МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут захисту інформації

На рецензію
Завідувач кафедри УІКБ
доктор економічних наук, професор
_____ С.В. Легомінова
«___» _____ 2022 р.

До захисту
Завідувач кафедри УІКБ
доктор економічних наук, професор
_____ С.В. Легомінова
«___» _____2022 р.

КВАЛІФІКАЦІЙНА РОБОТА

другого магістерського рівня вищої освіти

на тему:

ПІДХОДИ ДО ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ПРОЦЕСІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

СТУДЕНТ: Побойний Олексій Сергійович _____
(підпис)

КЕРІВНИК: к.в.н., доц. Якименко Юрій Михайлович _____
(підпис)

НОРМОКОНТРОЛЕР: к.держ.упр.,доц. Мужанова Тетяна Михайлівна _____
(підпис)

Київ – 2022

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою
Спеціальність «Кібербезпека»
Спеціалізація «Управління інформаційною безпекою»
Другого магістерського рівня вищої освіти

"ЗАТВЕРДЖУЮ"
Завідувач кафедри УІКБ
_____ С.В.Легомінова

“___”_____2022 р.

ЗАВДАННЯ
на кваліфікаційну роботу

студенту **Побойному Олексію Сергійовичу**
Тема РОБОТИ “ ПІДХОДИ ДО ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ПРОЦЕСІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ”,
затверджена наказом по університету від “___ ”_____ 2022 р. №____
Термін здачі студентом оформленої роботи «08» 12.2022 р.

1. **Об'єкт дослідження**: процеси забезпечення інформаційної безпеки на підприємстві.
2. **Предмет дослідження:** підходи до оцінювання ефективності процесів забезпечення інформаційної безпеки на підприємстві.
3. **Мета дослідження:** вивчення процесів забезпечення інформаційної безпеки
4. **Перелік питань, які мають бути розроблені:**
   4.1 Проаналізувати вимоги нормативних документів щодо забезпечення інформаційної безпеки на підприємстві.
   4.2 Проаналізувати напрями забезпечення інформаційної безпеки на підприємстві.
   4.3 Провести дослідження і розробити рекомендації щодо підвищення ефективності забезпечення інформаційної безпеки на підприємстві
5. **Дата видачі завдання «**26» вересня 2022 р.

Науковий керівник _____ Ю.М.Якименко
(підпис)

Завдання прийнято до виконання _____ О.С. Побойний
(підпис)

КАЛЕНДАРНИЙ ПЛАН
виконання кваліфікаційної роботи
студентом Побойним Олексієм Сергійовичем
Дата видачі завдання: «26» вересня 2022 р.

№ з/п	Етапи роботи	Термін виконання етапів	Примітка
1.	Визначення об'єкту, предмету, мети та завдань дослідження.	26.09.2022	
2.	Збір та аналіз літератури.	3.10.2022	
3.	Розділ 1. Аналіз вимог нормативних документів щодо забезпечення інформаційної безпеки на Підприємстві	17.10.2022	
4.	Розділ 2. Аналіз напрямів забезпечення інформаційної безпеки на підприємстві	31.10.2022	
5.	Розділ 3. Дослідження і розробка рекомендацій щодо підвищення ефективності для забезпечення інформаційної безпеки	14.11.2022	
6.	Формулювання висновків за результатами проведеного дослідження	01.12.2022	
7.	Оформлення роботи	8.12.2022р.	
8.	Оформлення презентації	15.12.2022р.	
9.	Отримання рецензії на роботу .	23.12.2022	
10.	Захист в ДЕК	___01.2023 р.	

Студент О.С. Побойний
(підпис)

Науковий керівник Ю.М. Якименко
(підпис)

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню проблем визначення підходів підходи до оцінювання ефективності процесів забезпечення інформаційної безпеки на підприємстві. Робота складається зі вступу, трьох розділів, що містять 22 рисунка, висновків та списку використаних джерел, що містить 41 найменувань. Загальний обсяг роботи становить 90 аркушів, з яких 5 аркушів займають перелік умовних скорочень та список використаних джерел.

Об'єктом дослідження є : процеси забезпечення інформаційної безпеки на підприємстві.

Предмет дослідження - підходи до оцінювання ефективності процесів забезпечення інформаційної безпеки на підприємстві.

Метою роботи є дослідження підходів до оцінювання ефективності процесів забезпечення інформаційної безпеки на підприємстві Для цього у роботі використовуються методи системного аналізу існуючих вимог до оцінювання ефективності процесів ІБ та узагальнення практичного досвіду підприємств щодо виконання процесів забезпечення інформаційної безпеки.

Як результат у роботі проведено аналіз вимог нормативних документів до організації інформаційної безпеки на підприємстві, зокрема стандартів ISO/IEC 27001 і 27002 та основних законів України; проаналізовані напрями забезпечення інформаційної безпеки підприємств, у тому числі методи забезпечення інформаційної безпеки: правовий, економічний і організаційно-технічний; досліджено на прикладі і розроблено рекомендації щодо підвищення ефективності забезпечення інформаційної безпеки на підприємстві.

Галузь застосування. Розроблені підходи можуть бути використані при плануванні та реалізації процесів забезпечення інформаційної безпеки при побудові системи управління інформаційною безпекою.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА, ОЦІНКА ЕФЕКТИВНОСТІ, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, ЗАБЕЗПЕЧЕННЯ. ПРОЦЕСИ, ЗАГРОЗИ, ВИМОГИ

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

СУІБ – система управління інформаційою безпекою
ІБ – інформаційна безпека
ІТ – інформаційні технології
ISO 27-k - позначення k – го з сімейства стандартів ISO
СІБ – система інформаційої безпеки
ІТКС - інформаційно-телекомунікаційна система
ДСТУ - державний стандарт України
ВСр - обчислювальна середа
ОСр - операційна середа
АС - автоматизована система
СРД - системи розмежування доступу
ЗІБ - забезпечення інформаційої безпеки

ВСТУП

Актуальність дослідження. З огляду на зростаючу роль інформаційно-телекомунікаційних технологій та розширення обсягів інформації, яка в них зберігається та циркулює, захист інформації та засобів її обробки зокрема та забезпечення інформаційної безпеки загалом є дуже важливою складовою функціонування сучасного підприємства. Забезпечення інформаційної безпеки - це не тільки захист інформації від несанкціонованого доступу. Забезпечення інформаційної безпеки - це в основному практика запобігання несанкціонованому доступу, використанню, розголошенню, зриву, модифікації, запису або знищенню інформації. Забезпеченню інформаційної безпеки в напряму підвищення ефективності виконаання її процесів останнім часом приділяється все більша увага. Створення системи забезпечення інформаційної безпеки в свою чергу розглядається в науково-дослідницьких працях як основна складова для побудови ефективної системи управління інформаційної безпеки будь-якого підприємства. Для ефективного забезпечення ІБ підприємства пропонується здійснювати комплекс різнопланових заходів, які можна об’єднати у три групи напрямів дій : нормативні, організаційні і . програмно-технічні. Повсякденному підвищенню ефективності забезпечення інформаційної безпеки підприємства завжди наділяється значна увага, що підтверджує актуальність обраної теми роботи для подальшого дослідження..

Мета і завдання дослідження. **Мета роботи** полягає в дослідженні підходів до оцінювання ефективності процесів забезпечення інформаційної безпеки на підприємстві

Досягнення мети обумовило необхідність вирішення таких **завдань:**

1. Проаналізувати вимоги нормативних документів щодо забезпечення інформаційної безпеки на підприємстві.

2. Проаналізувати напрями забезпечення інформаційної безпеки на підприємстві.

3. Провести дослідження і розробити рекомендації щодо підвищення ефективності забезпечення інформаційної безпеки на підприємстві

Для цього у роботі використовуються методи системного аналізу існуючих вимог до організації і побудови системи управління нформаційною безпекою, узагальнення практичного досвіду підприємств щодо виконання процесів забезпечення і визначення напрямів та методів по вдоконаленню її інформаційної безпеки.

Інформаційно-правову базу дослідження склали законодавчі та нормативно-правові документи України, Кабінету Міністрів України в галузі інформатизації та забезпечення інформаційної безпеки, публікації вітчизняних і зарубіжних авторів, дослідження фахівців з економічної та інформаційної безпеки.

Практичне значення отриманих результатів полягає у впровадженні розробок в систему управління підприємствами, що дозволить підвищити ефективність їх управлінських рішень при реалізації процесів забезпечення інформаційної безпеки.

Структура роботи. Дана дипломна робота складається із вступу, трьох розділів, висновків та списку використаної літератури.

РОЗДІЛ 1
АНАЛІЗ ВИМОГ НОРМАТИВНИХ ДОКУМЕНТІВ ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

На сьогоднішній день своєчасна та об’єктивна інформація є важливим фактором виробництва, який розглядають, як один з основних ресурсів розвитку суспільства. Сучасні інформаційні системи та технології є засобом підвищення продуктивності та ефективності роботи працівників. Проте глобальна комп’ютеризація у багатьох сферах управління та виробництва супроводжується появою принципово нових загроз інтересам особистості, підприємства, суспільства, держави [7].

Паралельно з розвитком і ускладненням засобів, методів, форм автоматизації процесів обробки інформації підвищується залежність суб’єктів підприємництва від ступеню безпеки використовуваних ними інформаційних технологій [2]. Постійна робота в сфері підтримки інформаційної безпеки (ІБ) на належному рівні є необхідною умовою ефективності підприємницької діяльності [20].

1.1 Основні вимоги нормативних документів до організації інформаційної безпеки

В процесі своєї діяльності будь-яке підприємство оперує інформацією як специфічним товаром високої цінності. Володіння інформацією, її оптимальне використання забезпечує ефективне функціонування суб'єкта господарювання як цілісного комплексу. Тому проблема забезпечення ІБ є надзвичайно актуальною на сучасному етапі розвитку інформаційних технологій, який супроводжується введенням інформаційних систем у всі сфери діяльності людини, постійною взаємодією підприємств на теренах саме інформаційного простору.

Система управління ІБ (Information Security Management System) є частиною загальної системи управління, що базується на аналізі ризиків і призначеної для проектування, реалізації, контролю, супроводу та вдосконалення заходів в області ІБ. Систему складають організаційні структури, політика, дії з планування, обов'язки, процедури, процеси і ресурси [8].

Основними цілями ІБ є:

- конфіденційність інформації,тобто необхідність введення обмежень доступу до даної інформації для певного кола осіб;

- неможливість несанкціонованого доступу до інформації, тобто ознайомлення з конфіденційною інформацією сторонніх осіб;

- цілісність інформації та пов'язаних з нею процесів(створення, введення, обробка і виведення), яка полягає в її існуванні в неспотвореному вигляді (незміненому по відношенню до деякому фіксованому її станом);

- доступність інформації,тобто здатність забезпечувати своєчасний і безперешкодний доступ осіб до цікавлячого їх інформації;

- мінімізація ризиків ІБ шляхом виконання компенсаційних заходів;

- облік усіх процесів, пов'язаних з ризиками [11, 29].

Досягнення заданих цілей здійснюється в ході вирішення наступних основних завдань:

- класифікації інформаційних ресурсів підприємства;
- визначення власників процесів, відповідальних за ІБ;
- розробки спектра ризиків ІБ та проведення їх експертних оцінок;
- визначення групи доступу до інформаційних ресурсів;
- розробки системи управління ризиками ІБ (методи та їх оцінка);
- складання переліків адміністративних і технічних заходів для мінімізації та компенсації ризиків;
- здійснення заходів ІБ та періодичного контролю за станом ризиків;
- забезпечення фізичної безпеки та безпеки персоналу;
- розробки вимог до інформаційної системи з погляду ІБ;
- контролінгу ІБ на підприємстві [9].

ISO / IEC 27-k – це перелік важливих міжнародних стандартів, які випущені групою з Міжнародної організації зі стандартизації (ISO – International organization for standardization) і Міжнародної Електротехнічної Комісії (IEC - The International Electrotechnical Commission). Стандарти ISO / IEC 27-k складаються з кращих рекомендацій і практик в сфері створення, розвитку та управління системами інформаційної безпеки (СІБ). Так само даний перелік містить в собі вимоги і до систем управління ризиками, інцидентами ІБ і безперервної готовності систем підприємства до виконання задач: їх створення, впровадження і експлуатації.

Структуру сімейства стандартів ISO 27-k можна представити у вигляді схеми (див. рис.1.1), що відображає взаємозв'язок і призначення основних її

стандартів у сфері управління ІБ і практик в сфері створення, розвитку та управління СІБ.

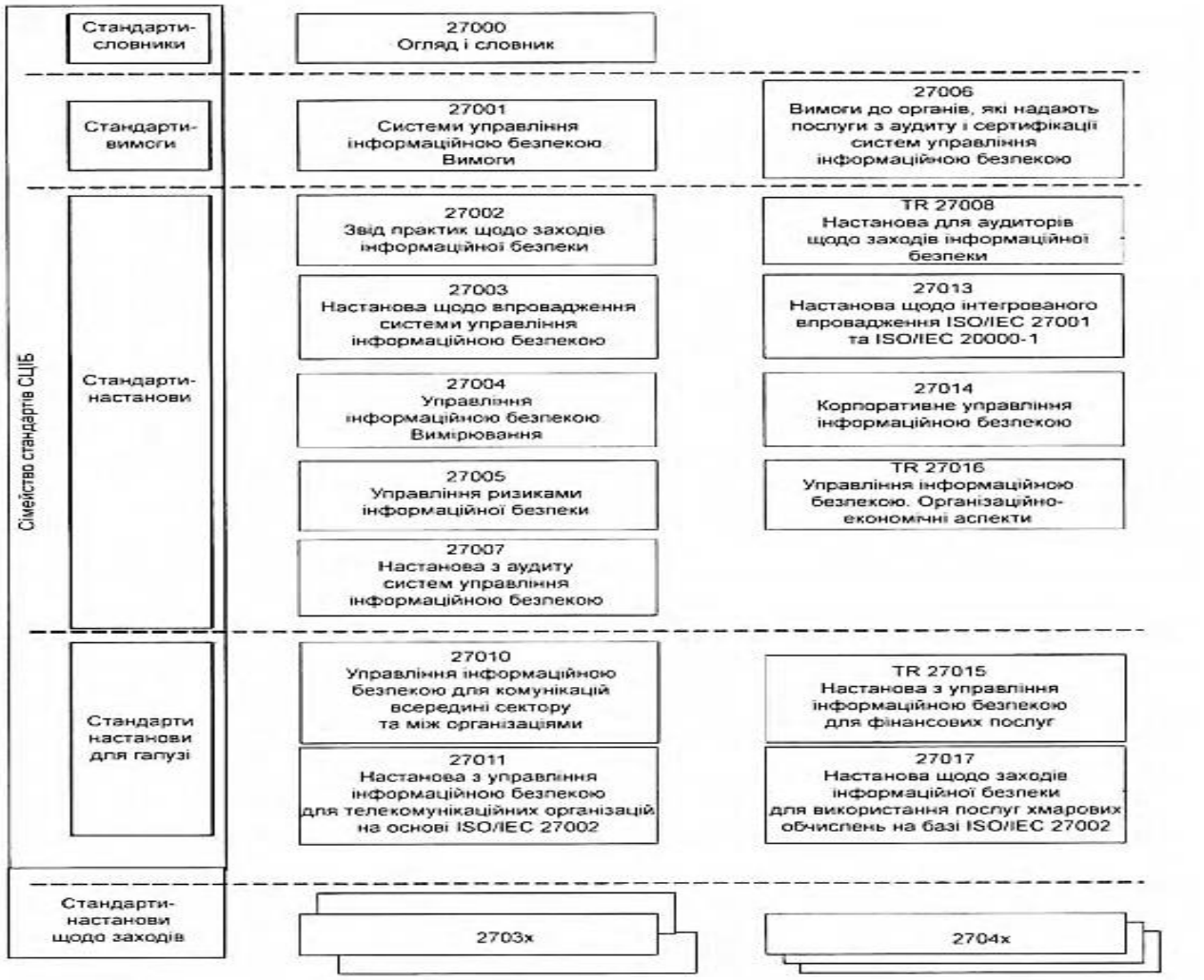

Рис.1.1. Схема структури сімейства стандартів ISO 27-k

Найперший стандарт ISO 27000 містить в собі основні визначення, які існують в сфері ІБ. А також він включає в себе:

- словник, інформаційні технології, системи менеджменту ІБ, засоби і методи забезпечення безпеки;
- описує і визначає вимоги до розробки, впровадження, підтримки, експлуатації і постійного поліпшенню системи управління інформаційною безпекою (СУІБ) в контексті організації.

ISO/IEC 27001 є мабуть, найбільш відомим, будучи третім за поширеністю сертифікатом ISO у світі, після ISO 9001 та ISO 14001. Він визначає вимоги до створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою (СУІБ|ISMS) в контексті організації

вимоги є загальними і призначені для застосування до всіх організацій, незалежно від типу, розміру або характеру. Кілька провідних компаній просять своїх ділових партнерів бути сертифікованими за стандартом ISO/IEC 27001 - наприклад, Netflix для партнерів з постпродакшну - і протягом багатьох років широко висвітлювалося досягнення ISO/IEC 27001 досягнення сертифікації ISO/IEC 27001 відомими технологічними провайдерами, в тому числі Apple Internet Services, Amazon Web Services, GE Digital, кілька бізнес-підрозділів Microsoft.

Основні частини стандарту ISO 27001 [31] представлені на рис.1.2. Запровадження СУІБ є стратегічним рішенням для підприємства. Розробка і впровадження її залежить від потреб і цілей підприємства, вимог з безпеки її процесів, розміру і структури. Всі ці фактори впливу з часом можуть змінюватись.

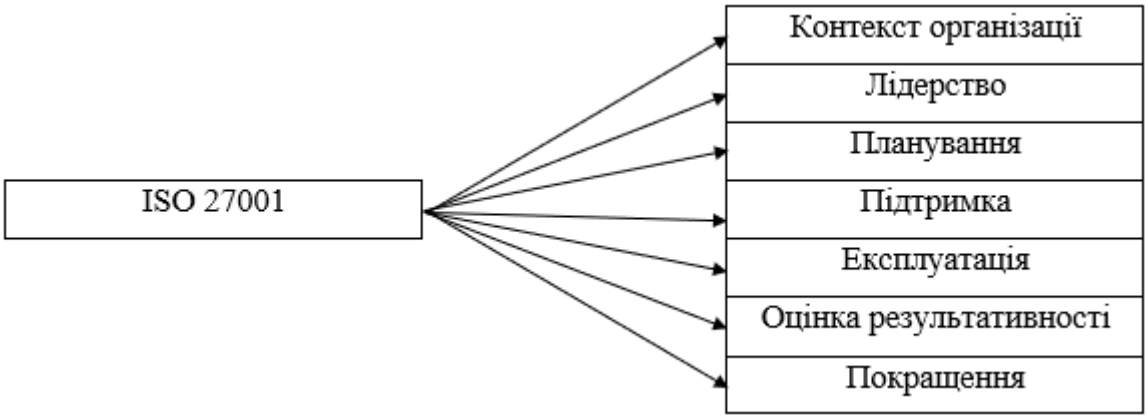

Рис. 1.2. Основні частини стандарту ISO 27001

Проведення комплексу заходів із побудови СУІБ відповідно до вимог стандарту ISO 27001 дозволить вирішити такі завдання:

- Підвищення рівня безпеки. Стандарт розроблений з урахуванням кращих світових практик забезпечення ІБ.
- Управління. Стандарт передбачає побудову циклічного і керованого процесу забезпечення ІБ.
- Оптимізація витрат. СУІБ дозволяє оптимізувати і обгрунтувати витрати на ІБ.

