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
«___»_____20__ р.

До захисту
Завідувач кафедри УІКБ
доктор економічних наук, професор
_____ С.В. Легомінова
«___»_____20__ р.

ДИПЛОМНА РОБОТА

на тему:

ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

СТУДЕНТ: Зіновський Ростислав Олександрович _____
(підпис)

КЕРІВНИК: к.держ.упр. Мужанова Тетяна Михайлівна _____
(підпис)

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

Київ – 2022

«ЗАТВЕРДЖУЮ»
Завідувач кафедри УІКБ
_____ С.В. Легомінова
«_____»_____ 20__ р.

ЗАВДАННЯ
на дипломну роботу

студенту Зіновському Ростиславу Олександровичу

Тема роботи: «ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА», затверджена наказом по університету № 170 від «11» жовтня 2021 р.

1. **Термін здачі** студентом оформленої роботи «___» _____ 20___ р.
2. **Об'єкт дослідження:** забезпечення інформаційної безпеки підприємства.
3. **Предмет дослідження:** організаційне забезпечення інформаційної безпеки підприємства.
4. **Мета дослідження** полягає у вивченні засад організаційного забезпечення інформаційної безпеки підприємства.
5. **Перелік питань, які мають бути розроблені:**

5.1 Встановити роль організаційних заходів у системі забезпечення інформаційної безпеки підприємства.

5.2 Дослідити засади організації діяльності підрозділу інформаційної безпеки підприємства.

5.3 З’ясувати особливості забезпечення режиму й охорони об’єктів інформаційної безпеки підприємства.

5.4 Проаналізувати нові підходи до організації інформаційної безпеки підприємства і запропонувати рекомендації щодо її удосконалення.

6. **Дата видачі завдання «**16» вересня 2021 р.

Науковий керівник _____ Т.М. Мужанова
підпис

Завдання прийнято до виконання _____ Р.О. Зіновський
підпис

Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
Кафедра управління інформаційною та кібернетичною безпекою

КАЛЕНДАРНИЙ ПЛАН
виконання дипломної роботи
студентом ЗІНОВСЬКИМ Ростиславом Олександровичем

Дата видачі завдання: «16» вересня 2021 р.

№ з/п	Етапи дипломної роботи	Термін виконання етапів	Примітка
	Визначення об'єкта, предмета, мети та завдань дослідження.	16.09.2021	
	Збір та аналіз літератури.	28.09.2021	
	Встановлення ролі організаційних заходів у системі забезпечення інформаційної безпеки підприємства.	12.10.2021	
	Дослідження засад організації діяльності підрозділу інформаційної безпеки підприємства.	26.10.2021	
	З'ясування особливостей забезпечення режиму й охорони об'єктів інформаційної безпеки підприємства.	09.11.2021	
	Аналіз нових підходів до організації інформаційної безпеки підприємства, розробка рекомендацій.	23.11.2021	
	Оформлення роботи.	07.12.2021	
	Оформлення презентації.	14.12.2021	
	Отримання рецензії на роботу.	24.12.2021	
	Захист у ДЕК.	__.01.2022	

Студент Р.О. Зіновський
(підпис)

Науковий керівник Т.М. Мужанова
(підпис)

РЕФЕРАТ

Дипломна робота присвячена дослідженню засад організаційного забезпечення інформаційної безпеки підприємства. Робота складається зі вступу, чотирьох розділів, що містять 15 рисунків, висновків та списку використаних джерел з 41 найменування. Загальний обсяг роботи становить 83 аркуші, 4 з яких займає список використаних джерел.

Об'єктом дослідження є забезпечення інформаційної безпеки підприємства.

Предметом дослідження є організаційне забезпечення інформаційної безпеки підприємства**.**

Метою роботи є вивчення засад організаційного забезпечення інформаційної безпеки підприємства.

Для цього у роботі використані методи аналізу, синтезу, класифікацій та порівняння, узагальнення, положення системного, комплексного і структурно-функціонального підходів, теорій інформаційної та фізичної безпеки.

Як результат у роботі встановлено роль організаційних заходів у системі забезпечення інформаційної безпеки підприємства; досліджено засади організації діяльності підрозділу інформаційної безпеки підприємства; з'ясовано особливості забезпечення режиму й охорони об'єктів інформаційної безпеки підприємства; проаналізовано нові підходи до організації інформаційної безпеки підприємства й запропоновано рекомендації щодо її удосконалення.

Галузь застосування. Розроблені підходи можуть бути використані у ході впровадження комплексу організаційних заходів забезпечення інформаційної безпеки підприємства, зокрема створення служби інформаційної безпеки, забезпечення режиму й охорони, виборі програмних засобів для організації інформаційної безпеки.

Ключові слова: ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА, ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА, СЛУЖБА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ОРГАНІЗАЦІЯ РЕЖИМУ Й ОХОРОНИ, НОВІ ПІДХОДИ ДО ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА.

ЗМІСТ

ВСТУП

У період масштабної і всеохоплюючої цифровізації сучасного суспільства основною цінністю й надбанням підприємства стає інформація, яка обробляється і передається корпоративними ІТКС. Захист конфіденційної інформації та засобів її обробки є не тільки обов'язком кожного підприємства, але й безперечною умовою його ефективного функціонування і ринкової конкурентоспроможності.

Відомо, що інформаційна безпека забезпечуються за допомогою комплексного використання різнопланових методів. Серед них особливу важливість мають організаційні заходи, які створюють умови для ефективного функціонування підприємства та забезпечення корпоративної інформаційної безпеки шляхом встановлення і розподілу повноважень, координації діяльності залучених суб'єктів, управління ресурсами і ліквідації відхилень у разі їх появи.

З огляду на зазначене актуальним є дослідження основних аспектів організаційного забезпечення інформаційної безпеки, в тому числі нових підходів, і розробка відповідних рекомендацій.

Мета і завдання дослідження. **Мета** роботи полягає у вивченні кадрових технологій в системі управління інформаційною безпекою підприємства.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Встановити роль організаційних заходів у системі забезпечення інформаційної безпеки підприємства.

2. Дослідити засади організації діяльності підрозділу інформаційної безпеки підприємства.

3. З'ясувати особливості забезпечення режиму й охорони об'єктів інформаційної безпеки підприємства.

4. Проаналізувати нові підходи до організації інформаційної безпеки підприємства й запропонувати рекомендації щодо її удосконалення

Об’єкт дослідження - забезпечення інформаційної безпеки підприємства. **Предмет дослідження** – організаційне забезпечення інформаційної безпеки підприємства.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу, синтезу, класифікацій та порівняння, структурно-функціонального підходу, положення концепції організації інформаційної безпеки компанії IBM ISS.

Наукова новизна одержаних результатів. У роботі досліджено організаційні аспекти забезпечення інформаційної безпеки, які можуть бути успішно впроваджені в системі управління інформаційною безпекою підприємства, зокрема новітні підходи до організації роботи служби ІБ, режиму й охорони, віддаленої роботи та програмного забезпечення.

Практичне значення одержаних результатів. Застосування отриманих напрацювань на практиці дасть змогу зменшити ризики інформаційній безпеці компанії завдяки застосуванню сучасних розробок, підходів та комплексних програмних продуктів для ефективної організації інформаційної безпеки підприємства.

РОЗДІЛ 1.
ОРГАНІЗАЦІЙНІ ЗАХОДИ У СИСТЕМІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

1.2. Загальні характеристики системи забезпечення інформаційної безпеки підприємства

У 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.

З огляду на зростаючі обсяги інформації, переведення значної її частини в електронну форму, використання інформаційних систем (далі – ІС), локальних і глобальних мереж у всіх сферах діяльності людини, виникають якісно нові загрози інформації, а вирішення завдань щодо її зберігання, передачі та обробки є надзвичайно актуальним.

Сучасний діловий світ, представлений головним чином фінансово-інформаційними корпораціями, страждає від інформаційної крадіжки. За даними світової статистики, втрата тільки 20% інформації веде до руйнування 65 % фірм і компаній. Тому інформаційна безпека (далі – ІБ) є одним із найважливіших показників успішної діяльності організації [36].

ІБ підприємства визначають як суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності ІС суб'єкта господарської діяльності [32].

У більш прикладному аспекті ІБ підприємства – це стан захищеності інформаційного середовища організації від внутрішніх та зовнішніх загроз.

ІБ підприємства характеризується конфіденційністю, цілісністю, доступністю та може розглядатися як сукупність таких елементів: безпечні умови функціонування ІТ, побудова ефективної інфраструктури інформаційного

простору, цілісного ринку інформації, створення оптимальних умов для проходження інформаційних процесів.

Метою ІБ є збереження цілісності, повноти та точності інформації, мінімізація ризику несанкціонованих змін у ІС [8].

До основних цілей забезпечення інформаційної безпеки (далі - ЗІБ) належать:

• запобігання витоку, розкраданню, втраті, спотворенню, підробці інформації;

• запобігання несанкціонованим діям із знищення, модифікації, спотворення, копіювання, блокування інформації;

• запобігання іншим формам незаконного втручання в інформаційні ресурси і системи, забезпечення правового режиму документованої інформації як об’єкту власності;

• захист конституційних прав громадян на збереження особистої таємниці і конфіденційності персональних даних, наявних в ІС;

• збереження конфіденційності документованої інформації відповідно до законодавства [22].

Система забезпечення інформаційної безпеки (далі - СЗІБ) - це частина загальної системи управління підприємства, що базується на аналізі ризиків і призначена для проектування, реалізації, контролю, супроводу та вдосконалення заходів в області ІБ. Цю систему складають організаційні структури, політика, дії з планування, обов'язки, процедури, процеси і ресурси.

Найбільш значущою метою більшості СЗІБ є захист бізнесу та інформації, знань компанії від знищення або витоку. Також однією з основних цілей СЗІБ є гарантія майнових прав та інтересів клієнтів. У той же час заходи з ІБ не повинні обмежувати або ускладнювати процеси обміну знаннями в компанії, оскільки це може поставити під загрозу розвиток організації.

Багато сучасних підприємств та організацій не в змозі самостійно і за прийнятну вартість досягти і підтримувати необхідний рівень ІБ. Серед основних

причин такого стану речей є відсутність належного розуміння у вищого керівництва щодо необхідності СЗІБ підприємства; немає чітко сформульованої мети СЗІБ або єдиного бачення з цього питання у керівництва підприємства і виконавців, не визначено повною мірою всі необхідні вимоги до результату ЗІБ організації. До другого блоку причин нездатності підприємства забезпечити належний стан захищеності інформації відносяться такі: повноваження щодо здійснення ЗІБ покладені керівництвом на працівників, які з різних причин (недостатні повноваження, брак часу, протиріччя з основними службовими обов'язками тощо) не в змозі якісно виконувати цю роботу; для виконання функцій із ЗІБ підібрані фахівці, що є недостатньо компетентними для вирішення цього завдання.

Часто причиною відсутності СЗІБ на підприємстві, яке потребує захисту конфіденційної інформації, є недостатність наявних коштів і ресурсів підприємства для здійснення ефективної діяльності у сфері ІБ [31].

СЗІБ має забезпечувати гарантію досягнення таких цілей як забезпечення конфіденційності критичної інформації, забезпечення неможливості несанкціонованого доступу до критичної інформації, цілісності інформації та пов'язаних з нею процесів (створення, введення, обробки і виведення) і ряду інших цілей [20].

Якісне ЗІБ базується на таких принципах:

- Комплексний підхід - ЗІБ має бути всеосяжним, охоплювати всі компоненти ІС і враховувати всі актуальні фактори формування ризиків, що діють в ІС підприємства та за її межами;

- Узгодженість з бізнес-завданнями і стратегією підприємства;

- Високий рівень керованості;

- Адекватність інформації, яка використовується і генерується;

- Ефективність - оптимальний баланс між можливостями, продуктивністю і витратами СЗІБ;

- Безперервність управління;

- Процесний підхід - зв'язування процесів управління в замкнутий цикл планування, впровадження, перевірки, аудиту та коригування, і підтримка нерозривному зв'язку між етапами циклу, що дозволяє зберігати і постійно підвищувати якість СЗІБ [34].

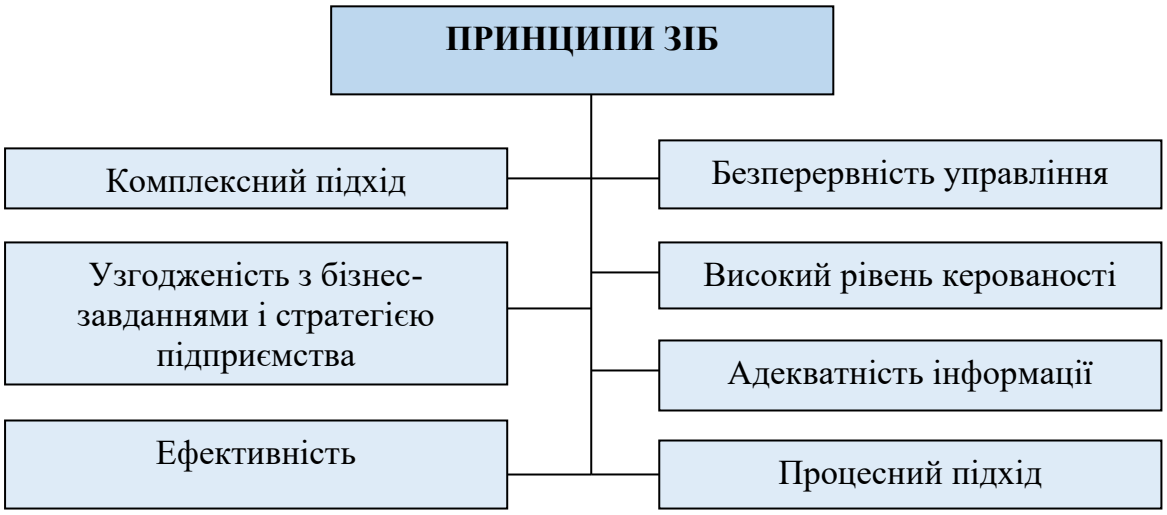

Рис. 1.1. Принципи ЗІБ

Також до принципів ЗІБ відносять принципи [1]:

Системності.

Комплексності.

Безперервності захисту.

Розумної достатності.

Гнучкості управління і застосування.

Відкритості алгоритмів і механізмів захисту.

Простоти застосування захисних заходів і засобів.

Важливими принципами ЗІБ є також економічна доцільність, підтримка та зацікавленість з боку керівництва і персоналу, чіткий розподіл повноважень і персональна відповідальність.

Не менш важливим є питання економічного обґрунтування витрат на ЗІБ. Адже чим вище рівень захищеності інформації, тим за інших рівних умов, буде нижче розмір можливих збитків, але тим вищою буде вартість захисту. Оптимальним розміром витрат на ІБ буде такий, при якому забезпечується рівень захищеності, що дорівнює мінімуму загальних витрат. Вартість збитків

визначається двома параметрами: ймовірністю реалізації різних загроз інформації; вартістю (важливістю) інформації, захищеність якої може бути порушена під впливом різних загроз. У зв'язку зі складністю дати кількісну оцінку збитків (сума втрат або розмір недоотриманого прибутку) причиною яких може бути витік, або втрата інформації, що захищається, в даний час найбільш доцільним є підхід на основі експертних оцінок [36].

Забезпечення (управління) інформаційної безпеки - це циклічний процес (Рис. 1.1.), що включає:

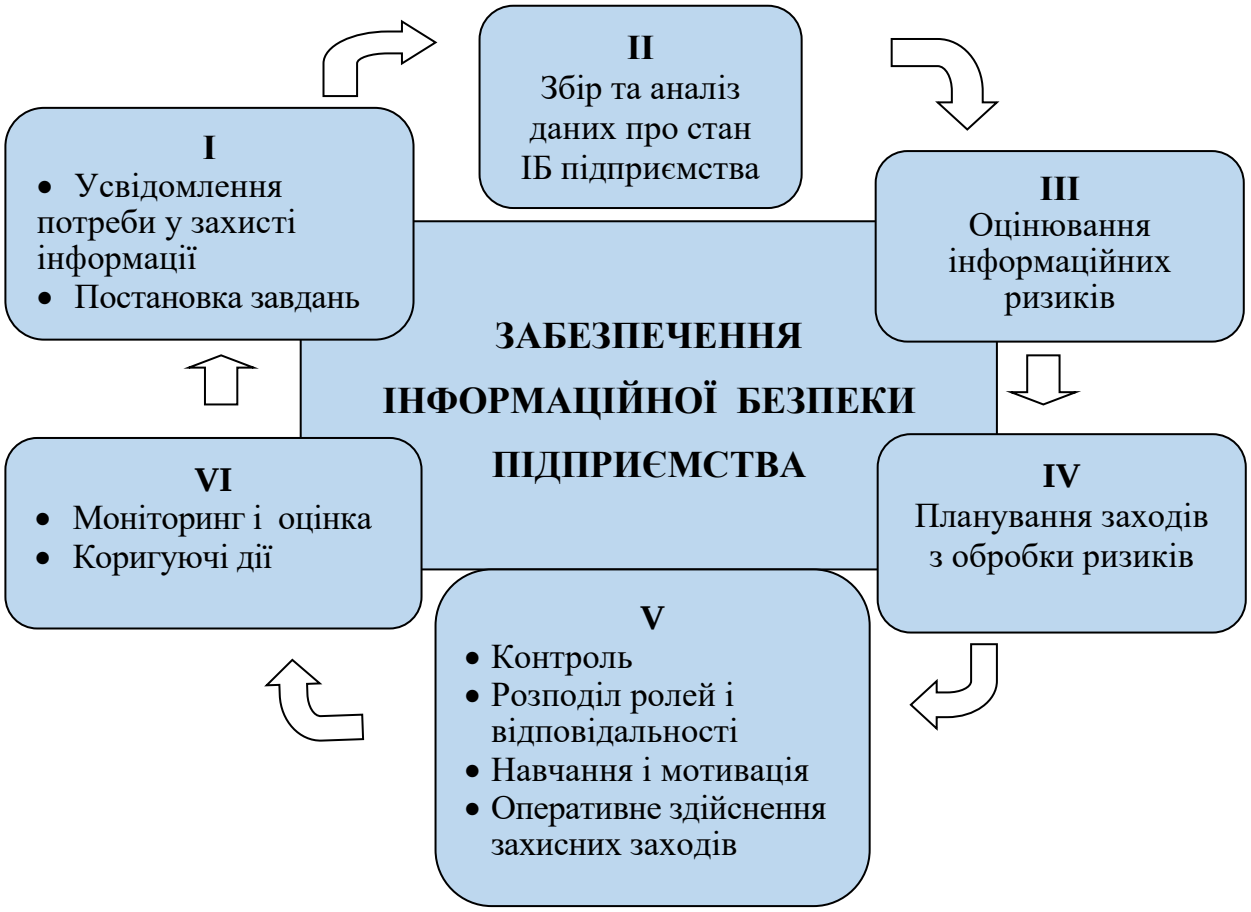

Рис. 1.2. Цикл забезпечення інформаційної безпеки підприємства

- усвідомлення потреби в захисті інформації та постановку завдань;
- збір та аналіз даних про стан ІБ в компанії;
- оцінку інформаційних ризиків;
- планування заходів з обробки ризиків;

- реалізацію і впровадження відповідних механізмів контролю, розподіл ролей і відповідальності, навчання і мотивацію персоналу, оперативну роботу по здійсненню захисних заходів;
- моніторинг функціонування механізмів контролю, оцінку їх ефективності та відповідні коригуючі дії.

