Лабораторна робота 1

ДОСЛІДЖЕННЯ ПРОЦЕДУРИ ОБСТЕЖЕННЯ ОБ'ЄКТУ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ТА ФОРМУВАННЯ ЗВІТНОЇ ДОКУМЕНТАЦІЇ

Мета – дослідження процедури обстеження об'єкту інформаційної діяльності, формування звітної документації.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Розглянемо Поради (рекомендації) щодо створення КСЗІ в ІТС, які використовуються для надання послуг доступу до мережі Інтернет, розроблені Державною службою спеціального зв'язку та захисту інформації України (http://surl.li/amfyb) .

На сьогодні, системи захисту інформації являють собою достатньо складні системи, що об'єднують у собі різні технології та засоби захисту, які об'єднуються у комплексну систему захисту інформації. В склад цієї системи обов'язково входить підсистема кіберзахисту.

Комплексна система захисту інформації (КСЗІ) являє собою сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в ІТС.

До складу КСЗІ входять заходи та засоби, які реалізують методи, механізми захисту інформації від несанкціонованих дій та несанкціонованого доступу до інформації, що можуть здійснюватися шляхом підключення до апаратури та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації, застосування закладних пристроїв чи програм, використання комп'ютерних вірусів та ін;

Для організації робіт зі створення КСЗІ в ІТС створюється служба захисту інформації, порядок створення, завдання, функції, структура та повноваження якої визначено в НД 1.4-001-2000.

Комплекс засобів захисту (КЗЗ) — сукупність програмно-апаратних засобів, які забезпечують реалізацію політики безпеки інформації.

Етапи створення КСЗІ

Дозволяється виключати окремі етапи робіт або поєднувати декілька етапів, а також включати нові етапи робіт. За необхідністю дозволяється змінювати послідовність виконання окремих етапів - виконувати одночасно декілька етапів робіт, окремі етапи виконувати до завершення попередніх і т.п., якщо це не призводить до зниження якості робіт і не суперечить цілям їх виконання.

1 Формування загальних вимог до КСЗІ в ІТС

1.2 Обстеження середовищ функціонування ІТС

1.2.2 Метою обстеження є підготовка засадничих даних для формування вимог до КСЗІ у вигляді опису кожного середовища функціонування ІТС та виявлення в ньому елементів, які безпосередньо чи опосередковано можуть впливати на безпеку інформації, виявлення взаємного впливу елементів різних середовищ, документування результатів обстеження для використання на наступних етапах робіт.

1.2.4 При обстеженні обчислювальної системи ІТС повинні бути проаналізовані й описані:

- загальна структурна схема і склад (перелік і склад обладнання, технічних і програмних засобів, їхні зв'язки, особливості конфігурації, архітектури й топології, програмні і програмно-апаратні засоби захисту інформації, взаємне розміщення засобів тощо);

- види і характеристики каналів зв'язку;

- особливості взаємодії окремих компонентів, їх взаємний вплив один на одного;

Мають бути виявлені компоненти обчислювальної системи, які містять і які не містять засобів і механізмів захисту інформації, потенційні можливості цих засобів і механізмів, їхні властивості і характеристики, в тому числі ті, що встановлюються за умовчанням та ін.

Метою такого аналізу є надання загального уявлення про наявність потенційних можливостей щодо забезпечення захисту інформації, виявлення компонентів ІТС, які вимагають підвищених вимог до захисту інформації і впровадження додаткових заходів захисту.

1.2.5 При обстеженні інформаційного середовища аналізу підлягає вся інформація, що обробляється, а також зберігається в ІТС (дані і програмне забезпечення). Під час аналізу інформація повинна бути класифікована за режимом доступу, за правовим режимом, визначені й описані види її представлення в ІТС.

Для кожного виду інформації і типу об’єкта, в якому вона міститься, ставляться у відповідність властивості захищеності інформації (конфіденційність, цілісність, доступність) чи ІТС (спостережність), яким вони повинні задовольняти.

