Програмний засіб для оцінювання та забезпечення рівня захисту інформаційних ресурсів підприємства

Доповідач:ст. гр. 1КІ-14сп Омельчук О.В.
Науковий керівник: к.т.н., доц. Цирюльник С.М.

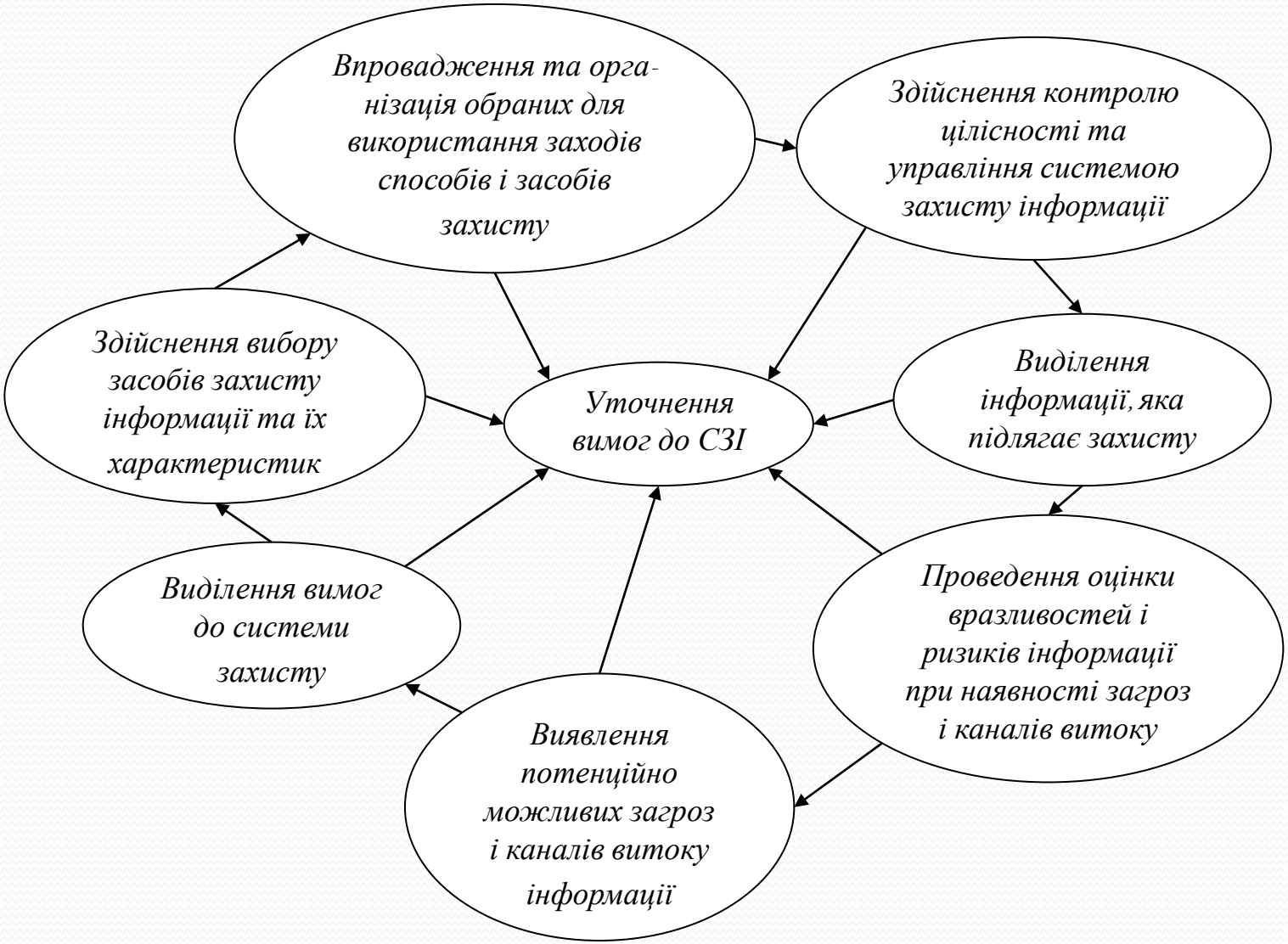
Актуальність теми:

Створення і підтримка захищеного середовища інформаційного обміну, що реалізує певні правила політики інформаційної безпеки сучасної організації.

