ТЕМА 1
ОСНОВНІ ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Загальні відомості

Поняття «інформаційна безпека» з'явилось завдяки розвитку засобів інформаційних комунікацій серед суспільства. У сучасному світі стрімкий розвиток інформаційних технологій не є новиною. Збільшується кількість інформаційних систем, програмних забезпечень, які допомагають персоналу підприємства управляти інформаційними потоками. Відповідно до цього збільшується кількість цінної інформації. Тому питання про її захист стоїть досить гостро. Необхідно зазначити, що у науковій літературі відсутній єдиний погляд на зміст поняття інформаційна безпека».

Під поняттям «інформаційна безпека» розуміють стан (рівень) захищеності інформаційних ресурсів – інформаційних об'єктів та інформаційних систем – від негативних впливів (як випадкових, так і здійснюваних навмисно), які можуть завдати шкоди самій інформації та засобам її передачі та обробки, а, отже, негативно відбитися на власниках інформаційних ресурсів, державі, суспільстві та інших учасниках процесів інформаційного обміну. Більшість сучасних інформаційних ресурсів, а також інформаційних систем практично не можуть розглядатися у відриві від комплексу елементів (факторів), пов'язаних із забезпеченням інформаційної безпеки: загроз для інформаційних ресурсів, різних засобів і заходів захисту, бар'єрів для проникнення, а також вразливостей в системах захисту інформації. *Таким чином, під інформаційною безпекою в більш загальному вигляді можна визначити як* сукупність засобів, методів і процесів (процедур), які забезпечують захист інформаційних активів і гарантують збереження ефективності та практичної корисності як технічної інфраструктури інформаційних систем, так і відомостей, які в таких системах зберігаються і обробляються. Мета інформаційної безпеки полягає в тому, щоб зберегти цілісність, повноту та точність інформації, зменшити ризик несанкціонованих змін в інформаційних системах. Для того, щоб забезпечити підприємству розвиток та конкурентоспроможність, необхідно створити систему управління інформаційною безпекою.

Система управління інформаційною безпекою СУІБ (*information security management system*, ISMS) – частина загальної системи управління, яка призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки.

Для процесів СУІБ застосована модель PDCA (плануй-виконуй-перевіряй-дій; *Plan-Do-Check-Act, PDCA*):

- Plan (планування) – фаза створення СУІБ, створення переліку активів, оцінки ризиків та вибору заходів;
- Do (дія) – етап реалізації та впровадження відповідних заходів;
- Check (перевірка) – фаза оцінки ефективності та продуктивності СУІБ. Зазвичай виконується внутрішніми аудиторами;
- Act (поліпшення) – виконання превентивних і коригуючих дій

Побудова СУІБ дозволяє чітко визначити, як взаємопов'язані процеси та підсистеми ІБ, хто за них відповідає, які фінансові та трудові ресурси необхідні для їх ефективного функціонування і т.д.

Основні функції системи управління інформаційною безпекою:

- виявлення та аналіз ризиків інформаційної безпеки;
- планування та практична реалізація процесів, спрямованих на мінімізацію ризиків ІБ;
- контроль цих процесів;
- внесення в процеси мінімізації інформаційних ризиків необхідних коригувань.

Якісне управління інформаційною безпекою базується на наступних принципах:

- комплексний підхід – управління ІБ має бути всеосяжним, охоплювати всі компоненти ІС і враховувати всі актуальні ризикоутворюючі фактори, що діють в інформаційній системі підприємства та за її межами;
- узгодженість з бізнес-задачами і стратегією підприємства;
- високий рівень керованості;
- адекватність інформації, яка використовується і генерується;
- ефективність – оптимальний баланс між можливостями, продуктивністю і витратами СУІБ;

- безперервність управління;
- процесний підхід – зв’язування процесів управління в замкнутий цикл планування, впровадження, перевірки, аудиту та коригування, і підтримка нерозривного зв’язку між етапами.

Відповідно до ISMS Framework (https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-isms/framework), що є Європейським аналогом СУІБ, який розроблено міжнародною європейскою агенцією з кібербезпеки, управління безпекою відбувається за схемою, відображеною на рисунку 1.1.