- Ризики. Зниження рівня фінансових ризиків, пов’язаних з інформаційною безпекою, шляхом їх ідентифікації, оцінки та прийняття адекватних захисних заходів.
- Привабливість. Підвищення ступеня привабливості компанії на внутрішньому і зовнішньому ринках (конкурентні переваги).
- Довіра. Підвищення довіри з боку акціонерів, клієнтів, партнерів і контрагентів.
- Репутація. Підвищення рівня ділової репутації шляхом сертифікації СУІБ, яка демонструє високий рівень зрілості компанії.

Вимоги до впровадження СУІБ поділяються на декілька етапів а саме створення, впровадження, розгортання, моніторинг, аналіз, підтримка, оновлення та вдосконалення, а також потреби організації. Впровадження СУІБ за стандартом ISO/IEC 27001 вимагає від компаній які хочуть відповідати вимогам цього стандарту пройти ряд поетапних заходів. Ці етапи включають в себе ряд вимог (обов'язкових вимог), де необхідно виконати певні дії, здійснити певні заходи, провести певні (обов'язкові вимоги), які необхідно виконати, впровадити певні процеси. Ці вимоги підпадають під наступні заголовки пунктів:

- Контекст організації
- Лідерство
- Планування
- Підтримка
- Операція
- Оцінка діяльності
- Удосконалення

Стандарт ISO / IEC 27002: 2016 [32] визначає принципи та є керівництвом з розробки, впровадження, супроводу та поліпшення СУІБ, а також описує механізми визначення цілей контролю і його коштів у таких областях:

- політика безпеки (встановлення принципів управління і засобів забезпечення захисту інформації);

- управління безперервністю бізнес-процесів (запобігання втручання в ділові операції і захист процесів обробки інформації від наслідків серйозних несправностей або катастроф);

- дотримання правових норм (виняток порушень кримінального та цивільного права, установлених законом зобов'язань, регулятивних або контрактних зобов'язань, а також вимог щодо безпеки);

- організація активів і ресурсів (управління захистом інформації всередині організації);

- фізична безпека і безпека навколишнього середовища (запобігання несанкціонованого доступу, пошкодження і проникнення в службові приміщення або втручання в ділову інформацію);

- класифікація і управління активами (виявлення та захист інформаційних активів);

- захист персоналу (зниження ризиків, пов'язаних з помилкою оператора, крадіжкою, шахрайством або зловживанням обладнанням);

- управління доступом (контроль доступу до інформації);

- управління засобами зв'язку і експлуатацією устаткування (коректне і безпечне функціонування засобів обробки інформації);

- розробка та обслуговування систем (впровадження засобів захисту в інформаційні системи).

Стандарт ISO/IEC 27002 надає збірку еталоних правил забезпечення інформаційної та кібербезпеки, включаючи вказівки щодо впровадження СМІБ на основі міжнародно визнаних найкращих практик.

Використання компаніями цього стандарту, зокрема в Україні, допоможе підвищити обізнаність працівників про інформаційну безпеку, краще контролювати інформаційні активи, ефективніше впроваджувати політики безпеки, виявляти й усувати вразливості ІБ та кібербезпеки компанії, дотримуватися законодавства та ін.

Вимогами стандарту [4, 5,28] на основних напрямках діяльності в сфері ІБ є:

1. Політики ІБ – забезпечити управління та підтримку інформаційної безпеки згідно з вимогами бізнесу та відповідними законами й нормативами.

2. Організація ІБ – визначити структуру управління для започаткування та контролю впровадження і функціонування ІБ в огранізації, забезпечити безпеку віддаленої роботи та використання мобільних пристроїв.

3. Безпека людських ресурсів – гарантувати, що найманий персонал та підрядники розуміють свої обов’язки, придатні до ролей, на які претендують,

впевнитися, що весь найманий персонал та підрядники усвідомлюють і виконують свої обов'язки з інформаційної безпеки, захистити інтереси огранізації як частини процесу зміни умов чи припинення найму.

4. Управління ресурсами СУІБ – ідентифікувати ресурси СУІБ організації і визначити відповідні обов'язки щодо їх захисту, забезпечити належний рівень захисту інформації відповідно до її важливості для організації, запобігти несанкціонованому розголошенню, модийфікації, вилученню або знищенню інформації, що зберігається на носіях.

5. Контроль доступу – обмежити доступ до інформації та засобів оброблення інформації, забезпечити санкціонований доступ користувача і запобігти несанкціонованому доступу до систем та послуг, зробити користувачів відповідальними за збереження їх інформації автентифікації, запобігти несанкціонованому доступу до систем та прикладних програм.

6. Криптографія – гарантувати відповідне та ефективне використання криптографії для захисту конфіденційності, автентичності та/або цілісності інформації.

7. Фізична безпека та безпека інфраструктура – запобігти несанкціонованому фізичному доступу, пошкодженню та втручанню в інформацію та засоби оброблення інформації, запобігти втратам, пошкодженню, крадіжці або компрометації ресурсів СУІБ та перериванню діяльності організації.

8. Безпека експлутації – забезпечити коректне та безпечне функціонування засобів оброблення інформації, гарантувати, що інформація та засоби оброблення інформації захищені проти зловмисного коду, захистити від втрати даних, записувати події та генерувати докази, гарантувати цілісність систем, що перебувають в експлутації, запобігати використанню технічних вразливостей, мінімізувати вплив аудиту на системи, які перебувають у промисловій експлутації.

9. Безпека комунікацій – забезпечити захист інформації в мережах та захист засобів оброблення інформації, що їх підтримує, підтримувати безпеку інформації, якою обмінюються всередині організації та з зовнішнім об'єктом.

10. Придбання, розроблення та підтримка інформацінйих систем – забезпечити, що безпека є невід'ємною частиною інформаційних систем протягом всього життєвого циклу, це включає вимоги для тих систем, які

забезпечують надання послуг з використанням публічних мереж, гарантувати, що ІБ проектують та впроваджують протягом життєвого циклу інформаційних систем, забезпечити захист даних, які використовуються для тестування.

11. Взаємовідносини з постачальниками – гарантувати захист ресурсів СУІБ огранізації, які можуть бути доступні постачальникам, підтримувати належний рівень ІБ та надання послуг відповідно до угод з постачальником.

12. Управління інцидентами інформаційної безпеки – гарантувати послідовний та ефективний підхід до управління інцидентами ІБ, охоплюючи поширення інформації про події безпеки та слабкі місця.

13. Аспекти інформаційної безпеки управління безперервністю бізнесу – забезпечити, що безперервність ІБ залучена в системи управління безперервністю бізнесу організації, гарантувати доступність обладнання для оброблення інформації.

Цей стандарт призначений для використання організаціями різного типу та з різних галузей. На основі довідникової інформації з нього компанії впроваджують дієві заходи безпеки та системи управління інформаційною безпекою.

Зокрема варто відмітити, що стандарт ДСТУ ISO/IEC 27002:2015 активно застосовується в фінансовій та банковій сфері України. Наприклад, за Постановою Правління Національного банку України від 28.10.2010 № 474 було прийнято та надано чинності модифікованому стандарту ISO/IEC 27002:2005, MOD, до якого були внесені окремі зміни зумовлені правовими вимогами і конкретними потребами банківської сфери діяльності. [33]

Питання ІБ також знайшли відображення у таких законах України: «Про основи національної безпеки України», «Про концепцію національної програми інформатизації», «Про національну програму інформатизації», «Про захист інформації в інформаційно-телекомунікаційних системах», "Про державну таємницю", "Про інформацію", а також у Стратегії національної безпеки України, яка затверджена Указом Президента. У Законі «Про основи національної безпеки України» надано офіційну оцінку значущості й системної сутності інформаційної безпеки як невід'ємної складової національної безпеки України.

У Стратегії національної безпеки, присвяченій стану ІБ в нашій державі, зазначено [5,38]:

- посилюється негативний зовнішній вплив на інформаційний простір України, що загрожує розмиванням суспільних цінностей і національної ідентичності;

- недостатніми залишаються обсяги вироблення конкурентоспроможного національного інформаційного продукту;

- наближається до критичного стан безпеки інформаційно-комп'ютерних систем у фінансовій і банківській сфері, сфері державного управління, енергетики, транспорту, внутрішніх та міжнародних комунікацій тощо.

Поняття ІБ можна розглядати у декількох ракурсах.

По-перше, це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання й розвиток в інтересах громадян, організацій, держави.

По-друге, це стан захищеності потреб в інформації особи, суспільства й держави, при якому забезпечується їх існування та прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз. Стан інформованості визначає ступінь адекватності сприйняття суб’єктами навколишньої дійсності і, як наслідок – обгрунтованість подальших рішень і дій.

В інформаційному праві ІБ – це одна із сторін розгляду інформаційних відносин у межах інформаційного законодавства з позиції захисту життєво важливих інтересів особистості, суспільства, держави, акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами. Тому Національний банк України зробив дуже важлийвий внесок для розвитку СУІБ своїм виданням постанови «Про набрання чинності стандартів з управління ІБ в банківській системі України». Таким чином НБУ ввів модифіковані під банківську систему стандарти ISO 27001 і ISO 27002 та підвищив рівень ІБ банківської системи в Україні.

Також через деякий час НБУ розробив методичні рекомендації щодо впровадження СУІБ та методики оцінки ризиків відповідно до введених стандартів в Україні. Це було продиктовано сучасними вимогами по відношенню до управління та зменшенню операційних ризиків банків.

Впровадження в банках України стандартів з управління ІБ дозволить:

- оптимізувати вартість побудови та підтримання СІБ;

- постійно відслідковувати та оцінювати ризики з урахуванням цілей бізнесу;

- ефективно виявляти найбільш критичні ризики та знижати ймовірність їх реалізації;

- розробити ефективну політику ІБ та забезпечити її якісне виконання;

- ефективно розробляти, впроваджувати та тестувати плани відновлення бізнесу;

- забезпечити розуміння питань ІБ керівництвом та всіма працівниками банку;

- забезпечити підвищення репутації та ринкової привабливості банків;

- знизити ризики рейдерських та інших шкідливих для банку атак;

Слід зазначити, що наведені вище переваги не можуть бути досягнуті шляхом лише "формального" підходу до розроблення, впровадження, функціонування СУІБ. Тому потрібно приділяти з боку керівництва і працівників банку значну і постійну увагу необхідності створенню і експлуатації ефективної СУІБ та підвищенню високого рівня ІБ.

1.2 Основні складові забезпечення інформаційної безпеки

При оцінці загроз безпеці інформації та виборі пріоритетів у системі захисту підприємства проаналізуємо практику захисту інформації та забезпечення безпеки діяльності підприємства. Інформація стала чинником, який може призвести до значних технологічних аварій, військових та політичних конфліктів, дезорганізувати на всіх рівнях державне управління і знизити рівень ІБ .

Метою захисту інформації має бути збереження цінності інформаційних ресурсів для їх власника. Виходячи з цього, безпосередні заходи захисту спрямовують не так на самі інформаційні ресурси, як на збереження певних технологій їх створення, обробки, зберігання, пошуку та надання користувачам.

Умовно виділяються три основних напрямки захисту інформації (рис.1.3):

Рис.1.3. Основні напрямки захисту інформації

Відповідно до основних напрямки захисту інформації [16]визначають загальні методи забезпечення ІБ, представлені на рис. 1.4.

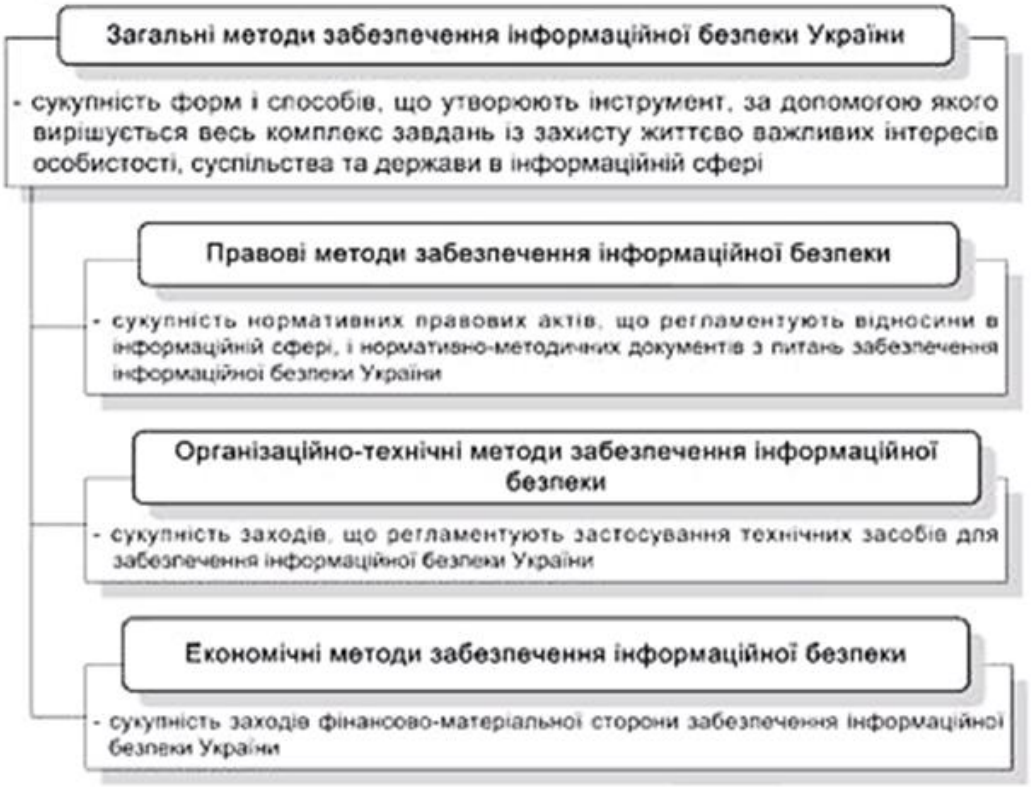

Рис.1.4. Загальні методи забезпечення інформаційної безпеки [21]

Завдання забезпечення ІБ має вирішуватися системно [40], це означає, різні засоби повинні застосовуватися одночасно і під централізованим управлінням.

1. Правовий метод забезпечення ІБ, спрямований на створення імунітету, заснованого на загрозі застосування репресивного інструменту відносно порушників інтересів користувачів системи, і встановлює механізм застосування

санкцій відносно правопорушника; правові методи включають сукупність нормативно-правових актів, які регулюють відносини, пов'язані з використанням інформації в діяльності підприємства. До правових заходів слід віднести розробку нормативних документів, що встановлюють відповідальність за комп'ютерні злочини й злочини в сфері технічного захисту інформації, захисту авторських прав і інше - відповідно до вимог карного й цивільного законодавств, а також судочинства. Правовий рівень захисту інформації передбачає також формування сукупності законодавчих актів, нормативно-правових документів, положень, інструкцій, посібників, вимоги яких є обов'язковими в рамках сфери їх діяльності в системі захисту інформації [4,19].

Таким чином, на правовому рівні забезпечення безпеки інформації повинні бути вироблені підходи щодо:

- системи нормативно-правового забезпечення робіт з захисту інформації на підприємстві;
- підтримки керівництвом організації заходів з забезпечення безпеки інформації на підприємстві, виконання правових та (або) договірних вимог з захисту інформації,
- визначення відповідальності посадових осіб, організаційної структури, комплектування і розподілу обов'язків співробітників служб захисту ІБ ;
- процедур доведення до персоналу та користувачів підприємства основних положень політики безпеки, навчання і підвищення їхньої кваліфікації з питань безпеки інформації;
- системи контролю за своєчасністю, ефективністю і повнотою реалізації на підприємстві рішень з захисту інформації, дотриманням персоналом і користувачами положень політики безпеки.

2. Економічний метод , що передбачає механізм усунення матеріального збитку, завданого власнику інформації в результаті несанкціонованих дій з нею з боку правопорушника [3].

3. Організаційно-технічний метод, в рамках якого створюється оболонка навколо об'єкта захисту, тобто інформаційних ресурсів, з певною мірою надійності виключає або суттєво утрудняє проведення маніпуляцій з інформацією в автоматизованих системах проти інтересів користувачів системи.

На організаційному рівні забезпечення безпеки інформації повинні бути вироблені підходи щодо:

• застосування режимних заходів на об'єктах підприємства, забезпечення їх фізичного захисту, носіїв інформації та інших ресурсів;

• організації проведення обстеження середовищ функціонування підприємства і порядку виконання робіт з захисту інформації та взаємодії з цих питань з іншими суб'єктами системи захисту інформації в державі;

• регламентації доступу сторонніх і власних користувачів та персоналу до інформаційної сфери підприємства;

• здійснення профілактичних заходів (наприклад, попередження ненавмисних дій, що призводять до порушення політики безпеки, попередження появи вірусів та ін.);

• реалізації окремих положень політики безпеки, найбільш критичних з точки зору забезпечення захисту аспектів (наприклад, організація віддаленого доступу до об'єктів підприємства),

• використання мереж передачі даних загального користування, зокрема Internet,

• використання несертифікованого програмного забезпечення та ін.

Програмно-технічні методи є основою для реалізації організаційно-технічного напрямку захисту інформації.

На технічному рівні забезпечення безпеки інформації повинні бути вироблені підходи щодо застосування технічних і програмно-технічних засобів, які реалізують задані вимоги з захисту інформації [12,23] .

Під час розгляду різних варіантів реалізації рекомендується враховувати наступні аспекти:

• інженерно-технічне обладнання виділених приміщень, в яких розміщуються компоненти організації, експлуатація і супроводження засобів блокування технічних каналів витоку інформації;

• реєстрація санкціонованих користувачів організації, авторизація користувачів в системі;

• керування доступом до інформації і механізмів, що реалізують послуги безпеки, включаючи вимоги до розподілу ролей користувачів і адміністраторів;

• виявлення і реєстрація небезпечних подій з метою здійснення повсякденного контролю або проведення службових розслідувань;

• перевірка і забезпечення цілісності критичних даних на всіх стадіях їхньої обробки на підприємстві;

- забезпечення конфіденційності інформації, у тому числі використання криптографічних засобів;
- резервне копіювання критичних даних, супроводження архівів даних і програмного забезпечення;
- відновлення роботи об'єктів організації після збоїв, відмов, особливо для об'єктів із підвищеними вимогами до доступності інформації;
- захист програмного забезпечення, що використовується у організації (на об'єктах організації) , від внесення несанкціонованих доповнень і змін;
- забезпечення функціонування засобів контролю, у тому числі засобів виявлення технічних каналів витоку інформації.

Організаційно-технічний напрям захисту інформації є найбільш реальним напрямом у захисті інформації підприємства. Організаційні методи полягають в забезпеченні збереження конфіденційної інформації підприємства шляхом формування корпоративної системи захисту [40,41].

У цьому напрямку доцільно виділити два основні завдання:

1) забезпечення цілісності самої інформації і процесів її обробки, передачі та зберігання;

2) забезпечення конфіденційності інформації обмеженого доступу.

При аналізі завдань захисту інформації введені поняття:

- Обчислювальна середа (ВСр) – складається з програм і даних, що розташовуються на внутрішніх накопичувачах автоматизованих систем (АС);
- Операційна середа (ОСр) - сукупність функціонуючих в даний момент часу елементів обчислювального середовища, що знаходяться в оперативній пам'яті АС;
- Зовнішній компонент ОСр - алгоритми управління АС через канали зв'язку;
- Внутрішній компонент ОСр - елементи ВСр даної АС [27].

