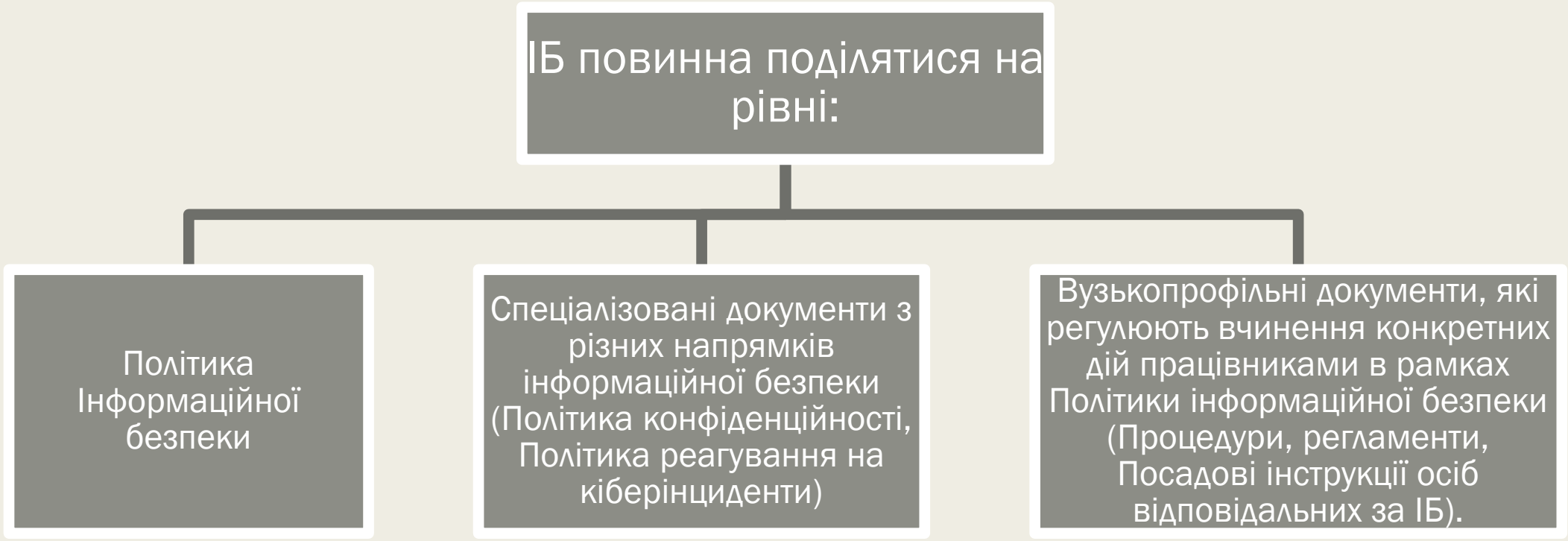
УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ

Лекція 2. Політика Інформаційної безпеки

1. Пакет документів з ІБ.
2. Основні принципи розробки політики інформаційної безпеки.
3. Види політик безпеки.
4. Основні принципи політики забезпечення ІБ підприємства.

Пакет документів з Інформаційної безпеки



*При розробці **Політики Інформаційної безпеки** та інших документів для забезпечення кібербезпеки на підприємстві, потрібно виходити з необхідності встановлення захисту системи від зовнішніх та внутрішніх атак та гнучкості, важливої для розуміння документів працівниками.*

Пакет документів з Інформаційної безпеки

Політики (Що?)

декларативно визначають стан безпеки відповідно до вимог законодавства, стандартів та найкращих світових практик кібербезпеки

Процедури (Як?)

описують дії, які треба виконати, щоб досягти стану безпеки, визначеного Політикою інформаційної безпеки, та підтримувати його на рівні, також визначеному цією Політикою

Посадові обов’язки (Хто?)

описують компетенції, якими повинні володіти люди, відповідальні за втілення політик у життя

Технічні завдання (Чим?)

встановлюють вимоги до інструментів реалізації політик

Ключові документи

Політика Інформаційної безпеки

- Набір вимог, правил, обмежень та рекомендацій, які регламентують порядок інформаційної діяльності в організації.
- *Така політика являє собою Конституцію з Інформаційної безпеки, яку повинен знати і виконувати кожен працівник компанії.*

Політика конфіденційності та захисту персональних даних

- Цей документ регулює порядок допуску працівників до конфіденційної інформації та інформації, що містить персональні дані.
- *Допоможе налагодити роботу з документами, що містять інформацію з обмеженим доступом та чітко пояснить працівникам, чому не можна розголошувати конфіденційну інформацію і якими наслідками це загрожує.*

Політика реагування на кіберінциденти

- Містить алгоритм дій відповідальних осіб та рядових працівників у випадку здійснення кібератаки, чи іншого кіберінцидента у компанії.
- *Політика реагування – це керівництво, яке містить порядок дій у випадку виникнення кіберінциденту, головна задача якого – миттєве реагування на критичну ситуацію, яке дасть змогу врятувати якомога більшу кількість даних, зберегти систему у максимально робочому стані та зібрати інформацію для майбутнього розслідування спеціалізованими правоохоронними органами.*

Ключові документи

Положення про внутрішні процеси роботи з персональними даними

- Регулює порядок зберігання, обробки та знищення персональних даних працівників, клієнтів та третіх осіб в розрізі конкретних обов’язків працівників в компанії .
- *Завданням цього внутрішнього положення є автоматизація процесу роботи працівників з персональними даними та регламентація їх прав та обов’язків.*

Положення про шифрування даних та ведення парольної політики

- Містить вимоги складення паролів та алгоритми шифрування даних, що використовуються компанією.
- *Дане Положення привнесе до життя компанії високі стандарти безпеки та порядок роботи з алгоритмом шифрування.*

Додаткові документи

Положення про порядок роботи з платіжними системами

- Набір вимог до працівників з використання платіжних систем та систем розрахунків з урахуванням вимог інформаційної безпеки.