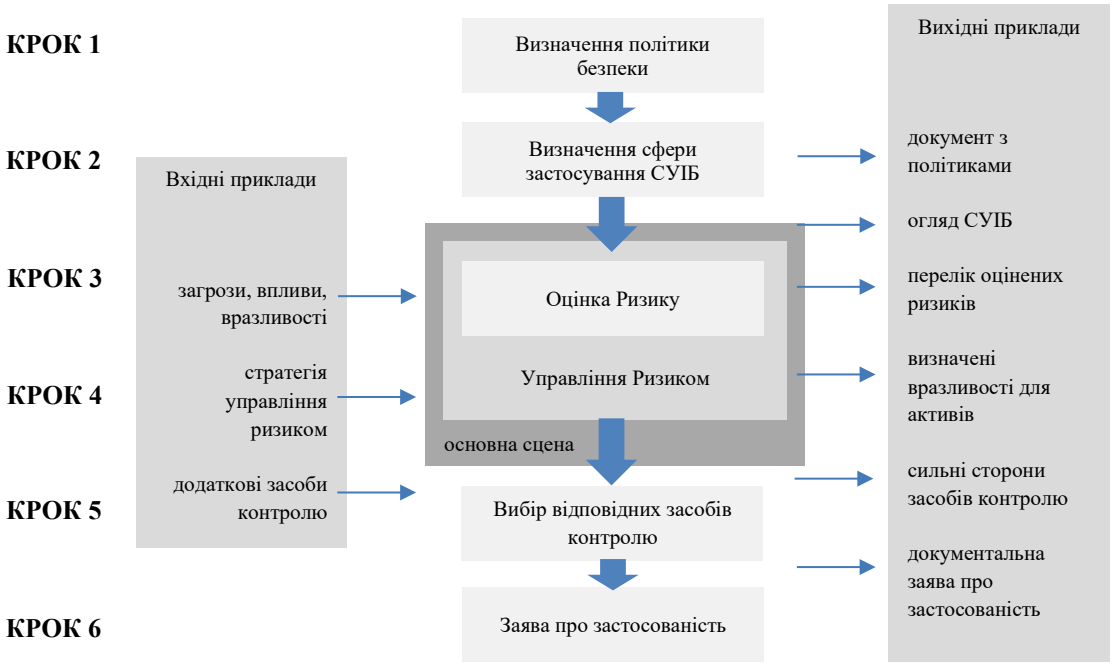

Рисунок 1.1 – СУІБ відповідно до фреймворку ISMS від ENISA

І розмір компанії, й конкретна діяльність організації диктує вимоги, пов’язані з безпекою, на правовому, регуляторному та операційному рівнях.

Малі підприємства з обмеженою інфраструктурою інформаційних систем, діяльність яких не вимагає обробки, зберігання та обробки персональних або конфіденційних даних, зазвичай стикаються з незначними ризиками або ризиками з меншою ймовірністю чи наслідком. Ці організації, швидше за все, не підтримують незалежну СУІБ та зазвичай займаються ризиками інформаційної безпеки спеціально або як частина більш широкого процесу управління ризиками.

Більші організації та організації, такі як банки та фінансові інститути, оператори телекомунікацій, лікарні та інститути охорони здоров'я, державні чи державні органи, мають багато причин для того, щоб дуже серйозно вирішувати питання захисту інформації. Законодавчі та нормативні вимоги, спрямовані на захист конфіденційних або особистих даних, а також загальні вимоги громадської безпеки спонукають їх приділяти найбільшу увагу та пріоритет ризикам інформаційної безпеки.

За цих обставин розробка та впровадження окремого та незалежного процесу управління, а саме Системи управління інформаційною безпекою, є єдиною альтернативою.

Як показано на рисунку вище, розробка системи СУІБ передбачає такі шість кроків:

- визначення політики безпеки;
- визначення сфери застосування СУІБ;
- оцінка ризику (як частина управління ризиками);
- управління ризиками;
- вибір відповідних засобів контролю;
- заява про застосовність

Етапи 3 та 4, процес оцінки та управління ризиками, складають суть СУІБ і є процесами, які, з одного боку, «перетворюють» правила та керівні принципи політики безпеки та цілей; а з іншого – перетворюють цілі СУІБ у конкретні плани реалізації засобів контролю та механізмів, спрямованих на мінімізацію загроз та вразливостей. Варто зазначити, що кроки 3 та 4 розглядаються як єдине ціле, а саме фактично – управління ризиками.

Процеси та дії, пов'язані з кроками 5 та 6, не стосуються інформаційних ризиків. Вони швидше пов'язані з оперативними діями, необхідними для технічного впровадження, обслуговування та контролю вимірювань безпеки.