Основне положення і розроблені моделі дозволяють виділити два основні класи задач захисту інформації:

1. Захист елементів обчислювального середовища - забезпечення цілісності даних, процедур обробки та конфіденційності інформації;

2. Контроль елементів операційного середовища - зовнішніх компонентів ОСР, цілісності внутрішніх компонентів і семантики даних.

Методи захисту елементів ВСр практично зводяться до методів захисту даних, а також до методів авторського захисту програм і даних на етапі їх розробки.

Системи розмежування доступу (СРД) забезпечують авторизований і санкціонований доступ до окремих груп елементів ВСр. До даного класу відносяться різного роду парольні системи та системи ідентифікації користувачів, що обмежують доступ як до системи в цілому, так і до окремих її елементів [5].

Типова система розмежування доступу включає підсистеми:

- ідентифікація користувача за індивідуальним паролем і забороною роботи з автоматизованою системою незареєстрованим користувачем;
- розмежування доступу до ресурсів для зареєстрованого користувача;
- автоматичної реєстрації дій користувача;
- автоматичного запиту підтвердження особи користувача після закінчення заданої паузи його неактивності;
- контролю за можливими спробами несанкційного доступу (НСД);
- адміністратора безпеки, що здійснює функції ведення списку користувачів і груп користувачів, визначення та зміни повноважень користувачів і т.д.;
- контролю цілісності та захисту від копіювання програмного забезпечення [13].

Програмно-технічні методи реалізуються за допомогою засобів програмного та апаратного забезпечення.

Власне захист програм забезпечується шляхом:

- захисту авторських прав;
- захисту програм від дослідження і копіювання;
- парольного захисту та захисту від несанкціонованого запуску;
- самотестування і самовідновлення виконуваного коду програми [5].

Питанням захисту авторських прав повинні приділяти увагу насамперед розробники програм.

Для парольного захисту і захисту від запуску програм використовуються ідентифікація користувача і обмеження на кількість запусків або за датою запуску, або з урахуванням кількості запусків.

Для самотестування і самовідновлення виконуваного коду програми вводяться модулі діагностики характеристик виконуваного коду програм: розмір файлу, контрольна сума, перелік контрольних точок і т.п. Крім того, існують алгоритми, здатні відновлювати штатний виконуваний код програми при деяких видах спотворення [5].

До числа засобів тестування і відновлення відносяться всі відомі антивірусні засоби.

На рис. 1.5 показано програмні засоби захисту [27].

Рис. 1.5. Програмні засоби захисту

Оптимальним варіантом забезпечення інформаційної безпеки є дотримання систематичного поєднання правових, організаційних та програмно-технічних методів у процесі управління підприємством.

Висновки до першого розділу

Проаналізовано основні вимоги нормативних документів до організації інформаційної безпеки. ISO / IEC 27-k – це перелік важливих міжнародних стандартів, вимоги яких складаються з кращих рекомендацій і практик в сфері створення, розвитку та управління системами інформаційної безпеки. Запровадження СУІБ є стратегічним рішенням для будь-якого підприємства, розробка і впровадження її залежить від потреб і цілей підприємства, вимог з безпеки її процесів, розміру і структури. Визначені основні завдання у

проведення комплексу заходів із побудови СУІБ. Приведені вимоги стандартів на основних напрямках діяльності в сфері інформаційної безпеки.Показано відображаннє питанн інформаційної безпеки у законах України і Стратегії національної безпеки України. Приведені переваги впровадження стандартів з управління інформаційною безпекою в банках України

Відмічено, що СУІБ є частиною загальної системи управління підприємства. Проаналізована практика захисту інформації та забезпечення безпеки діяльності підприємства.Показані негативні наслідки
погіршення параметрів інформації на підприємстві, виділені три основних напрямки захисту інформації і відповідно до них - загальні методи забезпечення інформаційної безпеки: правовий, економічний і організаційно-технічний. Відповідно до методів показані підходи їх застосування у вирішенні задач захисту інформації. Розглянуто основні класи задач захисту інформації.
Дотримання систематичного поєднання правових, організаційних та програмно-технічних методів у процесі управління підприємством дозволяє вийти на оптимальний варіант забезпечення інформаційної безпеки.

РОЗДІЛ 2
АНАЛІЗ НАПРЯМІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

Потреби забезпечення ІБ формуються під впливом цілої множини факторів: об’єктивних і суб’єктивних, внутрішніх і зовнішніх, прогнозованих і непередбачених тощо. У концентрованій формі вони можуть виступати як деструктивні, що негативно впливають на безпеку. В основі організації, планування й здійснення практичних дій щодо забезпечення ІБ є аналіз концепції загрози, оцінка характеру реальних і потенційних внутрішніх/зовнішніх небезпек і загроз, кризових ситуацій, а також інших несприятливих факторів, які спрямовані до інформації і інформаційних ресурсів будь-якої організації. На практиці основні підходи до захисту інформації і взагалі до забезпечення ІБ

здійснюють за трьома основними напрямками: правовий, організаційний і технічний захист [2,25,40].

Організація захисту від небезпек і загроз функціонуванню інформаційної системи підприємства відбувається шляхом побудови ефективної СІБ. В свою чергу побудова ефективної системи інформаційної безпеки - це комплексний процес, спрямований на мінімізацію зовнішніх і внутрішніх загроз при обліку обмежень на ресурси і час [13,40].

Сформована сукупність інженерно-технічних, організаційних та правових заходів відображається в політиці інформаційної безпеки. Політика безпеки повинна визначати системи захисту інформації і управління ІБ як систему забезпечення ІБ у вигляді сукупності правових норм, організаційних (правових) заходів, комплексу програмно-технічних засобів і процедурних рішень, спрямованих на протидію загрозам безпеці інформації з метою виключення або мінімізації можливих наслідків прояву інформаційних впливів.

Після прийняття того чи іншого варіанту політики ІБ необхідно оцінити рівень безпеки інформаційної системи організації. Оцінка захищеності на практиці проводиться за сукупністю показників, основними з яких є вартість, ефективність, реалізація. Завдання оцінки варіантів побудови системи захисту інформації досить складна, що вимагає залучення сучасних математичних методів багатопараметричної оцінки ефективності, до них відносяться: метод аналізу ієрархій, експертні методи, метод послідовних поступок і інші [26].

2.1. Методичні підходи до побудови системи забезпечення інформаційної безпеки

Побудову системи забезпечення інформаційної безпеки підприємства завжди починають з детального аналізу загроз її безпеці і вибором оптимального варіанту системи забезпечення інформаційної безпеки . Після використання обраного методу аналізу стану інформаційної безпеки підприємства поетапно переходять до створення системи забезпечення інформаційної безпеки, а завдяки організаційним і технічним напрямкам підвищують ефективність її процесів [12,26,40].

2.1.1 Аналіз загроз безпеки і вплив на побудову ефективної системи інформаційної безпеки

Можна виділити цілу низку джерел загроз ІБ сучасного підприємства:

- протизаконна діяльність деяких економічних структур у сфері формування, поширення і використання інформації;
- порушення встановлених регламентів збору, обробки та передачі інформації;
- навмисні дії та ненавмисні помилки персоналу інформаційних систем;
- помилки в проектуванні інформаційних систем;
- відмова технічних засобів і збої програмного забезпечення в інформаційних і телекомунікаційних системах тощо.

На сьогоднішній день фахівцями досліджується досить широкий перелік загроз безпеці інформаційних систем, які класифікують за рядом ознак (див. рис. 2.1).

Рис.2.1. Основні види загроз інформаційній безпеці [20]

Суттєвими загрозами безпеці є:

- витік або втрата інформаційних ресурсів;
- неофіційний доступ та зняття інформації, що охороняється, технічними засобами;
- перехоплення інформації, що циркулює в засобах і системах зв'язку та обчислювальної техніки, за допомогою технічних засобів негласного зняття інформації, несанкціонованого доступу до інформації та навмисних технічних впливів на них в процесі обробки та зберігання;
- підслуховування з використанням технічних засобів конфіденційних переговорів, що ведуться в службових приміщеннях, автотранспорті тощо.

Загрози інформаційним ресурсам можуть бути реалізовані шляхом:

- підкупу осіб, які мають безпосередній доступ до комерційної таємниці та іншої інформації з обмеженим доступом;
- необережного, недбалого поводження з комерційною таємницею та іншою інформацією з обмеженим доступом;
- недотримання вимог збереження інформації з обмеженим доступом, встановлених на підприємстві, при контактах з контролюючими і наглядовими органами внаслідок правової та психологічної непідготовленості відповідальних працівників тощо.

Протидія таким загрозам має полягати, насамперед, у:

- визначенні надійності працівників підприємства, які працюватимуть з комерційною таємницею та іншою інформацією з обмеженим доступом;
- організації спеціального діловодства з відомостями, що становлять та інформацію з обмеженим доступом;
- обґрунтуванні і закріпленні диференційованого доступу працівників до комерційною таємниці та іншої інформації з обмеженим доступом, при якому працівник може ознайомлюватися і вчиняти певні дії з нею виключно для виконання покладених на нього функціональних обов'язків;
- закріпленні персональної відповідальності працівника за збереження наданих йому або розроблених ним документів, інших носіїв інформації, що містять інформацію з обмеженим доступом підприємства;
- обмеженні доступу працівників і сторонніх осіб до приміщень, у яких обробляється (зберігається) інформація з обмеженим доступом;

- впровадженні заходів контролю за роботою працівників з носіями інформації з обмеженим доступом підприємства, а також ефективної системи виявлення і фіксації протиправних діянь з такою інформацією;
- впровадженні надійної і ефективної системи зберігання носіїв інформації, що виключає несанкціоноване ознайомлення з ними, їх знищення чи підробку [14,23].

Протидія таким загрозам може також полягати у широкому і головне економічно доцільному застосуванні технічних засобів безпеки інформаційної інфраструктури [6,28].

Конкретними заходами ліквідації загроз безпеці інформаційної інфраструктури підприємства мають бути:

- створення цілісності засобів захисту, технічного і програмного середовища, що полягає у фізичному збереженні засобів інформатизації, незмінності програмного середовища, виконанні засобами захисту передбачених функцій, ізольованості засобів захисту від користувачів;
- захист інформації від витоку внаслідок наявності фізичних полів за рахунок акустичних та побічних електромагнітних випромінювань і наводок на комунікаційні мережі та конструкції будівель;
- використання криптографічного захисту найбільш цінної інформації при її обробці в електронно-обчислювальних машинах (комп'ютерах), системах та комп'ютерних мережах і мережах електрозв'язку підприємства;
- надання диференційованого доступу працівникам для здійснення конкретних операцій (створення, читання, запис, модифікація, видалення) за допомогою програмно-технічних засобів, а також розмежування доступу користувачів до даних в електронно-обчислювальних машинах (комп'ютерах), системах та комп'ютерних мережах і мережах електрозв'язку банківської установи різного рівня та призначення;
- ідентифікація користувачів та здійснюваних ними процесів в електронно-обчислювальних машинах (комп'ютерах), системах та комп'ютерних мережах і мережах електрозв'язку установи на основі використання паролів, ключів, магнітних карт, цифрового підпису, а також біометричних характеристик особи як при доступі до інформаційно-телекомунікаційних систем;

- реєстрація (з фіксацією дати і часу) дій користувачів з інформаційними та програмними ресурсами в електронно-обчислювальних машинах (комп'ютерах), системах та комп'ютерних мережах, зокрема протиправних спроб доступу;
- попередження передачі інформації з обмеженим доступом по незахищених лініях зв'язку;
- запобігання впровадженню в інформаційно-телекомунікаційні системи програм-вірусів;
- регулярна перевірка технічних засобів і приміщень для виявлення наявності в них пристроїв несанкціонованого доступу до інформації;
- обладнання спеціальних приміщень для захисту мовної інформації при проведенні конфіденційних переговорів тощо [14].

Найбільш суттєвими загрозами безпеці «інформаційного поля» є підрив ділового іміджу підприємства, виникнення проблем у взаємостосунках з реальними та потенційними клієнтами, конкурентами, контролюючими та правоохоронними органами, спричиненими передусім поширенням недостовірної, заздалегідь неправдивої інформації про підприємство, здійсненням негативних інформаційних впливів на його керівництво, працівників тощо.

Конкретними заходами ліквідації загроз безпеці «інформаційного поля» підприємства є:

- створення досконалої інформаційно-аналітичної діяльності;
- оперативне реагування на випадки поширення неправдивої інформації про підприємство;
- скоординоване і централізоване поширення рекламної, маркетингової та іншої інформації, що підвищує імідж і сприйняття підприємства клієнтами;
- налагодження у межах чинного законодавства інформаційної співпраці з органами державної влади і місцевого самоврядування [6].

Отже, виходячи з низки зазначених загроз і шляхів їх подолання систему забезпечення інформаційної безпеки підприємства можна визначати як комплекс реалізації організаційних, технічних, програмних і криптографічних засобів і заходів задля:,

- захисту інформації з обмеженим доступом підприємства від несанкціонованого розповсюдження, використання і порушення її конфіденційності (таємності);
- забезпечення цілісності і доступності інформації, що обробляється, зберігається, циркулює в електронно-обчислювальних машинах (комп'ютерах), системах та комп'ютерних мережах і мережах електрозв'язку підприємства;
- протидії поширенню недостовірної, заздалегідь неправдивої інформації про банківську установу, здійсненню негативних інформаційних впливів на її керівництво [14].

Таким чином, в залежності від конфіденційності інформації, яка зберігається, обробляється та передається на підприємстві, рівня її критичності, величини можливих збитків від реалізації загроз, матеріальних, фінансових та інших її ресурсів, а також інших чинників може бути об'єктивно обґрунтована пропозиція щодо доцільності застосування варіантів побудови СІБ. З практики можливі наступні варіанти:

1. Досягнення необхідного рівня ІБ за мінімальних затрат і допустимого рівня обмежень на технології зберігання, оброблення та передавання інформації на підприємстві.
2. Досягнення необхідного рівня захищеності інформації за допустимих затрат і заданого рівня обмежень на технології зберігання, оброблення та передавання інформації на підприємстві.
3. Досягнення максимального рівня захищеності інформації за необхідних затрат і мінімального рівня обмежень на технології зберігання, оброблення та передавання інформації на підприємстві.

Якщо інформація становить державну таємницю, то необхідно застосовувати, як правило, третій варіант.

При оцінюванні витрат на забезпечення ІБ здійснюється первинне оцінювання допустимих витрат на блокування загроз, виходячи з вибраного варіанту побудови СІБ і виділених на це коштів. На етапі проектування СІБ, після формування пропозицій щодо складу заходів і засобів захисту, здійснюється оцінка залишкового ризику для кожної пропозиції (наприклад, за критерієм "ефективність/вартість"), вибирається найбільш оптимальна серед них і первинна оцінка уточнюється. Якщо залишковий ризик перевищує гранично допустимий, вносяться відповідні зміни до складу заходів і засобів захисту, після

чого всі процедури виконуються повторно до одержання прийнятного результату.

2.1.2 Побудова системи забезпечення інформаційної безпеки

Для того, щоб забезпечити повноцінну ІБ підприємства, з можливістю подальшого управління, важливо запровадити та підтримувати управління (менеджменту) інформаційної безпеки.

Система управління (менеджменту) інформаційної безпеки (Information Security Management System або ISMS) – нк система політик, процесів, стандартів, документів та засобів, що забезпечують для організації досягнення цілей управління ІБ. Структура процесів СУІБ, що найчастіше використовується на практиці, показана на рис. 2.2 [20]:

Рис. 2.2.Структура процесів СУІБ

1) Контроль – формування СУІБ в межах організації, формування організаційної структури для підготовки, затвердження та реалізації Політик інформаційної безпеки, розподіл відповідальності, формування документації з контролю.
2) Планування – розробити та рекомендувати підходящі метрики та способи виміру ІБ. Насамперед, планування повинно спиратися на вимоги та особливості конкретної організації. Джерелами інформації для формування вимог ІБ є бізнес, ризики, плани, стратегії, контракти.

3) Реалізація – забезпечити процедури, інструменти, контролі безпеки для підтримки Політик інформаційної безпеки. Серед заходів можна виділити класифікацію інформації.
4) Оцінка – перевірка Політик ІБ на відповідність вимогам ІБ, описаними, до прикладу, в стандартах ДСТУ ISO/IEC 27001:2015 та ДСТУ ISO/IEC 27002:2015, проведення регулярних перевірок стану ІБ ІТ- систем, надання інформації про результати перевірки зовнішнім аудиторам за необхідності.
5) Підтримка – покращення засобів та контролів ІБ. [20]

Головні функціональні напрями діяльності СУІБ та їх взаємодії показані на рис.2.3 [20]:

Рис. 2.3. Головні функціональні напрями діяльності СУІБ та їх взаємодії в межах СУІБ

Менеджмент ІБ має прямий вплив на функціонування СУІБ, адже саме його принципи та заходи безпеки формують основу діяльності в межах СУІБ. Те, як управління ІБ формує СМІБ, показано на рис.2.4:

Рис.2.4. Безперервний процес менеджмента ІБ із запровадженням СУІБ

Основні процеси впровадження СУІБ можна представити і в такому вигляді, як на рис.2.5.

Рис. 2.5.Основні процеси впровадження СУІБ

Комплекс робіт з побудови СУІБ [40] може включати наступні роботи (див. рис.2.6):

1. Визначення області дії СУІБ.

2. Попередній аудит на відповідність вимогам ISO 27001:

- збір вихідних даних про бізнес-процеси, структурні підрозділи, інформаційно-телекомунікаційну інфраструктуру, методи і засоби забезпечення ІБ;
- аналіз діючої організаційно-розпорядчої документації, що регламентує питання забезпечення ІБ;
- оцінку поточного рівня відповідності вимогам стандарту ISO 27001.

3. Проведення оцінки ризиків:

- розробку методики оцінки ризиків;
- інвентаризацію та класифікацію активів;
- формування карти загроз;
- аналіз і оцінку ризиків;
- розробку плану обробки ризиків.

4. Розробка процедур і документації СУІБ:

- розробку процесів управління ІБ;
- розробку процесів забезпечення ІБ;
- розробку комплекту організаційно-розпорядчої документації, що регламентує питання забезпечення ІБ;
- розробку програм підвищення обізнаності з питань управління та забезпечення ІБ.

5. Впровадження процедур і документації СУІБ:

- впровадження процесів управління ІБ;
- впровадження процесів забезпечення ІБ;
- навчання та підвищення обізнаності співробітників в області забезпечення ІБ.

6. Дослідна експлуатація СУІБ.

7. Сертифікаційний аудит і видача міжнародного сертифікату:

- взаємодія з органом сертифікації;
- консультаційна підтримка при проходженні сертифікаційного аудиту.