Політика щодо навчання з інформаційної безпеки

- Містить порядок проведення навчання з інформаційної безпеки з використанням власних та запрошених лекторів та вимоги до необхідного рівня знань для кожної категорії працівників компанії.

Положення про службу інформаційної безпеки

- Містить інформацію про структуру, регулює порядок роботи, підпорядкування та відповідальність працівників служби інформаційної безпеки.

Мінімальний набір документів, необхідних для ISO/IEC версії 2013:

№ п/п	Документи	Номер пункту стандарту
1	Область дії	4.3
2	Політика інформаційної безпеки	5.2, 6.2
3	Методологія оцінки і обробки ризиків	6.1.2
4	Положення про застосування	6.1.3 d)
5	План усунення ризиків	6.1.3 e), 6.2
6	Звіт про оцінку ризиків	8.2
7	Процедура управління документами	7.5
8	Процедура управління записами	7.5
9	Порядок внутрішнього аудиту	9.2
10	Порядок усунення несправностей	10.1

Мінімальний набір документів, необхідних для ISO/IEC версії 2013:

№ п/п	Документи	Номер пункту стандарту
11	Визначення ролей і обов’язків	A.7.1.2, A.13.2.4
12	Матеріально-технічні ресурси активів	A.8.1.1
13	Допустиме використання активів	A.8.1.3
14	Політика управління доступом	A.9.1.1
15	Політика управління IT	A.12.1.1
16	Принципи розробки захищеної системи	A.14.2.5
17	Політика безпеки постачальника	A.15.1.1
18	Процедура управління інцидентами	A.16.1.5
19	Процедурі безперервності бізнесу	A.17.1.2
20	Юридичні, регулюючі і договорні вимоги	A.18.1.1

Документи, що не є обов’язковими з точки зору стандарту:

№ п/п	Документи	Номер пункту стандарту
1	Політика використання власних пристроїв (BYOD)	A.6.2.1
2	Мобільні пристрої і політика віддаленого доступу	A.6.2.1
3	Політика класифікації інформації	A.8.2.1, A.8.2.2, A.8.2.3
4	Парольна політика	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.3
5	Політика знищення та утилізції	A.8.3.2, A.11.2.7
6	Процедура для роботи в контрольованих зонах	A.11.1.5
7	Політика чистого екрану і робочого столу	A.11.2.9
8	Політика управління змінами	A.12.1.2, A.14.2.4
9	Політика резервного копіювання	A.12.3.1
10	Політика передачі інформації	A.13.2.1, A.13.2.2, A.13.2.3
11	Аналіз впливу на бізнес	A.17.1.1
12	План тестування	A.17.1.3
13	Технічне обслуговування і огляд плану	A.17.1.3
14	Стратегія безперервності бізнесу	A.17.2.1

Типова структура документа СУІБ

1. Ціль створення документа
2. Область дії документа, ролі і обов’язки задіяних сторін
3. Посилання на перехресні документи
4. Основна частина документа, яка містить саму суть політики, процедури і т.д.
5. Розділ про перегляд документа з вказуванням терміну перегляду
6. Історія змін

Документ про політику інформаційної безпеки

Має містити:

- визначення інформаційної безпеки, її основні цілі і область її застосування, а також її значення як механізму, що дає можливість колективно використовувати інформацію
- виклад позиції керівництва по питаннях реалізації цілей і принципів інформаційної безпеки
- роз'яснення конкретних варіантів політики безпеки, принципів, стандартів і вимог до її дотримання, включаючи:
  - виконання правових і договірних вимог;
  - вимоги до навчання персоналу правилам безпеки;
  - політика попередження і виявлення вірусів;
  - політика забезпечення безперебійної роботи організації.
- визначення загальних і конкретних обов'язків по забезпеченню режиму інформаційної безпеки
- роз'яснення процесу повідомлення про події, що становлять загрозу безпеці

Законодавче регулювання Політик ІБ

На сьогодні в Україні немає чітко врегулювання вимог до Інформаційної безпеки на підприємствах. При цьому є вимоги, які ставляться до компаній, які працюють з персональними даними громадян Європейського союзу відповідно до вимог General data protection regulation (GDPR), та деяких інших нормативних актів.

GDPR – Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб щодо обробки персональних даних та про вільне переміщення таких даних; про відміну Директиви 95/46/ЄС (GDPR набрав чинності 25 травня 2018 року).

Основні вимоги GDPR:

1. **Дотримуватися принципів обробки персональних даних**
2. Персональні дані слід обробляти прозоро, справедливо та законно *(Lawfulness, fairness and transparency).*
3. Персональні дані можна обробляти лише для явно вказаних законних цілей *(Purpose limitation).*
4. Збирати та зберігати слід лише мінімальну кількість персональних даних, достатніх для зазначеної мети *(Data minimisation).*
5. Персональні дані мають обмежений термін зберігання, не більше ніж це необхідно для певної мети *(Storage limitation).*
6. Забезпечення точності персональних даних, а також можливості їх редагування та видалення *(Accuracy).*
7. Забезпечення безпеки, цілісності та конфіденційності персональних даних *(Integrity and confidentiality).*
8. Контролер повинен бути готовим і здатним продемонструвати дотримання вищезазначених принципів *(Accountability).*
9. **Реалізовувати права суб'єктів даних**

Основні принципи розробки політики інформаційної безпеки

Розробка та реалізація політик безпеки є важливим завданням для кожної організації, яка прагне захистити свої інформаційні активи. Ефективні політики безпеки допомагають знизити ризики кібератак, витоку даних, несанкціонованого доступу та інших загроз.

Розробка ефективної політики ІБ підприємства базується на кількох основних принципах:

Визначення мети та об'єктів захисту.