Відповідно до основоположного стандарту у сфері ІБ ISO/IEC 27001 основою для побудови СЗІБ є PDCA модель [12], що за загальною логікою відповідає попередньо представленій моделі:

- Plan (Планування) - фаза створення СЗІБ, створення переліку активів, оцінки ризиків та вибору заходів;
- Do (Дію) - етап реалізації та впровадження відповідних заходів;
- Check (Перевірка) - фаза оцінки ефективності та продуктивності СЗІБ. Зазвичай виконується внутрішніми аудиторами.
- Act (Покращення) - виконання превентивних і коригувальних дій.

Детальніше побудова СЗІБ підприємства передбачає здійснення таких кроків у рамках PDCA моделі:

• попередній аудит;

• визначення області дії і меж СЗІБ;

• призначення співробітників, відповідальних за ЗІБ (створення структури, яка буде впроваджувати і забезпечувати працездатність СЗІБ організації, наприклад, відділ ІБ);

• інвентаризація активів організації та визначення їх важливості;

• оцінка захищеності активів організації (аналіз існуючих загроз і вразливостей, а також ймовірностей їх реалізації);

• визначення корпоративного підходу до оцінки ризиків (компанія може запропонувати свій метод оцінки ризиків, і чим простіше буде цей метод, тим краще);

• підрахунок ризиків в компанії, як в якісних, так і в кількісних показниках;

• аналіз ризиків і прийняття рішень по обробці ризиків (прийняти ризик, зменшити ризик до допустимого рівня, передати третій стороні, уникнути ризику);

• вибір цілей управління і засобів обробки ризиків;

• аналіз існуючих контрзаходів (організаційні заходи та програмно-технічні засоби, спрямовані на захист визначених активів підприємства);

• аналіз процесної документації компанії (створюється список організаційних документів, що вимагають впровадження) [8].

Як відзначено вище, одним із основних принципів розробки та впровадження СЗІБ є дотримання комплексного підходу, сутність якого полягає у поєднанні в єдиний комплекс різнопланових заходів та засобів запобігання протидії загрозам ІБ. Організація захищеного середовища обробки й передавання інформації з використанням сукупності різнопланових заходів гарантує високий рівень ЗІБ, що є безсумнівною перевагою комплексного підходу. До недоліків цього підходу відносять: обмеження свободи дій персоналу та користувачів, чутливість до помилок встановлення й налаштування засобів захисту інформації, складність управління [24].

Для ЗІБ у рамках комплексного підходу використовують сукупність таких видів заходів:

- нормативно-правові (законодавчі);
- організаційно-адміністративні;
- програмні-технічні [38].

До нормативно-правових засобів ЗІБ належать діючі в державі законні та підзаконні акти (укази, постанови, розпорядження тощо), які регламентують питання захисту інформації в ІТКС, правила обробки і використання інформації обмеженого доступу (державна таємниця, комерційна таємниця, персональні дані та інші), встановлюють відповідальність за їх порушення. Таким чином держава обмежує можливості для несанкціонованого використання інформації

згаданих категорій і встановляє стримуючі чинники для потенційних порушників.

Організаційно-адміністративні заходи ЗІБ підприємства регламентують процеси розробки і функціонування корпоративних ІТКС; використання інформаційних ресурсів підприємства; діяльність персоналу, який має доступ до конфіденційної інформації та засобів її обробки, та підрозділу, який відповідає за впровадження заходів ІБ на підприємстві; засади роботи користувачів із ІТКС з метою запобігання чи, принаймні, мінімізації можливостей реалізації загроз ІБ.

До організаційних заходів фахівці відносять:

- розробку вимог ІБ (політики, процедур, регламентів та інших внутрішньо-корпоративних документів з ІБ), правил використання інформації обмеженого доступу та засобів її обробки;

- проектування, налаштування і супровід функціонування обчислювальних центрів та інших об'єктів ІТКС, в яких обробляється конфіденційна інформація (захист від природних загроз, запобігання технічним збоям та аваріям, охорона приміщень тощо);

- підбір і відбір персоналу, задіяного у сфері ІБ (ускладнена процедура перевірки кандидатів на зайняття вакантних посад, ознайомлення їх із вимогами до роботи з конфіденційною інформацією, встановлення відповідальності за порушення вимог ІБ; мотивування й формування лояльного персоналу з метою запобігання зловживанням і порушенням тощо);

- організація належного пропускного режиму на об’єкти ІБ;

- організація обліку, використання, розмноження, зберігання, забезпечення схоронності, передавання та знищення носіїв конфіденційної інформації;

- розмежування доступу (дотримання політики паролів, розподіл повноважень тощо);

- здійснення контролю за роботою персоналу та поведінкою користувачів корпоративних ІТКС;

- сертифікація апаратних і програмних засобів захисту інформації, ліцензування відповідної діяльності, розгляд, перевірка і затвердження всіх змін у розташуванні і функціонуванні елементів ІТКС відповідно до нормативних вимог ІБ тощо).

Часто до організаційних засобів ЗІБ відносять і заходи забезпечення фізичної безпеки об'єктів ІБ та відповідні засоби захисту, зокрема різні механічні, електричні і електромеханічні пристрої або споруди, призначені для фізичного перешкоджання спробам зловмисників отримати доступ і проникнути на об'єкти ІБ (турнікети, колючий дріт, кодові замки, системи охоронно-пожежної сигналізації тощо).

Програмно-технічні заходи ІБ включають широкий перелік різноманітних заходів щодо закупівлі, проектування, налаштування, введення в експлуатацію, супроводу при функціонуванні електронних пристроїв, спеціальних програм та цілих програмно-апаратних комплексів, які, зокрема, унеможливлюють витік, знищення та блокування інформації, порушення цілісності та режиму доступу до неї [1]: ідентифікацію і автентифікацію користувачів корпоративних ІТКС; розмежування доступу до інформаційних ресурсів обмеженого доступу; контроль доступності, цілісності та конфіденційності даних; аудит подій, що відбуваються в ІТКС; резервне копіювання ресурсів і компонентів ІТКС та багато інших.

У науковій думці інколи виділяють ще один окремий вид заходів ЗІБ - морально-етичні засоби, до яких відносять різноманітні норми поведінки, які традиційно склалися або складаються в суспільстві у міру комп'ютеризації та цифровізації усіх сфер його життєдіяльності. Ці норми бувають як неписаними (загальновизнані норми чесності, корпоративної відданості тощо), так і оформленими у певний кодекс поведінки чи звід правил для працівників компанії.

Таким чином, основними напрямами ЗІБ підприємства є нормативно-правові, організаційні та програмно-технічні (Рис. 1.3.).

Рис. 1.3. Основні напрями ЗІБ підприємства

Крім цього, заходи ЗІБ підприємства можуть бути класифіковані іншими критеріями, такими як: орієнтація на об'єкти захисту, характер загроз, способи дій, їх поширеність, охоплення і масштаб [38] (Рис 1.4.).

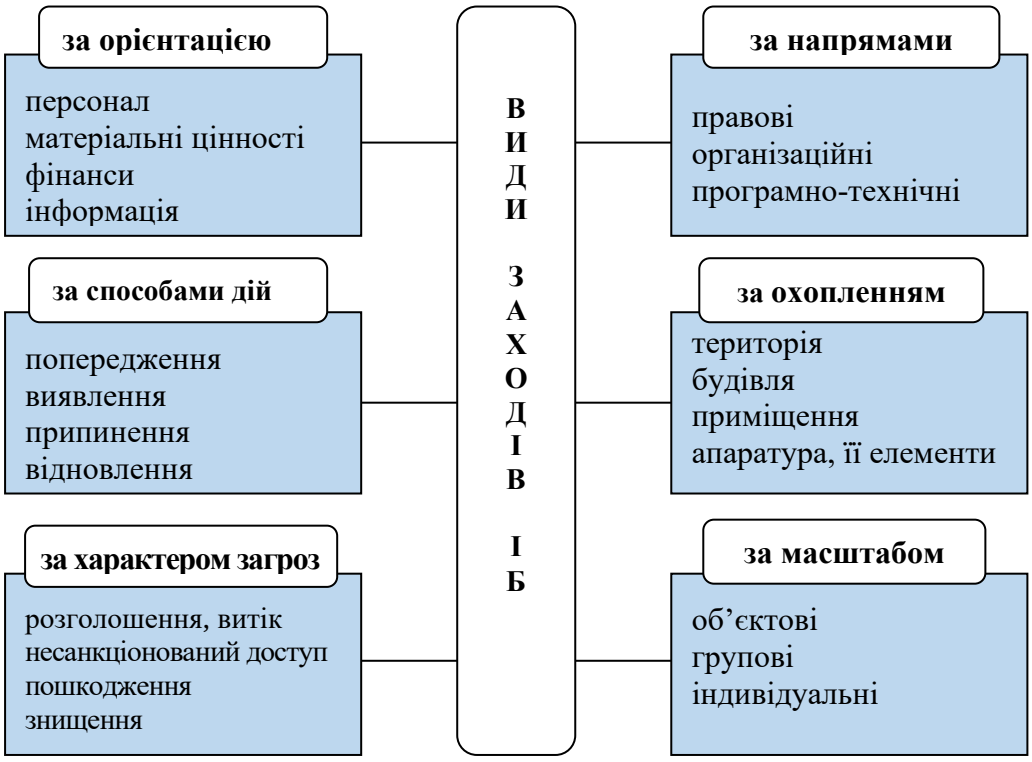

Рис. 1.4. Види заходів забезпечення інформаційної безпеки

1.2. Організаційне забезпечення інформаційної безпеки підприємства

Відповідно до теорії управління функція організації включає:

– визначення завдань, які мають бути виконані і їх групування за потреби;

– розподіл встановлених завдань між працівниками одночасно із визначення повноважень і відповідальності;

– делегування повноважень працівникам;

– встановлення зв’язків між повноваженнями і відповідальністю;

– координація запланованих дій персоналу [28].

Відповідно до іншого бачення організаційне забезпечення є сукупністю структур і правил, які створюють умови для належного протікання певних управлінських процесів, реалізації завдань і планів, підтримки функціонування системи управління на достатньо високому рівні за рахунок наявності необхідних ресурсів, організації й координації взаємозв’язків між окремими компонентами системи і ліквідації відхилень у випадку їх виникнення [29].

Загалом організаційна діяльність - це сукупність процесів, за допомогою яких керівництво організації може вирішити проблеми чи усунути конфлікти. Основними складовими організаційної діяльності є: розподіл праці, розподіл ресурсів, делегування повноважень, встановлення контролю за виконанням робіт, створення механізмів координації [22].

Характеризуючи організаційне забезпечення ІБ (далі - ОЗІБ), яке сьогодні є однією із найбільш важливих складових корпоративної СЗІБ, системи управління підприємством, засобом забезпечення його конкурентоспроможності та безперервності бізнесу, варто відзначити, що ОЗІБ має на меті досягнення таких цілей як забезпечення доступності, цілісності та конфіденційності, а також уникнення несанкціонованого доступу до критичної інформації і пов'язаних з нею процесів (створення, введення, і виведення, обробки) тощо.

Ключова роль ОЗІБ визначається винятковою важливістю своєчасного прийняття виважених і обґрунтованих управлінських рішень на основі аналізу

поточної ситуації та різних чинників впливу, врахування наявних потужностей, методів, засобів і способів захисту інформації, прогнозування наслідків управлінського впливу у рамках діючого нормативно-правового та методичного апарату [30].

ОЗІБ підприємства передбачає регулювання виробничої діяльності і взаємин виконавців відповідно до обмежень законодавства та нормативних документів, що суттєво ускладнює або запобігає несанкціонованому заволодінню, пошкодженню чи знищенню конфіденційної інформації, іншим проявам внутрішніх і зовнішніх загроз ІБ.

У межах ОЗІБ підприємства визначаються: схема і порядок функціонування основних підсистем ІБ та бізнесу, використання корпоративних інформаційних ресурсів та програмно-апаратних засобів, що використовуються у процесі їх обробки та передавання, відносини суб'єктів ІБ (керівництва, персоналу, користувачів) відповідно до діючих нормативно-правових вимог і правил.

Організаційні заходи відіграють ключову роль у забезпеченні надійності та ефективності СЗІБ підприємства, оскільки значна частина порушень ІБ (санкціонований доступ, витік, пошкодження чи знищення інформації, пошкодження елементів ІТКС, сприяння зовнішнім нападникам) найчастіше обумовлені зловмисними діями або халатністю, відсутністю належної професійної підготовки чи обізнаності з ІБ персоналу або користувачів.

Дію людського чинника практично неможливо локалізувати або зупинити за допомогою фізичних, програмно-апаратних чи криптографічних засобів захисту. Вирішити проблему негативного впливу різних дестабілізуючих факторів на СЗІБ підприємства можливо лише за умови використання сукупності організаційних заходів, нормативно-правових та програмно-технічних методів захисту інформації. Таким чином бізнес може уникнути, зменшити або повністю усунути втрати внаслідок дії деструктивних чинників.

Організаційні заходи є важливою складовою таких видів діяльності з ІБ:

- проектування, будівництво й обладнання будівель, приміщень, важливих елементів корпоративних ІТКС та інших об'єктів ІБ відповідно до вимог ІБ щодо запобігання загрозам несанкціонованого доступу, загрозам природного характеру та технічним аваріям;

- наймання і підготовка персоналу у сфері ІБ, де передбачаються перевірка кандидатів на зайняття посади, адаптація осіб, прийнятих на роботу, навчання правилам роботи з конфіденційними даними, ознайомлення з санкціями у випадку порушення правил ІБ, мотивування персоналу дотримуватися вимог ІБ;

- забезпечення належного зберігання й використання носіїв конфіденційної інформації (класифікація, реєстрація, маркування, встановлення правил роботи з конфіденційною документацією, забезпечення режиму її збереженості тощо);

- організація пропускного режиму до технічних засобів, корпоративних ІТКС та критичних інформаційних ресурсів (встановлення персональної відповідальності відповідних посадових осіб, розмежування доступу до об’єктів ІБ, контроль і ведення обліку трудової діяльності працівників у контексті дотримання засад захисту інформації);

- безпечна розробка та впровадження програмного забезпечення, що передбачає санкціонування будь-яких дій з боку керівництва, перевірку ПЗ на відповідність вимогам захисту, документальне фіксація усіх змін тощо [38].

На основі розглянутих вище підходів виділимо такі основні групи організаційних заходів:

- організація режиму й охорони з метою запобігання несанціонованому проникненню сторонніх осіб на територію і об’єкти ІБ; здійснення розмежування доступу персоналу та інших залучених працівників до критичних інформаційних ресурсів компанії та засобів їх обробки; організація ефективного пропускного режиму та контролю пересування персоналу й відвідувачів;

- робота з персоналом, що працює з конфіденційною інформацією або забезпечує захист засобів її обробки (наймання і проведення перевірки потенційних працівників, навчання правилам роботи з конфіденційною

інформацією і забезпечення дотримання вимог ІБ, встановлення обов'язку працівників не розголошувати конфіденційну інформацію та визначення відповідальності за його порушення;

- організація конфіденційного діловодства, включаючи встановлення правил розробки і використання документів та носіїв конфіденційної інформації, їх обліку, виконання, повернення, зберігання і знищення;

- використання спеціальних програмних і технічних засобів збирання, обробки, зберігання і передавання конфіденційної інформації компанії;

- аналітична діяльність з метою виявлення, ідентифікації та прогнозування внутрішніх і зовнішніх загроз ІБ, розробка заходів щодо захисту критичної інформації та засобів її обробки та передавання;

- здійснення систематичного контролю роботи працівників, які мають доступ до конфіденційної інформації, дотримання ними порядку обліку, зберігання та знищення документів та інших носіїв інформації обмеженого доступу (рис. 1.5.).