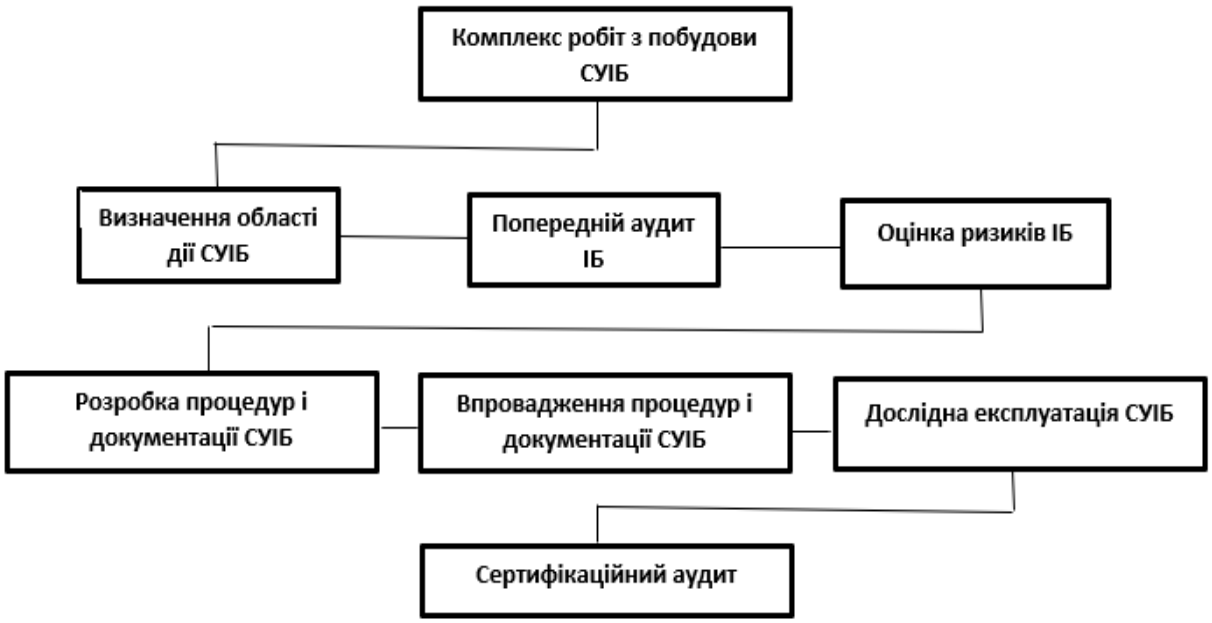

Рис.2.6. Комплекс робіт з побудови СУІБ

Підприємствам різних галузей доводиться функціонувати в умовах високої складності, невизначеності і динамічності навколишнього середовища. У зв'язку з цим виникає потреба у створенні адекватного механізму організації ІБ на підприємствах. Тому сьогодні спеціалізовані фірми пропонують широкий спектр засобів захисту інформаційних систем з урахуванням їх вартості та функціональних можливостей. Найбільш прийнятним підходом при виборі того чи іншого варіанту є дотримання принципу «розумної достатності», суть якого полягає в тому, що визначальними при проектуванні такого важливого документу, як політика ІБ, повинні бути: розмір підприємства, його ресурсні та фінансові можливості, поточний рівень ІБ. Постійна робота в сфері підтримки ІБ на належному рівні є необхідною умовою ефективності підприємницької діяльності.

Водночас безпека інформаційної системи має розглядатися як важлива складова загальної системи безпеки підприємства. Причому необхідна розробка концепції ІБ, в якій слід передбачити не тільки заходи, пов'язані з інформаційними технологіями (криптозахист, програмні засоби адміністрування прав користувачів, їх ідентифікації та автентифікації, брандмауери для захисту входів-виходів мережі тощо), але і відповідні заходи адміністративного та технічного характеру [15].

Метою захисту інформації має бути також збереження цінності інформаційних ресурсів для їх власника. Виходячи з цього, безпосередні заходи захисту спрямовують не так на самі інформаційні ресурси, як на збереження певних технологій їх створення, обробки, зберігання, пошуку та надання користувачам. Ці технології мають враховувати особливості інформації, які роблять її цінною, а також давати змогу користувачам різних категорій ефективно працювати з інформаційними ресурсами.

Зі зростанням науково-технічного прогресу буде зростати важливість питання ІБ і його постоянного впливу на виконання функціональнмх задач в діяльності підприємства. Це може привести до негативних наслідків:

Погіршення на підприємстві таких параметрів інформації, як конфіденційність, цілісність, доступність, вірогідність тощо, може призвести до негативних наслідків:

- погіршення ділових відносин із партнерами;
- зриви переговорів, втрата вигідних контрактів;
- невиконання договірних зобов'язань;
- необхідність проведення додаткових ринкових досліджень;
- відмовлення від рішень, що стали неефективними через розповсюдження інформації, і, як наслідок, – фінансові втрати, пов'язані з новими розробками;
- втрата можливості запатентувати результат науково-технічної діяльності або продати ліцензію;
- зниження цін або обсягів реалізації;
- втрати ділової репутації;
- більш жорсткі умови одержання кредитів;
- труднощі в постачанні і придбанні устаткування тощо.

У цих ситуаціях зневага питаннями захисту інформації може призвести до повного банкрутства. Дії внутрішніх порушників, такі як недбалість співробітників, крадіжки інформаційних ресурсів та ІТ-устаткування, фінансові й інші види шахрайства з використанням інформаційних систем і ресурсів тощо, не завжди стають предметом уваги при вирішенні проблем ІБ. Тому з практики підтверджується , що людський фактор завжди був і є одним із найважливіших ризиків будь-якого бізнесу, оскільки більшість інцидентів відбуваються саме з вини співробітників.

На сьогодні ще залишаються проблеми з віднощенням до створення СІБ на підприємствах. Першою і найбільшою проблемою у створенні СІБ є відсутність розуміння в керівництва необхідності створення такої системи. Друга проблема при створенні СІБ – відсутність достатньої кількості фінансових коштів,що зустрічається дуже часто. Третьою найнебезпечнішою проблемою є ситуація, коли є розуміння керівництва та необхідні кошти, але створення СІБ доручають фахівцям, що не мають ані відповідної освіти, ані достатнього досвіду. Найчастіше це бувають системні адміністратори або відділ технічної підтримки, які розцінюють створення СІБ як установку і налаштування антивірусу. Наявність внутрішнього зловмисника, найчастіше, узагалі не береться до уваги [6].

Тому в першу чергу необхідно подати проблему у зрозумілому для бізнесу вигляді. Це завдання лягає на керівництво служби ІБ підприємства, що має виявити і наочно показати власникам підприємства весь спектр загроз в інформаційній сфері, а також переконати, що протистояти їм можна тільки на основі створення і упровадження ефективних систем захисту інформації.

По-перше, для ефективного захисту інформаційних ресурсів потрібна реалізація цілої низки різнорідних заходів, які можна розділити на три групи: юридичні, організаційно-економічні й технологічні.

По-друге, хоча розробкою заходів у кожній із трьох груп повинні займатися фахівці відповідних галузей знань, які застосовують свої способи і методи для досягнення заданих цілей, кінцевий успіх значною мірою буде залежати від того, наскільки в рамках системного підходу вдасться визначити і реалізувати взаємні зв'язки між відповідними визначеннями, принципами, способами і механізмами захисту.

У сучасному поданні рольових функцій служби ІБ можна виділити чотири напрями, які зазначені на рис.2.7. [6].

Рис.2.7. Напрями функцій служби інформаційної безпеки

У рамках першого напряму мають вирішувати такі основні завдання[8]:

- аналіз і узагальнення потенційних загроз і таких, що реалізувалися, причин порушень вимог ІБ;
- аналіз ступеня забезпечення безперервності бізнес-процесів, що використовують ІТ, з точки зору ІБ;
- пошук нових загроз і вразливостей, пов'язаних з інформаційною взаємодією;
- побудова методик оцінки інформаційних ризиків;
- інформаційне обстеження підприємства та інформаційних ресурсів;
- розробка методів захисту інформації та ІТ і методик їх упровадження в діяльність підприємства;
- розробка і модифікація концепції та політики забезпечення ІБ;
- створення локальної нормативної бази із цих питань з урахуванням комплексного підходу до економічної безпеки;
- розробка методик оцінки рівня ІБ і визначення достатності захисту інформації та ІТ з урахуванням потреб бізнесу, а також існуючої і перспективної нормативної бази;
- аналіз виконання вимог ІБ всіх використовуваних процедур створення, обробки, пересилання, збереження, знищення інформації, у тому числі:

- процедур інформаційної взаємодії підрозділів підприємства між собою і із зовнішніми організаціями;
- порядків доступу співробітників підприємства і суміжних організацій, а також клієнтів до інформаційних ресурсів і зовнішніх комп'ютерних мереж;
- проектів розвитку ІТ, включаючи системи зв'язку і телекомунікацій;
- проектів договорів із зовнішніми організаціями, з якими здійснюється обмін інформацією;
- проектів інших нормативних документів, що передбачають інформаційну взаємодію;
- підготовка аналітичних записок, що містять висновки із проведеного аналізу і пропозиції щодо реалізації захисту інформації.

Другий напрям передбачає такі основні завдання[8]:

- планування на основі координації діяльності всіх підрозділів робіт із забезпечення ІБ підприємства;
- організація й участь у впровадженні методів забезпечення ІБ в діяльність підприємства.
- робота з персоналом, партнерами і клієнтами;
- узгодження заявок на доступ і порядку доступу співробітників і зовнішніх організацій до інформаційних ресурсів підприємства;
- процедур інформаційної взаємодії підрозділів із зовнішніми організаціями;
- договорів, з якими здійснюється інформаційна взаємодія; проектів наказів, розпоряджень, інших нормативно-розпорядницьких документів;
- рішення поточних практичних питань з ІБ, що виникають у підрозділах.

У рамках третього напряму мають вирішувати такі основні завдання[8]: підтримка ключових структур, використовуваних у зовнішніх і вбудованих засобах криптографічного захисту інформації; підтримка роботи інших засобів ІБ.

Четвертий напрям передбачає рішення таких основних завдань[8]:

- перевірка виконання вимог ІБ працівниками підприємства й іншими особами, що мають доступ до інформаційних ресурсів;

- моніторинг дій користувачів ІТ (несанкціонованої модифікації інформації, використання різних поштових та інших сервісів мережі Інтернет для відправлення конфіденційної інформації за межі підприємства тощо);
- контроль своєчасної зміни прав користувачів в інформаційних системах; блокування облікових записів звільнених (переведених на іншу роботу) користувачів;
- контроль дотримання настроювань безпеки, включаючи парольну політику, інші вбудовані СІБ, зовнішні засоби захисту інформації;
- моніторинг роботи систем виявлення (запобігання) мережних атак, систем оцінки якості побудови мережі й інших автоматизованих систем комп'ютерної безпеки;
- участь у розборі виявлених порушень ІБ і вимог нормативних документів із цих питань.
- підготовка пропозицій щодо попередження порушень;
- проведення внутрішнього аудиту питань ІБ;
- підготовка пропозицій щодо використання зовнішнього аудиту;
- проведення моніторингу можливого випливу конфіденційної інформації технічними каналами.

Вирішення цих завданнь здійснюється службою ІБ завдяки правилам і процедурам, які визначені таким документом, як політика безпеки підприємства.

Таким чином, у сучасних умовах інформаційна безпека є невід'ємною складовою системи надійного забезпечення всієї діяльності підприємства, що є неодмінною умовою переходу на модель його стійкого розвитку.

Завдання системи ІБ обумовлюються її призначенням і полягають у: забезпеченні безпечного, надійного зберігання і передачі інформації в електронному вигляді, розташованої на різних носіях; організації надійного доступу до електронної інформації; обмеження і контроль доступу до інформації, з якою працюють співробітники; створенні правил безпечної роботи з інформацією; проведенні заходів щодо резервування інформації; забезпеченні відновлення інформації в аварійних ситуаціях; підтримці інформаційної безпеки на заданому рівні.

Оскільки комплексна система захисту інформації призначена забезпечувати безпеку всієї захищаємої інформації, до неї повинні пред'являтися наступні вимоги:

- вона повинна бути прив'язана до цілей і завдань захисту інформації на конкретному підприємстві;

- вона повинна бути цілісною: містити всі її складові, мати структурні зв'язки між компонентами, що забезпечують її погоджене функціонування;

- вона повинна бути всеохоплюючою, враховуючі всі об'єкти і складові захисту, всі обставини і фактори, що впливають на безпеку інформації, і всі види, методи і засоби захисту;

- вона повинна бути достатньою для вирішення поставлених завдань і надійною у всіх елементах захисту, тобто базуватися на принципі гарантованого результату;

- вона повинна бути «вмонтованою» у технологічні схеми збору, зберігання, обробки, передачі і використання інформації;

- вона повинна бути компонентною, логічно, технологічно й економічно обґрунтованою;

- вона повинна бути реалізованими, забезпеченими всіма необхідними ресурсами;

- вона повинна бути простій і зручною в експлуатації і управлінні, а також у використанні законними споживачами;

- вона повинна бути безперервною;

- вона повинна бути досить гнучкою, здатною до цілеспрямованого пристосування при зміні компонентів її складових частин, технології обробки інформації, умов захисту [40].

Таким чином, забезпечення безпеки інформації - безперервний процес, що полягає в контролі захищеності, виявленні вузьких місць у системі захисту, обґрунтуванні і реалізації найбільш раціональних шляхів удосконалення і розвитку системи її захисту [29].

ІБ досягається шляхом впровадження сукупності необхідних засобів захисту інформації, до числа яких можуть входити політики, рекомендації, інструкції, організаційні структури і програмні функції. Ці засоби необхідно реалізувати для того, щоб гарантувати виконання вимог до безпеки на конкретному підприємстві.

Будь-яке підприємство повинно визначити свої вимоги до безпеки. При оцінці вимог використовуються три основні показники.

Першим показником служить оцінка небезпек, з якими стикається підприємство. Шляхом оцінки небезпек визначаються загрози для інформації, її вразливість та ймовірність виникнення загроз, а також можливий збиток.

Другий показник - це законодавчі, нормативні та договірні вимоги, які повинна дотримуватися підприємство, його партнери по бізнесу, підрядники та постачальники послуг.

Третій показник - це певний набір принципів, цілей і вимог до обробки інформації, розроблених підприємством для підтримки своєї діяльності.

Визначення вимог до безпеки проводиться шляхом методичної оцінки всіх процесів управління захистом інформації і ІБ в цілому.

2.1.3 Вибір методів аналізу стану забезпечення ІБ

Діяльність із забезпечення ІБ здійснюється за допомогою різних способів, засобів і прийомів, які у сукупності складають методи забезпечення інформаційної безпеки. Метод передбачає певну послідовність дій на підставі конкретного плану.

Вибір методів аналізу стану забезпечення ІБ залежить від конкретного рівня і сфери організації захисту (табл. 2.1) [9].

Таблиця 2.1

Рівні захисту інформаційної безпеки

РІВНІ ЗАХИСТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
Фізичний	Здійснюється організація і фізичний захист інформаційних ресурсів, інформаційних технологій, що використовуються і управлінських технологій;
Програмно - технічний	Здійснюється ідентифікація і перевірка дійсності користувачів, управління доступом, протоколювання і аудит, криптографія, екранування, забезпечення високої доступності;

Управлінський	Здійснюється управління, координація і контроль організаційних, технологічних і технічних заходів на всіх рівнях з боку єдиної системи забезпечення ІБ;
Технологічний	Здійснюється реалізація політики ІБ за рахунок застосування комплексу сучасних автоматизованих інформаційних технологій;
Рівень користувача	Реалізація політики ІБ спрямована на зменшення рефлексивного впливу на об'єкти ІБ, унеможливлення інформаційного впливу з боку соціального середовища;
Мережевий	Дана політика реалізується у форматі координації дій компонентів системи управління, які пов'язані між собою однією метою;
Процедурний	Вживаються заходи, що реалізуються людьми. Серед них можна виділити наступні групи процедурних заходів: управління персоналом, фізичний захист, підтримання працездатності, реагування на порушення режиму безпеки, планування реанімаційних робіт.

Методи можуть значно змінюватися і варіюватися в залежності від типу діяльності, в якій вони використовуються, а також сфери застосування.

Виділяють декілька типів методів забезпечення ІБ (див. рис.2.8):

- однорівневі методи, які будуються на підставі одного принципу управління ІБ;

- багаторівневі методи які будуються на основі декількох принципів управління ІБ, кожний з яких слугує вирішення власного завдання. При цьому приватні технології не пов'язані між собою і спрямовані лише на конкретні чинники інформаційних загроз;

- комплексні методи — багаторівневі технології, які об'єднані у єдину систему координуючими функціями на організаційному рівні з метою забезпечення ІБ, виходячи з аналізу сукупності чинників небезпеки, які мають

семантичний зв'язок або генеруються з єдиного інформаційного центру інформаційного впливу;

- інтегровані високоінтелектуальні методи — багаторівневі, багатокомпонентні технології, які побудовані на підставі могутніх автоматизованих інтелектуальних засобів з організаційним управлінням.

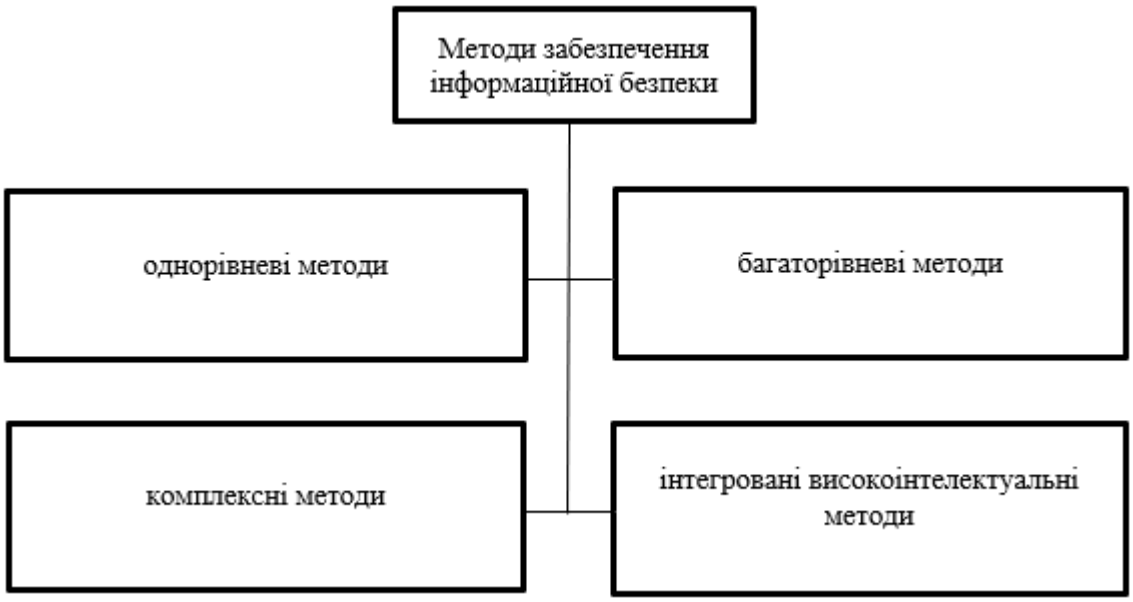

Рис.2.8. Типи методів забезпечення інформаційної безпеки

Методи забезпечення ІБ активно використовуються на будь-якій стадії управління загрозами. До таких стадій відносяться:

- прийняття рішення по визначенню області та контексту інформаційної загрози і складу учасників процесу протидії;
- ухвалення загальної стратегії і схеми дій в політичній, економічній, соціальній та інших сферах життєдіяльності;
- забезпечення адекватного сприйняття загрози та небезпеки у нижчих організаційних ланках системи управління національної безпеки;
- виділення необхідних політичних, економічних, соціальних, адміністративних і організаційних ресурсів, достатніх для реалізації програми відбиття інформаційної загрози і збереження сталого розвитку інформаційних ресурсів системи управління: трансформації результатів оцінки ризиків у відповідну політику безпеки, включаючи національну [10].