Варто враховувати, які дані ви плануєте захистити, та правильно розставити пріоритети.

Аналіз загроз і визначення ризиків.

Це можуть бути кібератаки, витік даних, несанкціонований доступ, фізичні загрози тощо.

Встановлення правил і процедур безпеки.

Необхідно розробити правила та процедури, які допоможуть розподілити доступ до інформації та використання інформаційних систем відповідно до особливостей кожного користувача.

Впровадження цих принципів під час розробки політик безпеки допоможе створити надійну систему захисту інформації, яка відповідатиме потребам бізнесу.

Компоненти політики інформаційної безпеки підприємства

- Аутентифікація та авторизація користувачів відповідно до рівня їх доступу до системи
- Шифрування конфіденційної інформації під час зберігання та використання
- Захист від витоку інформації шляхом встановлення чітких правил
- Моніторинг та аудиту безпеки

Рекомендується регулярно проводити навчання користувачів і реагувати на конкретні випадки, щоб створити якісну систему захисту інформації.

Етапи розробки та впровадження політик безпеки

Аналіз потреб користувачів і визначення конкретних вимог

- Варто проаналізувати потреби бізнесу, провести оцінку можливих ризиків і зібрати інформацію.

Розробка політик і процедур безпеки

- На цьому етапі розробляються чіткі та лаконічні правила, що охоплюють всі аспекти захисту інформації.

Тестування та впровадження політик безпеки.

- Потрібно перевірити працездатність розроблених рішень і впровадити їх в роботу.

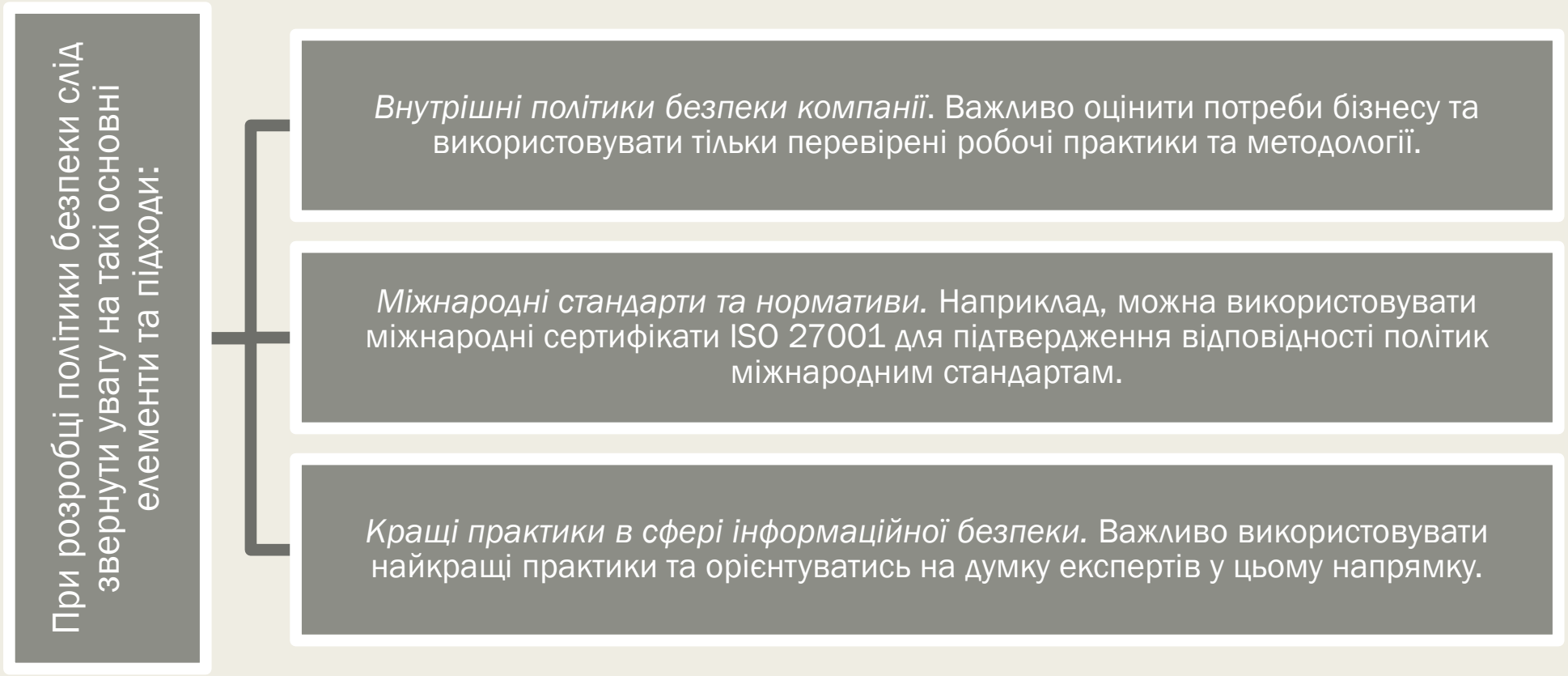
Постійне оновлення та адаптація політик до змін у загрозах і технологіях.

- Важливо слідкувати за всіма змінами та своєчасно впроваджувати оновлення.

Розробка та впровадження ефективних політик безпеки - це постійний процес, який потребує ретельного планування та виконання

Варто постійно оцінювати свою систему безпеки та вносити необхідні зміни, щоб вона залишалася ефективною.

Вибір та порівняння різних підходів до розробки політик безпеки



Слід використовувати комбінацію цих підходів для забезпечення всебічної та ефективної системи захисту інформації.

Розробка політик інформаційної безпеки під час забезпечення бізнес-процесів

Політика інформаційної безпеки виступає як документ або багаторівнева система документів, які визначають вимоги безпеки, систему заходів або порядок дій, відповідальність співробітників та механізми контролю задля забезпечення інформаційної безпеки підприємства.

