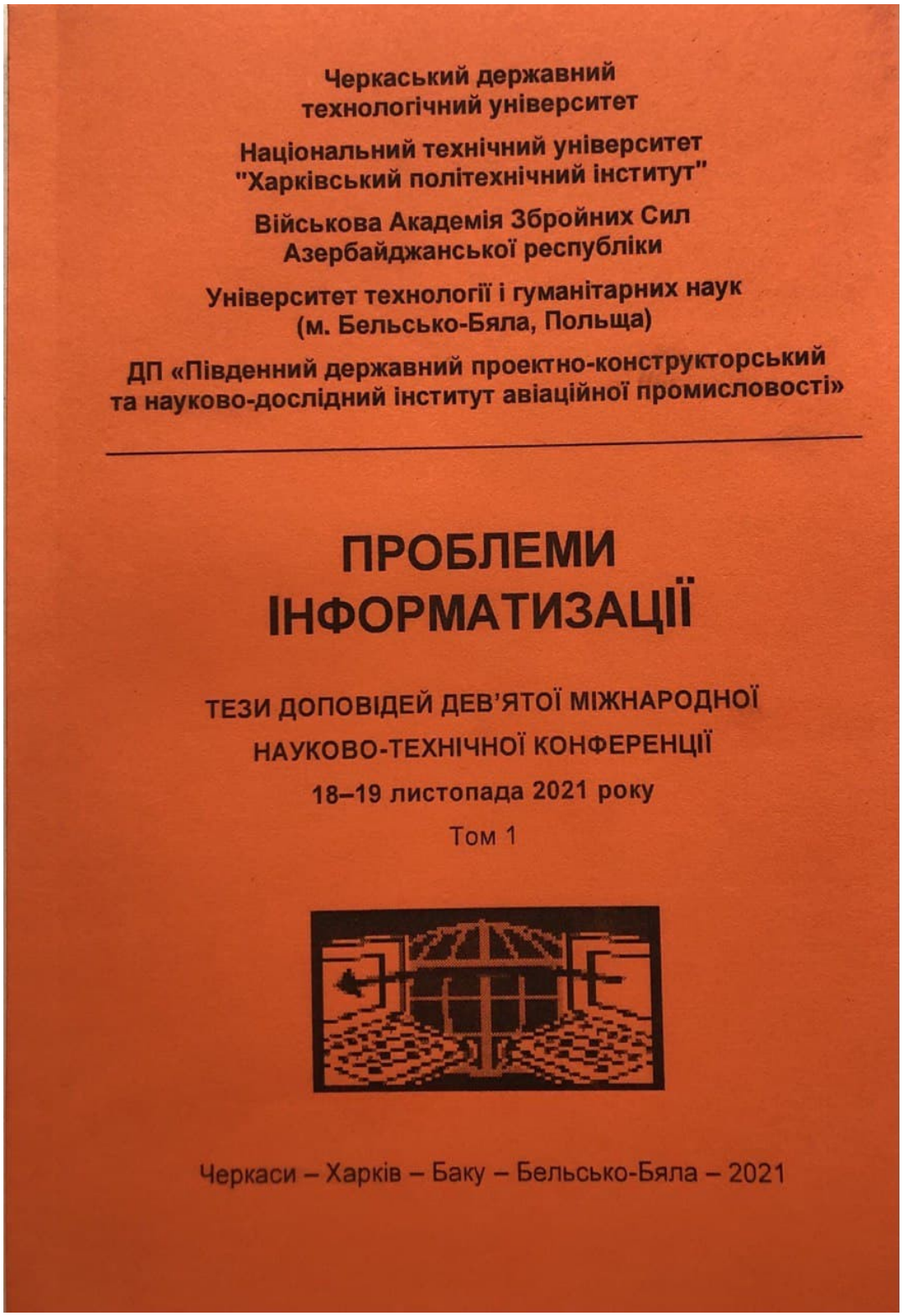
Таблиця 3.2 – Ймовірності реалізації загроз

ID загрози	I	II	III	IV	V	VI	VII	VIII	IX	X	XI	XII	XIII	XIV	XV	XVI	XVII	XVIII	XIX	XX	XXI	XXII	XXIII	XXIV
Ймовірність	2	1	2	3	1	2	2	4	2	2	2	3	2	2	2	4	3	3	3	2	2	3	3	2