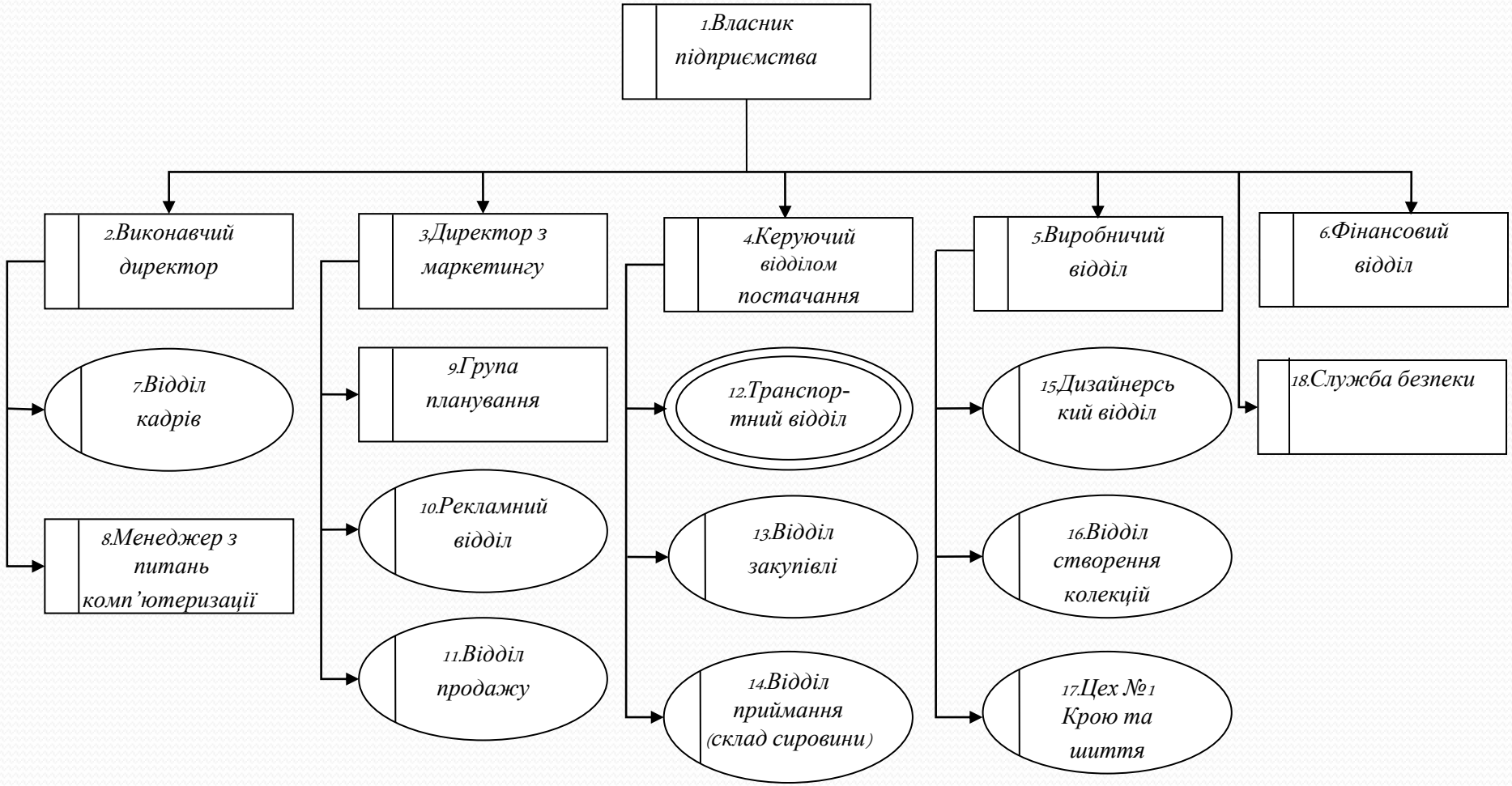
Мета:

Підвищення рівня захищеності системи комплексного захисту інформаційних ресурсів підприємства.