У документ політики безпеки рекомендовано вносити наступні розділи:	Вступний розділ, що підтверджує стурбованість керівництва проблемами інформаційної безпеки
	Організаційний розділ, що описує підрозділи, комісії, групи осіб, відповідальні за роботи в області інформаційної безпеки.
	Класифікаційний розділ, що описує матеріальні та інформаційні ресурси підприємства та необхідний рівень їх захисту
	Штатний розділ, що характеризує заходи безпеки щодо персоналу
	Розділ, що висвітлює питання фізичного захисту інформації
	Розділ управління, що описує підхід до управління комп'ютерами та комп'ютерними мережами пересилання даних.
	Розділ, що зазначає правила розмежування доступу до інформації.
	Розділ, що описує заходи, спрямовані на забезпечення безперервної роботи підприємства (доступності інформації).

Політика інформаційної безпеки

Політика інформаційної безпеки (ПІБ) – набір законів, правил і практичних рекомендацій і практичного досвіду, що визначають управлінські і проектні рішення в області ЗІ. На основі ПІБ будується керування, захист і розподіл критичної інформації в системі. Вона повинна охоплювати всі особливості процесу обробки інформації, визначаючи поводження ІС у різних ситуаціях.

Ефективна політика інформаційної безпеки визначає необхідний та достатній набір вимог безпеки. Вона мінімально впливає на продуктивність праці, враховує особливості бізнес-процесів підприємства, підтримується керівництвом, позитивно сприймається й виконується співробітниками підприємства.

Відповідно до запропонованого підходу політика (заходи) інформаційної безпеки реалізується відповідною структурою органів на основі нормативно-методичної бази з використанням програмно-технічних методів і засобів, що визначають архітектуру системи захисту.

ПІБ переслідує такі **головні цілі**:

- продемонструвати співробітникам важливість захисту мережного середовища,
- описати їхню роль у забезпеченні безпеки
- розподілити конкретні обов’язки по захисту інформації, що циркулює в мережі, так само як і самої мережі.

Принципи політики безпеки бізнес-процесів

Політика безпеки визначається як сукупність документованих управлінських рішень, спрямованих на захист інформації й асоційованих з нею ресурсів.
При розробці і проведенні її в життя доцільно керуватися наступними засадами:

Неможливість минати захисні засоби	Посилення самої слабкої ланки	Неприпустимість переходу у відкритий стан	Мінімізація привілеїв	Поділ обов'язків
• Стосовно межмережевих екранів принцип означає, що всі інформаційні потоки в мережу, що захищається, і з її повинні проходити через екран. Не повинно бути «таємних» модемних чи входів тестових ліній, що йдуть в обхід екрана.	• Надійність будь-якої оборони визначається самою слабкою ланкою. Часто самою слабкою ланкою виявляється не чи комп'ютер програма, а людина, і тоді проблема забезпечення інформаційної безпеки здобуває нетехнічний характер.	• При будь-яких обставинах (у тому числі позаштатних), СЗІ або цілком виконує свої функції, або повинна цілком блокувати доступ.	• Наказує виділяти користувачам і адміністраторам тільки ті права доступу, що необхідні їм для виконання службових обов'язків.	• Припускає такий розподіл ролей і відповідальності, при якому одна людина не може порушити критично важливий для організації процес. Це особливо важливо, щоб запобігти зловмисним чи некваліфікованим діям системного адміністратора.

Принципи політики безпеки бізнес-процесів

Політика безпеки визначається як сукупність документованих управлінських рішень, спрямованих на захист інформації й асоційованих з нею ресурсів.
При розробці і проведенні її в життя доцільно керуватися наступними засадами:

Багаторівневий захист	Розмаїтість захисних засобів	Простота і керованість інформаційної системи	Забезпечення загальної підтримки заходів безпеки
• наказує не покладатися на один захисний рубіж, яким би надійним він ні здавався. За засобами фізичного захисту повинні випливати програмно-технічні засоби, за ідентифікацією й автентифікацією – керування доступом і, як останній рубіж, – протоколювання й аудит.	• рекомендує організовувати різні за своїм характером оборонні рубежі, щоб від потенційного зловмисника було потрібно оволодіння різноманітними і, по можливості, несумісними між собою навичками подолання СЗІ.	• визначає можливість формального чи неформально доказу коректності реалізації механізмів захисту. Тільки в простій і керованій системі можна перевірити погодженість конфігурації різних компонентів і здійснити централізоване адміністрування.	• носить нетехнічний характер. Рекомендується із самого початку передбачити комплекс заходів, спрямований на забезпечення лояльності персоналу, на постійне навчання, теоретичне і, головне, практичне.

Види політики безпеки

Основу політики безпеки складає спосіб керування доступом, що визначає порядок доступу суб'єктів системи до об'єктів системи. Назву цього способу, як правило, визначає назва політики безпеки.

Для вивчення **властивостей способу керування доступом** створюється його формальний опис – **математична модель**. При цьому модель повинна відбивати стан всієї системи, її переходи з одного стану в інший, а також враховувати, які стани і переходи можна вважати безпечними в змісті даного керування. Без цього говорити про які-небудь властивості системи, і тим більше гарантувати їх, щонайменше некоректно.

В даний час найкраще вивчені **два види політики безпеки**: **виборча** і **повноважна**, засновані, відповідно на виборчому і повноважному способах керування доступом. Крім того, існує набір вимог, що підсилює дію цих політик і призначений для керування інформаційними потоками в системі.

Засоби захисту, призначені для реалізації будь-якого з названих способів керування доступом, тільки надають можливості надійного керування чи доступу до інформаційних потоків.

Визначення прав доступу суб'єктів до об'єктів і/чи інформаційних потоків (повноважень суб'єктів і атрибутів об'єктів, присвоєння міток критичності і т.д.) входить у компетенцію адміністрації системи.