Відповідні засоби контролю можуть бути отримані або з існуючих (вичерпних) наборів засобів контролю або механізмів, зазвичай включених до стандартів захисту інформації (наприклад, [ISO 17799]) та керівних принципів, або бути результатом поєднання або адаптації запропонованих засобів контролю до конкретних

організаційних вимог або експлуатаційні характеристики.

В обох випадках, кроком 6 є документоване відображення виявлених ризиків, застосованих до конкретної організації з технічним впровадженням механізмів безпеки, які організація вирішила застосувати.

Нарешті, слід зазначити, що хоча СУІБ – це повторюваний процес у цілому, у більшості типів організацій, згаданих вище, кроки 1 та 2 повторюються у більш тривалому циклі, ніж кроки 3,4,5 та 6. Так відбувається в основному тому, що встановлення політики безпеки та визначення сфери застосування СУІБ частіше є управлінськими та (до певної міри) стратегічними проблемами, тоді як процес управління ризиками є, «повсякденною» оперативною проблемою.

Одним з ключових чинників успішності системи управління інформаційною безпекою підприємства – це побудова її на базі міжнародних стандартів ISO/IEC 27001.

Міжнародний стандарт ISO 27001 надає інструмент для розробки, впровадження, супроводу, моніторингу, підтримки та вдосконалення добре документованої системи управління інформаційною безпекою в контексті розгляду бізнес ризиків.

СУІБ забезпечує вибір адекватних і пропорційних методів і засобів контролю та захисту інформації і, тим самим, довіру зацікавлених сторін. Проте слід брати до уваги й інші стандарти в сфері інформаційної безпеки. На даний момент у світовій практиці використовується велика кількість стандартів, методик та інших документів, що регламентують процеси управління інформаційною безпекою, наприклад ISM3, COBIT, ITIL / ITSM, BSI-100-2, ISO13335-4, CRAMM, ISO15408. Але варто відмітити, що всі вони сумісні з ISO 27001, а також подібні до нього.

Поняття інформаційної безпеки нерозривно пов’язане з **ризиками** для інформаційних ресурсів, під якими (ризиками) розуміється можливість (ймовірність) нанесення шкоди інформаційним ресурсам, зниження рівня їх захищеності.

1.2 Ризики, їх класифікація

Ризики можуть мати різну природу і характеристики; однією з основних класифікацій ризиків для інформаційної безпеки (так само, як і багатьох інших ризиків в економіці та управлінні) є їх поділ на:

- системні ризики – некеровані ризики, пов'язані з тим середовищем і технічною інфраструктурою, в якій функціонують інформаційні системи;
- операційні ризики – як правило, керовані ризики, пов'язані з особливостями використання певних інформаційних систем, їх технічної реалізації, застосовуваними алгоритмами, апаратними засобами тощо.

Всі негативні впливи на інформаційні активи, захист від яких (впливів) передбачає інформаційна безпека, можуть бути розділені на три основні види:

- порушення конфіденційності інформації;
- руйнування (втрата, необоротна зміна) інформації;
- недоступність інформаційних ресурсів – виникнення ситуацій, коли користувачі (всі або їх частина) на деякий період часу втрачають можливість доступу до необхідних даних (або інформаційних систем).

Безпосереднім джерелом ризиків і негативних впливів є загрози, під якими розуміються потенційні або реально можливі дії по відношенню до інформаційних ресурсів, що порушують інформаційну безпеку. Виділяється безліч типів загроз і безліч критеріїв для класифікації загроз інформаційній безпеці. Одним з **основних** таких **критеріїв є розташування джерела порушень** до інформаційних ресурсів, щодо яких здійснюється негативний вплив. Відповідно до цього критерію порушення можуть бути розділені:

- на обумовлені внутрішніми факторами (персоналом підприємства, роботою власних інформаційних систем);
- обумовлені зовнішніми факторами (зловмисниками, які не мають безпосереднього відношення до компанії – власника інформаційних активів, природними факторами тощо).

Іншим **важливим критерієм є наявність намірів здійснити порушення.** Відповідно до нього виділяють:

- цілеспрямовані дії (можуть бути здійснені як власним персоналом, так і зовнішніми противниками);
- випадковий вплив (помилки користувачів та адміністраторів, збої і випадкові порушення в роботі обладнання, непередбачений вплив природних факторів).