Таблиця 3.3 Рекомендовані контрзаходи

Цінний актив організації	Загрози	Ризик	Допустимий ризик	Планові заходи	Остаточний ризик
Інформація необхідна для реалізації призначення чи бізнес організації	VIII	48	Від 1 до 19	Система резервного копіювання, система захисту від НСД	12
	XIV	24		Система антивірусного захисту, міжмережеве екранування	12
	XVI	48		Облік носіїв інформації	12
	XXIII	24		Система антивірусного захисту, міжмережеве екранування; Організаційні заходи	8
Апаратно-програмний комплекс	IV	36	Від 1 до 19	Міжмережеве екранування, система довіреної загрузки, система антивірусного захисту; Організаційні заходи	12
	XII	36		Система відеонагляду, адекватні засоби фізичного захисту; Організаційні заходи	12
	XIII	24		Система міжмережевого екранування	12
	XV	24		Система міжмережевого екранування	12
	XIX	24		Система відеонагляду, адекватні засоби фізичного захисту; Організаційні заходи	8
Мережа	XIII	24	Від 1 до 19	Система міжмережевого екранування	12
	XV	24		Система міжмережевого екранування	12
	XXIII	24		Система антивірусного захисту, міжмережеве екранування; Організаційні заходи	8

ДОДАТОК Б. ПУБЛІКАЦІЯ ЗА ТЕМОЮ РОБОТИ



Черкаський державний
технологічний університет

Національний технічний університет
"Харківський політехнічний інститут"

Військова Академія Збройних Сил
Азербайджанської республіки

Університет технології і гуманітарних наук
(м. Бельсько-Бяла, Польща)

ДП «Південний державний проектно-конструкторський
та науково-дослідний інститут авіаційної промисловості»

**ПРОБЛЕМИ
ІНФОРМАТИЗАЦІЇ**

ТЕЗИ ДОПОВІДЕЙ ДЕВ'ЯТОЇ МІЖНАРОДНОЇ
НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

18–19 листопада 2021 року

Том 1

Черкаси – Харків – Баку – Бельсько-Бяла – 2021

РОЗРОБКА МЕТОДИКИ РОЗРАХУНКУ ІНФОРМАЦІЙНИХ РИЗИКІВ ПІДПРИЄМСТВА

Спєсівцева А.С., Золотарьов В.А.
Харківський національний університет радіоелектроніки, Харків, Україна

В умовах глобалізації забезпечення інформаційної безпеки на підприємстві є дуже важливим моментом і полягає в постійному контролі за джерелами виникнення потенційних загроз та необхідності здійснювати захист інформації будь-якими засобами.

Метою доповіді є визначення та оцінювання ризиків інформаційній безпеці для типової розподіленої інфокомунікаційної мережі підприємства.

Основний акцент зроблено на мінімізацію шкоди від кібератак, спрямованих на доступність програмно-апаратного комплексу інфокомунікаційної системи. Провідним методом для оцінювання та обробки ризиків був обраний якісний метод, як найбільш економічний, в умовах відсутності даних про кількість реалізованих атак на інфокомунікаційну систему за окремий проміжок часу. Ґрунтуючись на бізнес-процесах підприємства були виділені основні та другорядні активи, а також відповідні їм загрози інформаційній безпеці.

В роботі був проведений розрахунок ризиків інформаційній безпеці, заснований на виділенні цінних активів організації, ступеня потенційної шкоди під час реалізації загроз на такі активи та ймовірності реалізації загроз для аналізованої інфокомунікаційної мережі підприємства.

Також були виділені прийняті ризики, обробка яких не потрібна у зв'язку з тим, що фактична вартість їх мінімізації вища від реалізації відповідних їм загроз. Були запропоновані можливі заходи щодо мінімізації ризиків інформаційній безпеці, що включають:

систему резервного копіювання,
систему захисту від несанкціонованого доступу,
систему антивірусного захисту,
міжмережне екранування,
організаційні заходи фізичного захисту.

Була запропонована методика, яка дозволяє однозначно оцінити ризики інформаційній безпеці організації в умовах великого об'єму оброблюємої інформації та необмежного числа користувачів і потребує мінімальних фінансових вкладень. Застосування розглянутого методу на практиці буде сприяти ефективному виявленню основних загроз захисту безпеки та їхній мінімізації.

Список літератури

1. ISO/IEC 27001:2013. Information technology. Security techniques. Information security management systems. Requirements. Berlin: ISO/IEC JTC 1/SC 27. 2013. 23p.

2. Дорофеев А.В. Менеджмент инфоромационной безопасности: переход на ISO 27001:2013 // Вопросы кибербезопасности. 2014.No 3 (4). С. 69–73.

Позначення	Найменування	Дод. відомості
	Текстові документи	
1.	Пояснювальна записка	72
	Графічні документи	
2.	Слайди презентації	15
3.		

Змін.	Арк.	Номер докум.	Підпис	Дата	Розрахунок ризиків інформаційної безпеки інфокомунікаційного підприємства	Літ.	Аркуш	Аркушів
Розроб.		Спєсівцева				У	1	1
Перевір.		Золотарьов						
Н. контр.		Золотарьов			Відомість кваліфікаційної роботи	ХНУРЕ кафедра ІМІ		
Затв.		Безрук						