Виборча політика безпеки

Основою є виборче керування доступом, що має на увазі, що:
– усі суб'єкти й об'єкти системи повинні бути ідентифіковані;
– права доступу суб'єкта до об'єкта системи визначаються на підставі деякого правила (властивість вибірковості).

Для опису властивостей виборчого керування доступом застосовується **модель системи на основі матриці доступу (МД).** Така модель одержала назву матричної.

$$M = \begin{array}{c} \\ C_1 \\ C_2 \\ \cdot \\ \cdot \\ C_{l-1} \\ C_l \end{array} \begin{array}{c} \begin{array}{cccc} O_1 & O_2 & \ldots & O_k \end{array} \\ \begin{bmatrix} r, w, d & w & \ldots & 0 \\ r & r, w, d & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & r \\ 0 & w & \ldots & r, w, d \end{bmatrix} \end{array}.$$

Матриця доступу - прямокутна матриця, у якій об'єкту системи відповідає рядок, а суб'єкту стовпець. На перетинанні стовпця і рядка матриці вказується тип дозволеного доступу суб'єкта до об'єкта. Звичайно виділяють такі типи доступу суб'єкта до об'єкта, як "доступ на читання", "доступна запис", "доступ на виконання" і ін.

Безліч об'єктів і типів доступу до них суб'єкта може змінюватися відповідно до деяких правил, що існують у даній системі. Визначення і зміна цих правил також є задачею МД.

Виборча політика безпеки

Рішення на доступ суб'єкта до об'єкта приймається відповідно до типу доступу, зазначеним у відповідній осередку матриці доступу. Звичайно виборче керування доступом реалізує принцип "що не дозволено, те заборонено", що припускає явний дозвіл доступу суб'єкта до об'єкта. Матриця доступу – найбільш простий підхід до моделювання систем доступу.

Виборча політика безпеки найбільш широко застосовується в комерційному секторі, тому що її реалізація на практиці відповідає вимогам комерційних організацій по розмежуванню доступу і підзвітності, а також має прийнятну вартість і невеликі накладні витрати.

$$M = \begin{array}{c} \\ C_1 \\ C_2 \\ \cdot \\ \cdot \\ C_{l-1} \\ C_l \end{array} \begin{array}{c} \begin{array}{cccc} O_1 & O_2 & \ldots & O_k \end{array} \\ \begin{bmatrix} r, w, d & w & \ldots & 0 \\ r & r, w, d & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & r \\ 0 & w & \ldots & r, w, d \end{bmatrix} \end{array}.$$

Повноважна політика безпеки

Основу складає повноважне керування доступом, що має на увазі, що:
– усі суб’єкти й об’єкти системи повинні бути однозначно ідентифіковані;
– кожному об’єкту системи привласнена мітка критичності, що визначає цінність інформації, що міститься в ньому;
– кожному суб’єкту системи привласнений рівень прозорості, що визначає максимальне значення мітки критичності об’єктів, до яких суб’єкт має доступ.

У тому випадку, коли сукупність міток має однакові значення, вважається, що вони належать до одного рівня безпеки. Організація міток має ієрархічну структуру і, таким чином, у системі можна реалізувати ієрархічно спадний потік інформації (наприклад, від рядових виконавців до керівництва). Чим важливіший об’єкт чи суб’єкт, тим вище його мітка критичності. Тому найбільш захищеними виявляються об’єкти з найбільш високими значеннями мітки критичності.

Кожен суб’єкт, крім рівня прозорості, має поточне значення рівня безпеки, що може змінюватися від деякого мінімального значення до значення його рівня прозорості.

Основне призначення повноважної політики безпеки – регулювання доступу суб’єктів системи до об’єктів з різним рівнем критичності і запобігання витоку інформації з верхніх рівнів посадової ієрархії на нижні, а також блокування можливого проникнення з нижніх рівнів на верхні. При цьому вона функціонує на тлі виборчої політики, додаючи її вимогам ієрархічно упорядкований характер (відповідно до рівнів безпеки).

Склад та зміст основних заходів щодо розробки політики ІБ

Організація заходів щодо захисту інформації

- запрошення кваліфікованого консультанта з безпеки;
- створення правил безпеки, до яких буде мати відношення кожен співробітник;
- забезпечення користувачів керівництвом, у якому викладений матеріал прийнятного обсягу;
- надання разом із усіма правилами модельних процеду впровадження і прикладів.

Організація заходів щодо захисту інформації

У загальному виді сукупність заходів, спрямованих на запобігання погроз, визначається в такий спосіб:

- резервування технічних засобів
- регулювання доступу до технічних засобів, ПЗ, масивів інформації
- регулювання використання програмно-апаратних засобів і масивів інформації
- криптографічний захист інформації
- контроль елементів ІС
- реєстрація заходів
- своєчасне знищення непотрібної інформації
- сигналізація
- своєчасне реагування

Способи впливу на дестабілізуючі фактори

Фізичні засоби	Апаратні засоби	Програмні засоби	Організаційні заходи	Правові заходи	Морально-етичні норми
• механічні, електричні, електромеханічні, електронні, електронно-механічні й інші пристрої і системи, що функціонують автономно, створюючи різного роду перешкоди дестабілізуючим факторам	• різні електронні, електронно-механічні і подібні пристрої, що вбудовуються в апаратуру ІС чи, що сполучаються з нею спеціально для рішення задач захисту інформації.	• спеціальні пакети програм чи окремі програми, що використовуються для вирішення задач захисту	• організаційно-технічні заходи, передбачаються спеціально в ІС з метою рішення задач захисту	• законодавчо-правові акти, що існують у державі, спеціально видані закони, зв'язані з забезпеченням захисту інформації. • Регламентують права й обов'язки всіх осіб і підрозділів, що мають відношення до функціонування ІС, і встановлюють відповідальність за дії, наслідком яких може бути порушення захищеності інформації.	• сформовані в чи суспільстві колективі моральні норми й етичні правила, дотримання яких сприяє захисту інформації, а порушення їх прирівнюється до недотримання правил поводження в суспільстві

Для забезпечення ефективності захисту інформації усі використані засоби і заходи доцільно об'єднати в систему захисту інформації, що повинна бути функціонально самостійною підсистемою ІС. Головною властивістю побудови системи захисту повинна бути здатність до її пристосування при зміні структури технологічних чи схем умов функціонування ІС.