Аналіз технології обробки інформації повинен виявити особливості обігу електронних документів, мають бути визначені й описані інформаційні потоки і середовища, через які вони передаються, джерела утворення потоків та місця їх призначення, принципи та методи керування інформаційними потоками, складені структурні схеми потоків. Фіксуються види носіїв інформації та порядок їх використання під час функціонування ІТС.

Для кожного структурного елемента схеми інформаційних потоків фіксуються склад інформаційних об’єктів, режим доступу до них, можливий вплив на нього (елементу) елементів середовища користувачів, фізичного середовища з точки зору збереження властивостей інформації.

1.2.6 При обстеженні фізичного середовища здійснюється аналіз взаємного розміщення засобів обробки інформації ІТС на об’єктах інформаційної діяльності, комунікацій, систем життєзабезпечення і зв’язку, а також режим функціонування цих об’єктів.

Аналізу підлягають такі характеристики фізичного середовища:

- територіальне розміщення компонентів ІТС (генеральний план, ситуаційний план);

- наявність охорони території та перепускний режим;

- умови зберігання магнітних, оптико-магнітних, паперових та інших носіїв інформації;

1.2.7 При обстеженні середовища користувачів здійснюється аналіз:

- функціонального та кількісного складу користувачів, їхніх функціональних обов’язків та рівня кваліфікації;

- повноважень користувачів щодо управління КСЗІ;

- рівня можливостей різних категорій користувачів, що надаються (можуть бути доступними) їм засобами ІТС.

1.2.8 Результати обстеження середовищ функціонування ІТС оформлюються у вигляді акту і включаються, у разі необхідності, до відповідних розділів плану захисту інформації в ІТС (далі - План захисту), який розробляється згідно з НД ТЗІ 1.4-001-2000.

1.2.9 За результатами обстеження середовищ функціонування ІТС затверджується перелік об'єктів захисту (з урахуванням рекомендацій НД ТЗІ 1.4-001-2000, НД ТЗІ 2.5-008-2002, НД ТЗІ 2.5-010-2003 щодо класифікації об'єктів), а також визначаються потенційні загрози для інформації і розробляються модель загроз та модель порушника. Побудова моделей здійснюється відповідно до положень НД ТЗІ 1.1-002-99, НД ТЗІ 1.4-001-2000.

1.3 Формування завдання на створення КСЗІ

- здійснюється аналіз ризиків (вивчення моделі загроз і моделі порушника, можливих наслідків від реалізації потенційних загроз, величини можливих збитків та ін.) і визначається перелік суттєвих загроз;

- визначаються загальна структура та склад КСЗІ, вимоги до можливих заходів, методів та засобів захисту інформації, допустимі обмеження щодо застосування певних заходів і засобів захисту інші обмеження щодо середовищ функціонування ІТС, обмеження щодо використання ресурсів ІТС для реалізації задач захисту, припустимі витрати на створення КСЗІ, умови створення, введення в дію і функціонування КСЗІ (окремих її підсистем, компонентів), загальні вимоги до співвідношення та меж застосування в ІТС (окремих її підсистемах, компонентах) організаційних, інженерно-технічних, технічних, криптографічних та інших заходів захисту інформації, що ввійдуть до складу КСЗІ.

ЗАВДАННЯ НА ВИКОНАННЯ

1. Ознайомитися з теоретичними відомостями.
2. Ознайомитись з зазначеними нормативно-правовими документами.
3. Провести ознайомлення з представленим у додатку 1 прикладом Акту обстеження середовищ функціонування автоматизованої системи класу «2» адміністративної будівлі Приватного підприємства «УПК «КРОК»».
4. Вибрати об'єкт дослідження та провести аналіз відповідно до прикладу, що представлено у додатку 1.
5. Звіт представити у вигляді заповненого акту об'єкту інформаційної діяльності, де у якості директора зазначити своє прізвище та власне ім'я.

Додаток 1

ЗАТВЕРДЖУЮ

Директор ПП «УПК «КРОК»»

_____ Ю.О. Марчук

“____”_____2013 року

АКТ

обстеження середовищ функціонування автоматизованої системи класу «2» адміністративної будівлі Приватного підприємства «УПК «КРОК»»

Комісія у складі:

Голови: заступника директора з економічної безпеки Марченка О.Т.;

Членів: начальника служби охорони Панченка О.В., начальника електронно-обчислювального центру Присяжного В.Г.