Завдання забезпечення ІБ повинно вирішуватися системно, це означає, що різні засоби повинні застосовуватися одночасно і під централізованим управлінням. При цьому всі складові системи повинні «знати» про існування один одного, взаємодіяти і забезпечувати захист як від зовнішніх, так і від внутрішніх загроз.

В нинішній час для забезпечення належного стану ІБ потрібна не просто розробка окремих механізмів захисту, а реалізація системного підходу, що включає комплекс взаємопов'язаних заходів (використання спеціальних технічних і програмних засобів, організаційних заходів, нормативно-правових актів і т.д.). Головною метою будь-якої системи забезпечення ІБ є створення умов функціонування підприємства, запобігання загроз його безпеки, захист законних інтересів підприємства від протиправних посягань, недопущення розкрадання фінансових засобів, розголошення, втрати, витоку, спотворення і знищення службової інформації, забезпечення в рамках виробничої діяльності всіх підрозділів підприємства.

Рівень ІБ підприємства відображає захищеність інформаційного середовища та ефективність інформаційного забезпечення процесу управління на підприємстві [15,16,18].

Процес забезпечення ІБ підприємства можна представити як взаємодію трьох підсистем: підсистема інформаційного забезпечення процесу управління на підприємстві; підсистема захисту інформаційного середовища підприємства; підсистема діагностики рівня ІБ.

Для забезпечення захисту інформаційного середовища підприємства необхідне систематичне виконання наступних функцій системи ІБ (рис. 2.9):

- аналіз загроз інформаційній безпеці;
- планування та розробка заходів щодо забезпечення ІБ;
- оперативна реалізація запланованих дій.

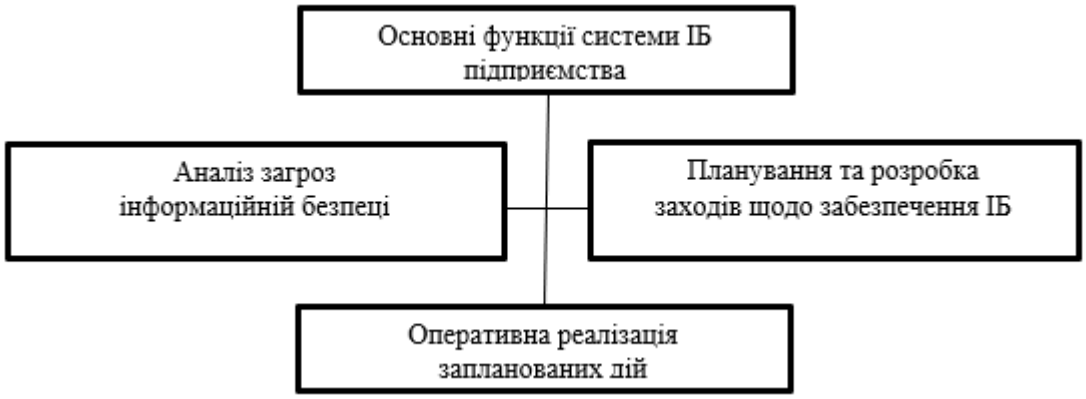

Рис. 2.9. Основні функції системи ІБ підприємства

Діагностику рівня ІБ підприємства пропонується проводити за трьома ключовими напрямками (рис.2.10): оцінка програмно-технічної захищеності інформації; оцінка інформаційної надійності персоналу; оцінка інформації, що надається особам, що приймають рішення, інформаційною службою підприємства [19,24].

Для оцінки інформаційної надійності персоналу пропонується розраховувати коефіцієнт правової захищеності інформації, коефіцієнт досвіду роботи персоналу, що забезпечує ІБ підприємства, коефіцієнт надійності персоналу, що забезпечує ІБ підприємства та коефіцієнт підготовленості персоналу до розпізнавання загроз [13-15].

Оцінку інформації, що надається особам, що приймають рішення, інформаційною службою підприємства пропонується проводити за допомогою трьох показників: коефіцієнт повноти інформації, коефіцієнт точності інформації та коефіцієнт суперечливості інформації, які варто доповнити коефіцієнтом своєчасності надання інформації та коефіцієнтом надійності інформації.

Рис. 2.10. Визначення стану інформаційної безпеки підприємства

Варто зазначити, що для отримання інформації, необхідної для розрахунку наведених показників, обов’язковою умовою є наявність системи моніторингу діяльності інформаційної служби підприємства [16].

Кількісний аналіз та моделювання є тими інструментальними засобами, які дають змогу оцінити, виокремити, нехай і наближено, суттєві ризики з несуттєвих (надуманих).Однак у більшості випадків одного лише якісного аналізу недостатньо для ідентифікації та виокремлення суттєвих чинників ризику й нехтування несуттєвими (надуманими). З цією метою необхідно здійснювати кількісний аналіз небезпеки. А це потребує здобуття відповідної інформації.

Методи експертних оцінки включають комплекс логічних і математико-статистичних методів і процедур, пов’язаних з діяльністю експерта по переробці необхідної для аналізу і прийняття рішень інформації. Центральною «фігурою» експертної процедури є сам експерт - це фахівець, який використовує свої здібності (знання, вміння, досвід, інтуїцію і т.п.) для знаходження найбільш ефективного рішення.

Експерти, що залучаються для оцінки небезпеки, в тому числі і інформаційної і політики безпеки, повинні: мати доступ до всієї наявної в розпорядженні розробника інформації; володіти достатнім рівнем креативності мислення та необхідними знаннями у відповідній предметній області; бути вільним від особистих переваг щодо проекту (не лобіювати його).

Можна виділити наступні основні методи експертних оцінок, що застосовуються для аналізу небезпеки: запитальники; SWOT-аналіз; роза і спіраль ризиків; оцінка ризику стадії проекту; метод Дельфі [19].

Важливими методами аналізу стану забезпечення ІБ є методи опису і класифікації. Для здійснення ефективного захисту системи управління ІБ слід, по-перше, описати, а лише потім класифікувати різні види загроз та небезпек, ризиків та викликів і відповідно сформулювати систему заходів по здійсненню управління ними.

У якості розповсюджених методів аналізу рівня забезпечення ІБ використовуються методи дослідження причинних зв'язків. За допомогою даних методів виявляються причинні зв'язки між загрозами та небезпеками;

здійснюється пошук причин, які стали джерелом і спричинили актуалізацію тих чи інших чинників небезпеки, а також розробляються заходи по їх нейтралізації. У числі даних методів причинних зв'язків можна назвати наступні: метод схожості, метод розбіжності, метод сполучення схожості і розбіжності, метод супроводжувальних змін, метод залишків.

Незалежно від розмірів організації і специфіки її інформаційної системи роботи щодо забезпечення режиму ІБ зазвичай складаються з наступних етапів:

- вироблення політики безпеки;

- визначення сфери (меж) системи управління ІБ та конкретизація цілей її створення;

- оцінка небезпек;вибір контрзаходів, які забезпечують режим ІБ;

- управління ризиками; аудит системи управління ІБ.

Для управління ІБ підприємства розробляється деяка стратегія управління небезпеками. Наприклад, тут можливі такі підходи до управління інформаційними ризиками компанії: зменшення ризику; ухилення від ризику; зміна характеру ризику;прийняття ризику.

Важливим методом забезпечення ІБ є метод критичних сценаріїв. У зазначених сценаріях аналізуються ситуації, коли уявний противник паралізує систему управління і відповідно знижує здатність підприємства управляти в межах оптимальних параметрів.

Існують методи, які можна вважати основоположними, що дозволяють створити надійну основу для реалізації ІБ. Ці методи або базуються на важливих законодавчих вимогах, або відносяться до загальновизнаних методів роботи в області управління ІБ.

З законодавчої точки зору найважливішими для організації вважаються наступні заходи: захист даних і нерозголошення особистої інформації; захист організаційних записів; захист прав на інтелектуальну власність.

До загальновизнаних методів забезпечення ІБ відносяться наступні: створення документа, що визначає політику ІБ; розподіл відповідальності за ІБ; навчання і підготовка в галузі ІБ; створення звітів про інциденти; підтримка безперервності бізнесу.

Ці методи можуть застосовуватися в більшості організацій і в більшості середовищ. Слід зауважити, що незважаючи на те, що всі описані методи є

важливими, значимість кожного методу слід визначати у світлі конкретних ризиків, з якими стикається підприємство.

2.1.4 Стадії створення системи забезпечення інформаційної безпеки

З огляду на зростаючу роль інформаційно-телекомунікаційних технологій та розширення обсягів інформації, яка в них зберігається та циркулює, захист інформації та засобів її обробки зокрема та забезпечення корпоративної ІБ загалом є дуже важливою складовою функціонування сучасного підприємства.

Інформація існує у багатьох формах, вона може бути надрукованою, збереженою в електронному вигляді, написана на папері, переслана поштою або допомогою електронних засобів, показана на плівці або записана у бесіді великої групи людей. Незалежно від набутого виду інформації або засобів, за допомогою яких вона зберігається або поширюється, інформація завжди повинна бути належним чином захищеною.

Забезпечення інформаційної безпеки (ЗІБ) - це не тільки захист інформації від несанкціонованого доступу. ЗІБ - це в основному практика запобігання несанкціонованому доступу, використанню, розголошенню, зриву, модифікації, запису або знищенню інформації. Інформація може бути фізичною або електронною. Інформація може бути будь-якою, наприклад персональні дані, відомості про профіль у соціальних мережах, особисті дані, які зберігаються в мобільному телефоні, біометричні дані тощо. Таким чином, ІБ має забезпечити захищеність стількох видів інформації обмеженого доступу, використовуючи різноманітні засоби, зокрема технічні і криптографічні, мобільні обчислення, методи кіберкриміналістики тощо [1,28,29].

Забезпечення ІБ має на меті досягнення трьох цілей:

1) цілісність;

2) конфіденційність;

3) доступність.

Цілісність означає підтримку даних у правильному стані та запобігання їх неправильному зміненню, випадково чи зловмисно. Багато методів, що забезпечують конфіденційність, також захищають цілісність даних - врешті-решт, хакер не може змінити дані, до яких він не має доступу. Але існують інші інструменти, які допомагають забезпечити глибокий захист цілісності. Наприклад, використання програмного забезпечення для контролю версій та регулярне створення резервних копій може допомогти відновити і привести дані до правильного стану, якщо це необхідно. Цілісність також охоплює поняття відмови, тобто можливість довести, що цілісність даних збережена, особливо в юридичному контексті.

Конфіденційність. Дані є конфіденційними, коли ними можуть користуватися лише ті люди, яким надано до них доступ; щоб забезпечити конфіденційність, потрібно мати можливість визначити, хто намагається отримати доступ до даних, та блокувати спроби тих, хто не має дозволу. Паролі, шифрування, автентифікація та захист від атак проникнення - всі ці методи призначені для забезпечення конфіденційності.

Доступність означає, що інформація повинна бути доступна авторизованому користувачу в разі потреби. Наприклад, коли потрібно отримати доступ до інформації конкретного працівника, щоб перевірити, чи він не перевищив кількість днів відпустки, це вимагає співпраці різних організаційних команд, таких як група мережевих операцій, операцій з розробки, реагування на інциденти та управління політикою / змінами. Атака відмови в обслуговуванні є одним із факторів, який може перешкоджати доступності інформації.

Отже, в основі ІБ лежить підтримання цілісності, конфіденційності та доступності інформації, гарантуючи, що інформація ні в якому разі не буде порушена, коли виникають критичні проблеми. Ці проблеми не обмежуються стихійними лихами, несправностями комп'ютера, сервера, тощо.

З огляду на швидке зростання сфери ІБ за останні роки пропонуються багато областей для спеціалізації, включаючи захист мереж та суміжної

інфраструктури, захист додатків та баз даних, тестування безпеки, аудит інформаційних систем, планування безперервності бізнесу тощо.

Підприємство повинно ідентифікувати свої вимоги безпеки. Існує три основних джерела формування вимог безпеки (див.рис.2.11):

Рис.2.11. Джерела формування вимог до безпеки підприємства

- Перше джерело формування вимог безпеки базується на оцінці ризиків для підприємства, беручи до уваги загальну корпоративну бізнес-стратегію та цілі. Під час оцінювання ризику ідентифікують загрози активам і оцінюють вразливість та ймовірність подій, визначають величину потенційного впливу.
- Другим джерелом є нормативно-правові та контрактні вимоги, які діють на підставі закону та повинні задовольняти і підприємство, і партнерів.
- Третім джерелом є власний набір принципів, цілей та бізнес-вимог щодо оброблення інформації, який організація розробила для підтримки свого функціонування.

Створення системи забезпечення ІБ найкраще цілеспрямовано розглянути одночасно зі створенням або розгортанням інформаційно-телекомунікаційної системи (ІТКС).

При цьому визначають такі стадії:

а) передпроектна стадія, що включає передпроектне обстеження створеної ІТКС, аналітичне обґрунтування необхідності створення системи її захисту та технічного завдання;

б) стадія проектування (розробка проектів), що включає розробку засобів захисту у складі ІТКС;

в) стадія введення в експлуатацію системи ЗІБ, що включає її дослідну експлуатацію і приймально-здавальні випробування, а також атестацію на відповідність вимогам безпеки [2,4] (рис.2.12).

Рис. 2.12. Схема створення системи забезпечення ІБ

На першій, передпроектній стадії виконуються в основному організаційні заходи, а саме:

а) проводиться класифікація інформації з точки зору потреб безпеки;

б) визначаються (уточнюються) загрози безпеки інформації і модель ймовірного порушника стосовно конкретних умов функціонування об'єкта, проводиться оцінка ризиків;

в) визначається конфігурація і топологія ІТКС в цілому і їх окремих компонентів, фізичні, функціональні і технологічні зв'язки як всередині системи, так і поза нею;

г) визначаються технічні засоби і системи, передбачувані до використання в системі, що розробляється, умови їх розташування, загальносистемні і прикладні програмні засоби, наявні на ринку і пропоновані до розробки;

д) залучаються фахівці для проведення робіт по проектуванню і налагодженню системи;

е) визначаються режими обробки інформації на ІТКС в цілому, в розробленій системі і її окремих компонентах;

ж) проводиться категоріювання системи;

з) визначається ступінь участі персоналу в обробці (обговоренні, передачі, зберіганні) інформації, характер взаємодії працівників між собою і зі службою безпеки;

і) визначаються заходи щодо забезпечення конфіденційності інформації на етапі проектування системи.

У результаті проведення даних заходів можна не тільки виявити і проаналізувати можливі шляхи реалізації загроз ІБ, а й оцінити ймовірність і збиток від їх реалізації, а також провести силами фахівців оцінку матеріальних, трудових і фінансових витрат на розробку і впровадження засобів захисту, орієнтовні терміни їх розробки і впровадження.

Наступна стадія - проектування та розробка засобів захисту в складі ІТКС. На цьому етапі здійснюються такі заходи, як:

а) будівельно-монтажні роботи відповідно до проектної документації, затвердженої замовником, розміщенням і монтажем технічних засобів і систем;

б) розробка організаційно-технічних заходів щодо захисту інформації відповідно до вимог;

в) закупівля сертифікованих зразків, які серійно випускаються в захищеному виконанні технічних засобів обробки, передачі і зберігання інформації, або їх сертифікація;

г) закупівля сертифікованих технічних, програмних і програмно-технічних засобів захисту і їх встановлення;

д) забезпечення участі фахівців у роботі з проектування системи, при необхідності їх навчання;

е) розробка або закупівля та подальша сертифікація по вимогам безпеки інформації засобів захисту в разі, коли на ринку відсутні необхідні сертифіковані програмні засоби;

ж) організація охорони та фізичного захисту об'єкта;

з) розробка і реалізація дозвільної системи доступу користувачів і експлуатаційного персоналу до оброблюваної інформації;

і) визначення замовником підрозділів і осіб, відповідальних за експлуатацію засобів захисту, навчання призначених осіб специфіці робіт із захисту інформації на стадії експлуатації системи;

к) розробка експлуатаційної документації на засоби захисту, а також організаційно-розпорядчої документації з ІБ (наказів, інструкцій та інших документів);

л) виконання інсталяції прикладних програм в комплексі з програмних засобів захисту інформації;

м) виконання інших заходів, специфічних для конкретних об'єктів інформатизації та напрямків захисту інформації.

На даному етапі велике значення матиме розробка організаційно-розпорядчих документів, що дають необхідну правову базу, формується служба безпеки і підрозділи щодо захисту інформації для проведення всього спектру захисних заходів, взаємодії із зовнішніми організаціями, залучення до відповідальності порушників тощо. До числа таких документів можна віднести концепцію ІБ, керівництво по захисту інформації, посадові інструкції, положення про категоріювання ресурсів ІТКС, розділи в положеннях про відділи і підрозділи, що стосуються питань ІБ та ін.

На стадії введення в експлуатацію системи необхідно передбачити виконання наступних заходів:

а) експлуатацію засобів захисту в комплексі з іншими технічними і програмними засобами системи з метою перевірки їх працездатності в складі ІТКС і відпрацювання технологічного процесу обробки (передачі) інформації;

б) приймально-здавальні випробування системи ЗІБ;

в) підбір кадрів, розстановку, навчання та перепідготовку наявного персоналу;

г) атестацію системи за вимогами безпеки інформації.

На даному етапі дається загальна оцінка проведеним роботам, а також визначається необхідність проведення додаткових робіт по вдосконаленню системи в разі виявлення можливих неполадок і недоробок. Тільки після виконання усіх цих заходів проводиться атестація системи. Одночасно з цими роботами проводиться підбір, розподіл фахівців, уточнення посадових обов'язків. При необхідності здійснюється підвищення кваліфікації та навчання співробітників.

У процесі експлуатації ІТКС необхідно забезпечити надійність і ефективність функціонування системи ЗІБ. Тому, на даному етапі необхідно виконувати такі заходи:

а) аналіз ІТКС і технології обробки інформації з урахуванням зміни обстановки;

б) переробка та оновлення розробленої на попередніх етапах документації планування проведення заходів щодо захисту інформації відповідно до висновків з аналізу;

в) навчання і перепідготовка персоналу і користувачів ІТКС;

д) дотримання режиму обмеження і розмежування доступу до інформації, контроль виконання встановлених правил роботи в ІТКС;

г) оцінка ефективності функціонування і вдосконалення системи, оновлення та доопрацювання наявних програмних і апаратних засобів захисту, заміна їх на більш досконалі.

При виконанні даних заходів необхідно особливу увагу приділяти таким питанням, як перепідготовка та підвищення кваліфікації кадрів, вибір процесів і технологій, а також проведення постійного моніторингу обстановки в галузі ІБ.

Відповідно до концепції CISCO інформаційна безпека відноситься до процесів та інструментів, розроблених та розгорнутих для захисту конфіденційної ділової інформації від модифікації, порушень, знищення та неавторизованого доступу [3].

ІБ підприємства є сукупністю таких складових: безпека додатків, безпека даних, криптографія та шифрування даних.

Безпека додатків - це широка тема, яка охоплює вразливості програмного забезпечення у веб- та мобільних додатках та інтерфейсах прикладного програмування. Ці вразливості можуть бути виявлені під час аутентифікації або авторизації користувачів, перевірки цілісності коду та конфігурацій, а також у зрілих політиках та процедурах. Вразливі місця програм можуть створювати точки входу для значних порушень ІБ. Захист додатків є важливою частиною захисту периметра ІБ.