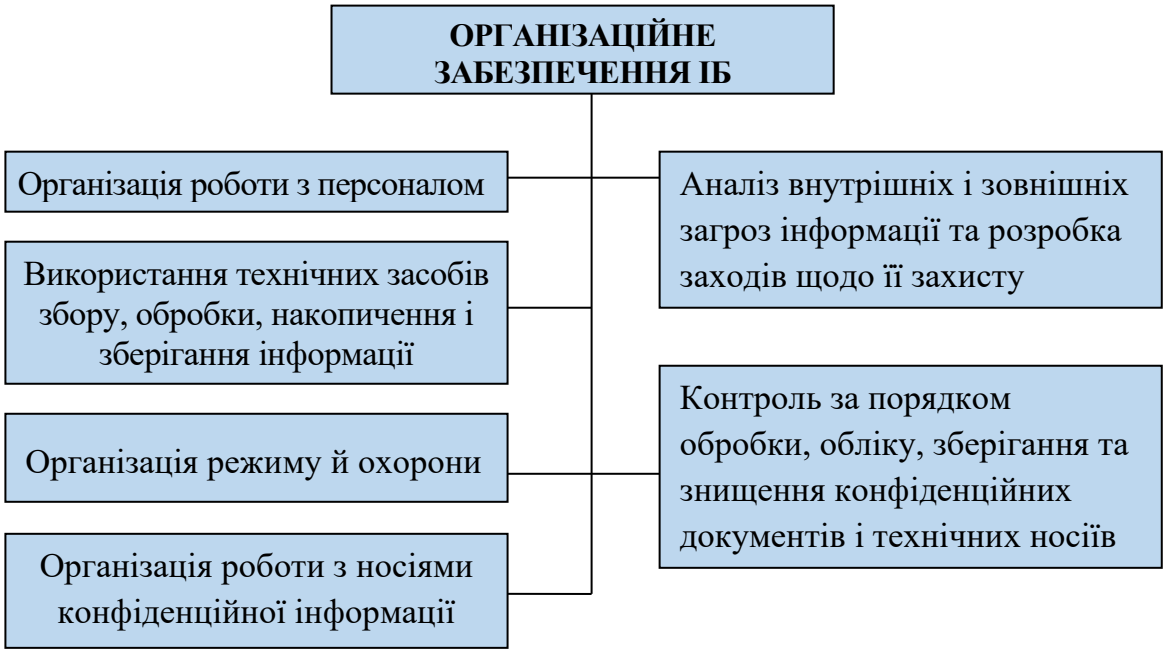

Рис. 1.5. Напрями організаційного забезпечення інформаційної безпеки

При впровадженні СЗІБ та організаційних заходів ІБ зокрема важливим є дотримання кількох основних принципів:

- дотримання комплексного підходу, тобто забезпечення ефективного застосування ресурсів, способів, засобів і методів захисту інформації для ситуаційного вирішення поставлених завдань з урахуванням впливу чинників підсилення або послаблення загроз ІБ;
- принцип адаптивності означає можливості СЗІБ пристосовуватися до динамічного середовища існування підприємства, нових ризиків, загроз і вразливостей і передбачає здійснення постійного комплексного аналізу функціонування СЗІБ з метою його своєчасного коригування, удосконалення й підвищення ефективності;
- оперативність ухвалення управлінських рішень є необхідною, оскільки істотно впливає на ефективність функціонування СЗІБ, дає можливість оперативно реагувати на зміни середовища ІБ та успішно вирішувати завдання щодо захисту інформації та ІТКС компанії;
- розподіл обов'язків і встановлення персональної відповідальності забезпечує найбільш ефективне розподілення повноважень і відповідальності між працівниками у сфері ІБ, перешкоджає розпорошенню відповідальності за критично важливі завдання між різними працівниками і, як наслідок, зменшує ризики порушень ІБ;
- принцип мінімізації привілеїв означає надання працівникам тільки тих прав доступу, які необхідні їм для виконання безпосередніх обов'язків;
- повне дотримання керівниками і працівниками компанії вимог ІБ, а також здійснення постійного контролю й обліку діяльності всіх учасників процесів забезпечення ІБ підприємства.

Останнім часом фахівці визначають ще кілька принципів ЗІБ, зокрема принцип ешелонування, відповідно до якого у нинішніх умовах необхідним є порядок ЗІБ підприємства, за якого всі рубежі системи захисту складаються з послідовно розташованих зон безпеки, найважливіша з яких знаходиться всередині системи.

Принцип безперервності означає, що робота всіх елементів системи ІБ повинна бути безперервною і функціонувати у режимі 24/7.

Принцип розумної достатності передбачає раціональне використання засобів захисту, які гарантують прийнятний рівень безпеки, без ідеї створення абсолютного захисту, що на сьогодні є неможливим. Забезпечення компанії високоефективною СЗІБ передбачає великі матеріальні витрати, що може виявитися не по кишені усім підприємствам [17].

У цьому контексті доцільно згадати, що важливим принципом ІБ є економічна обґрунтованість розробки і впровадження системи заходів ЗІБ, що виражається в тому, що вартість проектування й експлуатації СЗІБ не повинна перевищувати вартість можливих збитків підприємству у разі його функціонування без її впровадження.

Слід зазначити, що якими б досконалими були програмно-технічні засоби захисту інформації від несанкціонованого доступу, без належної організаційної підтримки і точного виконання передбачених проектною документацією процедур проблему забезпечення безпеки інформації в належній мірі не вирішити. Організаційні механізми захисту інформації визначають порядок і умови комплексного використання наявних сил і засобів, ефективність яких залежить від вживаних методів технічного і економічного характеру.

Висновки до розділу 1

Таким чином, СЗІБ як частина загальної системи управління підприємства, що базується на аналізі ризиків і призначена для проектування, реалізації, контролю, супроводу та вдосконалення заходів в галузі ІБ, має гарантувати досягнення таких цілей як забезпечення цілісності й конфіденційності, унеможливлення несанкціонованого доступу до критично важливої інформації підприємства та пов'язаних з нею процесів (створення, введення, обробки і виведення).

Відповідно до комплексного підходу у межах СЗІБ підприємства здійснюються нормативно-правові, організаційні та програмно-технічні заходи. Організаційні заходи ІБ включають забезпечення режиму і охорони, роботу з персоналом та документами, що містять конфіденційну інформацію, використання технічних засобів збирання й обробки конфіденційної інформації, аналіз внутрішніх і зовнішніх загроз ІБ та вироблення заходів щодо забезпечення захисту, систематичний контроль за діяльністю персоналу у сфері ІБ.

Ключова роль ОЗІБ визначається важливістю своєчасного прийняття виважених і обґрунтованих управлінських рішень на основі аналізу поточної ситуації та впливу різних чинників, врахування наявних ресурсів, методів, засобів і способів захисту інформації, прогнозування наслідків управлінського впливу у рамках діючого нормативно-правового й методичного апарату.

РОЗДІЛ 2.
ОРГАНІЗАЦІЯ ДІЯЛЬНОСТІ ПІДРОЗДІЛУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

2.1. Принципи побудови та структура служби інформаційної безпеки підприємства

Одним з найважливіших організаційних заходів є створення спеціальних штатних служб ІБ, захисту інформації в закритих інформаційних системах. Очевидно, що організаційні заходи повинні чітко плануватися, спрямовуватися і здійснюватися організаційною структурою, спеціально створеним для цих цілей структурним підрозділом, укомплектованим відповідними фахівцями з безпеки підприємницької діяльності та захисту інформації.

У законодавчих актах і стандартах з управління ІБ не вказані вимоги до структури, кадрового складу і компетенції служби ІБ, тому ці показники залежать від конкретних завдань із захисту інформації та індивідуальні для кожної організації з урахуванням її специфіки.

Як правило, перелік завдань і функцій служби ІБ визначається розміром організації, кількістю об'єктів, які підлягають захисту, сферою діяльності, особливостями бізнес-процесів організації, актуальними вимогами щодо захисту інформації, в т.ч. і законодавчими.

Результуючий рівень ІБ буде визначатися всім комплексом прийнятих організаційно-технічних заходів, тому важливо охопити всі доступні напрямки захисту інформації. Так, при побудові служби ІБ додатково можуть враховуватися внутрішня культура і традиції організації, корпоративні цінності і інші етичні та психологічні фактори [31].

Служба ІБ є самостійною організаційною одиницею компанії, що підпорядковується безпосередньо керівнику або профільному заступнику, якщо така посада передбачена. Очолює службу безпеки начальник служби.

Організаційна структура служби ІБ має відповідати її завданням і функціям, а також визначати ролі, відповідальність і повноваження персоналу, безпосередньо залученого до вирішення завдань ІБ.

На думку деяких фахівців, найбільш оптимальною є матрична форма структури, оскільки діяльність у сфері ІБ носить як проектний, так і операційний характер, а сама служба ІБ перебуває у стані постійного розвитку.

Кадровий склад служби ІБ визначає компетенцію і можливості служби у вирішенні завдань ІБ. Можна виділити штатних співробітників, які постійно працюють в службі, і залучених осіб, субпідрядників, необхідних тільки на період виконання проектів.

Матеріально-технічна база служби ІБ визначає сукупність технічних засобів, програмних продуктів та необхідного обладнання для вирішення поставлених завдань і обладнання робочих місць для співробітників. Організації необов'язково закуповувати обладнання, яке рідко використовується, допустимо для окремих робіт залучати субпідрядників.

Технології та сервіси служби ІБ визначають різноманітні засоби автоматизації, інформаційні системи і підсистеми управління, такі як контроль якості, технології перевірки та тестування, управління знаннями, аналітичне програмне забезпечення, необхідні для підвищення ефективності й оптимізації СЗІБ.

База знань служби ІБ необхідна для ефективного доступу до різноманітної довідкової інформації, накопиченому раніше досвіду, робочої документації, звітів, а також для підтримки роботи автоматизованих систем.

Оскільки служба ІБ за своїм родом діяльності повинна охоплювати всі бізнес-процеси організації і враховувати всі зміни в роботі організації, важливим завданням є організація та підтримка комунікацій між службою ІБ і об'єктами захисту. Крім того, служба ІБ повинна брати участь (хоча б консультативно) у всіх проектах, що стосуються розвитку і вдосконалення IT-інфраструктури організації [31].

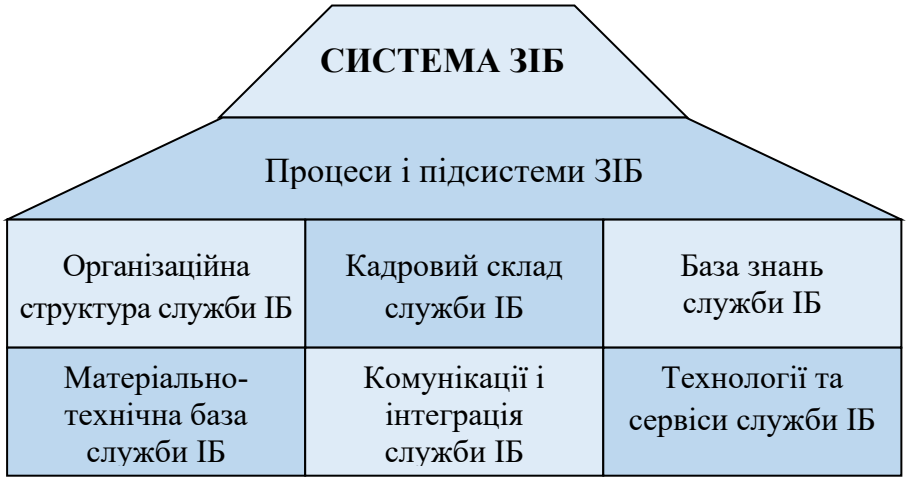

Рис. 2.1. Структура служби ІБ підприємства (за Сафроновим)

Для створення служби ІБ та організації її ефективної діяльності необхідним є дотримання таких принципів [9, 11]:

- чисельність служби ІБ має бути достатньою для виконання покладених на неї функцій;
- служба ІБ має підпорядковуватися посадовій особі, яка несе персональну відповідальність за питання забезпечення ІБ на підприємстві;
- штатний склад служби ІБ не має мати інших повноважень, пов’язаних з роботою ІС;
- співробітники мають мати право доступу в усі приміщення, де знаходиться апаратура щодо обробки та захисту інформації, право припиняти роботу автоматизованої системи обробки інформації у випадку виникнення загрози для конфіденційної інформації, право не допускати до роботи нові елементи ІС, якщо вони не відповідають вимогам захисту інформації;
- служба ІБ має мати усі умови та можливості для виконання своїх функцій.

Організаційно служба ІБ може складатися з таких структурних одиниць:

підрозділу режиму і охорони;

спеціального підрозділу обробки документів конфіденційного характеру;

інженерно-технічних підрозділів;

інформаційно-аналітичних підрозділів.

Можливим є наявність підрозділу економічної розвідки та контррозвідки [27].

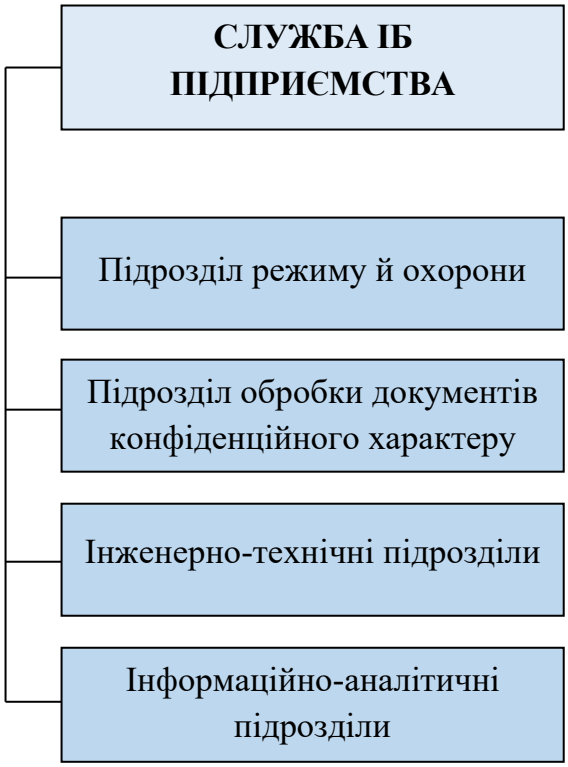

Рис. 2.2. Структура служби ІБ підприємства (за Ортинським)

Відділ режиму та охорони є самостійним структурним підрозділом служби безпеки і підпорядковується начальнику служби безпеки. Серед його завдань організація та підтримка пропускного режиму, організація проходу співробітників і відвідувачів в різні зони доступу, організація охорони конфіденційних приміщень та особистої охорони керівників та провідних співробітників, забезпечення безпеки транспортування вантажів і документів тощо.

Підрозділ обробки документів конфіденційного характеру займається питаннями обліку, збереження, використання, передачі та знищення конфіденційних документів, в тому числі розробкою відповідних інструкцій та контролем за їх дотриманням з боку задіяних працівників.

Основним завданням інженерно-технічних груп є забезпечення безпеки діяльності підприємства за допомогою технічних засобів захисту, зокрема

визначення меж охоронюваної (контрольованої) території з урахуванням можливостей технічних засобів, спостереження зловмисників; визначення технічних засобів, що використовуються для передачі, прийому та обробки конфіденційної інформації в межах контрольованої території зони; обстеження виділених приміщень, виявлення та оцінка ступеня небезпеки потенційних технічних каналів витоку інформації; розробка заходів щодо ліквідації (локалізації) встановлених каналів витоку інформації з використанням фізичних, апаратних і програмних засобів та математичних методів захисту [3].

Для ефективного ЗІБ підприємницької діяльності необхідно, щоб у складі служби ІБ функціонував інформаційно-аналітичний підрозділ, завданнями якого є збір усіх видів інформації, що стосується діяльності та відповідного її захисту від розповсюдження; аналіз інформації, що отримується; прогнозування тенденцій розвитку наукового і технологічного процесу в сфері технологій діяльності підприємства; оцінювання рівня ІБ підприємства за всіма її складовими, розроблення рекомендацій для його підвищення тощо.

Часто на практиці служба ІБ є підрозділом, що входить як структурна одиниця в департамент (управління) безпеки підприємства. Співробітники служби знаходяться в адміністративному та функціональному підпорядкуванні у керівника департаменту, який несе відповідальність за ЗІБ на підприємстві.

Виведення служби ІБ зі структури ІТ-служб на підприємствах є однією з важливих сучасних тенденцій в управлінні бізнесом, ІТ та ІБ, тому що, на думку деяких фахівців, у цих підрозділів є деякі частково взаємно суперечливі інтереси і тому деякі завдання не можуть бути ефективно вирішені в рамках одного структурного підрозділу.

У складі служби ІБ для підвищення ефективності роботи можуть бути виділені самостійні групи (відділи), що спеціалізуються на виконанні певних функцій:

- відділ нормативної (організаційної) документації;
- відділ адміністрування інформаційних систем;

• відділ впровадження інформаційних систем і систем захисту інформації ;

• відділ аудиту ІБ.

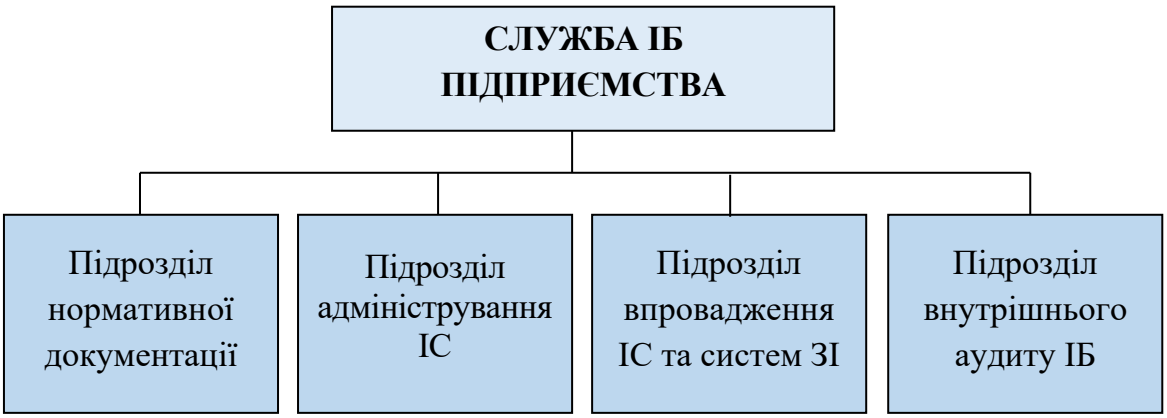

Рис. 2.3. Структура служби ІБ підприємства (за Балашовим)

Відділ нормативної документації вирішує завдання, пов'язані з формуванням, підтримкою і документальним забезпеченням політики ІБ підприємства, і повинен, головним чином, включати в себе фахівців з менеджменту та бізнес-аналізу, що пройшли додаткову підготовку в сфері ІБ. Також до складу такого відділу можуть входити юристи. Аналогічний кадровий склад може бути і у відділу внутрішнього аудиту ІБ. При цьому до кваліфікації співробітників відділу нормативної документації, як правило, повинні пред'являтися набагато вищі професійні вимоги.

Відділ адміністрування інформаційних систем, а також відділ впровадження інформаційних систем і систем захисту інформації, як правило, мають включати в себе фахівців з ІТ та засобів захисту інформації, які мають значний досвід впровадження та експлуатації корпоративних інформаційних систем.