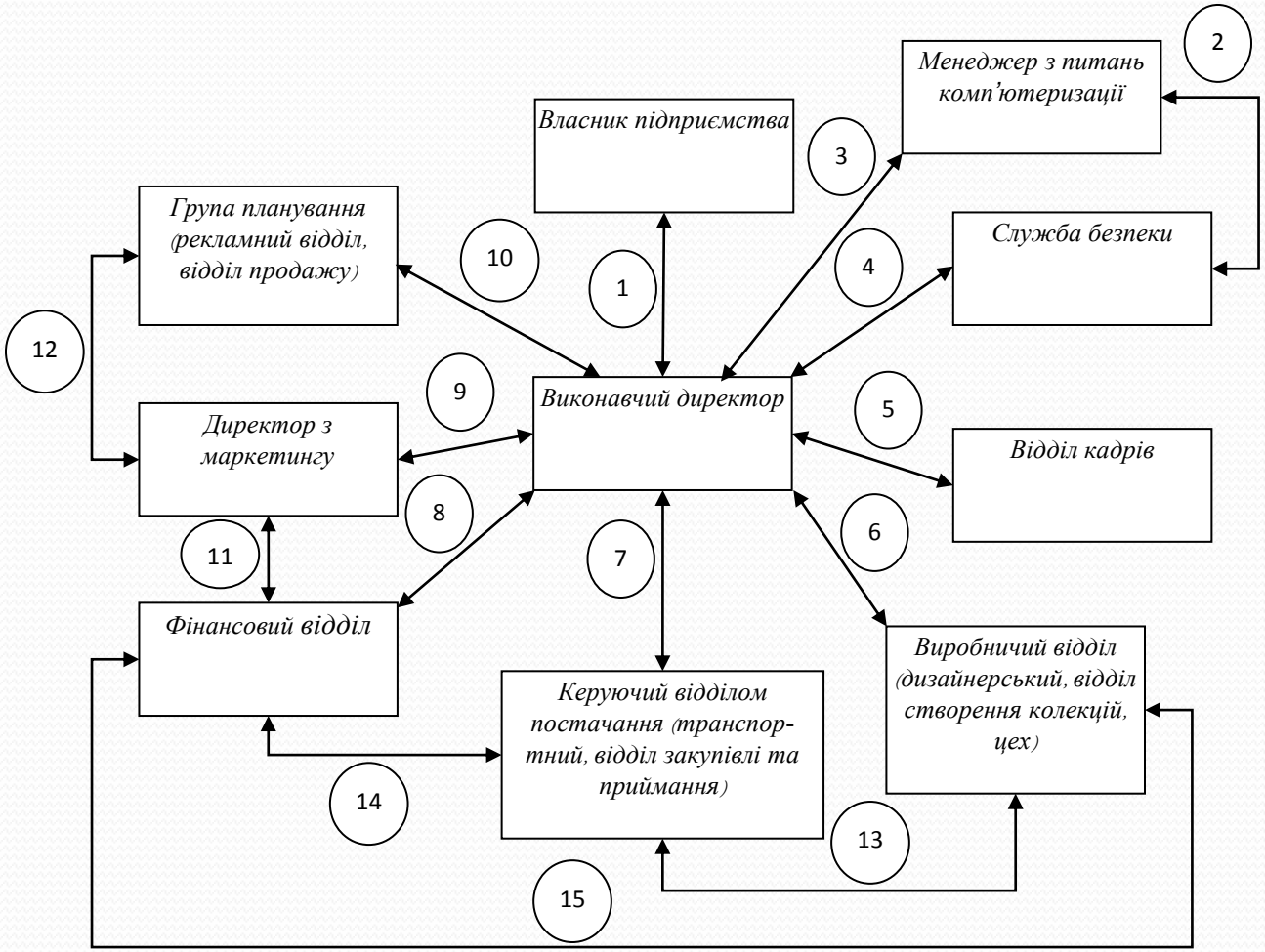
Процес створення програмного засобу представлений у вигляді безперервного циклу