Також можна виділити наступні **класифікації загроз:**

- за об'єктом (персонал, матеріальні та фінансові кошти, інформація);
- за величиною збитку (граничний, значний, незначний);
- за ймовірністю виникнення (дуже вірогідні, ймовірні, малоймовірні);
- за типом збитку (моральний, матеріальний);
- деякі інші.

1.3 Способи порушення інформаційної безпеки

На практиці основними найбільш поширеними способами порушення інформаційної безпеки є:

- отримання несанкціонованого доступу (у тому числі і шляхом перевищення прав при санкціонованій роботі з інформаційними системами) до певних відомостей або масивів даних, поширення яких обмежене, з метою їх вивчення, копіювання, поширення, незаконного використання тощо;
- несанкціоноване використання інформаційних ресурсів (ресурсів обчислювальних і телекомунікаційних систем) з метою отримання вигоди або нанесення збитку (як тим системам, які незаконно використовуються, так і третім особам);
- несанкціонована зловмисна модифікація (зміна) даних;
- крадіжка грошових коштів в електронних платіжних системах і системах «клієнт-банк»;
- виведення з ладу (повне або часткове) програмних і апаратних засобів обробки, передачі та зберігання інформації;
- здійснення атак типу «відмова в обслуговуванні» – DoS (зокрема, щодо серверів в мережі Інтернет);
- поширення вірусів і інших шкідливих програм, що здійснюють різні негативні впливи.

Сучасна практика використання інформаційних систем характеризується великою кількістю і постійним зростанням числа порушень інформаційної безпеки. Одним з важливих чинників цього є постійно зростаюча доступність сучасних інформаційних технологій для злочинців, а також постійно зростаюча привабливість інформаційних систем як потенційних об'єктів нападу. Також важливою обставиною

є постійне ускладнення і зростання різноманітності інформаційних систем, що використовуються, і, зокрема, програмних продуктів. З урахуванням того, що в середньому кожна тисяча рядків програмного коду може містити від 5 до 15 помилок, поява все більшого числа різних вразливостей, що створюють загрози для інформаційної безпеки, стає практично неминучою.

Результатом цього є постійне зростання кількості різних порушень, пов'язаних з інформаційною безпекою.

Таким чином, всі перераховані обставини: зростання різноманіття можливих порушень, збільшення їх кількості, збільшення складності інформаційних технологій, постійно зростаюча доступність комп'ютерів і телекомунікаційних засобів для злочинців – пояснюють зростання потреби власників інформаційних ресурсів (підприємств, організацій, державних відомств) у реалізації систематичних, всеосяжних заходів щодо забезпечення інформаційної безпеки.

Окремі процеси, процедури, механізми та інструменти захисту інформації, використовувані власниками інформаційних ресурсів та інформаційних систем, можуть бути спрямовані:

- на обмеження і розмежування доступу;
- інформаційне приховування;
- введення надлишкової інформації і використання надлишкових інформаційних систем (засобів зберігання, обробки і передачі інформації);
- використання методів надійного зберігання, перетворення і передачі інформації;
- нормативно-адміністративне спонукання і примус.

На практиці сучасні технології захисту інформації побудовані на різних базових сервісах (таких, як автентифікація, забезпечення цілісності, контроль доступу та ін.), і використовують різні механізми забезпечення безпеки (такі, як шифрування, цифрові підписи, управління маршрутизацією тощо). Однак комплексність і масовість використання інформаційних технологій, їх інтеграція в повсякденну діяльність підприємств, організацій, урядових установ не дозволяють вирішувати завдання інформаційної безпеки тільки одними технічними засобами.

1.4 Організаційне забезпечення інформаційної безпеки

У всьому комплексі діяльності із захисту інформації одне з найбільш важливих місць займає організаційно-управлінська діяльність – організаційне забезпечення інформаційної безпеки, яке являє собою один з чотирьох основних напрямків роботи в загальній системі заходів у сфері інформаційної безпеки, що включає в себе також розробку спеціалізованого програмного забезпечення, виготовлення і використання спеціальних апаратних засобів і вдосконалення криптографічних (математичних) методів захисту інформації (рисунок 1.2).