На думку вітчизняного фахівця з ІБ В. Домарєва [11], в структуру служби ІБ мають входити:

• керівник служби, підпорядкований безпосередньо керівнику компанії;

• заступник керівника служби, який часто керує системами фізичного і або технічного захисту підприємства;

• юрист;

- аналітик;
- спеціалісти у сфері ІБ, економічної розвідки, контррозвідки;
- технічні фахівці у сфері захисту інформації;
- співробітники охорони та пропускного режиму (наймані працівники), які підпорядковуються керівнику служби ІБ.

2.2. Типові функції служби інформаційної безпеки підприємства

У сучасному поданні функцій служби ІБ можна виділити такі напрями:

- формування, підтримка і документальне забезпечення корпоративної політики ІБ;
- розробка методології та методик аналізу загроз, оцінки рівня ІБ підприємства і системи її забезпечення;
- організація і здійснення конкретних видів діяльності із захисту інформації з персоналом, іншими підрозділами, партнерами;
- робота з конфіденційними документами;
- експлуатація технічних засобів захисту інформації: адміністрування ІС і систем захисту інформації, впровадження засобів захисту інформації;
- аудит і контроль функціонування системи ІБ;
- забезпечення внутрішнього та пропускного режимів і охорони підприємства (Рис. 2.4).

Функції, пов'язані з ***формуванням, підтримкою і документальним забезпеченням політики ІБ підприємства***, можуть включати в себе:

- консультування керівників і власників підприємства з питань розробки та вдосконалення політики ІБ;
- самостійна розробка політики ІБ, її узгодження і подання її керівництву підприємства для затвердження, а також внесення необхідних змін у міру зміни умов роботи підприємства;

Рис. 2.4. Функції служби ІБ підприємства

• самостійна розробка політик ІБ, що стосуються окремих питань захисту інформації (правил застосування ІКТ, вимог, обов'язкових для всіх використовуваних на підприємстві персональних комп'ютерів тощо);

• формування вимог і регламенту процедур перегляду політики ІБ, окремих правил, типових форм та інших документів;

• аналіз окремих договорів і угод зі сторонніми організаціями (постачальниками, покупцями, партнерами тощо) на предмет відповідності вимогам політики ІБ;

• аналіз та узагальнення передового досвіду та сучасних теорій у сфері ІБ з метою їх практичного застосування на підприємстві;

• залучення сторонніх фахівців, дослідників, консультантів (консалтингових компаній) для розробки та вдосконалення корпоративної політики ІБ та впровадження передових методів ЗІБ;

• організація навчання персоналу компанії (контроль за повнотою та правильністю матеріалів навчальних програм, пов'язаних з ІБ, забезпечення своєчасності проходження навчання тощо);

• консультування фахівців та керівників підрозділів підприємства з питань відповідності розроблюваних внутрішніх документів окремих підрозділів вимогам політики ІБ підприємства;

• контроль відповідності внутрішніх організаційних документів підприємства (правил внутрішнього розпорядку, посадових інструкцій, інструкцій з використання ІС, типових форм договорів тощо) вимогам політики ІБ, а також узгодження таких документів при їх затвердженні;

• розробка, ведення, оновлення та поповнення «Переліку відомостей конфіденційного характеру» та інших нормативних актів, що регламентують порядок забезпечення ІБ та захисту інформації [9, 17, 25].

У рамках напряму - ***розробка методології та методик аналізу загроз, оцінки рівня ІБ підприємства і системи її забезпечення*** - мають розв’язуватися такі основні завдання:

• 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 ризиків ІБ;

• інформаційне обстеження підприємства та інформаційних ресурсів;

• розробка методів захисту інформації та ІТ і методик їх упровадження в діяльність підприємства;

• 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 з зовнішніми організаціями;

• аналіз нормативних документів організації у контексті ІБ, зокрема 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.

Окремим блоком функцій у рамках зазначеного напряму є функції, пов’язані з виявленням суб’єктів, потенційно зацікавлених в отриманні конфіденційної інформації підприємства, зокрема:

• визначення кола осіб, які в силу займаного службового становища на підприємстві прямо або побічно мають доступ до конфіденційних відомостей;

• визначення кола сторонніх підприємств, пов'язаних з даним підприємством кооперативними зв'язками, на яких в силу виробничих відносин можливий вихід з-під контролю відомостей конфіденційного характеру;

• виявлення кола осіб, не допущених до конфіденційної інформації, але які виявляють підвищений інтерес до таких відомостей;

• виявлення кола підприємств, у тому числі й іноземних, зацікавлених в оволодінні охоронюваними відомостями з метою нанесення економічних збитків даному підприємству, усунення економічного конкурента або його компрометації [9, 17, 25].

Функції з ***організації і здійснення конкретних видів діяльності із захисту інформації*** передбачають у загальному керівництво роботами з організаційного регулювання відносин щодо захисту інформації і включають:

• планування на основі координації діяльності всіх підрозділів із ЗІБ підприємства;

• організація й участь у впровадженні методів ЗБ в діяльність підприємства.

• узгодження заявок на доступ і порядку доступу співробітників і зовнішніх організацій до інформаційних ресурсів підприємства, процедур інформаційної взаємодії підрозділів із зовнішніми організаціями, договорів, за якими здійснюється інформаційна взаємодія, проектів наказів, розпоряджень, інших нормативно-розпорядчих документів;

• здійснення керівництва службами та підрозділами ІБ підвідомчих підприємств, організацій, установ та іншими структурами в частині обумовлених у договорах умов щодо захисту конфіденційної інформації;

• організація та регулярне проведення обліку співробітників підприємства і служби ІБ за всіма напрямками захисту інформації та забезпечення безпеки виробничої діяльності;

• розв’язання поточних практичних питань з ІБ, що виникають у підрозділах.

Масштабним блоком функцій у рамках цього напряму є робота з персоналом, а також усіма причетними до організації суб’єктами, який передбачає зокрема:

• перевірку представником служби ІБ кандидата на зайняття посади і участь у співбесіді з ним, співбесіду з працівником, що звільняється та відстеження його подальших дій, потенційних можливостей розголошення ним конфіденційної інформації, що є власністю підприємства;

• навчання основам ІБ новоприйнятих працівників та сторонніх фахівців за контрактом;

• проведення регулярних навчань, тренінгів, інструктажів з персоналом підприємства з питань ІБ;

• проведення аналізу психологічного клімату в колективі, взаємовідносин між працівниками, пошук прихованих мотивацій для потенційного розголошення таємниці підприємства, облік порушень у сфері ІБ з боку персоналу тощо [8].

Варто відзначити, що ця робота проводиться спільно з іншими підрозділами підприємства, насамперед відділом управління персоналом, психологічною службою (за наявності), іншими службами підприємства.

Організація роботи з конфіденційними документами передбачає формування службою ІБ системи контролю і обліку конфіденційних документів, організацію і ведення конфіденційного діловодства, зокрема:

• розробка, ведення, оновлення та поповнення «Переліку відомостей конфіденційного характеру» та інших нормативних актів у сфері конфіденційного діловодства.

• здійснення обліку усієї документації підприємства з класифікацією за сферою застосування, датою, змістом тощо; реєстрацію і облік усіх вхідних/вихідних документів підприємства, документів, з яких роблять копії; облік даних про особливий режим знищення документів.

• розробка і здійснення спільно з іншими підрозділами заходів щодо забезпечення роботи з документами, що містять конфіденційні відомості;

• організація і контроль виконання вимог щодо роботи з джерелами конфіденційної інформації при всіх видах робіт [9, 17].

У рамках напряму з ***експлуатації технічних засобів захисту інформації*** виконуються такі основні завдання:

1) із впровадження засобів захисту інформації:

• аналіз сучасних програмних і апаратних засобів захисту інформації та пов'язаних з ними методик захисту, а також ринку доступних засобів захисту інформації, застосовуваних для різних цілей, і підготовка обґрунтованих пропозицій щодо придбання певних продуктів у певних постачальників;

• аналіз закуповуваних ІС (операційних систем, прикладних програм, телекомунікаційного устаткування, обчислювальної техніки тощо) на предмет їх потенційної надійності та наявності вразливостей;

• залучення сторонніх експертів і консультантів для аналізу закуповуваних і використовуваних засобів захисту інформації з точки зору їх надійності, а також з точки зору доцільності їх застосування (впровадження);

• формулювання вимог (пов'язаних із забезпеченням ІБ) до програмних продуктів, які розробляються організацією самостійно або створюються на замовлення сторонніми розробниками;

• участь у проектуванні нових ІС, а також тестуванні знову розроблених і впроваджуваних програмних продуктів;

• розробку техніко-економічного обґрунтування для проектів впровадження засобів захисту інформації, а також залучення для цих цілей сторонніх аналітиків і консультантів, що спеціалізуються на питаннях аналізу засобів захисту інформації;

• підготовку обґрунтованих рішень про вибір між самостійною розробкою засобів захисту інформації (наприклад, програмних модулів, що здійснюють шифрування даних) і передачею їх розробки стороннім компаніям.

2) з адміністрування ІС і систем захисту інформації:

• виконання деяких функцій з адміністрування окремих ІС (баз даних, систем колективної роботи з документами, поштових систем тощо), а також адміністрування та конфігурування систем захисту інформації (міжмережевих екранів, систем виявлення вторгнень тощо);

• визначення необхідних типових налаштувань і конфігурацій робочих станцій (персональних комп'ютерів), що мають відношення до ІС підприємства (зокрема, підключених до його локальної мережі);

• залучення сторонніх організацій для здійснення поточного адміністрування ІС і систем захисту інформації, а також для консультаційної та технічної підтримки при виникненні інцидентів, пов'язаних з ІБ (зокрема, при здійсненні нападів на ІС підприємства);

• установку (в тому числі і спільно з фахівцями ІТ-підрозділу) програмних і апаратних засобів захисту інформації на робочі місця користувачів і в інші елементи ІС;

• консультування користувачів з виникаючих питань, пов'язаних з ІБ, і оперативне вирішення виникаючих у них проблем;

• реагування на різні інциденти, пов'язані з порушенням ІБ;

• прийняття активних зустрічних заходів при виявленні вторгнень в ІС (інформування правоохоронних органів, самостійний пошук нападників і т.п.);

• генерування паролів користувачів ІС та забезпечення їх збереження;

• участь у відновленні працездатності ІС після збоїв і порушень в роботі [9, 17, 25].

Заходи в рамках напряму з ***аудиту і контролю функціонування СЗІБ підприємства*** передбачають:

• збір та аналіз відомостей про порушення різних вимог політики ІБ, що надходять з різних джерел (у тому числі і від адміністраторів ІС) і визначення пріоритетних напрямів контрольної роботи;

• перевірку організаційної документації окремих підрозділів підприємства на предмет відповідності вимогам політики ІБ (в тому числі і своєчасності внесення всіх необхідних змін в діючі внутрішні організаційні документи);

• перевірку стану (правильності ведення) поточної господарської та кадрової документації окремих підрозділів підприємства, пов'язаної із ЗІБ (правильності і своєчасності заповнення журналів, своєчасність оформлення зобов'язань про нерозголошення відомостей співробітниками тощо);

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

• моніторинг дій користувачів ІС (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 ІС;

• блокування облікових записів звільнених (переведених на іншу роботу) користувачів;

• контроль дотримання налаштувань безпеки, включаючи парольну політику, інші вбудовані системи ІБ, зовнішні засоби захисту інформації;

• моніторинг роботи систем виявлення (запобігання) мережних атак, систем оцінки якості побудови мережі й інших автоматизованих систем комп'ютерної безпеки;

• організацію контрольних перевірок захищеності окремих елементів ІС (серверів, сегментів мережі тощо);

• проведення внутрішнього та комплексних аудитів ІБ на підприємстві;

• залучення сторонніх організацій для проведення аудитів ІБ на підприємстві, перевірок надійності ІС.

• підготовка пропозицій щодо використання зовнішнього аудиту [18].

Також діяльність з аудиту і контролю СЗІБ підприємства включає:

• вивчення всіх сторін виробничої, комерційної, фінансової та іншої діяльності для виявлення і подальшої протидії будь-яким спробам нанесення збитку у сфері ІБ, ведення обліку та аналізу порушень режиму ІБ, накопичення та аналіз даних про злочинні наміри конкурентної та інших організацій, про діяльність підприємства і його клієнтів, партнерів, суміжників; підготовка пропозицій щодо попередження порушень;

• організація та проведення службових розслідувань за фактами розголошення відомостей, втрат документів, витоку конфіденційної інформації та інших порушень безпеки підприємства;

• підтримка контактів з правоохоронними органами та службами безпеки сусідніх підприємств в інтересах ІБ і надання взаємної допомоги в кризових ситуаціях.

Крім перерахованих функцій, безпосередньо пов'язаних із захистом інформаційних ресурсів, велике значення має також виконання функцій, пов'язаних з ***організацією внутрішнього та пропускного режиму й охорони***

підприємства і вирішенням завдань, які пов'язані з забезпеченням безпеки підприємства в більш широкому сенсі. Зокрема, для ЗІБ має значення виконання таких функцій, як:

• охорона території та майна підприємства, а також охорона персоналу;

• забезпечення пропускного та внутрішнього режиму на території, у будівлях та приміщеннях, контроль дотримання вимог режиму співробітниками, суміжниками, партнерами та відвідувачами;

• ведення обліку та суворого контролю виділених для конфіденційної роботи приміщень, технічних засобів в них, що володіють потенційними каналами витоку інформації і каналами проникнення до джерел конфіденційної інформації;

• визначення на підприємстві ділянок, технологічного обладнання, уразливих в аварійному відношенні, вихід з ладу яких може завдати матеріальної шкоди підприємству;

• спостереження за територією і приміщеннями (у тому числі за допомогою відеокамер);

• контроль за ввезенням на територію підприємства і вивезенням готової продукції, матеріалів, документів та іншого майна;

• контроль за дотриманням часового режиму роботи, а також за дотриманням правил внутрішнього розпорядку [26].

Висновки до розділу 2

Таким чином, у результаті дослідження з’ясовано, що служба ІБ є самостійною організаційною одиницею підприємства, що підпорядковується безпосередньо керівнику підприємства.

Організаційна структура служби ІБ формується у відповідності із її завданнями і функціями, серед яких доцільно виділити такі як: формування, підтримка і документальне забезпечення політики ІБ підприємства; розробка

методології та методик аналізу загроз, оцінка рівня ІБ підприємства і системи її забезпечення; організація і здійснення конкретних видів діяльності із захисту інформації з персоналом, іншими підрозділами підприємства, партнерами; робота з конфіденційними документами; експлуатація технічних засобів захисту інформації; аудит і контроль функціонування системи забезпечення ІБ підприємства; забезпечення внутрішнього та пропускного режимів і охорони.

З огляду на виділені функції служба ІБ має включати інформаційно-аналітичні відділи (зокрема нормативної документації, аудиту ІБ); інженерно-технічні підрозділи (адміністрування та впровадження ІС та систем захисту інформації, інші); відділ роботи з персоналом; відділ конфіденційного діловодства (за потреби); службу режиму й охорони.

РОЗДІЛ 3.
ЗАБЕЗПЕЧЕННЯ РЕЖИМУ Й ОХОРОНИ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

3.1. Організація внутрішнього і пропускного режимів на підприємстві

Впровадження внутрішнього (внутрішньо-об'єктного) режиму є необхідним у випадках, коли підприємство працює з конфіденційною інформацією. Це означає, що потреба в організації спеціального режиму роботи є у кожної компанії, оскільки фактично всі підприємства володіють комерційною таємницею або розпоряджаються персональними даними персоналу і клієнтів.

Внутрішній і пропускний режими – це важливі елементи системи захисту інформації підприємства.

Організація внутрішньо-об'єктного режиму

Внутрішній режим - комплекс заходів, які мають на меті забезпечення належного режиму секретності безпосередньо в структурних підрозділах, на об'єктах і в службових приміщеннях підприємства, схоронності матеріальних цінностей, інформаційних ресурсів, фізичної і пожежної безпеки, особистої безпеки персоналу.

Внутрішньо-об'єктний режим передбачає:

- розробку і впровадження розпорядку роботи на внутрішніх об'єктах компанії;

- формування обмежень щодо допуску персоналу до режимних приміщень підприємства;

- визначення обов'язків працівників підприємства щодо дотримання вимог внутрішньо-об'єктного режиму і встановлення відповідальності за його порушення;

- розробку і забезпечення дотримання процедур щодо

відмикання, замикання і здачу під охорону робочих приміщень;

видачі і зберігання ключів від робочих приміщень, печаток для опечатування дверей робочих приміщень;

користування індивідуальними картками для доступу на територію чи в режимні приміщення підприємства через автоматизовані системи доступу;

дій персоналу та працівників охорони у випадку виявлення пошкоджень відбитків печаток, втрати карток, перепусток, ключів, або металевих печаток, відмов у роботі індивідуальних карток;

дій персоналу і працівників охорони у разі виникнення позаштатних ситуацій (пожежі, стихійні лиха, напад на режимні об’єкти тощо);

доступу у режимні приміщення в неробочий час, святкові і вихідні дні.

Організація пропускного режиму

Пропускний (контрольно-пропускний) режим передбачає встановлення належного порядку доступу на територію підприємства через контрольно-пропускні пункти, який унеможливлює безконтрольний вхід (вихід) на територію підприємства, режимні приміщення та з метою несанкціонованого відвідування персоналу.

Пропускний режим встановлює порядок пропуску працівників об’єкта, відвідувачів, транспорту і матеріальних засобів і включає комплекс організаційних заходів адміністративно-обмежувального характеру, інженерно-технічних рішень і дій служби безпеки.

Організація пропускного режиму включає розробку і впровадження порядків і процедур щодо:

- приймання відвідувачів і видачі перепусток;
- пропуску осіб;
- пропуску транспортних засобів і матеріальних цінностей;
- документування випадків порушень пропускного режиму.

Засобами організації пропускного режиму є функціонування стаціонарних постів (пропускних пунктів) та використання відповідних технічних засобів відповідно до внутрішнього розпорядку роботи.