Структурна схема

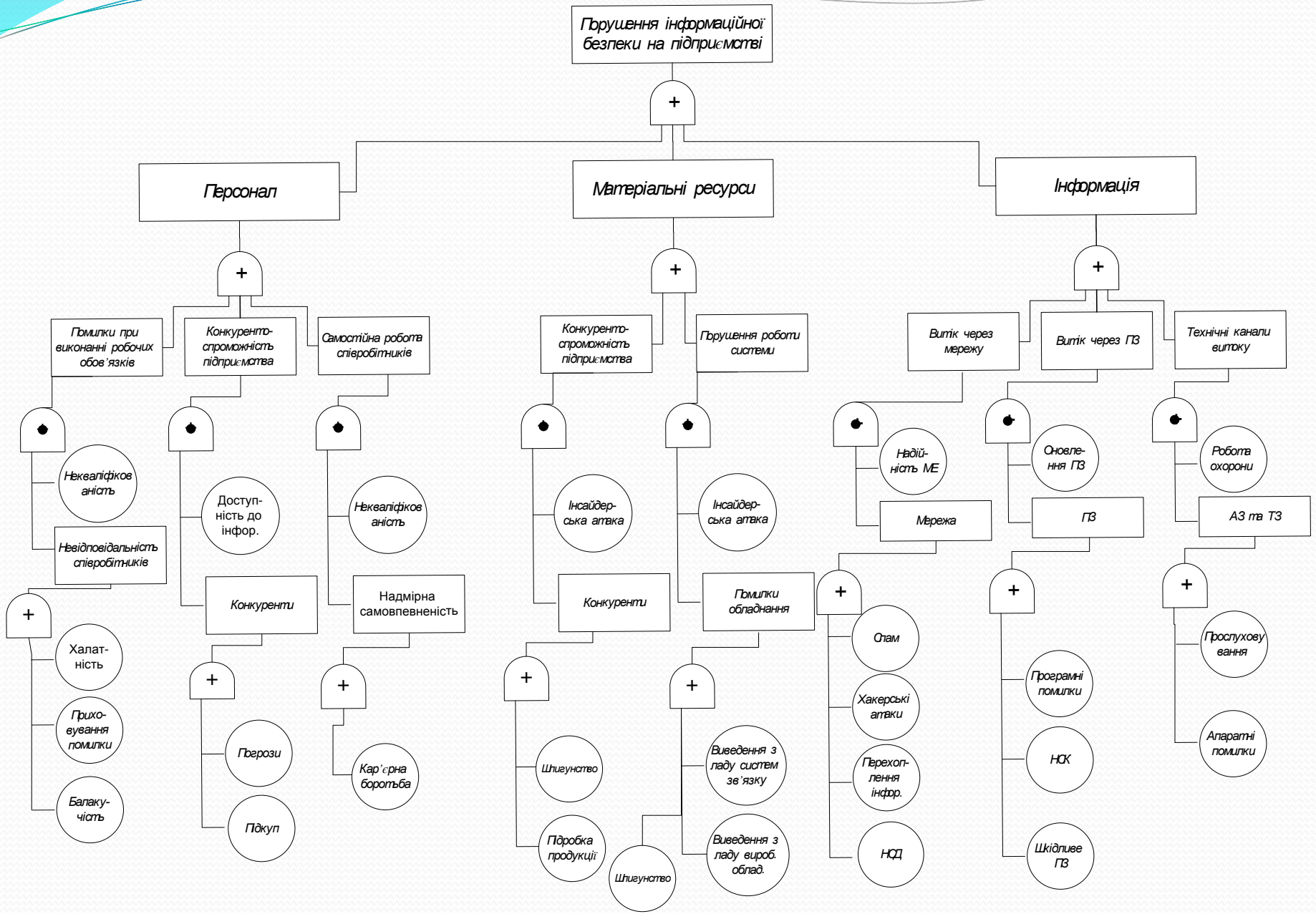


Модель інформаційних потоків підприємства:



- інформаційні потоки № 1, 3, 6, 7, 9, 10 інформація по виконаній роботі;
- інформаційний потік № 2 служба безпеки та відділ комп'ютеризації тісно пов'язані, їм необхідно співпрацювати разом особливо у випадках, коли є ймовірність виникнення загрози в комп'ютерних мережах;
- інформаційний потік № 4 інформація про стан організаційної безпеки підприємства;
- інформаційний потоки № 5 персональні дані працівників, які працюють чи мають працювати на фірмі;
- інформаційний потік № 8 фінансові та бухгалтерські звіти;
- інформаційні потоки № 11, 14 інформація про надання фінансів для реалізації планів компанії;
- інформаційний потік № 12 директор з маркетингу та група планування разом з відділом продаж контролює стан зовнішнього ринку;
- інформаційний потік № 13 склад зберігає та видає сировину виробничому відділу, веде облік наявної кількості сировини та виданої на виробництво;
- інформаційний потік № 15 фінансовий відділ виділяє кошти на виробництво, звіти по витратах на виробництво.

Логіко-ймовірнісна модель



Оцінювання рівня загрози

Для оцінювання рівня загроз використовується формула:

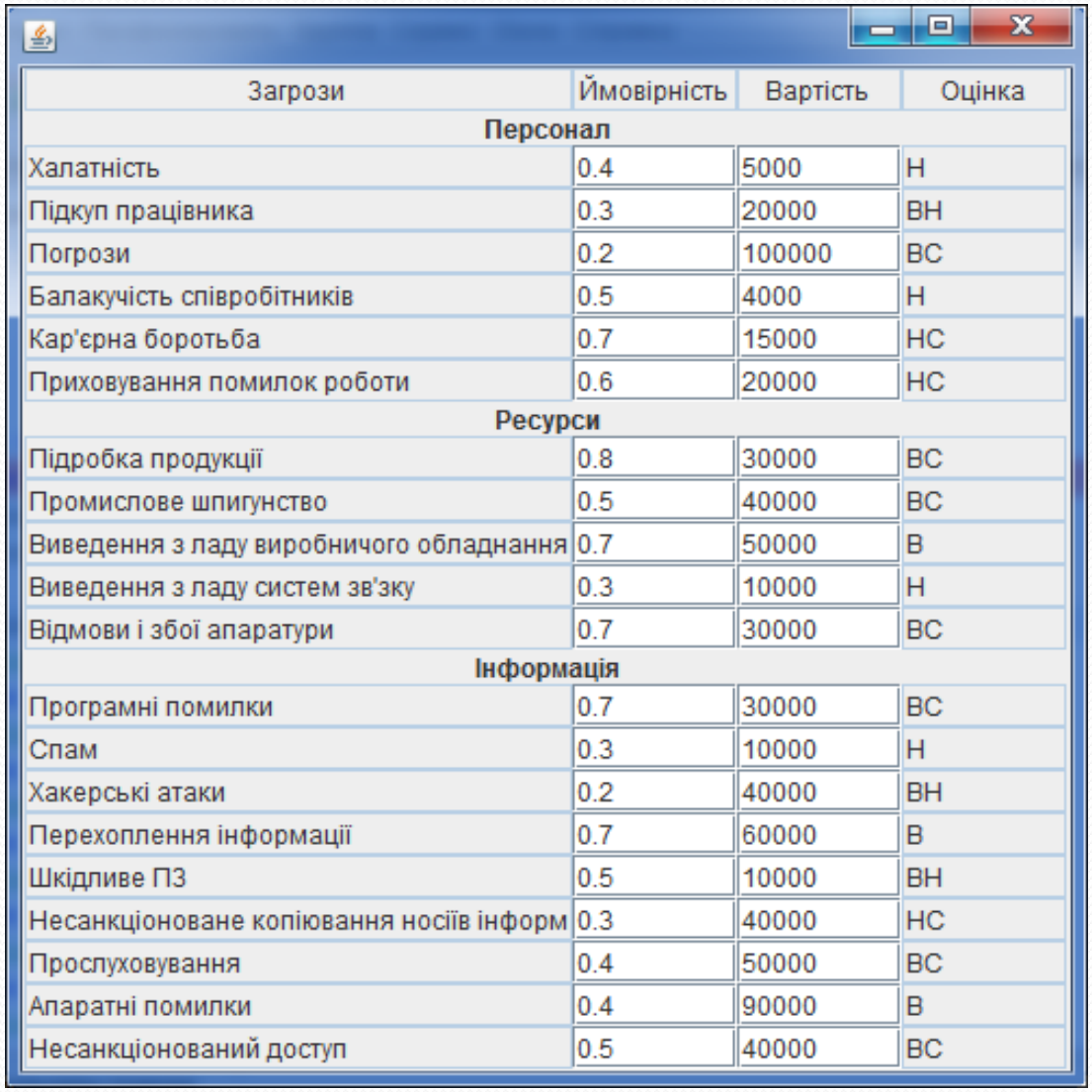
$$N=P*V,$$

де N – оцінка рівня загрози, P – ймовірність виникнення, V – вартість загрози.