Відповідно до вимог НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі», здійснила обстеження середовищ функціонування автоматизованої системи класу «2» адміністративної будівлі Приватного підприємства «УПК «КРОК»».

В ході роботи встановлено:

1. Обстеження обчислювальної системи:

Обчислювальна система є локальною мережею, яка складається з 18 однотипних АС класу «1» (ПЕОМ), що знаходяться по одному в кожному приміщенні приміщенні. Крім цього, для забезпечення функціонування ІТС використується 1 комутатор та 1 маршрутизотор. Склад і характеристика складових ІТС наведені у таблиці 1:

Таблиця 1 – Характеристика складових ІТС наявних у системі

Пристрій	Характеристика	Заводський номер / рік виробництва
Системний блок		2334512 /2009
Монітор	23"SAMSUNG 23xi (C3Z94AA)	110322345 /2004
Клавіатура	Rapoo E9070 Black	30012567 /2011
Миша	Logitech Mouse M175 Black	0 1-2347856 /2012
Принтер	Canon 400 M451dn (CE957A) + USB cable	7689504932 /2009
Блок безпереб. живлення	Chieftec CTG-650C	2674857564739 /2011
Модем (роутер)	Novatel Ovation MC990D	36454533663 /2008
Комутатор	D-Link DGS-1210-20	01-230886 /2011

В АС (ІТС) класу 2 встановлено наступне програмне забезпечення:

- Операційна система Windows Seven Ultimate;
- Пакет прикладних програм Microsoft Office 2007;
- Adobe Photoshop CS6;
- Total Commander 7.0;
- Антивірус ESET NOD32;
- Антивірус USB Disk Security;
- ABBYY FineReader – Professional;

Для забезпечення функціонування ІТС використовується комутатор, який об'єднує об'єкти АС в локальну комп'ютерну мережу, використовуючи з'єднувальні кабелі UTP категорії 5е, які не мають виходу за межі об'єкта інформаційної діяльності.

2. Обстеження інформаційного середовища:

2.1. Інформація що планується до обробки за допомогою АС.

Відповідно відомостей, що наведені в Акті визначення вищого ступеню доступу до інформації, яка циркулюватиме в ІТС класу «2» адміністративної будівлі Приватного підприємства «УПК «КРОК»», матиме вищий гриф секретності « суворо конфіденційно».

За режимом доступу інформація, яка планується для обробки за допомогою ІТС, поділяється на:

- Відкриту інформацію загального користування;
- Інформація з обмеженим доступом – конфіденційна інформація (далі – ІзОД).

ІзОД буде представлена в ІТС у вигляді електронних документів створених за допомогою пакету прикладних програм Microsoft Office 2007, Adobe Photoshop CS6 або у роздрукованому паперовому вигляді.

Доступ до ІзОД мають зареєстровані в системі користувачі, що належать до адміністративної ланки підприємства та безпосередньо працівники відділів, що розміщені в адміністративній будівлі даного підприємства.

2.2. Технологія обробки інформації за допомогою ІТС

ІзОД буде відпрацьовуватися за допомогою ІТС, в якій створена КСЗІ, тільки зареєстрованими в ІТС користувачами за допомогою прикладних програм Microsoft Office 2007, Adobe Photoshop CS6.

ІзОД, яка буде відпрацьовуватися в ІТС, буде зберігатися:

- На жорсткому магнітному диску;
- На пристроях зовнішньої пам'яті: DVD-дисках, CD-дисках, флеш накопичувачах.

Документи, в яких містяться ІзОД, будуть друкуватися за допомогою принтерів , які входять до складу ІТС. Копіювання на гнучкі носії та флеш накопичувачі здійснюється з дозволу адміністраторів безпеки ІТС. Перелік відомостей, що становлять комерційну таємницю є.