Організація контрольно-пропускного режиму характеризується певними особливостями. Зокрема, механізм здійснення контрольно-пропускного режиму ґрунтується на використанні обмежень і заборон щодо осіб, які перетинають межі об’єктів під охороною, з метою забезпечення інтересів підприємства. Такий механізм має повною мірою відповідати вимогам чинного законодавства [4].

Обов’язковою умовою функціонування ефективного пропускного режиму є дотримання переліку вимог, серед яких розробка і дотримання інструкції про пропускний режим, де визначається система організаційно-правових заходів, що встановлюють дозвільний порядок (режим) проходу (проїзду) на об’єкт (з об’єкта); встановлення персональної відповідальності керівників, у повноваження яких входять питання організації і практичного керівництва контрольно-пропускною системою.

Важливим напрямом забезпечення пропускного режиму є розробка і забезпечення дотримання вимог щодо пропуску працівників підприємства, відряджених осіб і відвідувачів через контрольно-пропускні пункти (КПП), допуску на об’єкт транспортних засобів, вивезення документів і матеріальних цінностей, а також обліку і звітності, зберігання печаток, індивідуальних карток, перепусток та інших засобів обмеження доступу.

Створюючи систему пропускного режиму компанії необхідно чітко визначити вимоги до обладнання контрольно-пропускних пунктів. Обов’язковими елементами обладнання КПП є:

· засоби механізації, автоматизації системи контролю доступу;

· фізичні бар’єри (огорожі, турнікети, хвіртки);

· основне і резервне електропостачання;

· засоби зв’язку й аварійної сигналізації;

· системи відеоспостереження [26].

Інколи КПП доповнюють внутрішніми системами контролю доступу (СКД) до певних об’єктів або приміщень.

Електронні СКД можуть бути: аудіовізуальними, тобто передавати зображення за допомогою спеціальних камер; такими, що працюють з пластиковими картами (в тому числі - безконтактними); заснованими на введенні ідентифікаційних кодів з клавіатури; біометричними (сканують сітківку ока або відбитки пальців). Комбінація контролера з виконуючим пристроєм, може перевіряти інформацію в електронному пропуску, надаючи можливість проходу, якщо дана особа має право доступу. Це можуть бути: турнікети; шлюзи; електромеханічні замки; ростові кабінки [7].

Основною метою впровадження внутрішнього і пропускного режимів на підприємстві є забезпечення дотримання персоналом компанії, відрядженими особами та відвідувачами належного режиму секретності.

Режим секретності - це встановлений нормативними документами компанії єдиний порядок забезпечення безпеки відомостей обмеженого доступу (комерційна таємниця, службова інформація, персональні дані тощо), які належать або обробляються підприємством. Режим секретності є системою адміністративно-правових, організаційних, інженерно-технічних та інших заходів.

Отже, внутрішній і пропускний режими є невід’ємною частиною СЗІБ підприємства, спрямованою на захист конфіденційної інформації та її носіїв.

Основні напрями організації внутрішнього та пропускного режимів підприємства показані на рис. 3.1.

Основними *заходами з організації внутрішнього та пропускного режимів* на підприємстві є:

• віднесення конфіденційних відомостей до різних категорій обмеженого доступу;

• виявлення можливих каналів витоку конфіденційних відомостей, планування та реалізація комплексу заходів, спрямованих на запобігання витоку конфіденційних відомостей, і втрат носіїв цих відомостей;

Рис. 3.1. Напрями організації пропускного та внутрішнього режимів

• розробка системи організаційних і технічних заходів, що регламентують внутрішній режим підприємства, і контроль за їх виконанням;

• визначення загальних вимог та забезпечення режиму секретності та порядку роботи співробітників підприємства з носіями відомостей, що містять конфіденційну інформацію, відповідно до положень нормативних документів підприємства та законодавства;

• участь у визначенні внутрішнього розпорядку та регламенту підприємства;

• допуск і безпосередній доступ працівників підприємства до інформації обмеженого доступу (їх носіїв), обмеження кола осіб, що допускаються до цих даних;

• організація контролю з боку посадових осіб і структурних підрозділів ІБ за виконанням вимог внутрішнього режиму на підприємстві;

• проведення роз'яснювальної роботи серед персоналу, допущеного до роботи з конфіденційною інформацією, щодо вимог режиму секретності, підвищення пильності й персональної відповідальності за збереження довірених відомостей;

• розробка вимог до режимних приміщень, проведення їх атестації, здійснення контролю доступу персоналу та відвідувачів в ці приміщення, унеможливлення безконтрольного доступу;

• організація встановлення та експлуатації технічних засобів захисту інформації, здійснення контролю за дотриманням порядку їх використання;

• контроль за порядком виготовлення, обліку, зберігання, використання бланків службових посвідчень, печаток, штампів підприємства;

• організація та ведення обліку порушень вимог режиму секретності, аналіз причин цих порушень, організація та проведення службових розслідувань за фактами порушень внутрішнього режиму на підприємстві;

• проведення аналітичної роботи, вироблення на її основі рекомендацій щодо вдосконалення режиму обмеженого доступу на підприємстві тощо [23, 26].

Загалом внутрішній і пропускний режими на підприємстві організовуються з метою унеможливлення:

• несанкціонованого доступу сторонніх осіб на охоронювану (режимну) територію та об'єкти підприємства, а також у службові приміщення, де проводяться роботи з використанням інформації обмеженого доступу;

• відвідування режимних приміщень без службової необхідності працівниками підприємства, що не працюють у них безпосереднього, а також відрядженими особами, яким не надано право на їх відвідування (роботу в них);

• внесення (ввезення) на територію підприємства недозволених, особистих технічних засобів (кіно-, фото-, відео-, звукозапису апаратури й інших технічних засобів);

• несанкціонованого винесення (вивезення) з території підприємства носіїв конфіденційних відомостей;

• порушення встановленого регламенту службового часу, розпорядку роботи структурних підрозділів ІБ, а також встановленого порядку та режиму роботи працівників підприємства і відряджених осіб з носіями відомостей обмеженого доступу [26].

Порядок організації внутрішнього та пропускного режимів, завдання, які вирішуються посадовими особами та структурними підрозділами підприємства, відображаються у внутрішніх організаційно-розпорядчих документах, що затверджуються керівником підприємства.

У ході формування системи внутрішнього та пропускного режимів обов'язковим є встановлення персональної відповідальності керівників підрозділів, посадових осіб, відповідальних за ІБ та розмежування функцій, покладених на відповідні структурні підрозділи підприємства (служба ІБ, режимно-секретний підрозділ, служба охорони та інші).

Важливим є комплексне використання наявних сил і засобів для вирішення завдань ІБ та повне охоплення всіх напрямків діяльності підприємства, в ході роботи по яких можливий витік конфіденційних відомостей або втрата носіїв інформації обмеженого доступу.

Вимоги до приміщень, в яких проводяться роботи з конфіденційною інформацією або зберігаються носії інформації обмеженого доступу

Організація внутрішнього і пропускного режимів має на меті виключення проникнення сторонніх осіб в режимні приміщення підприємства, а також несанкціонованого відвідування таких приміщень співробітниками підприємства та відрядженими особами, які не мають прямого відношення до здійснюваних у них робіт.

У нормативних документах встановлюється низка вимог до приміщень, де проводяться роботи з використанням інформації обмеженого доступу або зберігаються носії цінної інформації. Завдяки дотриманню цим вимог

зберігається в тамниці факт проведення режимних робіт у зазначених приміщеннях, а також забезпечується надійний захист наявних там носіїв конфіденційної інформації.

Розташування й обладнання режимних приміщень має унеможливлювати безконтрольне проникнення в них сторонніх осіб і гарантувати схоронність носіїв конфіденційної інформації, які перебувають у роботі. Так, вхідні двері таких приміщень обладнуються кодовими та електронними замками, автоматичні турнікети посилюють захист і забезпечують безпеку закритих приміщень в неробочий час. Також можливим є обладнання дверей внутрішніми засувами [10].

Режимні приміщення, де зберігаються носії інформації обмеженого доступу в неробочий час, оснащуються охоронною сигналізацією, яка перебуває у зв’язку з приміщенням вартового, пультом централізованого спостереження служби охорони та черговим на підприємстві. Режимні об’єкти, де знаходяться технічні засоби, проектують, випробовують або експлуатують вироби спеціального призначення, обладнуються відповідно до засад протидії технічним розвідкам та вимог технічного захисту інформації.

У режимні приміщення допускається обмежене коло працівників підприємства, які мають безпосереднє відношення до здійснюваних у них робіт. Крім того, в них допускаються керівник підприємства, його заступник, керівник служби безпеки. Доступ інших працівників підприємства є можливим у випадку крайньої службової необхідності за наявності офіційного дозволу, наданого заступником керівника з питань ІБ, керівником служби безпеки.

Для приймання і видачі носіїв інформації обмеженого доступу в режимних приміщеннях відповідних структурних підрозділів (служби безпеки або окремих її підрозділів) обладнуються спеціальні вікна, які не повинні виходити в місця загального користування, або виділяється частина робочого кабінету, відділена спеціальним бар'єром. Розмір режимних приміщень визначається виходячи з їхніх

функцій. У приміщеннях служби безпеки (чи її підрозділів) виділяються спеціальні кімнати (кабіни) для ознайомлення й роботи з носіями закритої інформації.

У режимних приміщеннях служби безпеки дозволяється працювати тільки з документами, які мають безпосереднє відношення до діяльності підрозділу, забороняється зберігати сторонні предмети. Для зберігання носіїв інформації обмеженого доступу приміщення забезпечуються бажаною кількістю сховищ та сейфів, замки яких передбачають можливість опечатування. Облік сховищ, сейфів і ключів від них здійснює служба безпеки [10].

Сховища, сейфи, а також вхідні двері приміщень, де вони розташовані, обладнуються надійними замками. Передбачено наявність двох різних замків та двох примірників ключів від них, один з яких зберігається в опечатаному пеналі (пакеті) у керівника служби безпеки. Другий примірник ключів в опечатаному вигляді знаходиться у керівника підприємства або його заступника з ІБ [26].

Усі сховища, сейфи і режимні приміщення у кінці робочого дня замикаються і опечатуються різними печатками так, щоб зробити неможливим втручання без пошкодження відтиску печатки. У неробочий час ключі від вхідних дверей режимних приміщень, сховищ і сейфів, які там знаходяться, в окремих опечатаних тубусах (пеналах) передаються на зберігання у службу охорони або черговому по підприємству. В облікових документах зазначається час прийому-здачі та проставляються відповідні відмітки про вмикання та вимикання охоронної сигналізації.

Здачу під охорону і відкривання приміщень здійснюють відповідальні за ці приміщення працівники підприємства на підставі затверджених керівником списків осіб із зразками їхніх підписів. Співробітники підприємства, яким надано право відкривання, здачі під охорону та опечатування приміщень, відповідають за дотримання в цих приміщеннях встановлених вимог режиму секретності.

Перед відкриттям приміщень відповідальні працівники перевіряють цілісність печаток і справність замків. При виявленні порушення цілісності відбитків печаток, пошкодження замків, а також інших ознак, що вказують на можливе проникнення

в ці приміщення або сховища сторонніх осіб, відкриття не здійснюється, а складається відповідний акт, який негайно доводять до відома керівника підприємства, керівника служби безпеки (режимно-секретного підрозділи) та представників органу безпеки. Одночасно забезпечується охорона місця події до прибуття фахівців органу безпеки, відкривати режимні приміщення суворо забороняється. У разі втрати ключа від сховища або від вхідних дверей режимного приміщення у встановленому порядку здійснюють заміну замка чи його секрету [7, 26].

Варто відзначити, що сьогодні для запобігання порушенням захищеності приміщень, де відбувається обробка або зберігання носіїв конфіденційної інформації, а також і для організації пропускного режиму, використовують автоматичні системи контролю доступу, які для відкриття дверей використовують картки з магнітною смугою, електронні кодові замки Keypad (клавіатури для введення пароля) і електронні ключі типу Touch-memory, які потрібно прикласти до спеціального гнізда.

Останнім часом з'явився ще одне винахід - зчитувачі карт Proximity, де в якості ключа використовується безконтактна картка або брелок, який досить піднести до зчитувача на певну відстань, навіть не виймаючи з гаманця або сумки. У порівнянні з магнітними картками в системі Proximity значно вищі ступінь секретності коду і довговічність зчитувача і карти. При втраті картки її код просто вилучається з пам'яті системи.

3.2. Організація охорони об'єктів підприємства

Організація охорони - складова частина загальної системи захисту конфіденційної інформації підприємства. Питання забезпечення надійної охорони території підприємства і його об'єктів нерозривно пов'язані з завданнями організації пропускного режиму на підприємстві. Сили і засоби, що

беруть участь у вирішенні цих завдань, є складовими елементами системи охорони підприємства.

Від ефективності функціонування системи охорони повною мірою залежать можливість і рівень вирішення завдань пропускного та внутрішнього режимів. Системи пропускного та внутрішнього режимів утворюють такі рубежі безпеки (після системи охорони), що запобігають доступу зловмисника до охоронюваної підприємством інформації.

Практика показує, що найчастіше зустрічаються такі причини порушення порядку охорони об'єктів як недооцінка можливих загроз безпеки об'єкта на конкретних рубежах (територіях) охорони; неякісне (недбале) виконання обов'язків співробітниками охорони при несенні чергування; використання порушником (зловмисником) випадкової (нештатної) ситуації.

Окремим випадком у подібній ситуації може бути навмисне створення персоналом служби охорони умов, що сприяють таким зловмисним діям.

З огляду на це основними цілями охорони підприємства є:

- запобігання спробам проникнення сторонніх осіб (зловмисників) на територію (об'єкти) підприємства;
- своєчасне виявлення і затримання осіб, які протиправно проникли (намагалися проникнути) на охоронювану територію;
- забезпечення збереження носіїв конфіденційної інформації та матеріальних засобів, що знаходяться на території і підлягають охороні, і запобігання, таким чином, нанесення шкоди підприємству;
- попередження інцидентів на охоронюваному об'єкті і ліквідація їх наслідків [23].

Особливими об'єктами охорони є керівництво підприємства, персонал, допущений до конфіденційної інформації. Основні цілі охорони керівництва і персоналу підприємства - забезпечення їх особистої безпеки в повсякденних умовах і при виникненні надзвичайних ситуацій, запобігання можливим спробам заволодіння зловмисниками об’єктами, що охороняються, шляхом фізичного та

іншого насильницького впливу на цих осіб, вироблення рекомендацій охоронюваним особам за особливостями поведінки в різних ситуаціях.

Зазначені цілі досягаються в тісній взаємодії з підрозділами внутрішніх справ, органами безпеки, а також підрозділами охорони інших підприємств.

Завдання охорони (Рис. 3.2):

- контроль об'єкта і території, що охороняється, в тому числі території з особливим режимом пропуску, з метою виявлення і запобігання спроб несанкціонованого проникнення на них сторонніх осіб (зловмисників);

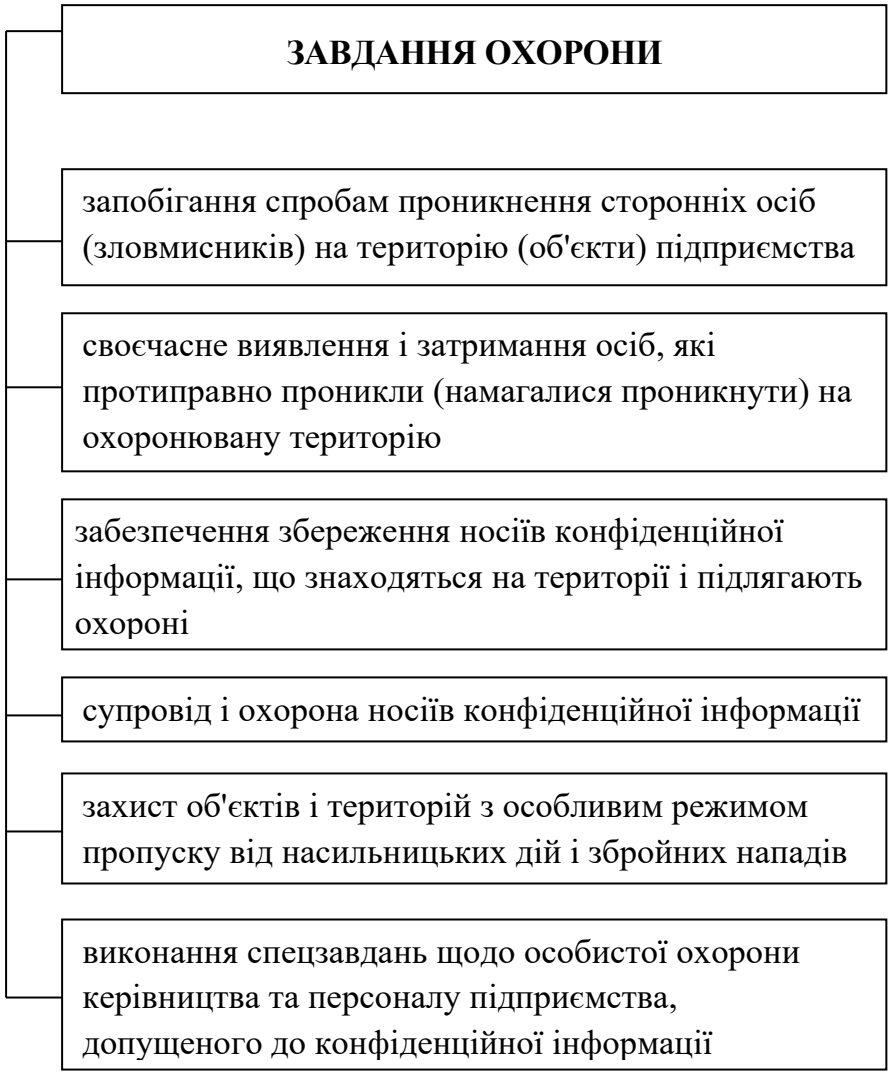

Рис. 3.2. Завдання охорони об’єктів підприємства

- забезпечення конфіденційності та збереження в таємниці фактів проведення закритих заходів на підприємстві (його об'єктах), обговорюваних або розглянутих на них питань;

- супровід і охорона носіїв конфіденційної інформації, в тому числі службових документів підприємства, матеріальних цінностей та вантажів при їх транспортуванні і перевезення (доставки);
- захист об'єктів і територій з особливим режимом пропуску від насильницьких дій і збройних нападів, які можуть завдати шкоди підприємству;
- виконання в необхідних випадках спеціальних завдань із забезпечення особистої охорони керівництва підприємства та персоналу підприємства, допущеного до конфіденційної інформації;
- участь у забезпеченні пропускного режиму для відвідувачів, транспортних засобів та вантажів на території, що охороняється (об'єктах підприємства) з метою встановлення особи та обліку відвідувачів, контролю за ввезенням, вивезенням носіїв конфіденційної інформації, матеріальних цінностей, запобігання їх несанкціонованого переміщення, а також фіксації слідів прихованих і відкритих спроб розкрадання іншого майна підприємства;
- систематичний аналіз ефективності системи охорони, прийнятих посадовими особами заходів з охорони об'єктів підприємства та забезпечення збереження носіїв конфіденційної інформації, матеріальних цінностей і вироблення пропозицій щодо вдосконалення системи охорони;
- співпраця з правоохоронними органам та службами безпеки у вирішенні покладених на них завдань [26].