Безпека даних у хмарі фокусується на створенні та розміщенні захищених програм у хмарних середовищах та безпечному споживанні сторонніх хмарних додатків. “Хмарна” програма просто означає, що програма працює у спільному середовищі. Компанії повинні переконатися, що існує достатня ізоляція між різними процесами у спільних середовищах.

Шифрування даних під час передачі та у стані спокою допомагає забезпечити їх конфіденційність та цілісність. Цифрові підписи зазвичай використовуються в криптографії для перевірки достовірності даних. Криптографія та шифрування стають все більш важливими. Хорошим прикладом використання криптографії є Advanced Encryption Standard (AES). AES - це симетричний ключовий алгоритм, який використовується не тільки для захисту інформації в організації, а й для секретної державної інформації.

Найважливими задачами ІБ для підприємства розглядаються [3] :

- Захист інфраструктури.

- Реагування на інциденти.
- Управління вразливостями.

Захист інфраструктури займається захистом внутрішніх та зовнішних мереж, лабораторій, центрів обробки даних, серверів, робочих столів та мобільних пристроїв.

Реагування на інциденти - це функція, яка контролює та розслідує потенційно шкідливу поведінку. Готуючись до порушень, персонал ІТ повинен мати план реагування на аварії для знешкодження загрози та відновлення мережі. Крім того, відповідно до плану має бути створена система збереження доказів для судового аналізу та потенційного переслідування. Ці дані можуть допомогти запобігти подальшим порушенням та виявити зловмисника.

Управління вразливостями - це процес сканування середовища на наявність слабких місць (наприклад, невідпрацьоване програмне забезпечення) та визначення пріоритетів усунення на основі ризику. У багатьох мережах компанії постійно додають додатки, користувачів, інфраструктуру тощо. З цієї причини важливо постійно перевіряти мережу на наявність потенційних вразливостей. Знайшовши вразливість заздалегідь, підприємство може заощадити потенційні витрати внаслідок порушення ІБ бізнесу [30].

Питання ІБ виходять на перший план у разі, якщо порушення в роботі та помилки, що виникають в системах управління можуть привести до серйозних наслідків. І під завданнями системи забезпечення ІБ передбачають завжди багатопланові комплексні заходи. Наприклад, вони включають запобігання неправомірного використання, пошкодження, спотворення, копіювання і блокування інформації. Сюди відноситься відстеження та запобігання несанкціонованого доступу осіб без належного рівня авторизації, запобігання витоку інформації і всіх можливих загроз її цілісності та конфіденційності.

Таким чином, розглянута вище побудова СУІБ може бути представлена у вигляді моделі процесів ІБ (див. рис.2.13), що відповідає спеціальним нормативним документам щодо системного забезпечення ІБ [40].

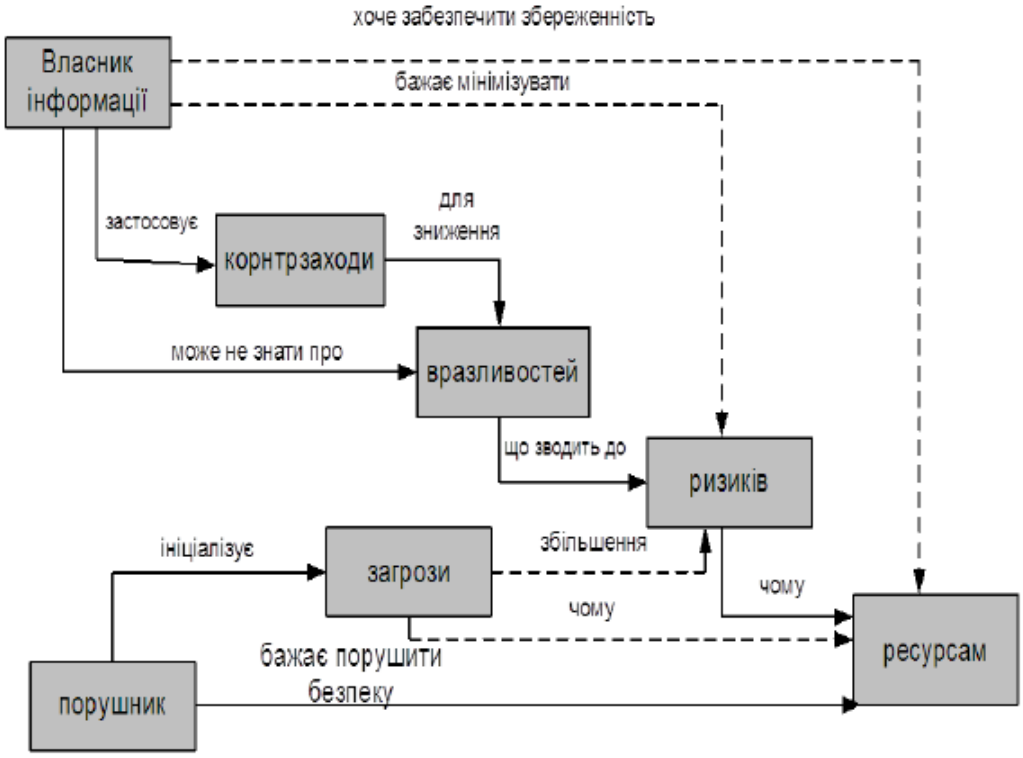

Рис.2.13.Схема СУІБ у вигляді моделі процесів інформаційної безпеки .

У схемі показані об'єктивні фактори:

- загрози ІБ. Вони характеризуються ймовірністю виникнення і реалізації;

- вразливості системи інформаційної безпеки, які впливають на ймовірність реалізації загрози;

- втрати, що відображають реальний збиток в результаті реалізації загрози ІБ.

- ризики, що відображають завдання шкоди організації в результаті реалізації загрози ІБ.

2.2. Аналіз організаційних напрямів підвищення ефективності процесів забезпечення інформаційної безпеки

На думку фахівців, організаційні заходи підвищення ефективності процесів забезпечення ІБ відіграють велику роль в створенні надійного механізму захисту інформації, так як можливості несанкціонованого використання конфіденційних відомостей в значній мірі обумовлені не

технічними аспектами, а зловмисними діями, недбальством, недбалістю і халатністю користувачів або персоналу захисту.

До таких організаційних заходів відносяться:

- заходи, здійснювані при проектуванні, будівництві та обладнанні службових і виробничих будівель і приміщень;
- заходи, здійснювані при підборі персоналу;
- організація та підтримка надійного пропускного режиму, охорони приміщень і території, контролю за відвідувачами;
- організація зберігання і використання документів та носіїв конфіденційної інформації;
- організація захисту інформації;
- організація регулярного навчання співробітників.

Одним з основних компонентів організаційного забезпечення ІБ організації є служба ІБ. Ця служба є органом управління системою захисту інформації.

До основних організаційних заходів підвищення ефективності процесів забезпечення ІБ також відносяться (див рис.2.14):

- організація режиму і охорони. Їх мета - виключення можливості таємного проникнення на територію і в приміщення сторонніх осіб;
- організація роботи зі співробітниками, яка передбачає підбір і розстановку персоналу, включаючи ознайомлення зі співробітниками, їх вивчення, навчання правилам роботи з конфіденційною інформацією, ознайомлення з заходами відповідальності за порушення правил захисту інформації та ін.;
- організація роботи з документами та документованою інформацією, включаючи організацію розробки і використання документів та носіїв конфіденційної інформації, їх облік, виконання, повернення, зберігання і знищення;
- організація використання технічних засобів збору, обробки, накопичення і зберігання конфіденційної інформації;

- організація роботи з аналізу внутрішніх і зовнішніх загроз конфіденційній інформації та вироблення заходів щодо забезпечення її захисту;
- організація роботи з проведення систематичного контролю за роботою персоналу з конфіденційною інформацією, порядком обліку, зберігання та знищення документів і технічних носіїв.

Рис.2.14. Схема організаційних заходів підвищення ефективності процесів забезпечення ІБ

У кожному конкретному випадку організаційні заходи носять специфічну для даної організації форму і зміст, спрямовані на забезпечення безпеки інформації в конкретних умовах. До організаційних заходів підвищення ефективності процесів забезпечення ІБ відносяться також формування політики безпеки організації; охорона об'єктів, які підлягають захисту; ретельний підбір спеціалістів на відповідні посади і покладання відповідальності на них; наявність плану відновлення працездатності об'єктів, вибір місця розташування об'єкта тощо.

Формування політики безпеки підприємства розглядаєтьтся як один з найбільш ефективних методів оптимізації рівня інформаційної безпеки, спрямованих на підвищення ефективності процесів забезпечення ІБ.

Політика безпеки – це набір законів, правил і практичних рекомендацій, на основі яких будується управління, захист і розподіл критичної інформації в системі. Вона повинна охоплювати всі особливості процесу обробки інформації, визначаючи поведінку системи в різних ситуаціях. Політика безпеки реалізується за допомогою організаційних заходів і програмно-технічних засобів, що визначають архітектуру системи захисту, а також за допомогою засобів управління механізмами захисту.

У загальному випадку можна виділити наступні процеси, пов'язані з розробкою і реалізацією політики безпеки.

1. Комплекс заходів, пов'язаних з проведенням аналізу ризиків. До цієї групи можна віднести:

- облік матеріальних або інформаційних цінностей;
- моделювання загроз інформації системи;
- власне аналіз ризиків з використанням того або іншого підходу — наприклад, вартісний аналіз ризиків.

2. Заходи щодо оцінки відповідності заходів по забезпеченню захисту інформації системи деякому еталонному зразку: стандарту, профілю захисту й т.п.

3. Дії, пов'язані з розробкою різного роду документів, зокрема звітів, діаграм, профілів захисту, заданих по безпеці.

4. Дії, пов'язані зі збором, зберіганням і обробкою статистики по подіях безпеки для організації;

Крім того, існує набір вимог, що підсилюють дію цих політик і призначений для управління інформаційними потоками в системі.

Основу повноважної політики безпеки становить управління доступом, яке має на увазі, що:

- всі суб'єкти і об'єкти системи повинні бути однозначно ідентифіковані;
- кожному об'єкту системи присвоєно точну критичність, що визначає цінність інформації, що міститься в ньому;

- кожному суб'єктові системи привласнений рівень прозорості, що визначає максимальне значення мітки критичності об'єктів, до яких суб'єкт має доступ.

Конкретна програма політики ІБ підприємства повинна формуватися відповідно до норм чинного законодавства.

Політика безпеки підприємства включає:

- Базову політику безпеки.
- Спеціалізовані політики безпеки.
- Процедуру безпеки.

Схема політики безпеки на підприємстві представлена на рис.2.15.

Рис.2.15. Схема політики безпеки на підприємстві

Під базовою політикою безпеки розуміється, як підприємство обробляє інформацію, хто може одержати до неї доступ і який спосіб. Підхід, реалізований базовою політикою безпеки, дає можливість поступово і послідовно виконувати роботу зі створення системи безпеки, не намагаючись відразу виконати її цілком. Базова політика є основною для організації або підприємства.

З урахуванням особливостей застосування, спеціалізовані політики безпеки можна розділити на дві групи:

- політики, що зачіпають значне число користувачів;
- політики, пов'язані з конкретними технічними галузями.

До спеціалізованих політик, які торкаються значного числа користувачів, належать:

- політика припустимого використання;
- політика віддаленого доступу до ресурсів мережі;
- політика захисту інформації;
- політика захисту паролів та ін.

Для будь-якого підприємства процедури безпеки є необхідним і важливим доповненням до політик безпеки. Оскільки політики безпеки тільки описують, що повинне бути захищене і які основні правила захисту, то процедури безпеки визначають, як захистити ресурси і які механізми виконання політики, іншими словами - як реалізувати політику безпеки.

Політику безпеки на підприємстві можна також розділити на три рівні:

- Верхній.
- Середній.
- Нижній.

Верхній рівень політики безпеки визначає рішення, які торкаються підприємства в цілому. Ці рішення носять досить загальний характер і виходять, в основному, від керівництва підприємства. Політика безпеки верхнього рівня формулює цілі підприємства в галузі ІБ в термінах цілісності, доступності і конфіденційності інформації.

Середній рівень політики безпеки визначає рішення питань, які не є основними і стосуються окремих аспектів ІБ, але важливих для різних систем, які експлуатуються організацією.

Нижній рівень політики безпеки відноситься до конкретних сервісів. Ця політика містить у собі два аспекти: цілі і правила їх досягнення. На відміну від двох верхніх рівнів, розглянута політика повинна бути більш детальною.

При формулюванні цілей політики безпеки нижнього рівня можна виходити з міркувань цілісності, доступності і конфіденційності, але вона не повинна ними обмежуватися. У загальному випадку цілі повинні зв'язувати між собою об'єкти сервісу і осмислені дії з ними.

Політика відносно СУІБ у стандарті ISO/IEC 27001 розглядається як розширена версія політики у сфері захисту інформації, тобто як документ внутрішнього користування вона розробляється більше як звід правил, ніж заява стосовно намірів.

Наприклад, наведена у мережі Інтернет Типова політика інформаційної безпеки компанії, що має вихід в Інтернет і володіє ресурсами, до яких необхідний доступ з Інтернет, містить розділи, що стосуються: мережевої безпеки (головний файервол, світч, електронна пошта, система виявлення атак, протоколювання і регулярний моніторинг доступу); локальної безпеки (антивірусний контроль, захист від несанкціонованого доступу,

криптографічний захист даних, захист персональних даних файерволом, резервування даних, протоколювання доступу); фізичної безпеки.

Окремі фрагменти Типової політики… мають вигляд:

- «Резервування даних». Обов'язковим є резервування користувачами важливих даних на персональних комп'ютерах на внутрішньому сервері даних компанії. Обов'язкова наявність бекап-диску для сервера даних. Бекап виконується або щотижня, або після серйозних змін у системі. Необхідно зберігати три цикли генерації бекапа.
- «Протоколювання доступу».При локальному доступі користувача до робочої станції ведеться лог-файл його відвідин (записуються усі вдалі та невдалі спроби входу до системи). При локальному доступі адміністратора до серверів ведеться лог-файл його відвідин (записуються всі вдалі і невдалі спроби входу до системи).

Для зовнішнього користування можна включити до загальної корпоративної політики заяву про політику, що належить до СУІБ, наприклад: «Заява про політику щодо СУІБ».

Виходячи з європейського досвіду, політика ІБ вимагає, щоб у всіх державах-членах та асоційованих країнах застосовувалися загальноприйняті визначення, основні положення та вміння орієнтуватися в сучасних умовах. Впровадження політики інформаційної безпеки розглядається як невід'ємна частина їх загальної структури корпоративного управління, управління ризиками та забезпечення відповідності для боротьби з ризиками та загрозами кіберзлочинності на належному рівні.

Підприємства повинні працювати над інтегруванням політики інформаційної безпеки як міжфункціональної дисципліни в:

- інформаційну безпеку;
- традиційну корпоративну безпеку, включаючи фізичну;
- управління корпоративними ризиками;
- управління безперервністю ІТ-послуг (ITSCM) та управління безперервністю бізнесу (BCM);
- стійкість організації;
- затвердження достовірності інформації.

На практиці, для розробки політики ІБ необхідні дані про вплив на підприємство успішних кібератак (або їх спроб). Підприємства також можуть

використовувати багато відкритих джерел інформації для формування достатньо обґрунтованої картини, включаючи:

- оцінку вартості витоку інформації (щорічну);
- комерційні дослідження порушень ІБ (щорічні або менш часті);
- комерційні дослідження стану ІБ (як правило, щорічні);
- дослідження команди реагування (CERT) на комп'ютерні надзвичайні ситуації.

Таким чином, емпіричні дані є вагомим підґрунтям сценарію ІБ як необхідного для захисту безпеки і тим самим - підвищити ефективність процесів забезпечення ІБ . Політика ІБ, затверджена в організації, повинна охоплювати робочі матеріали та результати попередніх фаз життєвого циклу безпеки підприємства, а також увесь національний і європейський внесок, доступний у відкритих джерелах (результати аналізу впливу на бізнес та оцінюванням ризиків, аналізу загроз і вразливостей, звітування про інциденти, навчаннь з ІБ).

На думку фахівців міжнародної компанії IBM, розробка корпоративних керівних документів в напрямку підвищення ефективності процесів забезпечення ІБ повинна починатися зі створення політики інформаційної безпеки. Компанія IBM виділяє наступні основні етапи розробки політики безпеки:

- визначення інформаційних ризиків компанії, здатних завдати максимальної шкоди, для розробки надалі процедур і заходів по попередженню їх виникнення;
- розробка політики безпеки, що описує заходи захисту інформаційних активів, адекватні цілям і завданням бізнесу;
- прийняття планів дій у надзвичайних ситуаціях для зменшення збитку у випадках, коли обрані заходи захисту не змогли запобігти інцидентам в галузі безпеки;
- оцінка залишкових інформаційних ризиків і ухвалення рішення про додаткові інвестиції в засоби і заходи безпеки. Рішення приймає керівництво на основі аналізу залишкових ризиків.

2.3. Аналіз технічних напрямів підвищення ефективності процесів забезпечення інформаційної безпеки

До технічних заходів**,** які впливають на підвищення ефективності процесів забезпечення ІБ можна віднести:

- захист від несанкціонованого доступу до комп'ютерних систем шляхом використання спеціальних паролів, шифрування файлів, резервування особливо важливих її підсистем,
- організацію обчислювальних мереж з можливістю перерозподілу ресурсів у разі порушення працездатності окремих елементів,
- контроль електромагнітного й акустичного стану простору, виявлення й пригнічення технічних каналів витоку інформації,
- монтаж обладнання виявлення й гасіння пожежі, обладнання виявлення води, застосування конструктивних заходів захисту від розкрадань, саботажу або диверсій,
- установку резервних систем електроживлення,
- оснащення приміщень замками, установку сигналізацій тощо [12].

Ядром інженерно-технічного напряму є програмно-апаратні засоби захисту інформації. До апаратних засобів відносяться механічні, електромеханічні, електронні, оптичні, лазерні, радіо - і радіотехнічні, радіолокаційні та інші пристрої, системи та споруди, призначені для забезпечення безпеки і захисту інформації.

Під програмним забезпеченням безпеки інформації розуміється сукупність спеціальних програм, що реалізують функції захисту інформації та режиму функціонування.

На сьогоднішній день існує великий арсенал засобів забезпечення ІБ:

- засоби антивірусного захисту;
- засоби шифрування інформації, що зберігається на комп'ютерах і переданої мережами;
- інструменти перевірки цілісності вмісту дисків;
- віртуальні приватні мережі;
- міжмережеві екрани;
- віртуальні приватні мережі;

- засоби контентної фільтрації;
- засоби аутентифікації користувачів;
- системи виявлення вразливостей мереж і аналізатори мережевих атак.

Кожний з перерахованих засобів може використовуватись як самостійно, так і в інтеграції з іншими. Це робить можливим створення систем інформаційного захисту для систем будь-якої складності та конфігурації, незалежно від використовуваних платформ.

Ідентифікація та авторизація – це ключові елементи ІБ. При спробі доступу до інформаційних активів функція ідентифікації дає відповідь на питання: чи ви є авторизованим користувачем мережі. Функція авторизації відповідає за те, до яких ресурсів конкретний користувач має доступ. Функція адміністрування полягає у наділенні користувача певними ідентифікаційними особливостями в рамках даної мережі і визначенні обсягу допустимих для нього дій.