Основними завданнями організаційно-управлінської діяльності (менеджменту) у сфері інформаційної безпеки є:

- забезпечення комплексності всіх рішень, реалізованих у процесі забезпечення інформаційної безпеки;
- забезпечення безперервності і цілісності процесів інформаційної безпеки;
- вирішення методичних завдань, що лежать в основі ефективного управління інформаційною безпекою, таких, як питання управління ризиками, економічне моделювання, тощо;
- управління людськими ресурсами та поведінкою персоналу з урахуванням необхідності вирішення завдань інформаційної безпеки.

Рисунок 1.2 – Структура діяльності в сфері інформаційної безпеки

Під комплексністю вирішення завдань інформаційної безпеки маються на увазі взаємопов'язані виявлення всіх значущих інформаційних об'єктів, а також існуючих і потенційно можливих загроз. На основі цього аналізу необхідно забезпечити вичерпно повне (комплексне) впровадження і застосування засобів захисту

інформації, які в тій чи іншій мірі могли б нейтралізувати всі істотні загрози на всіх потенційно вразливих ділянках проходження інформаційних потоків протягом всіх етапів життєвого циклу інформаційних систем та організаційних процедур. Заходи щодо нейтралізації ризиків також повинні бути реалізовані в комплексі з іншими механізмами, такими, як, наприклад, страхування. Іншими словами, завданням менеджменту є системне використання всіх необхідних (вузькоспеціальних) технологій і рішень для кожної конкретної ситуації таким чином, щоб у всій системі заходів із захисту інформаційних ресурсів не залишилося «вузьких місць» – уразливих ділянок, через які можуть бути здійснені напади і в яких можуть відбутися ненавмисні порушення. Складність такого роду завдань пов'язана з тим, що вони припускають по можливості вичерпний аналіз як всіх інформаційних ресурсів, так і всіх можливих сценаріїв нападу на них та подальший підбір найбільш придатних засобів захисту.

Неперервність процесів забезпечення інформаційної безпеки передбачає виділення необхідних ресурсів та організацію виконання необхідних функцій із захисту інформації протягом усього часу функціонування інформаційних систем і виконання бізнес-функцій.

Розробка, вдосконалення та підтримка в актуальному стані методичних основ управління інформаційною безпекою включає в себе, головним чином, застосування загальних для багатьох сфер менеджменту концепцій і теорій – таких як, наприклад, математичні моделі оцінки ризиків або теорія інвестиційного аналізу – стосовно до ресурсів, що використовуються для забезпечення інформаційної безпеки та інформаційних процесів.

Управління людськими ресурсами в рамках управління інформаційною безпекою включає в себе комплекс завдань, що охоплює всі основні аспекти діяльності людей: відбір і допуск персоналу до роботи з певними інформаційними ресурсами, навчання, контроль правильності виконання обов'язків, створення необхідних умов для роботи тощо.

При цьому конкретна структура і склад всіх основних завдань управління та організації у сфері інформаційної безпеки, а також методи, що безпосередньо використовуються, будуть визначатися як рівнем, на якому здійснюється

управлінська та організаційна діяльності, так і конкретними умовами, в яких функціонують інформаційні системи, які потребують захисту. Курс заснований на концепції поділу усього різноманіття методів і завдань організації та управління у сфері інформаційної безпеки на кілька основних рівнів і подальшому поданні організаційно-управлінських методів для кожного з цих рівнів.

Під організаційним забезпеченням та менеджментом у сфері інформаційної безпеки зазвичай прийнято розуміти рішення управлінських питань на рівні окремих суб'єктів (підприємств, організацій) або груп таких суб'єктів (партнерів по бізнесу, організацій, що спільно вирішують певні завдання і потребують захисту інформації).

Однак складність і комплексність сучасних проблем у сфері інформаційної безпеки, глобалізація інформаційних взаємодій вимагають більш повного і широкого розуміння організаційної роботи та менеджменту в цій галузі.

Зокрема, в час глобалізації інформаційних взаємодій, ускладнення програмних і апаратних засобів обробки інформації, проникнення інформаційних технологій у повсякденну діяльність всіх організацій і життя більшості людей з'явилася необхідність в спеціальних організаційних і управлінських зусиллях, спрямованих не скільки на забезпечення захищеності окремих інформаційних активів, як на підтримку різних елементів інформаційної інфраструктури, яка в тій чи іншій мірі працює на забезпечення інформаційної безпеки певних спільнот (заздалегідь не визначеної множини користувачів інформаційних систем і власників інформаційних ресурсів).