Для реалізації головних цілей і основних завдань охорони підприємства (його об'єктів) створюється система охорони. *Система охорони підприємства* - сукупність використовуваних для охорони підприємства сил і засобів, а також способів і методів охорони підприємства та його об'єктів.

Вона включає особовий склад підрозділів охорони (караулів); технічні засоби охорони; місця розміщення особового складу, який виконує завдання охорони, і технічних засобів, що використовуються; методи охорони об'єктів. В якості місць розміщення особового складу охорони може бути використаний один з основних елементів системи організації пропускного режиму - КПП.

Для охорони підприємства використовують технічні засоби охорони, які поділяються на дві групи:

- засоби виявлення (пожежна та охоронна сигналізація, «тривожне» оповіщення, охоронне телебачення, охоронне освітлення, апаратура перевірки поштової кореспонденції, радіозв'язок, прямий внутрішній зв'язок, прямий телефонний зв'язок з міліцією та ін.);
- засоби виявлення і ліквідації (засоби пожежогасіння, засоби індивідуального захисту, газові пастки, автотранспорт, зброю, інженерно-технічні засоби та ін.).

Загалом системи охоронної і пожежної сигналізації поєднують використання технічних засобів для:

- виявлення порушень (сповіщувачі);
- збирання й обробки інформації (приймально-контрольні прилади, системи передачі сповіщень тощо);
- оповіщення (звукові та світлові оповіщувачі, модеми та інші).

Відповідно до вітчизняних нормативних документів встановлення охоронної сигналізації здійснюється за трьома рубежами. Зазвичай першим кордоном охоронної сигналізації захищають периметр будівель (двері, вікна, стіни, стелі, підлоги, вентиляційні канали та інші елементи будівель, доступні для проникнення ззовні). Другий рівень охоронної сигналізації захищає внутрішні об'єми, площі та внутрішні двері приміщень, а третій - безпосередньо матеріальні цінності: сховища, сейфи, металеві шафи та ящики, у випадку ІБ – критичні інформаційні ресурси та засоби їх обробки, важливі елементи ІТКС.

Для охорони підприємств та їх об'єктів створюються штатні підрозділи охорони, які організаційно можуть бути об'єднані в службу охорони. Служба охорони включає пости охорони, групи (підрозділу) співробітників охорони (у тому числі підрозділ особистої охорони керівництва та персоналу), групу охорони та супроводу конфіденційних документів, матеріальних цінностей та

вантажів, «тривожну» групу (групу швидкого реагування), а також підрозділи сторожових собак (при необхідності).

Однак досить часто підрозділи охорони разом з іншими підрозділами, що вирішують завдання з різних напрямків захисту інформації, об'єднуються в службу безпеки підприємства.

Охорона підприємства може забезпечуватися не тільки шляхом створення підрозділів охорони, а й шляхом використання послуг приватних охоронних підприємств, що мають право відповідно до законодавства здійснювати цей вид діяльності.

Для організації охорони підприємства можуть бути також використані сили і засоби підрозділів позавідомчої охорони при органах внутрішніх справ [13].

Головна вимога, що висувається до системи охорони підприємства та його об'єктів, - її надійність, яка досягається ефективним застосуванням сил і засобів охорони, правильною організацією і пильним несенням служби працівниками охорони (особовим складом караулів) на постах охорони.

Вибір конкретних сил і засобів, що застосовуються для охорони об'єкта підприємства, здійснюється на основі аналізу можливих загроз його безпеці. Важливе значення при цьому має рівень підготовки і професіоналізм співробітників охорони, що безпосередньо несуть чергування. Наявність конкретних загроз і можливість їх реалізації в конкретній обстановці є найважливішими факторами, що впливають на прийняття керівництвом підприємства рішення про вибір сил і засобів охорони його об'єктів.

Висновки до розділу 3

Встановлено, що питання організації внутрішнього та пропускного режиму, забезпечення охорони території компанії та її об'єктів нерозривно пов'язані і становлять складову СЗІБ підприємства.

Внутрішній і пропускний режими на підприємстві організовуються з метою виключення несанкціонованого проходження на територію та об'єкти підприємства сторонніх осіб та персоналу, які не мають прав доступу; внесення на територію підприємства недозволених, особистих технічних засобів; несанкціоноване винесення з території підприємства носіїв конфіденційних відомостей; порушення встановленого регламенту службового часу, розпорядку роботи структурних підрозділів ІБ, а також встановленого порядку та режиму роботи працівників компанії і відряджених осіб з носіями конфіденційних даних.

Заходи з охорони мають на меті запобігання спробам проникнення сторонніх осіб на територію (об'єкти) підприємства; своєчасне виявлення і затримання осіб, які протиправно намагалися проникнути на охоронювану територію; забезпечення збереження носіїв конфіденційної інформації та матеріальних засобів, що знаходяться на території і підлягають охороні; попередження інцидентів на об'єктах ІБ та ліквідація їх наслідків.

РОЗДІЛ 4.
НОВІ ПІДХОДИ ДО ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

4.1. Методика організації інформаційної безпеки ADDME від IBM ISS

Практика ЗІБ свідчить, що без всебічного комплексного підходу, який встановлює єдину політику безпеки і строгий поточний контроль, практично неможливо досягти належного рівня захищеності інформаційного середовища підприємства. Постійний розвиток ІТ викликає цілий ряд нових проблем. З появою нових неврахованих загроз і вразливостей СЗІБ стає значно важче забезпечити захищеність інформаційних активів та корпоративних ІТКС.

Багато різних експертних організацій (ISO, ITIL, NIST та інші) постійно працюють над удосконаленням методів організації ІБ для того, щоб відповідати нових викликам інформаційної сфери. Аналогічну позицію зайняли й провідні виробники програмного й апаратного забезпечення із захисту інформації, пропонуючи власні всеохоплюючі рішення для забезпечення ІБ. Так, експерти компанії Internet Security Systems, постачальника програмного забезпечення для безпеки, яка стала частиною IBM у 2006 році, здійснили аналіз особливостей забезпечення ІБ на початку XXI ст. і запропонувала свій підхід до вирішення існуючих проблем у цій сфері [39].

Аналітики IBM ISS дійшли висновку, що найбільшою проблемою ІБ залишається складність, а ключем до управління вартістю та складністю ІТ-ландшафту, який постійно розвивається є інтеграція.

Ключовими чинниками, які треба враховувати, прагнучи досягнути стану захищеності інформаційних активів підприємства, визначено: 1) загрози, які постійно вдосконалюються; 2) технології, які активно розвиваються; 3)

зростаючі вимоги щодо нормативної відповідності; 4) зростаючі бізнес-потреби та 5) зростаюча економіка (Рис. 4.1).

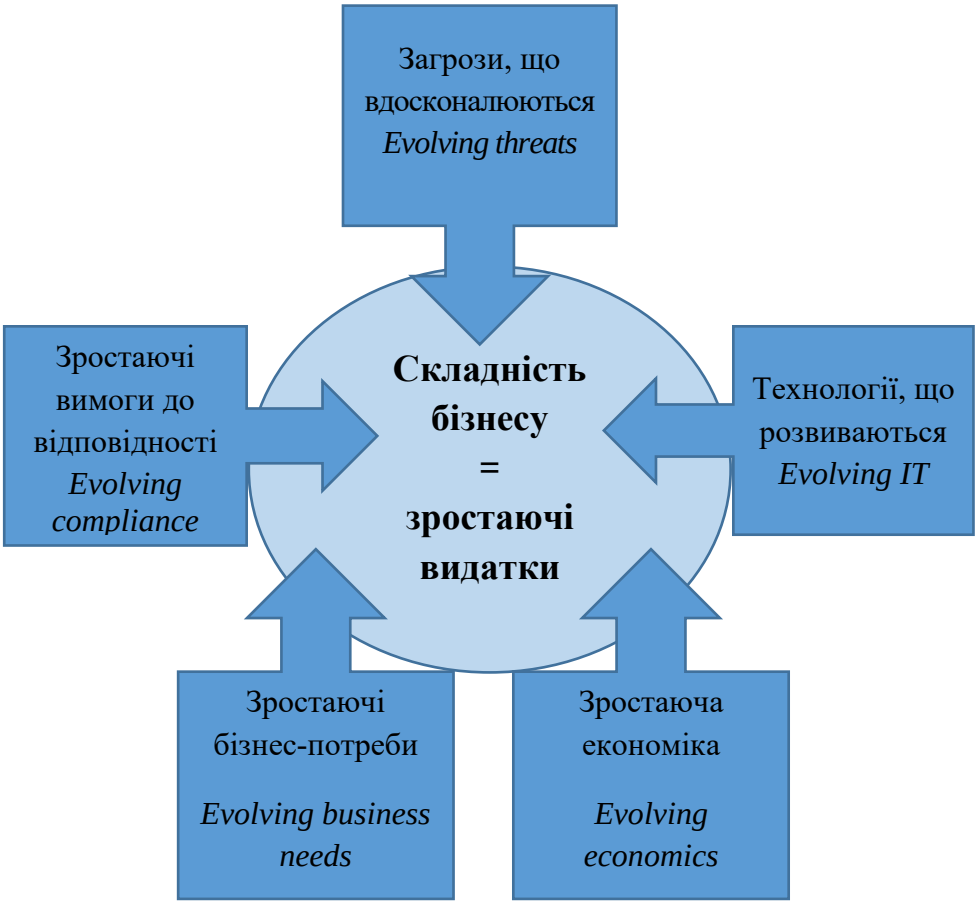

Рис. 4.1. Особливості ІБ підприємства у сучасних умовах від IBM ISS

В огляді від IBM ISS зазначено, що сучасне підприємство існує в умовах, коли щораз постає величезна кількість нових ризиків ІБ, загрози ІБ постійно вдосконалюються, а їхня складність невпинно зростає. Порушники ІБ під впливом нових мотивів використовують новостворені методи здійснення несанкціонованих дій.

Відзначено, що розширення електронної злочинності викликане низкою чинників, серед яких орієнтація великого бізнесу на прибуток, що мотивує злочинців; впровадження інновацій відкривають зловмисникам широкі можливості захоплення нових ринків (жертв); технічні можливості сегментації жертв і зосередження на конкретних категоріях; використання технологій приховування неправомірної діяльності; прискорення темпів атак на

інформаційні активи, внаслідок чого реагування перестає бути ефективним; можливості завдавати величезної шкоди шляхом застосування незначних зловмисних зусиль.

Реалізація загроз ІБ дає можливості зловмисникам отримати фінансову вигоду, найпоширенішими способами крадіжка ідентичності, даних кредитних карток, комп'ютерне шахрайство. Також засоби порушення ІБ дозволяють досягти масштабних цілей у політичній та військовій сферах: відмова в обслуговування сайтів важливих державних органів та установ, кібертероризм, атаки на замовлення конкуруючих держав, інсайдерські загрози. Результатами атак є виведення з ладу об'єктів критичної інфраструктури, витік або знищення важливої інформації, збої в роботі життєзабезпечувальних процесів і сервісів.

На думку експертів IBM ISS, поява IT-інновацій вимагає інноваційних підходів для забезпечення нових форм і способів співпраці у сфері забезпечення ІБ; необхідною є гнучкість у використанні бізнес-методів, щоб покращити роботу і якість обслуговування; зростання вимог до нормативної відповідності (відповідності діяльності положенням законодавства і нормативних документів) у нових умовах передбачає інвестування в більше точкових (одиничних) продуктів для вирішення більшої кількості точкових проблем, тобто використання індивідуального підходу; глобальна економіка вимагає створення нових вимог до підтримки безпеки.

Враховуючи зазначені вище обставини, для вирішення проблем у сфері ІБ керівництву компаній та менеджерам вищого рівня з ІБ необхідно змінювати свої підходи до планування й реалізації заходів захисту, розробляти стратегії управління ІБ в умовах невизначеного середовища.

Нові підходи мають забезпечити скорочення видатків на ІБ на найближчу перспективу, продовжуючи стимулювати структурні зміни шляхом скорочення операційних витрат на ІБ; відкладення довгострокових проектів на користь короткострокової окупності інвестицій (ROI); відстрочення або зменшення капітальних витрат; перегляд існуючих контрактів на обслуговування з огляду

на специфіку ситуації; забезпечення підвищення продуктивності в існуючій інфраструктурі; відстрочку найму додаткового персоналу ІТ та ІБ; відкладення запуску нових ініціатив. Оптимізація безпеки має допомогти підвищити операційну ефективність та потенціал ІТ, щоб заощадити гроші та збільшити інвестиції в нові рішення.

Важливим і актуальним завдання у сфері ІБ є оптимізація безпеки та стійкості. Для цього необхідно переглянути існуючі ризики, спростити засади управління ризиками, переоцінити бізнес-пріоритети, щоб збалансувати ризики у світлі зростаючих викликів ІБ і вимог бізнесу. Сучасне підприємство має створити структуру всеохоплюючої безпеки (Total Security Framework) і володіти потужним набором рішень, щоб переглянути поточні практики ІБ і забезпечити безперервність бізнесу, з максимальною віддачею використати наявні інновації, механізми інтеграції та навчання, а також глобальний досвід у сфері ІБ. Важливим є спростити життєвий цикл управління ІБ та ризиками, узгодити процеси ІБ з бізнес-процесами для забезпечення постійного вдосконалення, зменшення витрат і подолання складності механізмів запобігання й протидії загрозам ІБ.

IBM ISS пропонує рішення для забезпечення ІБ та стійкості через здійснення стабільних та оптимізованих ділових операцій з управління безпекою, ризиками та забезпечення відповідності. Зазначене рішення має меті: зробити можливими інновації у захищеній наскрізній інфраструктурі та платформах; зменшити кількість і складність необхідних заходів безпеки; зменшити зайві витрати на безпеку; покращити організаційну й операційну гнучкість та стійкість; максимально використовувати галузевий досвід для уніфікації управління політикою; забезпечити необхідну прозорість, контроль та автоматизацію процесів ІБ.

Як видно на рис. 4.2, основними елементами системи безпеки IBM ISS в умовах спільної політики, управління подіями і звітування є: люди й ідентичність; дані й інформація; застосунки і процеси; мережі, сервери і кінцеві точки; фізична інфраструктура [39]. Саме для досягнення захищеності

зазначених елементів компанія пропонує надання професійних і керованих послуг, відповідне апаратне і програмне забезпечення.

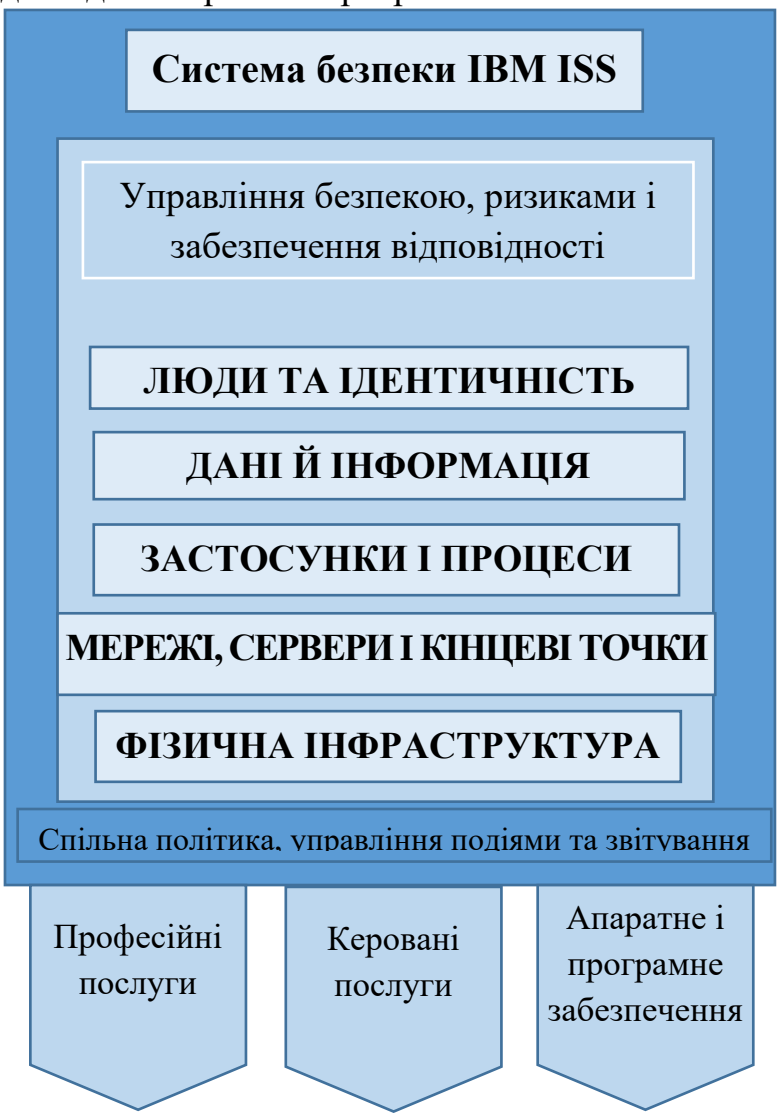

Рис. 4.2. Система безпеки IBM ISS

Методика ADDME

У рамках розглянутого підходу експерти IBM ISS також запропонували перевірену методику організації ІБ – ADDME [21, 39] (Рис. 4.3.), яка є послідовністю таких кроків:

I. Оцінювання (Assess).

II. Проектування (Design).

III. Розгортання (Deploy).

IУ. Управління і підтримка (Manage and Support).