Лінгвістична шкала оцінювання рівня загроз:

- низький (0 - 5000);
- нижче середнього (5000 - 10000);
- середній (10000 - 15000);
- вище середнього (15000 - 20000);
- нижче вищого (20000 - 25000);
- високий (25000 - 30000);
- вище вищого (30000 - 50000);
- дуже високий від 50000.

Оцінювання рівнів загроз



Загрози	Ймовірність	Вартість	Оцінка
Персонал			
Халатність	0.4	5000	Н
Підкуп працівника	0.3	20000	ВН
Погрози	0.2	100000	ВС
Балакучість співробітників	0.5	4000	Н
Кар'єрна боротьба	0.7	15000	НС
Приховування помилок роботи	0.6	20000	НС
Ресурси			
Підробка продукції	0.8	30000	ВС
Промислове шпигунство	0.5	40000	ВС
Виведення з ладу виробничого обладнання	0.7	50000	В
Виведення з ладу систем зв'зку	0.3	10000	Н
Відмови і збої апаратури	0.7	30000	ВС
Інформація			
Програмні помилки	0.7	30000	ВС
Спам	0.3	10000	Н
Хакерські атаки	0.2	40000	ВН
Перехоплення інформації	0.7	60000	В
Шкідливе ПЗ	0.5	10000	ВН
Несанкціоноване копіювання носіїв інформ	0.3	40000	НС
Прослуховування	0.4	50000	ВС
Апаратні помилки	0.4	90000	В
Несанкціонований доступ	0.5	40000	ВС

В результаті оцінювання критичними напрямами захисту підприємства є:

1) апаратні помилки;
2) виведення з ладу виробничого обладнання;
3) шкідливе програмне забезпечення;
4) промислове шпигунство;
5) підробка продукції.