Системи шифрування дозволяють мінімізувати втрати у випадку несанкціонованого доступу до даних, що зберігаються на жорсткому диску або іншому носії, а також перехоплення інформації при її пересиланні по електронній пошті або передачу з мережних протоколах. Завдання даного засобу захисту ─ забезпечення конфіденційності. Основні вимоги, що пред'являються до систем шифрування - високий рівень криптостійкості та легальність використання на території держави.

Міжмережевий екран являє собою систему або комбінацію систем, що утворить між двома чи більш мережами захисний бар'єр, що оберігає від несанкціонованого потрапляння в мережу або виходу з неї пакетів даних.

Основний принцип дії міжмережевих екранів ─ перевірка кожного пакету даних на відповідність вхідної та вихідної IP адреси базі дозволених адрес. Таким чином, міжмережеві екрани значно розширюють можливості сегментації інформаційних мереж та контролю за циркулюванням даних.

Говорячи про криптографію і міжмережеві екрани, слід згадати про захищені віртуальні приватні мережі. Їх використання дозволяє вирішити проблеми конфіденційності і цілісності даних при їх передачі по відкритим комунікаційних каналам.

Використання віртуальних приватних мереж можна звести до вирішення трьох основних завдань:

- захист інформаційних потоків між різними офісами компанії (шифрування інформації проводиться тільки на виході у зовнішню мережу);
- захищений доступ віддалених користувачів мережі до інформаційних ресурсів компанії, як правило, здійснюваний через Internet;
- захист інформаційних потоків між окремими додатками всередині корпоративних мереж (цей аспект також дуже важливий, оскільки більшість атак здійснюється з внутрішніх мереж) [11].

Ефективний засіб захисту від втрати конфіденційної інформації - фільтрація вмісту вхідної і вихідної електронної пошти. Перевірка поштових повідомлень на основі правил, встановлених в організації, дозволяє також забезпечити безпеку компанії від відповідальності за судовими позовами і захистити їх співробітників від спаму.

Засоби контентної фільтрації дозволяють перевіряти файли всіх розповсюджених форматів, у тому числі стислі і графічні. При цьому пропускна здатність мережі практично не змінюється.

Всі зміни на робочій станції або на сервері можуть бути відслідковані адміністратором мережі або іншим авторизованим користувачем завдяки технології перевірки цілісності вмісту жорсткого диску (integrity checking). Це дозволяє виявляти будь-які дії з файлами та ідентифікувати активність вірусів, несанкціонований доступ або крадіжку даних авторизованими користувачами. Контроль здійснюється на основі аналізу контрольних сум файлів (CRC сум).

Сучасні антивірусні технології дозволяють виявити практично всі вже відомі вірусні програми через порівняння коду підозрілого файлу із зразками, що зберігаються в антивірусні базі. Крім того, розроблені технології моделювання поведінки, що дозволяють виявляти новостворювані вірусні програми. Виявлені об'єкти можуть піддаватися лікуванню, ізолюватися (міститися в карантин) або видалятися. Захист від вірусів може бути встановлено на робочі станції, файлові і поштові сервера, міжмережеві екрани, що працюють під практично будь-якою з поширених операційних систем (Windows, Unix- і Linux-системи, Novell) на процесорах різних типів.

Фільтри спаму значно зменшують невиробничі затрати праці, пов'язані з розглядом спаму, знижують трафік і завантаження серверів, покращують психологічний фон в колективі і зменшують ризик залучення співробітників компанії в шахрайські операції. Крім того, фільтри спаму зменшують ризик

зараження новими вірусами, оскільки повідомлення, що містять віруси (навіть ще не включені до бази антивірусних програм) часто мають ознаки спаму і фільтруються.

Для протидії природним загрозам ІБ в компанії має бути розроблений і реалізований набір процедур щодо запобігання надзвичайних ситуацій (наприклад, щодо забезпечення фізичного захисту даних від пожежі) та мінімізації збитків у тому випадку, якщо така ситуація все-таки виникне. Один з основних методів захисту від втрати даних - резервне копіювання з чітким дотриманням встановлених процедур (регулярність, типи носіїв, методи зберігання копій і т.д) [12].

Висновки до другого розділу

Відмічено, що організація захисту від небезпек і загроз функціонуванню інформаційної системи підприємства відбувається шляхом побудови ефективної системи інформаційної безпеки . Показана роль політики інформаційної безпеки, яка повинна визначати системи захисту інформації і управління інформаційною безпекою як обєднану систему забезпечення ІБ у вигляді сукупності правових норм, організаційних (правових) заходів, комплексу програмно-технічних засобів і процедурних рішень, спрямованих на протидію загрозам безпеці інформації. Приведена від фахівців класифікація основних видів загроз безпеці інформаційних систем. Показані суттєві загрози, шляхи їх реалізації і протидії, застосування технічних засобів безпеки і заходів їх ліквідації. Конкретизовано визначення системи забезпечення інформаційної безпеки підприємства як комплекс реалізації організаційних, технічних, програмних і криптографічних засобів і заходів захисту інформації. Обґрунтована пропозиція щодо доцільності застосування варіантів побудови системи інформаційної безпеки - по досягненню необхідного рівня безпеки, захищеності інформації, обмежень на технології і затрат.

Ілюстрована структура процесів СУІБ, що найчастіше використовується вна практиці. Показано функціональні напрями діяльності і основні процеси впровадження СУІБ, їх взаємодії і вплив менеджмента підприємства на функціонування СУІБ. Розкрито комплекс робіт з побудови СУІБ. Але ще існують проблеми з відношенням до створення СУІБ на підприємствах. Виділені чотири напрями і завдання сучасних рольових функцій служби інформаційної

безпеки підприємства. Розкрито завдання системи інформаційної безпеки, вимоги до комплексної системи захисту інформації і показники для оцінки цих вимог.

Показано підход до вибору метода аналізу стану забезпечення інформаційної безпеки, який залежить від конкретного рівня і сфери організації захисту. Методи можуть значно змінюватися і варіюватися в залежності від типу діяльності, в якій вони використовуються, а також сфери застосування, тому виділяють декілька типів методів забезпечення: однорівневі,
багаторівневі, комплексні і інтегровані. Приведені стадії управління загрозами для активного використання цих методів забезпечення. Завдання забезпечення інформаційної безпеки підприємства повинно вирішуватися системно, це означає, що різні засоби повинні застосовуватися одночасно і під централізованим управлінням. Процес забезпечення інформаційної безпеки підприємства можна представити як взаємодію трьох підсистем: підсистема інформаційного забезпечення процесу управління на підприємстві; підсистема захисту інформаційного середовища підприємства і підсистема діагностики рівня інформаційної безпеки. Для забезпечення захисту інформаційного середовища підприємства необхідне систематичне виконання наступних функцій СУІБ: аналіз загроз, планування та розробка заходів щодо забезпечення безпеки і оперативна реалізація запланованих дій. Діагностику рівня ІБ підприємства необхідно проводити за трьома ключовими напрямками: оцінка програмно-технічної захищеності інформації; оцінка інформаційної надійності персоналу; оцінка інформації, що надається інформаційною службою. Показано роль метода експертних оцінок, методами аналізу стану, методи дослідження причинних зв'язків і інших в оцінці рівня інформаційної безпеки підприємства.

Показано підхід до створення системи забезпечення інформаційної безпеки: її зміст, досягнення цілі досягнення – в їх основі лежить підтримання цілісності, конфіденційності та доступності інформації. Розкриті джерела формування вимог до безпеки підприємства і підхід до створення системи забезпечення на прикладі інформаційно-телекомунікаційної системи – на стадіях предпректування, проектування і введення в експлуатацію. Найважливими задачами інформаційної безпеки для підприємства розглядаються: захист інфраструктури, еагування на інциденти і управління вразливостями. Представлена схема СУІБ у вигляді моделі процесів ІБ, що відповідає

спеціальним нормативним документам щодо системного забезпечення інформаційної безпеки для підприємства.

Окремо проаналізовано організаційні напрями підвищення ефективності процесів забезпечення інформаційної безпеки. Одним з основних компонентів організаційного забезпечення є служба інформаційної безпеки, яка є органом управління системою захисту інформації.Детально розглянуто формування політики безпеки підприємства, як один з найбільш ефективних методів оптимізації рівня інформаційної безпеки, її зміст, структура і процеси, пов'язані з розробкою та реалізацією основних спеціалізованих політик.

Ядром інженерно-технічного напряму підвищення ефективності процесів забезпечення інформаційної безпеки визначено програмно-апаратні засоби захисту інформації. Розкриті технічних заходи **,** які впливають на підвищення ефективності процесів забезпечення, і сукупність спеціальних програм, що реалізують функції захисту інформації та режиму функціонування

Розділ 3. ДОСЛІДЖЕННЯ І РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ДЛЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Під інформаційною безпекою промислового підприємства розуміються всі елементи системи управління підприємством, пов’язані з визначенням,

досягненням конфіденційності, цілісності, доступності, неспростовності, підзвітності, автентичності та достовірності інформації або засобів її обробки.

Для ефективного виконання такого завдання необхідна система відповідного забезпечення. Основними елементами такої системи повинні бути принципи побудови системи ІБ, цільові характеристики системи, її завдання, основні загрози та заходи щодо нейтралізації загроз.

Побудована за наведеними принципами система ІБ має бути налаштована на досягнення визначених цілей, специфіка яких буде великою мірою визначати як структуру системи так і основні параметри її функціонування.

Тому для проведення дослідження і розробки рекомендацій щодо підвищення ефективності для забезпечення ІБ необхідно уяснити кожну характеристику самої інформації, яка визначає її безпеку. Докладно до інформації для промислового підприємства з основними цілями досягнення високого рівня ІБ є забезпечення конфіденційності, цілісності, доступності, достовірності та неспростовності інформації.

Конфіденційність - це стан доступності інформації тільки авторизованим користувачам, процесів і пристроїв. Необхідно підкреслити, що конфіденційність є однією з основних цільових характеристик інформації, а її забезпечення – найголовнішою функцією системи інформаційної безпеки. Категорія конфіденційності є особливо важливою для промислових підприємств на етапі проведення науково-дослідницьких робіт та впровадження інновацій. Основними методами забезпечення конфіденційності інформації є закриття, шифрування, приховування та подрібнення.

Цілісність - це відсутність неправомочних спотворень, доповнень або знищення інформації [31]. Гарантія цілісності особливо важлива в тих випадках, коли інформація представляє велику цінність і не повинна бути втрачена, а також коли дані можуть бути навмисно змінені з метою дезінформації одержувача. Як правило, від стирання інформацію захищають методами, що забезпечують конфіденційність, і резервним копіюванням, а відсутність спотворень перевіряють з допомогою хешування.

Доступність - це забезпечення своєчасного і надійного доступу до інформації і інформаційних сервісів [31]. Типовими випадками порушення доступності є збій в роботі програмних/апаратних засобів і розподілена атака типу «відмова в обслуговуванні» (DDoS). Від збоїв інформаційну систему

захищають усуненням причин збоїв, а від DDoS-атак - відсіканням паразитного трафіку.

Справжність або автентичність - можливість однозначно ідентифікувати автора/джерело інформації [31]. Автентичність електронних даних часто засвідчується таким засобом, як електронно-цифровий підпис.

Неспростовність - неможливість зречення від авторства інформації, а також факту її відправки або отримання [31]. Неспростовність можна гарантувати електронно-цифровим підписом та іншими криптографічними засобами і протоколами. Неспростовність актуальна, наприклад, у системах електронних торгів, де вона забезпечує відповідальність друг перед іншому продавців і покупців.

По всіма цим питанням проведено дослідження на прикладі віртуального підприємства.

3.1 Аналіз результатів досліджень функціонування системи забезпечення інформаційної безпеки

На прикладі віртуального підприємства - ТОВ «Феракс» система ІБ може бути спрямована на забезпечення специфічних властивостей інформації, наприклад підзвітність, адекватність та інші.

Для досягнення названих цілей система ІБ повинна бути спроможною виконувати наступні завдання:

- забезпечення захищеного зберігання інформації на різних носіях;
- захист даних, що передаються по каналах зв'язку;
- розмежування доступу до різних видів документів;
- створення резервних копій, післяаварійне відновлення інформаційних систем.

Забезпечення ІБ підприємства ТОВ «Феракс» можливо тільки при системному і комплексному підході до захисту інформації. В системі ІБ повинні враховуватися всі актуальні комп'ютерні загрози та вразливості (рис 3.1).

Загрози ІБ на підприємстві ТОВ «Феракс» - це можливі дії або події, які можуть вести до різних порушень процесів . Вони також є кінцевими цілями (або результатами) діяльності порушників. Види загроз ІБ можуть бути дуже різноманітні і мати безліч класифікацій. В якості приклада

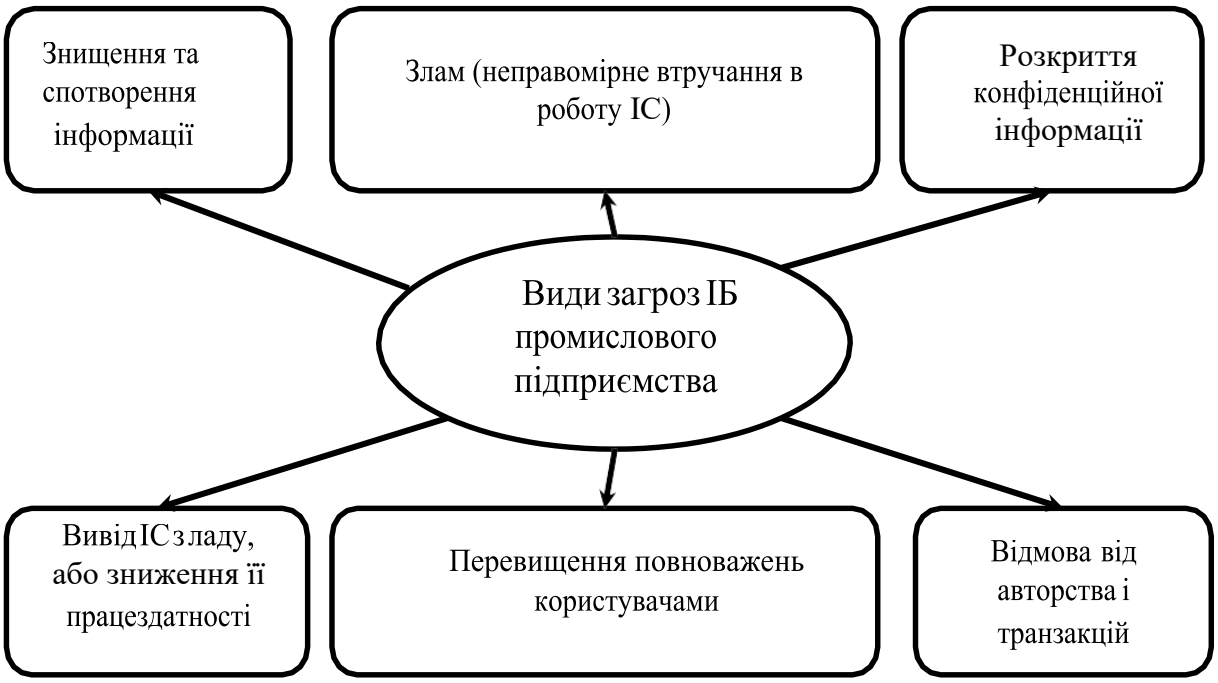

Рис. 3.1 Загрози інформаційній безпеці підприємства ТОВ «Феракс»

Повноцінна ІБ підприємства ТОВ «Феракс» передбачає безперервний контроль в реальному часі всіх важливих подій і станів, що впливають на безпеку даних. Захист має здійснюватися цілодобово і цілорічно і охоплювати весь життєвий цикл інформації - від її надходження або створення до знищення або втрати актуальності.

На рівні підприємства ТОВ «Феракс» за ІБ відповідають відділи інформаційних технологій, економічної безпеки, кадрів та інші служби.

Необхідно також відзначити, що рівень загроз і, відповідно рівень ІБ підприємства підприємства ТОВ «Феракс», постійно змінюються під дією різних факторів. Найбільш впливовими з них є наступні:

- розширення співпраці підприємства з партнерами;
- автоматизація бізнес-процесів на підприємстві;
- розширення кооперації виконавців при побудові і розвитку інформаційної інфраструктури підприємства;
- зростання обсягів інформації підприємства, яка передається по відкритих каналах зв'язку;
- ріст комп'ютерних злочинів.

Для досягнення задовільного рівня ІБ на підприємстві ТОВ «Феракс» необхідно застосування комплексу організаційних і технічних заходів, спрямованих на захист корпоративних даних. Організаційні заходи включають документовані процедури і правила роботи з різними видами інформації, ІТ-сервісами, засобами захисту і т. д. Технічні заходи полягають у використанні апаратних і програмних засобів контролю доступу, моніторингу витоків, антивірусного захисту, міжмережевого екранування, захисту від електромагнітних випромінювань і ін.

При виборі програмно-технічних рішень із забезпечення ІБ підприємства ТОВ «Феракс», перевага віддається рішеням, які забезпечують дотримання основних принципів ІБ, а також відповідаючих наступним критеріям:

- підтримка міжнародних, національних, промислових та Інтернет стандартів (перевага віддається міжнародним стандартам);
- підтримка найбільшою мірою інтеграції з корпоративними програмно-апаратними платформами і використовуваними СЗІ;
- уніфікація розробників і постачальників використовуються продуктів;
- уніфікація засобів і інтерфейсів управління підсистемами ІБ.

Таким чином, за результатами проведених досліджень, можна сформувати методичний підхід до побудови системи інформаційної безпеки підприємства ТОВ «Феракс» (рис. 3.2).

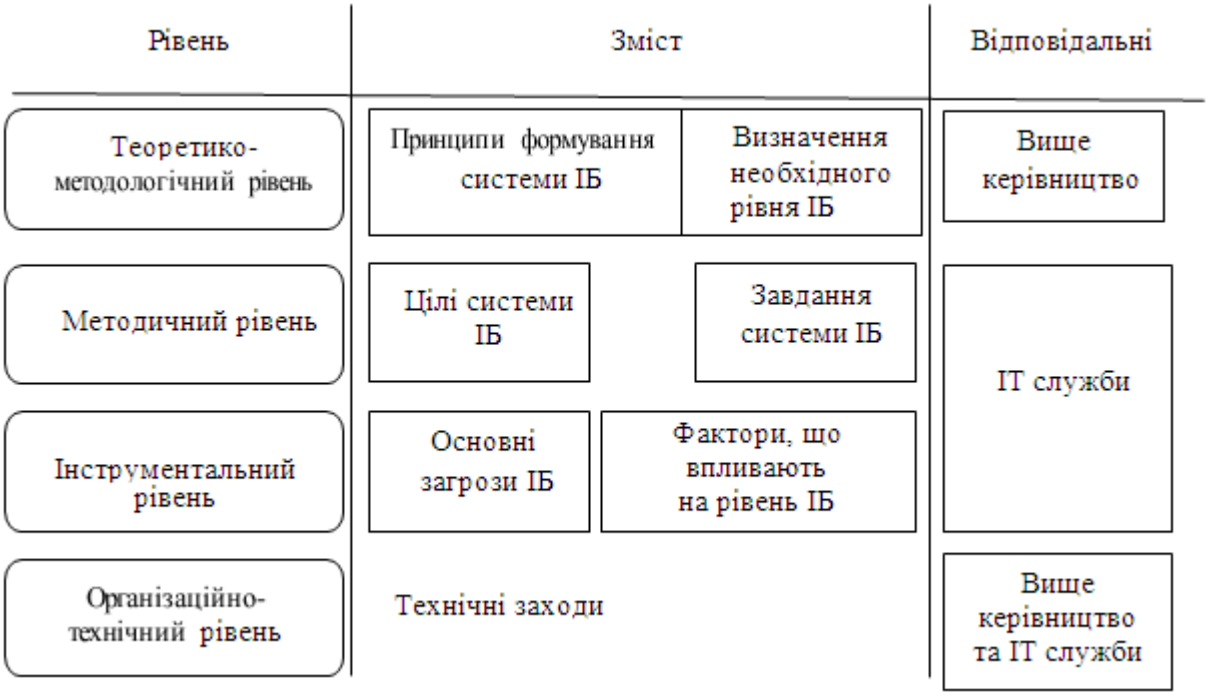

Рис. 3.2. Методичний підхід до формування системи ІБ підприємства ТОВ «Феракс»

Із наведеного рис. 3.3 видно, що основні елементи методичного підходу до формування системи управління ІБ розділені на чотири рівні, кожному з яких відповідає визначений рівень управління підприємством.