У. Навчання (Education).

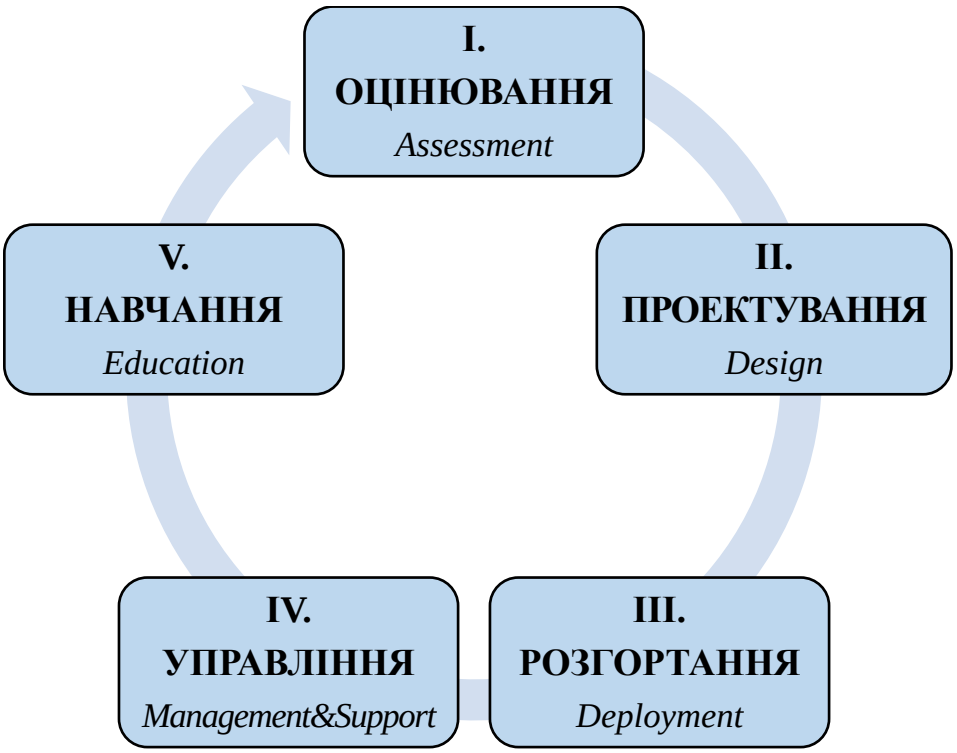

Рис. 4.3. Методика ADDME від IBM ISS

Перший етап - оцінка (Assess), в процесі якої фахівці в галузі ІБ отримують відповіді на такі питання: «Які ресурси є в організації?», «Яка їхня вартість?», «Хто має до них доступ?» На цьому етапі здійснюється ідентифікація і інвентаризація всіх ресурсів організації (робочі станції і сервери, користувачі, дані та інше). Ця інформація потім використовується на всіх наступних етапах побудови комплексної СЗІБ. На даному етапі здійснюються аналіз ризиків (risk assessment), а також пошук вразливостей (vulnerability assessment), тестування на проникнення (penetration assessment) і оцінка загроз (threat assessment).

Другий етап - проектування (Design). На цьому етапі розробляється політика ІБ підприємства і виробляються принципи оцінки ефективності, пропонованих у ній заходів (законодавчих, організаційних, програмно-технічних). При цьому враховуються зібрані на першому етапі дані про користувачів, наявні мережеві пристрої, розташування критичних інформаційних ресурсів тощо.

Третій етап - розгортання (Deploy). На відміну від перших двох етапів, результатом яких є відповідні документи, на третьому етапі реалізуються плани, розроблені на етапі проектування. У рамках даного етапу здійснюються роботи зі

встановлення засобів захисту, їх інтеграції та тестування в прийнятій технології обробки інформації, з навчання користувачів вимогам політики безпеки і правилам експлуатації встановлених захисних засобів.

Четвертий етап – управління і підтримка (manage and support). На цьому етапі оцінюється ефективність вжитих заходів і їх відповідність положенням розробленої політики безпеки. У разі виникнення інцидентів, пов'язаних з її порушенням, реалізується розроблений на другому етапі план реагування на інциденти і, як наслідок, здійснюється перегляд деяких положень політики безпеки. Зміна технології обробки інформації, поява нових технологій захисту та інші чинники також є поштовхом до перегляду розроблених документів.

Останній, п'ятий етап - навчання (Education). Цей етап не є наслідком попереднього. Навчання - це постійний процес, який здійснюється на всіх етапах побудови комплексної СЗІБ. У ньому беруть участь всі працівники організації: оператори, адміністратори, керівники, усі безпосередньо або опосередковано залучені у процеси ЗІБ [21].

4.2. Сучасні тенденції й рекомендації щодо організації інформаційної безпеки компанії

Багато нових тенденцій у сфері ІБ так чи інакше пов'язані з пандемією коронавірусу та її наслідками для бізнесу. Компанії прагнуть до реальної, а не «паперової» безпеки, розвивають системи захисту для віддаленої роботи і переходять на зовнішні спеціалізовані сервіси в галузі ІБ.

Проактивна стратегія організації ІБ

Компанії-виробники розпочали випуск продуктів нового покоління - т.зв. метапродуктів, які повністю орієнтовані на ідею результативної ІБ, залучення мінімальної експертизи і зусиль з боку фахівців на організацію захисту, а також виявлення атак в автоматичному режимі з чітко вимірюваним

ефектом. Тобто основне завдання - автоматично виявити і зупинити порушника до того, як він спричинить неприйнятні для компанії збитки.

Такий підхід розглядає неприпустимість реалізації значущих для бізнесу загроз, що, в кінцевому рахунку, потенційно розширює ринок, якісно його змінюючи: пріоритетний вибір буде на користь тих рішень і технологій, які дозволяють ефективно вирішувати такі завдання.

На думку фахівців, в нинішніх умовах, коли неможливо убезпечити бізнес від усіх загроз, найбільш прагматичним для управлінців є такий підхід до ІБ в компанії, за якого відбувається виокремлення головних загроз серед загального переліку усіх наявних загроз.

У цьому контексті в управлінні ІБ доцільне використання проактивної стратегії, яка передбачає не тільки моніторинг атак і дій хакерів, а й активне запобігання. Для недопущення загроз необхідним є зміна ІТ-інфраструктури, ІТ-систем і навіть бізнес-процесів компанії, а не просто встановлення нових чи додаткових засобів захисту і відстеження. При цьому для забезпечення стійкості ІБ обов'язковим є проведення регулярних навчань персоналу з актуальних питань захисту і верифікація неприпустимості ризиків. Відповідно до цього підходу перебудовуються всі сервіси підприємства: консалтинг, проектування, протидія кіберзагрозам.

Навіть і сьогодні багато компаній застосовують «клаптиковий» підхід при побудови СЗІБ, тобто їх захист складається з безлічі різних пристроїв і програмних додатків від різних виробників з обмеженою можливістю їх інтеграції. Крім цього такий підхід має наслідком необхідність залучення безлічі фахівців різного профілю для обслуговування великої кількості підсистем від різних виробників. І ц е все в умовах зазвичай дуже обмежених ресурсів на впровадження і обслуговування системи ІБ.

Однак, щораз все більше підприємств обирають впровадження комплексного рішення у сфері ІБ від одного вендора. Відповідно виробники таких продуктів, відповідаючи на запити ринку, розпочали просування

інноваційних продуктів з ІБ - екосистем з інформаційної/кібербезпеки. По-перше, це забезпечує безшовну інтеграцію різних модулів в єдиний комплекс із загальним центром управління, по-друге, дозволяє знизити операційні витрати, оскільки вимагає меншого числа фахівців для обслуговування системи. По-третє, закупівля всіх компонентів у одного виробника дає можливість скоротити початкову вартість проекту. Загалом екосистеми продуктів і сервісів з безпеки на відміну від окремих рішень дозволяють вибудувати ефективний ешелонований захист. Наприклад, в Україні одними із найбільш популярних є комплексні продукти від компаній Fortinet і Trend Micro [14].

Посилення тенденцій щодо застосування екосистем безпеки відбулося під час пандемії COVID-19 за умов невизначеності для бізнесу і населення, масового переведення співробітників на віддалену роботу, а отже, втрати контролю над корпоративною інфраструктурою і потребою успішно реагувати на появу нових загроз безпеці швидко, ефективно і за допомогою довірених осіб з перевіреним досвідом і репутацією.

Розвиток систем захисту віддаленого доступу

У нинішніх умовах, коли вже відбувся авральний перехід на віддалену роботу продовжується планомірна переорганізація як бізнес-процесів підприємств, так і процесів забезпечення корпоративної ІБ. На перший план виходять завдання захисту даних при їх передачі відкритими каналами зв'язку з використанням засобів VPN, багатофакторної аутентифікації при використанні особистих гаджетів для роботи, децентралізації інфраструктури в умовах територіальної розподіленості робочих місць персоналу.

У віддаленому режимі роботи розмиті межі між особистим і професійним життям, викликає збільшення ризиків потрапляння конфіденційної інформації в чужі руки. «Домашні» офіси є менш захищеними, ніж централізовані, які мають засоби захисту периметру. Багато працівників використовують свої особисті пристрої для двохфакторної аутентифікації. Крім того, ті, хто працює віддалено, часто підключаються з робочих пристроїв до загальнодоступних мереж Wi-Fi і

використовують інструменти для спільної віддаленої роботи, які часто не можуть забезпечити належний захист від загроз, внаслідок чого зростають ризики порушень ІБ компанії.

Отже, одна із тенденцій ІБ полягає в тому, що підприємство має зосередити увагу на вирішенні проблем безпеки персоналу незалежно від місця їх роботи. Одним із засобів є реалізація моделі нульового довіри (Zero Trust Network Access), відповідно до якої користувачі, їх комп'ютери, а також додатки перевіряються на справжність кожного разу, коли запитують доступ до ресурсів компанії [16].

Збільшення кількості хмарних сервісів і загроз хмарної безпеки

Одна з актуальних тем кібербезпеки - вразливість публічних хмар. Швидке і повсюдне впровадження віддаленої роботи під час пандемії різко збільшило потребу в хмарних сервісах та інфраструктурі, але невірно налаштовані конфігурації хмарних платформ, а також неуважність або недбалість користувачів (відкриті серверні і мережеві порти, використання слабких паролів до хмарних облікових записів, відмова від шифрування даних, маскування даних при розробці) викликають негативні наслідки для безпеки організацій, зокрема випадки витоку даних і несанкціонованого доступу, злому облікових записів.

Крім витоків даних при перенесенні інфраструктури компанії в публічні хмари виникають проблеми, пов'язані із забезпеченням відповідності нормативним вимогам вітчизняних і міжнародних регуляторів, а також збільшення кількості потенційних точок входу для зловмисників. Однак при грамотному виборі хмарної платформи, використанні додаткових засобів захисту від DDoS-атак, витоків даних, WAF та інших інструментів, а також проведенні консультацій для безпечної міграції в хмару зазначені вище ризики можна мінімізувати.

Затребуваність сервісів ІБ

Із зростанням рівня розуміння сутності і життєвої необхідності ІБ для підприємства в бізнес-середовищі поступово відбувається зміна

пріоритетів власники та керівників багатьох компаній: створення і вдосконалення систем корпоративної ІБ стають одним із першочергових завдань. Для вирішення цього завдання в умовах гострого дефіциту досвідчених кадрів у сфері ІБ зростає зацікавленість бізнесу у використанні зовнішніх спеціалізованих сервісів ІБ, а послуги за моделлю «Security as a Service» стають більш гнучкими і адаптивними під вимоги різних замовників.

На думку фахівців, усе більше рішень для ІБ буде надаватися у вигляді хмарних сервісів. Такий спосіб надання функцій ІБ дозволяє не тільки зробити їх більш доступними, а й підвищує можливості для захисту клієнтів від дуже потужних кібератак , які реалізують зловмисники з використанням масштабних ботнетів на основі слабо захищених гаджетів, пристроїв Інтернету речей. А ймовірність зростання потужності атак, реалізованих ботнетами, з розвитком зв'язку 5G істотно зростає.

Зростання інтенсивності й успішності атак на ІБ

За даними Ради національної безпеки і оборони України у 2020 році в Україні зафіксували близько 1 мільйона випадків кібератак [6]. Однак, експерти прогнозують продовження тенденції активного зростання інтенсивності атак. За їх словами, швидкості атак в кілька Тб/с вже стали доступні на замовлення, а, отже, онлайн-сервіси неминуче зіткнуться з такими масованими нападами. Раніше атаки інтенсивністю більше 1 Тб/с могли тривати кілька годин, були добре підготовленими, при цьому коштували десятки тисяч доларів і були точково спрямовані на конкретну жертву. Нині зростає популярність спеціальних сервісів для організації DDoS-атак - так званих «бутерів» (booters), за допомогою яких можна організувати кількахвилинну атаку на будь-який IP швидкістю в кілька Тб/с всього за пару сотень доларів.

Нещодавно з'явився тренд, відповідно до якого медіанна тривалість DDoS-атаки становить не більше 5 хвилин, оскільки в разі провалу зловмисники не витрачають час на продовження атаки, а замовник не платить гроші за її

проведення. Крім зростання інтенсивності атак значно зросла кількість успішних атак [41].

З огляду на такі обставини компанії часто замінюють операторські рішення замінюють хмарними, оскільки перші істотно відстають від темпів зростання атак. Так, у регіонах, де переважали операторські рішення безпеки, кількість успішних атак значно зросла. Причиною цього є те, що рішення щодо захисту від DDoS-атак операторів зв'язку виявилися не готові до збільшеного числа нападів. Крім того, операторам зв'язку невигідно щороку оновлювати обладнання, тому що це вимагає великих капіталовкладень, при цьому за відсутності атак ці ресурси можуть не використовуватися.

Новий підхід до підготовки кадрів ІБ

Ще один тренд, про який говорять експерти, пов'язаний з новим підходом до підготовки фахівців в області ІБ та кібербезпеки, попит на яких останнім часом зріс.

Оскільки підготовка кваліфікованого фахівця є досить трудомістким, довготривалим, а також дороговартісним процесом, сучасні компанії докладають колосальних зусиль, щоб скоротити час підготовки кадрів і підтримувати експертів на високому рівні. Працюючи в умовах масштабного кіберзлочинного бізнесу, для бізнесу критично важливо, щоб його фахівці мали «бойову» практику, тренувалися запобігати і відбивати напади реального атакуючого трафіку, вчилися захищати реальні об'єкти критичної інфраструктурою в режимі актуального часу. У цьому сенсі добре показують себе кібернавчання і кіберполігони з цифровими двійниками. На думку фахівців, цей формат підготовки фахівців ІБ стане основним у найближчі роки.

Удосконалення механізмів управління ІБ

Сьогодні багато компаній, яких можна вважати зрілими у розумінні й усвідомленні важливості ІБ для бізнесу, стикаються з проблемами вибудовування процесу управління ІБ, взаємодії з суміжними бізнес-

підрозділами й оцінювання ризиків ІБ. Тому, на думку фахівців, у зв'язку з цим на ринку очікується зростання кількості систем класу SOAR і SGRC.

SOAR. Системи оркестрації, автоматизації, реагування на інциденти ІБ (SOAR - Security Orchestration, Automation and Response) виконують такі функції: оркестрації (об'єднання і централізоване управління ІТ та ІБ-системами, що використовуються при обробці інцидентів ІБ); автоматизації, тобто алгоритмізації процесів обробки інцидентів ІБ шляхом реалізації бізнес-логіки регламентів реагування на інциденти в плейбук (runbook або playbook) - сценаріях реагування, які в вигляді блок-схем і графічних елементів дозволяють вибудувати чітку, структуровану логіку роботи аналітиків ІБ; реагування, в ході якого забезпечується збір інформації про загрозу і активну протидію (локалізацію і усунення), а також спільну роботу аналітиків над інцидентами ІБ (кейс-менеджмент) у вигляді зручної платформи комунікації та обміну інформацією.

Додатково в рішення класу SOAR можуть бути включені модулі управління даними кіберрозвідки), управління конфігураціями, управління оновленнями (патчами) і вразливостями програмного забезпечення, а також модулі аналітики і візуалізації інформації (дашборди, звіти, метрики), а також функціонал штучного інтелекту, машинного навчання та аналізу Big Data [33].

SGRC. Системи управління безпекою, ризиками і відповідністю законодавству (SGRC - Security Governance, Risk Management and Compliance) - це, фактично, система для автоматизації побудови комплексної системи управління ІБ (СУІБ).

Системи SGRC включають в себе три основні підходи до побудови СУІБ:

1. управління процесами забезпечення ІБ (Governance). Системи класу SGRC акумулюють в єдиному інформаційному просторі дані, зібрані з безлічі наявних в організації ІТ-джерел і систем захисту інформації: інформацію про стан інфраструктури ІТ та ІБ, процеси забезпечення ІБ, відповідність корпоративним і законодавчим вимогам тощо. Завдяки отриманню цієї

інформації керівництво компанії набуває ситуаційної обізнаності щодо стану ІБ в компанії і отримує можливість приймати вірні і обґрунтовані рішення не тільки з питань управління ІБ, але і при вирішенні бізнес-завдань.

Безумовно, чим більше IT-систем підприємства підключені до SGRC, тим точніші дані будуть надаватися для звітності, тому з точки зору коректного вибудовування системи управління ІБ до SGRC має бути підключено максимальну кількість джерел.

2. Захист інформаційних активів з ризик-орієнтованим підходом (Risk Management) передбачає вибір і застосування тих заходів забезпечення ІБ, які були розраховані й оцінені, і забезпечує баланс між витратами на забезпечення ІБ і отриманими результатами.

3. Управління відповідністю вимогам регуляторів, внутрішніх і зовнішніх стандартів, кращих практик в області ІБ (Compliance).