Організація заходів щодо захисту інформації

Іншими принципами можуть бути:	мінімізація витрат, максимальне використання серійних засобів;
	забезпечення рішення необхідної сукупності задач захисту;
	комплексне використання засобів захисту, оптимізація архітектури;
	зручність для персоналу;
	простота експлуатації.

СЗІ доцільно будувати у виді взаємозалежних підсистем, а саме:

Підсистема криптографічного захисту

- поєднує засоби такого захисту інформації і по ряду функцій кооперується з підсистемою захисту від НСД.

Підсистема забезпечення юридичної значимості електронних документів

- служить для додання юридичного статусу документам в електронному представленні і є визначальним моментом при переході до безпаперової технології документообігу.

Підсистема захисту від НСД

- запобігає доступу несанкціонованих користувачів до ресурсів ІС.

Підсистема керування СЗІ

- призначена для керування ключовими структурами підсистеми криптографічного захисту, а також контролю і діагностування програмно-апаратних засобів і забезпечення взаємодії всіх підсистем СЗІ.

Підсистема організаційно-правового захисту

- призначена для регламентації діяльності користувачів ІС і являє собою упорядковану сукупність організаційних рішень, нормативів, законів і правил, що визначають загальну організацію робіт із захисту інформації в ІС.

Політики безпеки для Internet

Ціль політики– прийняти рішення про те, як організація збирається захищатися. ПІБ звичайно складається з двох частин – загальних принципів і конкретних правил роботи. Загальні принципи визначають підхід до безпеки в Internet. Правила ж визначають що дозволено, а що – заборонено. Правила можуть доповнюватися конкретними процедурами і різними посібниками.

Internet при проектуванні і не задумувався як захищена мережа, тому його**проблемами в поточній версії TCP/IP** є:

– *Легкість перехоплення даних і фальсифікації адрес машин у мережі* – основна частина трафіку Internet – це нешифровані дані. E-mail, паролі і файли можуть бути перехоплені, використовуючи легко доступні програми.
– *Уразливість засобів TCP/IP* – ряд засобів TCP/IP не був спроектований бути захищеними і може бути скомпрометований кваліфікованими зловмисниками; засоби, що використовуються для тестування, особливо уразливі.
– *Відсутність політики* – багато сайтів через незнання сконфігуровані таким чином, що надають широкий доступ до себе з боку Internet, без огляду на можливість зловживання цим доступом; багато сайтів дозволяють роботу більшого числа сервісів TCP/IP, ніж їм потрібно для роботи і не намагаються обмежити доступ до інформації про свої комп'ютери.
– *Складність конфігурування* – засоби керування доступом хоста складні; найчастіше складно правильно сконфігурувати і перевірити ефективність налаштувань. Засоби, що помилково неправильно сконфігуровані, можуть призвести до неавторизованого доступу.

Рівні політики безпеки

Основні принципи політики забезпечення ІБ підприємства

Основними **принципами** інформаційної безпеки є:

– забезпечення цілісності і збереження даних, тобто надійне їх зберігання в неспотвореному вигляді;
– дотримання конфіденційності інформації (її недоступність для тих користувачів, які не мають відповідних прав);
– доступність інформації для всіх авторизованих користувачів за умови контролю за всіма процесами використання ними отриманої інформації;
– безперешкодний доступ до інформації в будь-який момент, коли вона може знадобитися підприємству.

Ці принципи неможливо реалізувати без особливої **інтегрованої системи ІБ**, що виконує наступні функції:

– розробка політики інформаційної безпеки;
– аналіз ризиків (тобто ситуацій, в яких може бути порушена нормальна робота інформаційної системи, а також втрачено або розсекречено дані);
– планування заходів щодо забезпечення ІБ;
– планування дій в надзвичайних ситуаціях;
– вибір технічних засобів забезпечення інформаційної безпеки.

Етапи проведення робіт із забезпечення інформаційної безпеки підприємства

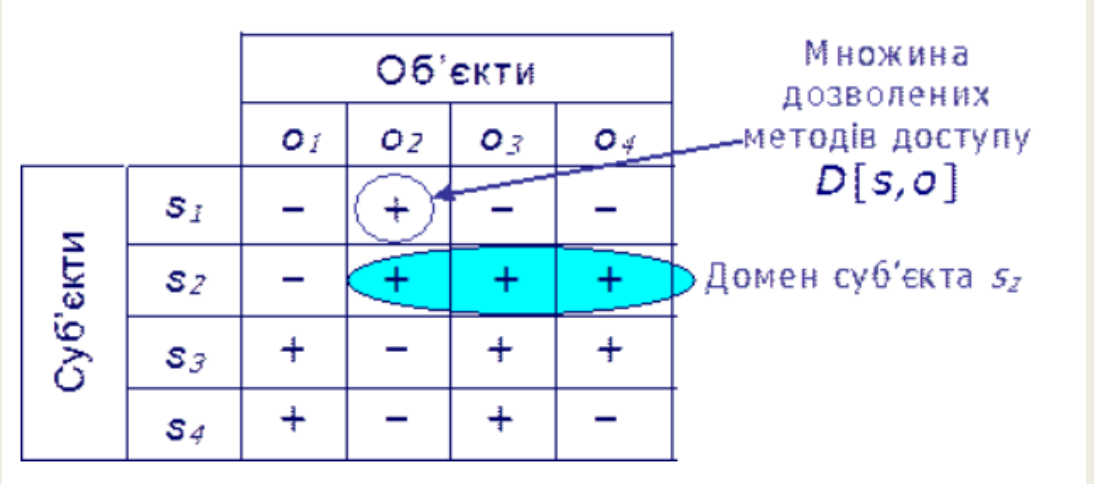
1. Проведення обстеження підприємства на предмет виявлення реальних загроз несанкціонованого доступу до конфіденційної інформації.
2. Розробка політики безпеки, організаційно-розпорядчих документів і заходів щодо забезпечення ІБ системи відповідно до вимог по захищеності технічних і програмних засобів від витоку конфіденційної Інформації.
3. Проектування системи ІБ.
4. Створення прототипу системи ІБ.
5. Розробка зразка системи ІБ.
6. Впровадження системи ІБ в діючу структуру підприємства.
7. Навчання персоналу.
8. Атестація системи інформаційної безпеки підприємства.