3. Обстеження фізичного середовища:

3.1 Характеристика об’єктів, де розташовані компоненти ІТС

ІТС розміщена у 20 приміщеннях адміністративної будівлі, що знаходиться за адресою: м. Житомир, вул. Героїв Пожежних, 122. Об'єкт розташований на околиці міста, оточений з трьох сторін спорудами різного призначення і відомчої приналежності. Схема розташування будівлі наведена на рисунку А.1., що розміщено в Додатку.

З боку вулиці планується розміщення торгівельного центру на відстані 20–25 м. Зліва від об'єкту розташована висотна адміністративна будівля, в якій розміщені різні державні підприємства. Праворуч від об'єкту на відстані 45–50 м розташований п’ятнадцятиповерховий житловий будинок.

Прямо перед будівлею через проїжджу частину вулиці на відстані близько 100 м розташовано житлові будинки середньої поверховості..

3.2 Характеристика складових об’єктів

Висота стель (м): h - 3.30 м

- підвісний гіпсолітовий, зазор h - 0,4 м

Перекриття (потовк, пів), товщина (мм) :

- залізобетонні перекриття
- паркет: деревинно-дубовий на спецклеї

Стінні перегородки:

- Глухі стаціонарні офісні перегородки в основі яких лежить алюмінієвий каркас.
- інші матеріали: двосторонній гипрок на металевому каркасі.

Стіни зовнішні: цегельні

- товщина (см) 80
- цеглина керам. порожнистий
- акустична штукатурка: відсутній.
- інші матеріали: з внутрішньої сторони стіни оброблені під «євростандарт» (гипрок).

Вікна:

- розмір отвору: 200х80 см
- кількість отворів: 3
- наявність плівок (призначення, тип, марка) відсутні
- тип вікна (однокамерний склопакет з енергозберігаючим склом.): товщина скла 4 мм.
- інше: мезонін – 1, 200х80 см

- наявність захисних решіток – є

Двері:

- розмір отвору: одностулкові 220х90 см
- двері: 220х90 см одностулкові;
- тип: металеві з «холодним» профілем для внутрішніх дверей, та з «теплим»- для зовнішніх.

Система електроживлення (освітлення):

- мережа: 220 В/50 Гц
- автономний агрегат електроживлення: автономно-трансформаторна підстанція і дизель-генератор
- наявність підстанції на контрольованій території: відсутній
- тип світильників і їх кількість: світлодіодна панель (6 шт.)(40Вт) розміром (595 мм х 595 мм)

Система заземлення: є

Системи сигналізації (тип):

- пожежна (фотооптичні детектори) – 4 шт.,
- охоронна (акустичні детектори) - 6 шт.

Система вентиляції (тип): припливно-витяжна, отвір 365х165 мм.

Система опалювання:

- центральне : водяне
- наявність екранів на батареях: декоративне укриття.
- калорифер (тип): Лунок

Телефонні лінії:

- кількість і тип ТА: 2 шт.
- міська мережа - 1 шт., два паралельні апарати (звичайний і безпровідною)
- місцевою АТС - 1 шт.
- тип розеток: (євророзетка)
- тип проводки – двопровідні лінії.
- Інші дротяні|провід| лінії:
- радіотрансляція (місцева, міська): відсутній
- Засоби зв'язку: Мобільний телефон стандарту NMT-450

Оргтехніка: ПЕВМ в повній конфігурації – 1 шт в кожному кабінеті

Спеціальні технічні засоби захисту інформації: відсутні

Схема розміщення ІТС представлена на рисунку А.3, допоміжних технічних засобів: ліній електроживлення ОІД, системи охоронної та пожежної сигналізації ОІД наведена на рисунку А.4.

4. Обстеження середовища користувачів:

Відповідно до рівня повноважень щодо доступу до інформації, характеру робіт, які виконуються у процесі функціонування ІТс, доступ до ІТС матимуть:

- Користувачі ІТС – особи, які працюють з інформацією (читають, редагують, друкують тощо). Користувачами ІТС є директор, комерційний директор, технічний директор, заступник директора з виробництва, заступник директора з економічної безпеки, заступник директора з економіки й

управління, персонал бухгалтерії, відділів ЗЕД, маркетингу, збуту, закупівель, кадрів, відділу економічної безпеки, фінансового відділу, договірно-планового відділу, начальник служби охорони.