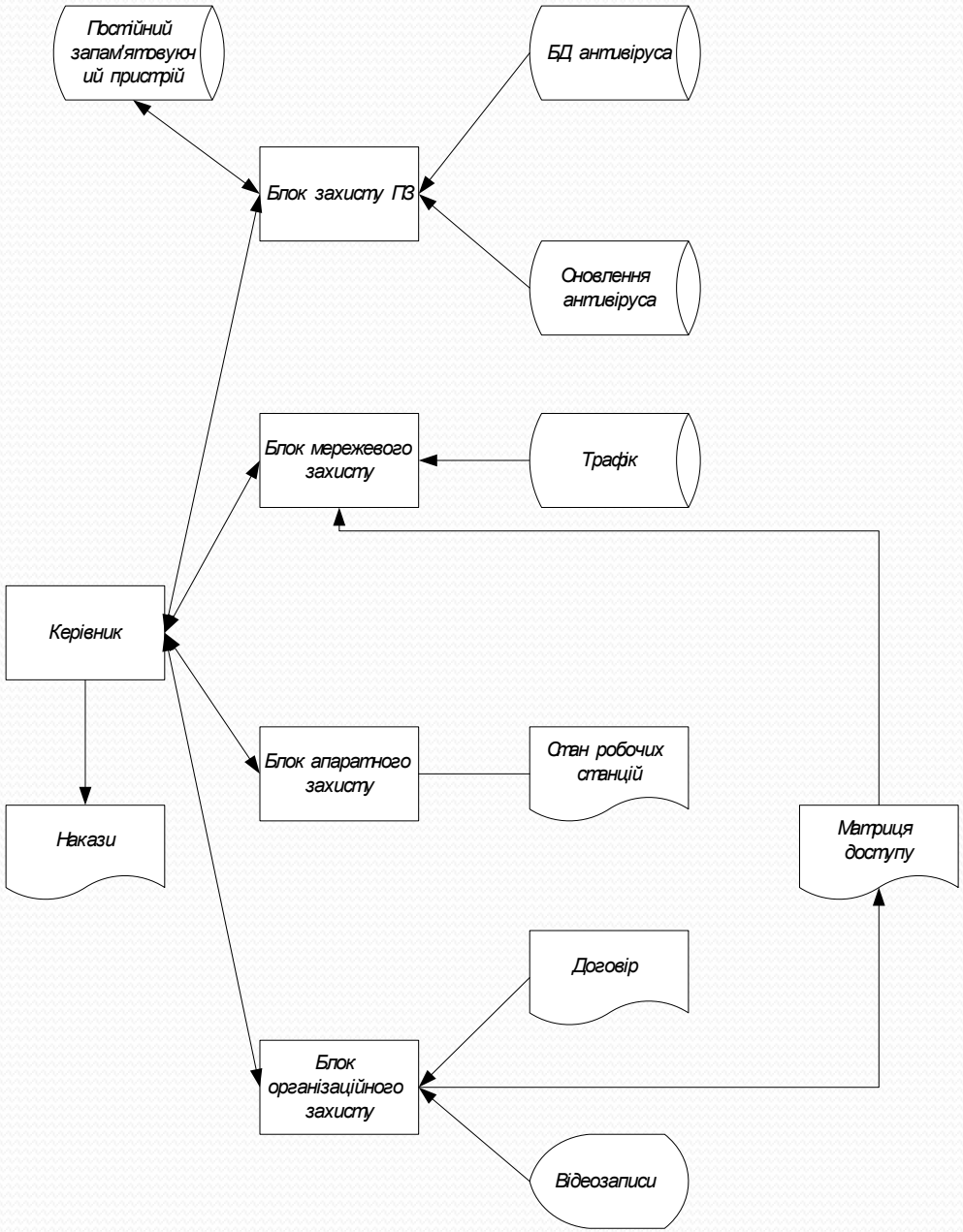
Політика інформаційної безпеки

Політика інформаційної безпеки розробляється у вигляді декількох документів.

Основними розділами політики інформаційної безпеки є:

- використання програмних засобів;
- протидія апаратним помилкам;
- інструктажі співробітників підприємства;
- аналітична робота;
- захист продукту від підробки.

Архітектура система захисту



Оптимізація системи захисту інформації

Програмні засоби	Ефективність	Ціна
Dr.Web Security Space PRO	0,44	495
D-Link DFL-260 UTM Net Defend VPN Firewall	0,62	6130
PowerCom War 400A	0,5	308
KPC-S510 D	0,55	520
Договір	0,55	500
		7953

Дякую за увагу!