Таким чином, з розвитком інформаційних технологій і інтенсифікацією інформаційного обміну організаційна та управлінська робота у сфері інформаційної безпеки виявляється спрямованою не тільки на власне захист певних інформаційних ресурсів, але і на більш «глобальний» об'єкт – створення і розвиток безпечної інформаційної інфраструктури (у різних значеннях цього терміну і з урахуванням різних його аспектів). На практиці така інфраструктура може включати в себе:

- надійну інфраструктуру передачі інформації і ринок послуг доступу до таких каналів зв'язку;
- ринок програмних і апаратних засобів, що забезпечують захист інформації;
- систему підготовки, перепідготовки та підвищення кваліфікації фахівців у

сфері інформаційної безпеки;

- загальні правила використання інформації, а також її передачі, спільної експлуатації інформаційних мереж (у тому числі протоколи інформаційного обміну);
- систему обміну інформацією та поширення знань про існуючі вразливості тих чи інших інформаційних технологій, про можливі загрози інформаційній безпеці та способи їх нейтралізації;
- законодавчу і правочинну систему, що забезпечує охорону майнових та інших інтересів всіх учасників інформаційного обміну;
- інші складові.

Потреба в цілеспрямованому розвитку та підтримці такої інфраструктури породжує необхідність у виробленні специфічних організаційних і управлінських прийомів, як правило, не характерних для інформаційної безпеки в звичному («вузькому») її розумінні.

Таке розширення сфери інтересів менеджменту інформаційної безпеки пояснює причини, за якими необхідно розділяти кілька відносно самостійних організаційних рівнів, що характеризуються специфічними завданнями, підходами до вирішення цих завдань і організаційними методами, які застосовуються.

- Рівень міжнародних професійних об'єднань (як правило, неурядових і некомерційних), так чи інакше пов'язаних зі сферою інформаційних технологій, телекомунікацій та інформаційної безпеки.
- Рівень великих компаній, що працюють у сфері інформаційних технологій і значною мірою визначають (прямо чи опосередковано) стан інформаційної безпеки в співтоваристві користувачів інформаційних систем, а також впливають на безпеку різних елементів інформаційної інфраструктури.
- Державний рівень – рівень державних і міжурядових організацій, які так чи інакше впливають на життя суспільства, стан правової системи, розвиток економіки і технологій.
- Рівень окремих компаній (підприємств та організацій) – спільнота користувачів інформаційних систем, так чи інакше зацікавлених у власній інформаційній безпеці та забезпечують захист наявних у них інформаційних

ресурсів власними силами.

Також окремо можна виділити додатковий проміжний рівень, до складу якого входять консалтингові та впроваджувальні компанії, навчальні центри (включаючи також спільноту фахівців, що займаються консультаціями, впровадженням і навчанням в індивідуальному порядку), що працюють у сфері інформаційної безпеки та діють як сполучна ланка між різними організаційними рівнями, а також представляють інтереси різних учасників інформаційної взаємодії. Всі ці складові утворюють своєрідну організаційну ієрархію, представлену на рисунку 1.3.