- Технічний персонал – системний адміністратор, персонал обчислювального центру.

Користувачі ІТС матимуть доступ до наступних видів інформації:

- Відкрита інформація загального користування;
- Інформація з обмеженим доступом, що має гриф «конфіденційно», «суворо конфіденційно».

5. Обстеження інформаційних потоків підприємства:

Схема інформаційних потоків підприємтсва з використанням моделі «граф-розгалуджене дерево» наведено на рисунку А.5.

6. Висновок:

Умови функціонування ІТС на ОІД не в повній мірі відповідають вимогам, які дають можливість відпрацювати в АС інформацію з обмеженим доступом.

Інформація, яка планується до обробки за допомогою ІТС, підлягає технічному захисту за рахунок створення в ІТС комплексної системи захисту інформації.

Голова комісії:
Заступника директора з
економічної безпеки О.Т. Марченко

Члени комісії:

Начальник служби охорони О.В. Панченко

Начальник електронно-
обчислювального центру В.Г. Присяжний

Додаток А

Рисунок А.1 – План розміщення будівлі

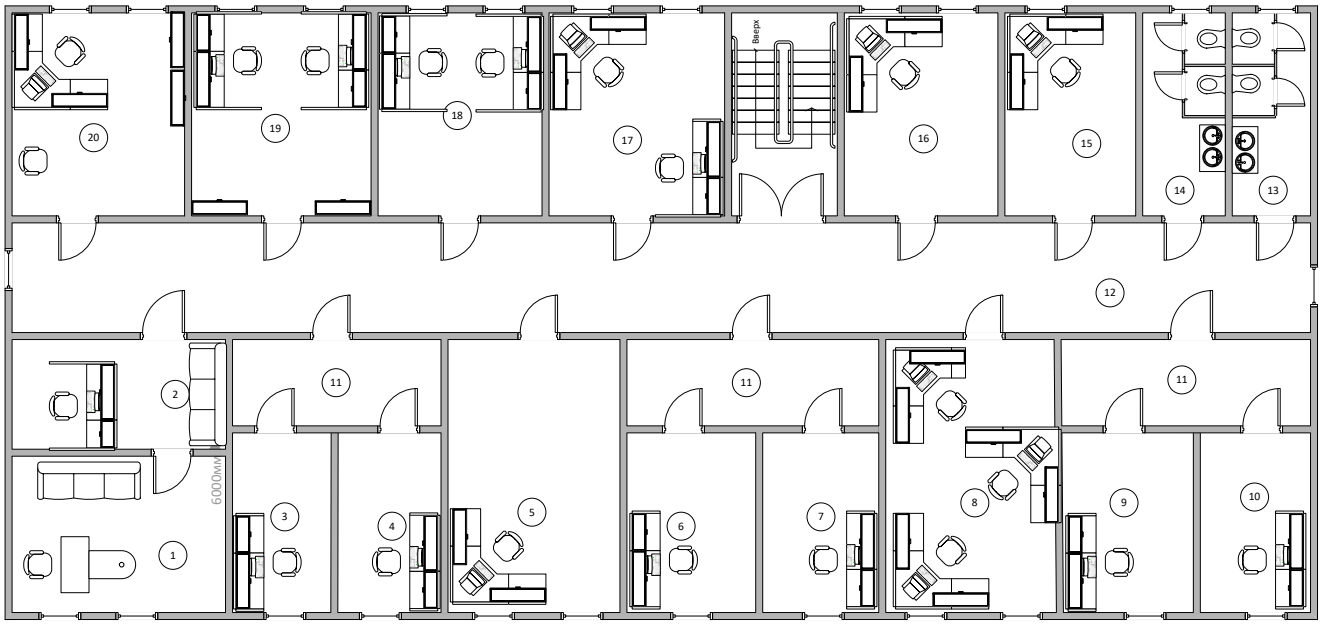

Рисунок А.2 – Ситуаційний план приміщень

Таблиця А.1 - Реплікація приміщень

Позначення	Назва приміщення	Площа, $м^2$
1	Кабінет директора	16
2	Приймальня	11
3	Кабінет технічного директора	9
4	Кабінет заступника директора з виробництва	9
5	Кабінет заступника директора з економічної безпеки	25
6	Відділ економічної безпеки	11
7	Заступник директора з економіки та управління	11
8	Бухгалтерія	25
9	Відділ збуту	11
10	Відділ закупівель	11
11	Холл	7,5
12	Коридор	48
13	Туалет, чоловічий	6,5
14	Туалет, жіночий	6,5
15	Договірно-плановий відділ	12
16	Відділ маркетингу	14
17	Відділ кадрів	14
18	Відділ ЗЕД	14
19	Фінансовий віділ	14
20	Комерційний директор	14

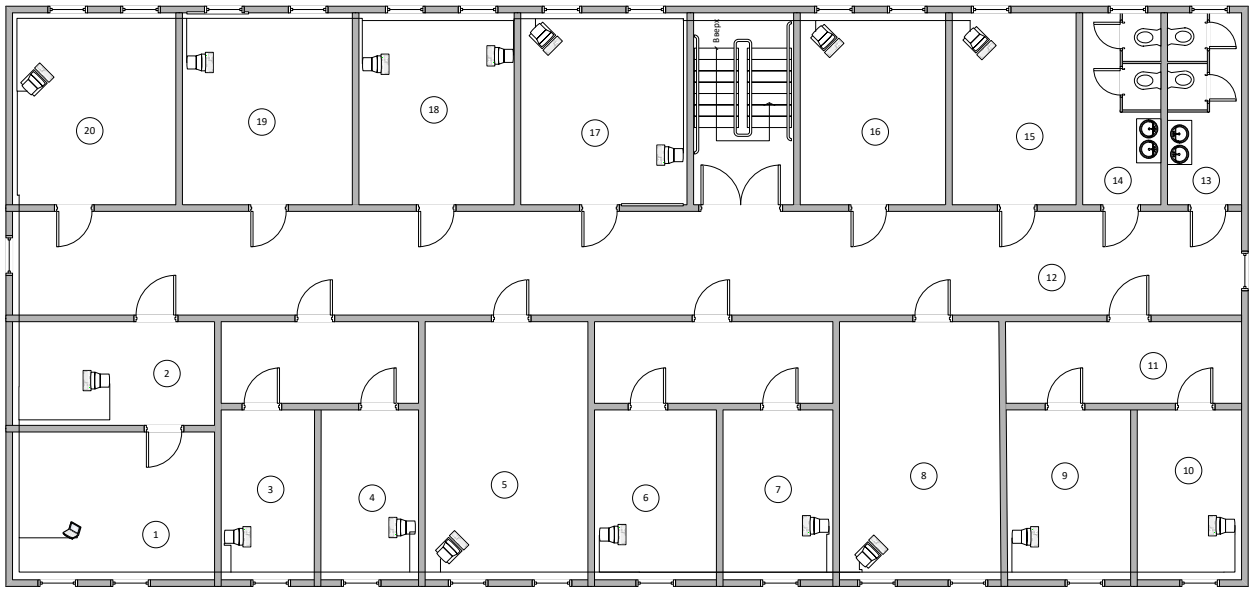

Рисунок А.3 – Схема ІТС адміністративної будівлі ПП «УПК «КРОК»»