Метою комплексної інформаційної безпеки є збереження інформаційної системи підприємства, захист і гарантування повноти і точності виданої нею інформації, мінімізація руйнувань і модифікації інформації.

Види моделей розробки політики інформаційної безпеки

Дискреційна політика безпеки (ДПБ)

Основою є дискреційне управління доступом (Discretionary Access Control – DAC), яке визначається двома властивостями:
– усі суб'єкти й об'єкти мають бути однозначно ідентифіковані;
– права доступу суб'єкта до об'єкта системи визначаються на основі певних зовнішніх відносно системи правил.



Ця політика одна з найпоширеніших в світі, в системах по замовчуванню мається на увазі саме вона. ДПБ реалізується за допомогою матриці доступу, яка фіксує множинуоб'єктів та суб'єктів, доступних кожному суб'єкту.

Дискреційна політика безпеки

- **Перевага дискреційної політики безпеки** - проста реалізація системи розмежування доступу і, як наслідок, її широка розповсюдженість на практиці. Разом з цим ця політика вважається недосконалою через низку суттєвих недоліків.

- **Недоліки політики:**

- статичність правил розмежування доступу, які не враховують динаміку змін стану комп'ютерної системи;
- у випадку використання дискреційної політики безпеки, при доступі суб'єкта до об'єкта кожного разу необхідно визначати права доступу та аналізувати їх вплив на безпеку системи, що знижує її прозорість;
- у загальному випадку для систем дискреційного політики задача перевірки безпеки є алгоритмічно нерозв'язною. Доведення того факту, що система, у якій реалізовано дискреційну політику, є захищеною у заданому стані, має бути проведено для кожної конкретної системи і для кожного стану цієї системи;
- широковідомою практичною проблемою систем дискреційної політики є проблема їх нечутливості до впливу троянських програм ("троянських коней").

Мандатна політика безпеки (МПБ)

Основу становить мандатне управління доступом (Mandatory Access Control – MAC), яке передбачає, що:
– всі суб'єкти й об'єкти повинні бути однозначно ідентифіковані;
– у системі визначено лінійно упорядкований набір міток секретності;
– кожному об'єкту системи надано мітку секретності, яка визначає цінність інформації, що міститься в ньому – його рівень секретності в АС;
– кожному суб'єкту системи надано мітку секретності, яка визначає рівень довіри до нього в АС, – максимальне значення мітки секретності об'єктів, до яких суб'єкт має доступ; мітка секретності суб'єкта називається його рівнем доступу.

Основна мета МПБ – запобігання витоку інформації від об'єктів з високим рівнем доступу до об'єктів з низьким рівнем доступу, тобто протидія виникненню в КС інформаційних каналів згори вниз.

Пристрій мандатного контролю називають монітором звернень. Мандатний контроль, який ще називають обов'язковим, оскільки його має проходити кожне звернення суб'єкта до об'єкта, організується так:
– монітор звернень порівнює мітки рівня секретності кожного об'єкта з
мітками рівня доступу суб'єкта;
– за результатом порівняння міток приймається рішення про допуск.

Найчастіше МПБ описують у термінах, поняттях і визначеннях властивостей **моделі Белла-Лападула**. У рамках цієї моделі доводиться важливе твердження, яке вказує на принципову відмінність систем, що реалізують мандатний захист, від систем з дискреційним захистом: «якщо початковий стан системи безпечний і всі переходи системи зі стану до стану не порушують обмежень, сформульованих ПБ, то будь-який стан системи безпечний».

Мандатна політика безпеки (МПБ)

Переваги МПБ порівняно з ДПБ:
1. Для систем, де реалізовано МПБ, є характерним вищий ступінь надійності. Це пов’язано з тим, що за правилами МПБ відстежуються не тільки правила доступу суб’єктів системи до об’єктів, а й стан самої КС. 2. Правила МПБ ясніші і простіші для розуміння розробниками і користувачами АС, що також є фактором, який позитивно впливає на рівень безпеки системи.
3. МПБ стійка до атак типу «Троянський кінь».
4. МПБ допускає можливість точного математичного доведення, що система в заданих умовах підтримує ПБ.

Недолік – дуже складна для практичної реалізації і вимагає значних ресурсів КС. Це пов’язано з тим, що інформаційних потоків у системі величезна кількість і їх не завжди можна ідентифікувати.

МПБ прийнята всіма розвинутими державами світу. Вона розроблялася, головним чином, для збереження секретності (тобто конфіденційності) інформації у військових організаціях. Питання цілісності за її допомогою не розв’язуються або розв’язуються частково, як побічний результат захисту секретності.

Рольова політика безпеки (РПБ)

Рольову політику безпеки (РПБ) (Role Base Access Control – RBAC) не можна віднести ані до дискреційної, ані до мандатної, тому що керування доступом у ній здійснюється як на основі матриці прав доступу для ролей, так і за допомогою правил, які регламентують призначення ролей користувачам та їх активацію під час сеансів.