Так, принципи формування системи ІБ, що віднесені до теоретико-методологічного рівня запропонованого підходу, є тим елементом системи, за формування якого відповідає вище керівництво підприємства.

Також на цьому рівні мають бути сформовані основні вимоги до необхідного підприємству рівня ІБ. Далі ІТ служби відповідають за виконання заходів, віднесених до методичного та інструментального рівня, тобто вони повинні сформулювати основні цілі та завдання системи ІБ, а також визначити основні загрози ІБ та фактори, що впливають на її рівень. Після цього, ІТ служби мають розробити план технічних ат організаційних заходів, спрямованих на досягнення визначеного рівня ІБ. Після цього план погоджується вищим керівництвом підприємства і розпочинаються роботи по його практичному впровадженню. Особливо слід відзначити необхідність обов’язкової участі вищого керівництва підприємства у реалізації заходів організаційно-технічного рівня.

На цьому етапі керівництво підприємства повинно зрозуміти, що просте впровадження «додаткових заходів» без зміни всієї системи управління не забезпечить необхідного рівня ІБ.

Важливою умовою ефективного функціонування системи ІБ є її повна інтеграція в оперативну діяльність компанії. Її впровадження неодмінно буде вимагати коригування, а іноді і докорінної зміни більшості бізнес процесів. Можлива поява принципово нових бізнес-процесів, пов’язаних із забезпеченням функціонування системи ІБ. Це вимагає внесення змін в описі бізнес-процесів, регламентацію всіх нововведень та визначення нових меж відповідальності виконавців. Також необхідно ввести в практику постійні навчання та тренування з питань ІБ.

3.2 Дослідження і розробка рекомендацій в напрямах підвищення ефективності забезпечення інформаційної безпеки

Сучасний стан ІБ відрізняється її нестабільністю. Це означає, що підприємство повинно застосовувати щоденні методи захисту, які відповідали б його специфіці.

Для вдосконалення організації системи ІБ підприємства ТОВ «Феракс», потрібно провести необхідні заходи. Для її формування необхідно розробити і затвердити політику ІБ. Слід зазначити, що політика повинна узгоджуватися з існуючими законами і правилами, які стосуються умов діяльності підприємства, тобто ці закони і правила необхідно виявляти і брати до уваги при розробці політики. Чим надійніше система, тим суворіше і різноманітніше повинна бути політика безпеки. Залежно від сформульованої політики можна вибирати конкретні механізми, що забезпечують безпеку системи в цілому.

Щоб поліпшити організацію системи ІБ підприємства ТОВ «Феракс», можна запропонувати наступні заходи:

- організація робіт з навчання персоналу навичкам роботи з новими програмними продуктами за участю кваліфікованих фахівців;

- розробка необхідних заходів спрямованих на вдосконалення системи економічної, соціальної та інформаційної безпеки підприємства;

- провести інструктаж для того, щоб кожен співробітник усвідомив всю важливість і конфіденційність ввіреної йому інформації, тому що, як правило, причиною розголошення конфіденційної інформації є недостатнє знання працівниками правил захисту комерційних секретів і нерозуміння (або нерозуміння) необхідності їх ретельного дотримання;

- строгий контроль дотримання співробітниками правил роботи з конфіденційною інформацією;

- контроль за дотриманням правил зберігання робочої документації співробітників підприємства;

- планове проведення зборів, семінарів, обговорень з питань інформаційної безпеки підприємства;

- регулярна (планова) перевірка і обслуговування всіх інформаційних систем та інформаційної інфраструктури на працездатність.

Програмно-технічні засоби є одними з найважливіших компонентів в реалізації інформаційної захисту підприємства, тому для підвищення рівня

захисту інформації підприємства ТОВ «Феракс» необхідно ввести і застосувати наступні заходи:

- введення паролів користувачів;

- розмежування доступу до файлів, каталогів, дисків. Розмежування доступу до файлів і каталогів буде здійснюватися системним адміністратором, який дозволить доступ до відповідних дисків, папок і файлів для кожного користувача конкретно;

- регулярне сканування робочих станцій і оновлення баз антивірусної програми. Дозволить виявляти і нейтралізувати шкідливі програми, ліквідувати причини заражень. Необхідно виконати роботи з установки, настройки і забезпечення функціонування засобів і систем антивірусного захисту.

- установка на комп'ютер-сервер мережевого екрану, який блокує атаки з мережі Інтернет;

- застосування джерел безперебійного живлення. Найбільш надійним засобом запобігання втрат інформації при короткочасному відключенні електроенергії в даний час є установка джерел безперебійного живлення (UPS).

Різні за своїми технічними і споживчими характеристиками, подібні пристрої можуть забезпечити харчування всієї локальної мережі або окремого комп'ютера протягом якогось проміжку часу, достатнього для відновлення подачі напруги або для збереження інформації на магнітні носії.

В іншому випадку використовується наступна функція подібних пристроїв:

- комп'ютер отримує сигнал, що UPS перейшов на роботу від власних акумуляторів і час такої автономної роботи обмежена. Тоді комп'ютер виконує дії щодо коректного завершення всі програми, і відключається (команда SHUTDOWN). Більшість джерел безперебійного живлення одночасно виконує функції і стабілізатора напруги, є додатковим захистом від стрибків напруги в мережі. Багато сучасні мережеві пристрої - сервери, концентратори, мости і ін. оснащені власними дубльованими системами електроживлення;

- криптографічний захист інформації надається з метою забезпечення режиму конфіденційності та цілісності інформації при її передачі по каналах передачі даних;

- протоколювання і аудит є невід'ємною частиною забезпечення ІБ. Ці поняття мають на увазі збір, накопичення і аналіз подій, що відбуваються в інформаційній системі в реальному часі.

Реалізація протоколювання і аудиту вирішує наступні завдання:

- забезпечення підзвітності користувачів і адміністраторів;
- забезпечення можливості реконструкції послідовності подій;
- виявлення спроб порушень ІБ;
- надання інформації для виявлення і аналізу проблем.

При протоколюванні події рекомендується записувати, по крайній мірі, наступну інформацію:

- дата і час події;
- унікальний ідентифікатор користувача - ініціатора дії;
- тип події;
- результат дії (успіх або невдача);
- джерело запиту (наприклад, ім'я терміналу);
- імена порушених об'єктів (наприклад, що відкриваються або файлів, що видаляються);
- опис змін, внесених до баз даних захисту (наприклад, нова мітка безпеки об'єкта).

Проблема ІБ має дуже загострений характер, оскільки разом з величезною кількістю методів захисту інформації, збільшується та урізноманітнюється кількість потенційних загроз і дестабілізуючих факторів.

Таким чином, керівництво підприємства ТОВ «Феракс» повинно прогнозувати можливі чинники зниження захищеності інформації та оснащувати себе системами захисту від них.

На сьогодні, питання безпеки інформації потрібно розглядати не просто як розробку приватних механізмів захисту, а як реалізацію системного підходу, що включає комплекс взаємопов'язаних заходів, які повинні розширюватись та вдосконалюватись. Тому впровадження регламентів ІБ при використанні телекомунікацій, дотримання персоналом внутрішніх нормативних актів, а також досягнення конфіденційності, цілісності та доступності інформації дозволять не тільки підвищити результативність системи ІБ, але і будуть сприяти зміцненню зовнішніх позицій підприємства.

Висновки до третього розділу

Запропоновано використання приклада віртуального підприємства.для проведення дослідження і розробки рекомендацій щодо підвищення ефективності для забезпечення інформаційної безпеки.

Для досягнення задовільного рівня ІБ на підприємстві ТОВ «Феракс» необхідно застосування комплексу організаційних і технічних заходів, спрямованих на захист корпоративних даних. Організаційні заходи включають документовані процедури і правила роботи з різними видами інформації, IT-сервісами, засобами захисту і т. д. Технічні заходи полягають у використанні апаратних і програмних засобів контролю доступу, моніторингу витоків, антивірусного захисту, міжмережевого екранування, захисту від електромагнітних випромінювань і ін. При виборі програмно-технічних рішень із забезпечення інформаційної безпеки підприємства ТОВ «Феракс», перевага віддається рішеням, які забезпечують дотримання основних принципів управління безпекою.За результатами проведених досліджень, можна сформувати методичний підхід до побудови системи інформаційної безпеки підприємства ТОВ «Феракс» з чотирьмя рівнями управління підприємством: теоретико-методологічний, методичний, інструментальний і організаційно-технічний. За теоретико-методологічний рівень запропонованого підходу в формуванні системи управління підприємством, як підтерджує практика, напряму відповідає вище керівництво підприємства, тому що на цьому рівні мають бути сформовані основні вимоги до необхідного підприємству рівня інформаційної безпеки, після чого повинно бути розроблено план технічних і організаційних заходів, спрямованих на досягнення визначеного рівня безпеки Відмічено про необхідність обов’язкову участі вищого керівництва підприємства у реалізації запланованих заходів заходів організаційно-технічного рівня.

Щоб поліпшити організацію системи інформаційної безпеки підприємства ТОВ «Феракс» у напрямку підвищення ефективності забезпечення безпеки , запропоновано проведення організаційних заходів.

ВИСНОВКИ

Реальність сьогодення, яке складається у світі, вимагає принципово нових підходів до осмислення ситуацій, що складаються. Особливо це важливо для України як і усіх інших країн, які переживають етап кардинальних трансформаційних, а сьогодні – і кризових змін на рівні держави.

Праналізовано вимоги нормативно-методичних документів до організації інформаційної безпеки. Стандарти залишаються як кращі практичні ради по управлінню ІБ для тих, хто відповідає за створення, реалізацію або обслуговування систем управління інформаційною безпекою . Представлена схема СУІБ у вигляді моделі процесів ІБ, що відповідає спеціальним нормативним документам щодо системного забезпечення інформаційної безпеки для підприємства.

Реалізація інформаційної безпеки повина будуватися навколо основних трьох аспектів безпеки, які полягають в підтримці конфіденційності, цілісності

та доступності до інформації. Найбільший ефект захисту інформації досягається тоді, коли всі використовувані засоби, методи та заходи поєднуються в єдиний цілісний механізм – систему захисту інформації.

Організація захисту від загроз функціонуванню інформаційної системи підприємства відбувається шляхом побудови ефективної системи інформаційної безпеки . Показана роль політики інформаційної безпеки, яка повинна визначати системи захисту інформації і управління інформаційною безпекою як обєднану систему забезпечення ІБ .

Визначена системи забезпечення інформаційної безпеки підприємства як комплекс реалізації організаційних, технічних, програмних і криптографічних засобів і заходів захисту інформації. . Ядром інженерно-технічного напряму підвищення ефективності процесів забезпечення інформаційної безпеки визначено програмно-апаратні засоби захисту інформації. Розкриті технічних заходи , які впливають на підвищення ефективності процесів забезпечення, і сукупність спеціальних програм, що реалізують функції захисту інформації та режиму функціонування.

Необхідність підвищення ефективності системи забезпечення інформаційної безпеки пов'язана із загостренням проблем захисту інформації. Для найкращего вирішення цього питання пропонується використовувати системно – при створенні (або вдосконаленні) системи управління інформаційною безпекою підприємства. А потім використовувати напрацювання цієї системи переходити на утворення її системи забезпечення і забезпечення інформаційної безпеки підприємства в цілому.

Процес забезпечення інформаційної безпеки підприємства можна представити як взаємодію трьох підсистем: підсистема інформаційного забезпечення процесу управління на підприємстві; підсистема захисту інформаційного середовища підприємства і підсистема діагностики рівня інформаційної безпеки.

Обґрунтована пропозиція щодо доцільності застосування варіантів побудови системи інформаційної безпеки - по досягненню необхідного рівня безпеки, захищеності інформації, обмежень на технології і затрат.

Пошук напрямів і розробка рекомендацій щодо вдосконалення організації управлінських процесів в тому числі і в забезпеченні безпеки завжди залишаються актуальними в дослідженні системи управління інформаційною

безпекою на підприємстві. За результатами проведених досліджень, можна сформувати методичний підхід до побудови системи інформаційної безпеки підприємства з чотирьмя рівнями управління підприємством: теоретико-методологічний, методичний, інструментальний і організаційно- технічний.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аніловська Г.Я. Інформаційна безпека підприємства в умовах використання сучасних інформаційних технологій / Г.Я.Аніловська URL: http://www.nbuv.gov.ua/portal/chem_biol/nvnltu/18_9/270_Anilowska_18_9.pdf

2. Бєгун А. В. Щодо питань про сучасні методи регулювання безпеки / А. В. Бєгун, В. Ф. Гречанінов, В. П. Клименко // Математичні машини і системи. — 2013. — № 4. — К. : ІПММС, 2013. — С. 135-146.

3. Білоконь Д. С., Федулова І. В. Процес управління ризиками інформаційної безпеки / Д. С. Білоконь, І. В. Федулова // Менеджмент і стратегічне управління. – Наукові праці НУХТ, 2016. – Том 22, № 6. – С. 84-91

4. Велігура А. В. Оцінювання стану інформаційної безпеки підприємства [Електронний ресурс] / Управління проектами та розвиток виробництва. - № 4(52), 2014. URL: www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe.

5. Галузевий стандарт України: Інформаційні технології. Методи захисту. Система управління інформаційною безпекою (Вимоги Iso/Iec 27001: 2015, Mod) / НБУ URL: http://auditagency.com.ua.

6. Голов А. Интегрированная архитектура системы информационной безопасности / А. Голов URL: http://www.connect.ru/article.asp?id=7120

7. Гриджук Г. С. Систематизація методів інформаційної безпеки підприємства. URL: http://www.nbuv.gov.ua/portal/natural/Vntu/2012_19_1/pdf/64.pdf.

8. Єрмолаєв П. В. Функціональний профіль економічної безпеки підприємства: методичні та прикладні аспекти [Текст] / П. В. Єрмолаєв // Управління проектами та розвиток виробництва: Зб.наук.пр. – Луганськ: вид-во СНУ ім. В.Даля, 2013. – № 1(45). - С. 26-33

9. Єрмошин В. В., Невойт, Я. В. Аналіз і оцінка ризиків інформаційної безпеки для банківських та комерційних систем [Електронний ресурс] /В. В. Єрмошин, Я. В. Невойт // Сучасний захист інформації. – № 4, 2014. URL: http://journals.dut.edu.ua/index.php/dataprotect/ article/view/256

10. Кавун С. В. Інформаційна безпека: підручник / С. В. Кавун, , В.В. Носов, О.В. Мажай. - Харків : Вид. ХНЕУ, 2009. - 352 с. - URL: http://www.repository.hneu.edu.ua/jspui/handle/123456789/3068

11. Литвинюк А.А. Основи інформаційної безпеки. Комплексна система захисту інформації: структура, встановлення та підтримка функціонування // А.А. Литвинюк. URL: http://www.cvk.gov.ua/visnyk/pdf/2008_4/visnik_st_08.pdf

12. Метрики оцінювання ефективності СУІБ С. 1-26, URL: https://docplayer.ru/34817016- Ocenka-effektivnosti-sistemy-upravleniya-ib.html

13. Низенко Е. І., Каленяк В. Забезпечення інформаційної безпеки підприємництва: Навч. посіб. — К. : МАУП, 2006. — 134 с.

14. Побойний О. С. Виявлення та нейтралізації внутрішніх загроз інформаційної безпеки Тези. К.: ДУТ, 2023.- С. 195-196 URL: https://m.books.ru/books/bezopasnost-informatsionnykh-tekhnologii-sistemnyi-podkhod-229927/.

15. Сороківська О.А., Гевко В.Л. Інформаційна безпека підприємства: нові загрози та перспективи / О.А. Сороківська, В.Л. Гевко. URL: http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2010_2_2/032-035.pdf

16. Телекомунікаційні системи та мережі. Том 1. Структура й основні функції.- URL: https://www.znanius.com/3849.html.

17. Цирлов В.Л. Основы информационной безопасности автоматизированных систем. краткий курс М.: Изд-во Феникс 2008 .- 173 с .- URL https://www.studmed.ru/cirlov-vl-osnovy-informacionnoy-bezopasnosti-avtomatizirovannyh-sistem_7f1ee989425.html

18. Шаньгін В. Ф., Захист інформації в комп'ютерних системах і мережах/ В. Ф. Шаньгін – Київ: МК Прес, 2012. - 592 с.

19. Семененко В.А. Информационная безопасность: Учебное пособие. 2-е изд., стереот. / В.А. Семененко. - М.: МГИУ, 2005. - 215 с.

20. What is Information Security? URL: https://www.geeksforgeeks.org/what-is-information-security/ (дата звернення: 01.06.2021)

21. What is Information Security? URL: https://www.cisco.com/c/en/us/ products/ security/what-is-information-security-infosec.

22. ДСТУ ISO/IEC 27001:2015 Методи захисту системи управління інформаційною безпекою. Вимоги.

23. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки

24. ISO/IEC 27002:2005, MOD. СОУ Н НБУ 65.1 СУІБ 2.0:2010. Чинний від 2010-10-28. Вид. офіц. Київ : Нац. банк України, 2010. 195 с.

25. ISO/IEC 27003:2010. Information technology — Security techniques — Information security management system implementation guidance (Інформаційні технології. Методи безпеки. Керівництво з упровадження системи управління інформаційною безпекою).

26. ISO/IEC 27004:2009. Information technology — Security techniques — Information security management — Measurement (Інформаційні технології. Методи безпеки. Управління інформаційною безпекою. Вимірювання).

27. ISO/IEC CD 27007. Information technology — Security techniques — Guidelines for information security management systems auditing (Проект. Інформаційні технології. Методи безпеки. Настанова з аудиту систем управління інформаційною безпекою).

28. ISO/IEC 27011:2008. Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 (Інформаційні технології. Методи безпеки. Настанови з

управління інформаційною безпекою для телекомунікаційних компаній, базовані на ISO/IEC 27002).

29. Про рішення Ради національної безпеки і оборони України від 29.12.2016 «Про Доктрину інформаційної безпеки України» : Указ Президента України. 25.02.2017 № 47/2017 // База даних «Законодавство України/ ВР України.

30. Черевко О.В. Теоретичні засади поняття інформаційної безпеки та класифікація загроз системі інформаційного захисту. Киів: Ефективна економіка № 5, 2014 - 6с.

31. Якименко Ю.М., Савченко В.А., Легомінова С.В. Системний аналіз інформаційної безпеки: сучасні методи управління: підручник. Київ: Державний університет телекомунікацій, 2022. 308 с. URL: https://dut.edu.ua/uploads/l_2230_88161692.pdf.