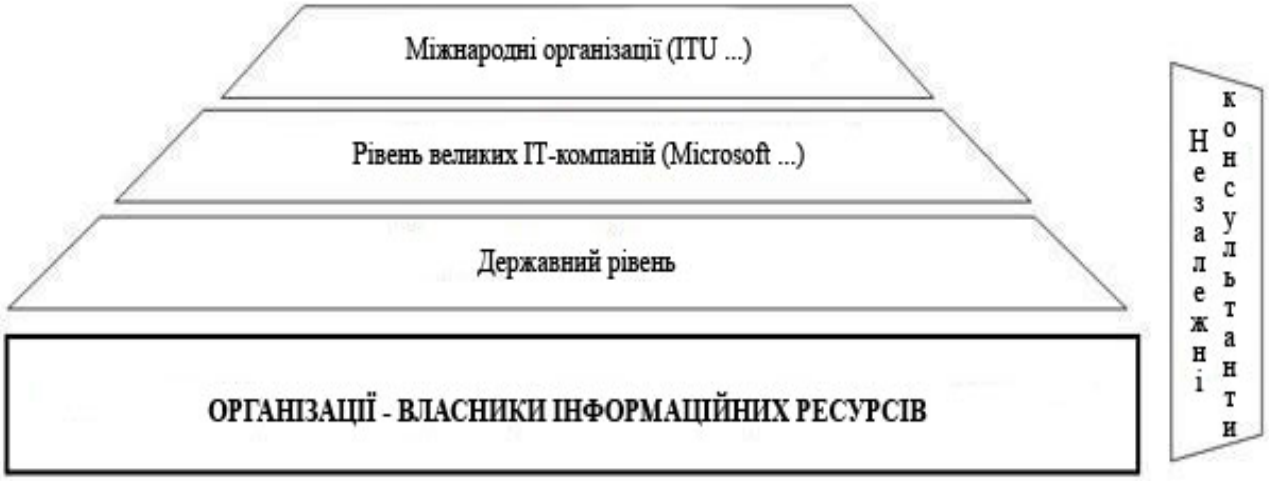

Рисунок 1.3 – Ієрархія рівнів організаційної роботи у сфері інформаційної безпеки

Слід розуміти, що суб'єкти, що перебувають на верхніх щаблях цієї ієрархії (зокрема, державні органи, великі IT-корпорації), виступають не тільки як володільці власних інформаційних ресурсів, що вимагають захисту, але і як суб'єкти, які впливають на інфраструктуру, що лежить в основі обміну та збереження інформації, а також на суспільно-економічні відносини, що впливають на інформаційну безпеку. І той факт, що такі суб'єкти самі приділяють значну увагу захисту власних ресурсів (вкладають істотні кошти в забезпечення інформаційної безпеки, ініціюють нові розробки для власних потреб, використовують найбільш передові технології в цій сфері тощо), не повинен відволікати увагу від тієї обставини, що ці суб'єкти фактично створюють інфраструктуру для повсякденної діяльності безлічі компаній, організацій, людей, професійних і бізнес-співтовариств і використовують для цього організаційні методи та прийоми, які суттєво відрізняються за своєю природою від

методів, характерних для роботи із забезпечення інформаційної безпеки окремих суб'єктів і захисту окремих інформаційних активів.

Отже, необхідність самостійного розгляду суб'єктів, які належать до верхнього рівня, з точки зору організаційного забезпечення інформаційної безпеки обумовлена тим, що у зв'язку зі своєю особливою («інфраструктурною») роллю в системі суспільних відносин та інформаційного обміну ці суб'єкти використовують специфічні методи організаційно-управлінської роботи. При цьому, як правило, паралельно із застосуванням таких специфічних методів вони використовують і методи, характерні для суб'єктів нижнього рівня представленої ієрархії, так як є володільцями власних інформаційних ресурсів.