Рольова модель є цілком новим типом політики, яка базується на компромісі між гнучкістю керування доступом, характерною для ДПБ, і жорсткістю правил контролю доступу, що притаманна МПБ. У РПБ класичне поняття «суб'єкт» заміщується поняттями «користувач» і «роль».

Користувач – це людина, яка працює з системою і виконує певні службові обов'язки.
Роль – це активно діюча в системі абстрактна сутність, з якою пов'язаний обмежений, логічно зв'язаний набір повноважень, необхідних для здійснення певної діяльності.

РПБ застосовується досить широко, тому що вона є дуже близькою до реального життя.

З точки зору РПБ має значення не особистість користувача, що здійснює доступ до інформації, а те, які повноваження йому необхідні для виконання його службових обов'язків.

Рольова політика безпеки (РПБ)

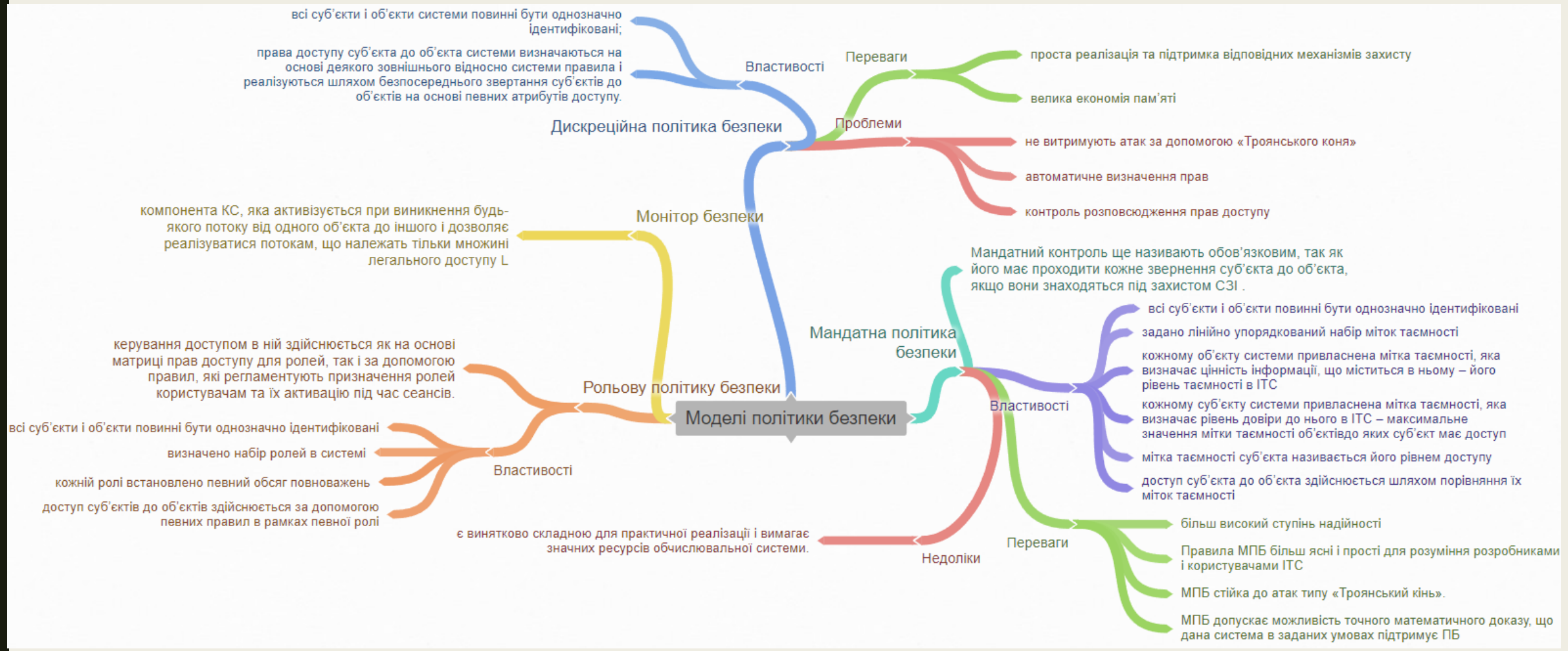
Переваги

- гнучкість та широкі можливості
- такий підхід дозволяє отримати прості й зрозумілі правила контролю доступу, які легко застосовувати на практиці
- оперувати ролями набагато зручніше, ніж суб’єктами, оскільки це більше відповідає поширеним технологіям обробки інформації
- може використовуватися одночасно з іншими ПБ, коли повноваження ролей, що призначаються користувачам, контролюється ДПБ або МПБ, що дозволяє будувати багаторівневі схеми контролю доступу.

Недоліки

- практично не гарантує безпеку за допомогою формального доведення, а тільки визначає характер обмежень, виконання яких і є критерієм безпеки системи
- позбавляє систему теоретичної доказової бази

Моделі політики безпеки



Висновки

- Політика безпеки інформації є частиною загальної політики безпеки організації і повинна успадкувати основні її принципи.
- Для забезпечення достатнього рівня інформаційної безпеки компанії потрібно розробляти Політику інформаційної безпеки з урахуванням того, що вона є складовою системи безпеки підприємства, і пам’ятати, що вона повинна бути орієнтованою на кожного працівника, а також не навантажувати головний документ інформацією, направленою на окремих працівників. Для цього потрібно розробляти документи нижчого рівня.
- В більшості випадків пересічний користувач не зрозуміє реальних ризиків від вчинених ним дій, навіть якщо чітко пояснити, що просте відкриття листа з невідомої електронної пошти може призвести до зламу всієї мережі підприємства. Тому Положення повинно мати структуру чітких рекомендацій, щоб коли хтось не зрозуміє, навіщо воно потрібно, він все одно зміг виконувати його рекомендації.