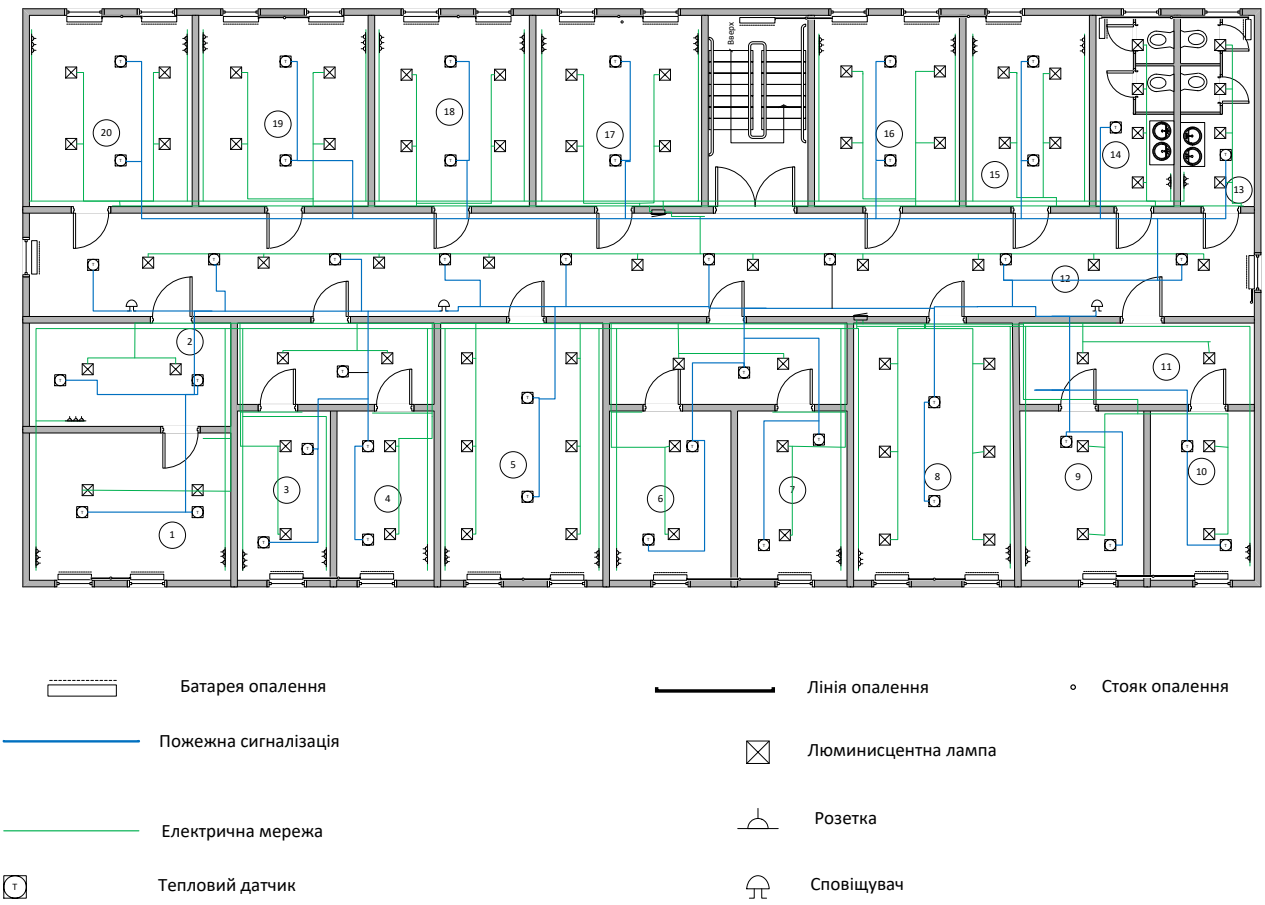

Рисунок А.4 – Схема електромережі та протипожежної сигналізації

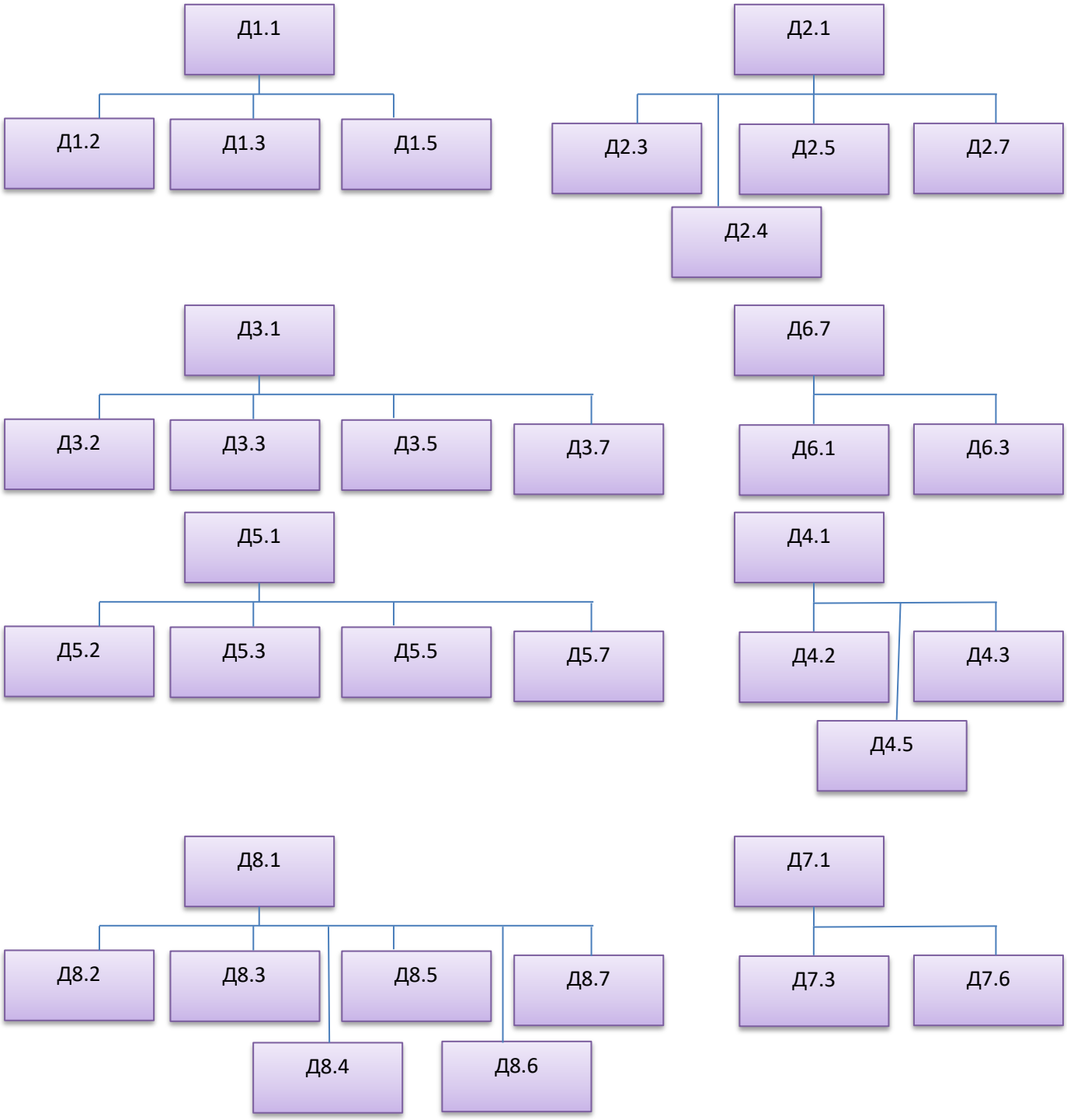

Рисунок А.5 – Схема інформаційних потоків

1 – директор,

2 – комерційний директор, заступник директора з виробництва, технічний директор, заступник директора з економіки й управління,

3 – заступник директора з економічної безпеки,

4 – відділ кадрів,

5 – відділ економічної безпеки,

6 – начальник служби охорони,

7 – бухгалтерія, відділів ЗЕД, маркетингу, збуту, закупівель, фінансового відділу, договірно-планового відділу,

Д1 – Відомості стратегічного характеру

Д2 – Ділова інформація

Д3 – Відомості по фінансам

Д4 – Відомості економічного характеру

Д5 – Відомості технічного характеру

Д6 – Відомості по касі

Д7 – Відомості про стан режиму безпеки

Д8 – Інші відомості