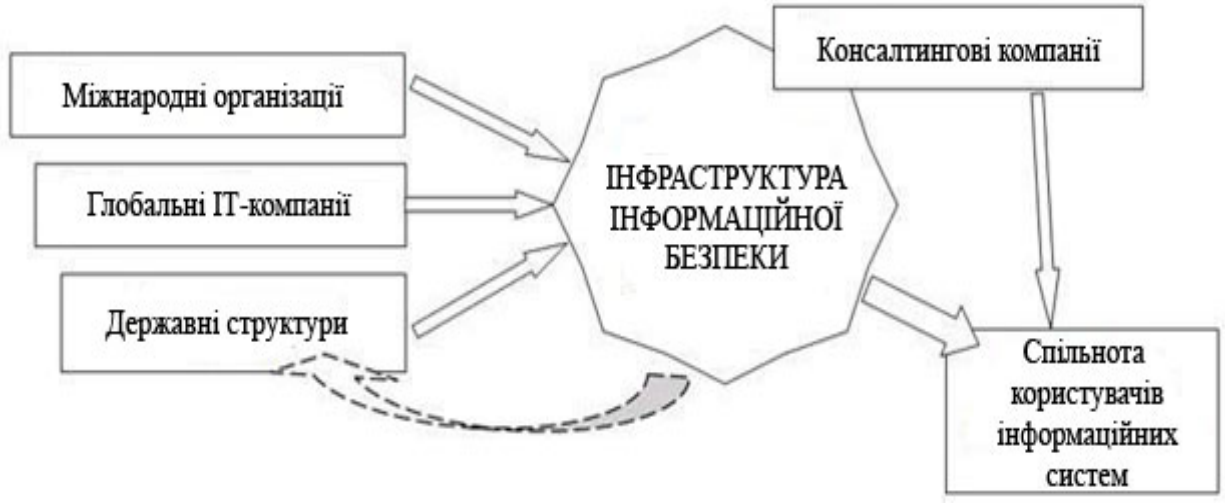

Рисунок 1.4 – Взаємозв'язки рівнів організації інформаційної безпеки

Представлений поділ на рівні повинен бути основою для більш цілеспрямованого розвитку системи менеджменту та налагодження взаємозв'язків між різними рівнями організаційної роботи (див. рисунок 1.4). Важливість виділення і самостійного розгляду верхніх рівнів управлінської роботи обумовлена тим, що цілеспрямоване усвідомлення організаційних питань, специфічних для верхніх рівнів ієрархії та їх вирішення дозволить більш ефективно вирішувати завдання розвитку національних та регіональних економік в цілому та окремих галузей (телекомунікації, фінансові послуги тощо), а не тільки вирішувати завдання окремих суб'єктів, що беруть участь в інформаційному обміні.

Основні особливості організаційної роботи на кожному з перерахованих рівнів організації представлені в таблиці 1.1.

Таблиця 1.1 – **Завдання, ролі і методи, що використовуються на різних рівнях організаційної роботи у сфері інформаційної безпеки**

Організаційний рівень	**Основні завдання і ролі**	**Основні специфічні методи організаційної роботи**
1. Міжнародні організації	Розробка правил і стандартів (у тому числі і мережевих протоколів), що мають глобальне значення. Обмін актуальною інформацією і попередженнями про нові загрози	Координація роботи фахівців, експертів та дослідників, що представляють різні зацікавлені сторонни
2. Глобальні IT-компанії	Методологічна та організаційна підтримка використання продуктів і послуг, що поставляються на ринок	Гнучка взаємодія з клієнтами (користувачами продуктів і послуг) з метою підвищення ефективності використання інформаційних систем і отримання відгуків для подальшого підвищення якості наданих продуктів і послуг
3. Державні організації	Регулювання використання інформаційних систем і поширення інформації з метою недопущення протиправних дій, збитку іншим учасникам інформаційного обміну, суспільству та державним органам	Розробка національних і міжнародних правил (законів, конвенцій, угод тощо), що регулюють відносини в інформаційній сфері. Здійснення контролю (в різних формах). Здійснення правочинної та правоохоронної діяльності
4. Користувачі інформаційних систем – власники інформації	Захист власних інформаційних ресурсів	Виділення підрозділів та фахівців, що відповідають за ІБ. Розробка і застосування внутрішніх політик і правил безпеки
5. Консалтингові та впроваджувальні компанії, що працюють в сфері ІБ	Виконання деяких функцій ІБ на умовах аутсорсингу. Розробка та впровадження індивідуальних рішень у сфері ІБ більш ефективно, ніж це могли б зробити самі власники інформаційних ресурсів	Накопичення та узагальнення теоретичних знань і практичних навичок з метою створення та впровадження організаційних і технічних рішень в інтересах клієнтів

Таблиця 1.1, а також рисунок 1.3 наочно демонструють причини, за якими кожен з рівнів організаційної роботи у сфері інформаційної безпеки потребує індивідуального підходу й застосування специфічних методів організації та управління. Відповідно до цього поділу і будується структура даного курсу – вона включає в себе розгляд основних форм і прийомів організації роботи щодо забезпечення інформаційної безпеки на основних організаційних рівнях:

- на рівні міжнародних професіональних організацій та бізнес-спільнот;
- на рівні великих постачальників технічних (програмних і апаратних) засобів обробки і передачі інформації, що мають вплив на стан інформаційної безпеки великого числа підприємств, організацій та індивідуальних користувачів;
- на рівні державних органів (зокрема, урядів окремих країн);
- на рівні окремих підприємств, установ та організацій, що є безпосередніми власниками та користувачами інформаційних ресурсів.

Також розглядаються питання роботи спеціалізованих компаній (консалтингових, технологічних, страхових), що надають різні послуги, які пов'язані із забезпеченням інформаційної безпеки.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ:

1. Дайте визначення поняття інформаційна безпека. Назвіть основні чинники, які на неї негативно впливають, та методи, завдяки яким цьому можна запобігти.
2. Що таке загроза?
3. Назвіть види загроз.
4. Дайте визначення поняття ризик.
5. Назвіть види ризиків.
6. Назвіть основні способи порушення інформаційної безпеки.
7. Дайте визначення поняття СУІБ.
8. Прокоментуйте модель PDCA.