Всі основні компоненти функціоналу SGRC-рішень тісно взаємопов'язані і збагачують один одного, забезпечуючи синергетичний ефект.

Системи SGRC адаптуються під локальні вимоги, норми і стандарти, а також під індивідуальні потреби та особливості бізнес-процесів замовника, а це вносить корективи в підходи і методи автоматизації. Стандартні рішення продуктів цього класу призначені для вирішення набору стандартних, найбільш актуальних завдань і включає засоби управління IT-активами й інцидентами ІБ, конструктор робочих процесів, звітів і дашборда, коннектори до джерел даних, модулі управління вразливостями, ризиками ІБ і відповідністю нормативним вимогам, а також модулі бази знань, аудитів та документів ІБ.

Проектні рішення мають значно більш широкий набір функцій і можливостей гнучкого налаштування до IT-інфраструктури й особливостей бізнес-процесів замовника. Крім того, за необхідності компанія може здійснювати додаткове налаштування проектного рішення для того, щоб відповідати внутрішньо-корпоративних регламентами і вимогам законодавства, які періодично змінюються [34].

Також експерти відносять до актуальних тенденцій у сфері ІБ збільшення кількості SOC-центрів і рішень класу MDR, як усередині компаній, так і використання їх в якості послуги. Вони допомагають контролювати складні інциденти і дозволяють зосередитися на основній діяльності.

SOC. Один із способів захисту IT-інфраструктури компанії - організація Центру ІБ (Security Operations Center – SOC). SOC, фактично, є центром у складі фахівців з ІБ, які цілодобово відстежують стан IT-інфраструктури компанії на предмет потенційних зломів та інших загроз. Для цього вони використовують сучасні інструменти автоматизації безпеки і оркестровки, системи виявлення вторгнень, контролю доступу, збору даних і захисту кінцевих пристроїв, аналізу та запобігання інцидентам а також рішення для забезпечення безпеки інформації та управління подіями (SIEM).

Колектив центру працює за правилами екстрених служб у сфері IT та ІБ, виконуючи завдання не допускати ніяких інцидентів в сфері ІБ або оперативно встановлювати і усувати причини у випадку їх виникнення. Загальна мета SOC - підвищення рівня забезпечення ІБ компанії.

Основні завдання фахівців SOC включають:

– постійний пошук, моніторинг та аналіз вторгнень.

– проактивне запобігання загрозам.

– перевірка мереж компанії на вразливості й аналіз інцидентів безпеки.

– фільтрація помилкових спрацьовувань і швидка реакція на підтверджені інциденти.

– підготовка звітів про актуальний стан IT-інфраструктури, зареєстровані інциденти і дії потенційних зловмисників.

Завдяки створенню SOC та налагодженню його ефективної роботи підприємство отримує такі переваги: забезпечення контролю функціонування всіх IT-систем компанії; впровадження єдиної схеми роботи з даними і, відповідно, зниження ризиків втрати критичної інформації; узгоджена робота експертів різного профілю для запобігання й вирішення проблем ІБ;

забезпечення безперервного захисту об’єктів ІТКС компанії у форматі 24/7; зниження витрат на забезпечення ІБ за рахунок усунення проблем на ранніх етапах їх виникнення; відповідність галузевим стандартам у сфері ІБ [37].

MDR. Інструментом моніторингу подій безпеки, виявлення загроз і реагування на інциденти є MDR - Managed Detection and Response. Це послуга, яка задовольняє потреби організацій, яким бракує часу та ресурсів, щоб бути повністю здатними виявляти й ідентифікувати ризики, перевіряти та реагувати на загрози та/або інциденти безпеки.

Завдання, які вирішуються у складі сервісу:

1. Полювання на кіберзагрози (Cyber threat hunting) - ручний і напівавтоматизований попереджувальний пошук загроз ІБ мереж і кінцевих точок для виявлення шкідливих, підозрілих або ризикованих дій, які не були виявлені автоматичними інструментами. Тактика попереджувального пошуку загроз застосовується з метою використання нової інформації про загрози на основі раніше зібраних даних для виявлення і класифікації потенційних загроз, зокрема APT (Advanced Persistent Threat).

2. Безперервний моніторинг безпеки та сортування оповіщень (Continuous Security Monitoring & Alert Triage) передбачає аналіз мережевих даних, пов'язаних з безпекою, щоб знаходити приховані загрози, які не були виявлені традиційними засобами безпеки. Для цього використовують журнали подій, оповіщення, NetFlow, повне захоплення пакетів, NIDS, SIEM, EDR, IDS, виявлення атак нульового дня і багато інших методів, засобів і ресурсів.

3. Реагування на інциденти кібербезпеки й експертний аналіз (Cyber Incident Response & Forensic Analysis) є методом розслідування і відновлення після інцидентів, виявлених на цифрових пристроях, для виявлення та аналізу будь-якої злочинної або хакерської діяльності. Для виконання цієї функції залучаються фахівці із зазначених напрямів, які мають великий досвід і знання в області реагування на інциденти і використовують ці знання в поєднанні з

сучасними інструментами кіберкриміналістичної експертизи для всебічного аналізу даних про інциденти, незалежно від типу і розміру події.

4. Розвідка загроз безпеки (Threat Intelligence) зазвичай включає компіляцію даних розвідки з відкритим вихідним кодом, розвідки з прихованої мережі dark web та запатентованої розвідки з внутрішніх джерел або на основі підписки. Розвідка загроз допомагає виявляти і запобігати атакам, надаючи інформацію про зловмисників, їх мотиви і можливості [40].

Основні тенденції організації ІБ підприємства можна подати у вигляді схеми (Рис. 4.3.)

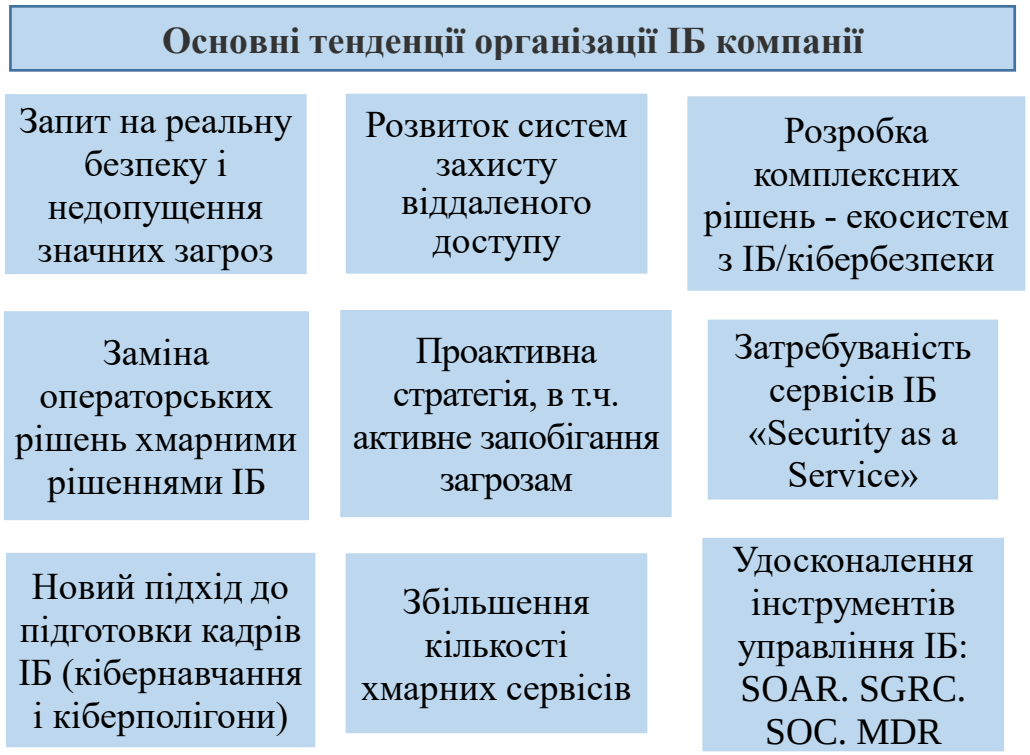

Рис. 4.4. Основні тенденції організації ІБ компанії

Висновки до розділу 4

У результаті аналізу концепції ЗІБ від IBM ISS встановлено, що найбільшою проблемою ІБ залишається складність, а ключем до управління вартістю та складністю IT-ландшафту, який постійно розвивається є інтеграція. Ключовими чинниками, які треба враховувати при організації ІБ є: загрози, які постійно

вдосконалюються; технології, які активно розвиваються; зростаючі вимоги щодо нормативної відповідності; зростаючі бізнес-потреби та зростаючу економіку. У рамках розглянутого підходу експерти IBM ISS також запропонували апробовану на практиці методику організації ІБ – ADDME, яка є послідовністю таких кроків: оцінювання (Assess); проектування (Design); розгортання (Deploy); управління і підтримка (Manage and Support); навчання (Education).

На основі аналізу сучасних тенденцій розвитку середовища ІБ запропоновано такі рекомендації щодо удосконалення організації ІБ: спрямовувати стратегію ІБ на використання превентивних та проактивних заходів; застосовувати комплексні рішення-екосистеми з ІБ; замінювати операторські рішення хмарними з метою скорочення витрат; використовувати сервіси ІБ від надійних і кваліфікованих провайдерів для підвищення рівня ефективності забезпечення ІБ; впроваджувати нові підходи до навчання персоналу з питань ІБ, зокрема організовувати кібернавчання, кіберполігони; удосконалювати інструменти організації ІБ шляхом створення центрів ІБ (SOC), які забезпечують безперервний моніторинг, запобігання й реагування на загрози ІБ; впроваджувати комплексні автоматизовані системи управління ІБ SOAR, SGRC, MDR та інші, які поєднують виконання багатьох функцій ІБ: моніторингу подій безпеки, виявлення загроз; управління ризиками; реагування на інциденти та інші.

ВИСНОВКИ

У результаті дослідження встановлено, що СЗІБ як частина загальної системи управління підприємства, що базується на аналізі ризиків і призначена для проектування, реалізації, контролю, супроводу та вдосконалення заходів в галузі ІБ, має гарантувати досягнення таких цілей як забезпечення цілісності й конфіденційності, унеможливлення несанкціонованого доступу до критично важливої інформації підприємства та пов'язаних з нею процесів (створення, введення, обробки і виведення).

Відповідно до комплексного підходу у межах системи забезпечення ІБ підприємства здійснюються нормативно-правові, організаційні та програмно-технічні заходи. Організаційні заходи ІБ включають забезпечення режиму і охорони, роботу з персоналом та документами, що містять конфіденційну інформацію, використання технічних засобів збирання й обробки конфіденційної інформації, аналіз внутрішніх і зовнішніх загроз ІБ та вироблення заходів щодо забезпечення захисту, систематичний контроль за діяльністю персоналу у сфері ІБ.

Ключова роль ОЗІБ визначається важливістю своєчасного прийняття виважених і обґрунтованих управлінських рішень на основі аналізу поточної ситуації та впливу різних чинників, врахування наявних ресурсів, методів, засобів і способів захисту інформації, прогнозування наслідків управлінського впливу у рамках діючого нормативно-правового й методичного апарату.

З’ясовано, що служба ІБ є самостійною організаційною одиницею підприємства, що підпорядковується безпосередньо керівнику підприємства. Організаційна структура служби ІБ формується у відповідності із її завданнями і функціями, серед яких доцільно виділити такі як: формування, підтримка і документальне забезпечення політики ІБ підприємства; розробка методології та методик аналізу загроз, оцінка рівня ІБ підприємства і системи її забезпечення; організація і здійснення конкретних видів діяльності із захисту інформації з

персоналом, іншими підрозділами підприємства, партнерами; робота з конфіденційними документами; експлуатація технічних засобів захисту інформації; аудит і контроль функціонування корпоративної системи ІБ; забезпечення внутрішнього та пропускного режимів і охорони підприємства.

З огляду на виділені функції служба ІБ має включати інформаційно-аналітичні відділи (зокрема нормативної документації, аудиту інформаційної безпеки); інженерно-технічні підрозділи (адміністрування та впровадження ІС та систем захисту інформації, інші); відділ роботи з персоналом; відділ конфіденційного діловодства (за потреби); службу режиму й охорони.

Встановлено, що питання організації внутрішнього та пропускного режиму, забезпечення охорони території підприємства і його об'єктів нерозривно пов'язані і становлять складову системи забезпечення ІБ підприємства.

Внутрішній і пропускний режими на підприємстві організовуються з метою виключення несанкціонованого проходження на територію та об'єкти компанії сторонніх осіб та персоналу, що немає прав доступу, внесення на територію підприємства недозволених, особистих технічних засобів; несанкціоноване винесення з території підприємства носіїв конфіденційних відомостей; порушення встановленого регламенту службового часу, розпорядку роботи структурних підрозділів ІБ, а також встановленого порядку та режиму роботи працівників підприємства і відряджених осіб з носіями конфіденційних даних.

Заходи з охорони мають на меті запобігання спробам проникнення сторонніх осіб на територію або об'єкти підприємства; своєчасне виявлення і затримання осіб, які протиправно намагалися потрапити на закриту територію; забезпечення збереження носіїв конфіденційної інформації та матеріальних засобів, що знаходяться на території і підлягають охороні; запобігання інцидентам і ліквідація їх наслідків на об'єктах, що підлягають охороні.

У результаті аналізу концепції ЗІБ від компанії IBM ISS встановлено, що ключовими чинниками, які треба враховувати при організації ІБ є: загрози, які постійно вдосконалюються; технології, які активно розвиваються; зростаючі

вимоги щодо нормативної відповідності; зростаючі бізнес-потреби та зростаючу економіку. Відповідно до підходу IBM ISS запропоновано апробовану на практиці методику організації ІБ – ADDME, яка є послідовністю таких кроків: оцінювання (Assess); проектування (Design); розгортання (Deploy); управління і підтримка (Manage and Support); навчання (Education).

На основі аналізу сучасних тенденцій розвитку середовища ІБ запропоновано такі рекомендації щодо удосконалення організації ІБ:

– спрямовувати стратегію ІБ на використання превентивних та проактивних заходів;

– застосовувати комплексні рішення-екосистеми з ІБ;

– замінювати операторські рішення хмарними з метою скорочення витрат;

– використовувати сервіси ІБ від надійних і кваліфікованих провайдерів для підвищення рівня ефективності забезпечення ІБ;

– впроваджувати нові підходи до навчання персоналу з питань ІБ, зокрема організовувати кібернавчання, кіберполігони;

– удосконалювати інструменти організації ІБ шляхом створення центрів ІБ (SOC), які забезпечують безперервний моніторинг, запобігання й реагування на загрози ІБ;

– впроваджувати комплексні автоматизовані системи управління ІБ SOAR, SGRC, MDR, які поєднують виконання багатьох функцій ІБ: моніторингу подій ІБ, виявлення загроз; управління ризиками; реагування на інциденти ІБ та інші.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Аникин И., Глова В., Нейман Л., Нигматуллина А. Теория информационной безопасности и методология защиты информации. Учебное пособие. Казань: Изд-во Казан. гос. техн. ун-та, 2008 с. 358.
2. Аніловська Г. Я. Інформаційна безпека підприємства в умовах використання сучасних інформаційних технологій. Науковий вісник НЛТУ України. 2008. Вип. 18.9. С. 270–273.
3. Балашов П. Разработка структуры службы безопасности предприятия. URL: www.cprspb.ru/bibl/opv/balashov.doc (дата звернення: 25.11.2021)
4. Березюк Л. Организационное обеспечение информационной безопасности: учеб. Пособие. Хабаровск : Изд-во ДВГУПС, 2008. 188 с.
5. Бурцева К., Тимофєєв Д. Підвищення рівня інформаційної безпеки за допомогою організаційних заходів на комерційних підприємствах. URL: http://ir.nmu.org.ua/bitstream/handle/123456789/1673/6.pdf?sequence=1 (дата звернення: 25.11.2021)
6. В Україні в 2020 році зафіксували 1 мільйон кібератак – РНБО. URL: https://ms.detector.media/kiberbezpeka/post/25227/2020-08-07-v-ukraini-v-2020-rotsi-zafiksuvaly-1-milyon-kiberatak-rnbo/ (дата звернення: 25.11.2021)
7. Внутриобъектовый режим на предприятии. URL: https://businessfaq.ru/ vnutriobektovyj-rezhim-na-predpriyatii.html (дата звернення: 25.11.2021)
8. Герасименко О. В. Козак А. В. Інформаційна безпека підприємства: поняття та методи її забезпечення. URL: http://intkonf.org/ken-gerasimenko-ov-kozak-avinformatsiyna-bezpeka-pidpriemstva-ponyattyata-metodi-yiyi-zabezpechennya (дата звернення: 25.11.2021)
9. Гриджук Г. С. Систематизація методів інформаційної безпеки підприємства. URL: http://www.nbuv.gov.ua/ portal/natural/Vntu/2009_19_1/pdf/64.pdf (дата звернення: 25.11.2021)

10. ДБН В.2.2-14-2004 Приміщення для зберігання секретних документів та роботи з ними. URL: https://dbn.co.ua/load/normativy/dbn/1-1-0-997 (дата звернення: 25.11.2021)
11. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. К.: ООО "ТИД "ДС", 2002. 688 с.
12. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT). 2015. 32 с.
13. Економічна безпека підприємства. URL: http://subject.com.ua/economic/ safety/50.html (дата звернення: 25.11.2021)
14. Экосистема ИТ-безопасности как ответ актуальным угрозам. URL: https://itbiz.ua/ru/stati-i-obzory/ruekosistema-it-bezopasnosti-kak-otvet-aktualnym-ugrozamekosistema-it-bezreki-yak-vidpovid-aktualnim-zagrozam/ (дата звернення: 25.11.2021)
15. Информационная безопасность для организаций с высоким уровнем риска: новые угрозы и возможные подходы к их нейтрализации. URL: https://www.jetinfo.ru/informatsionnaya-bezopasnost-dlya-organizatsij-s-vysokim-urovnem-riska-novye-ugrozy-i-vozmozhnye-podkhody-k-ikh-nejtralizatsii/ (дата звернення: 25.11.2021)
16. Информационная безопасность (тренды). URL: https://www.tadviser.ru/ (дата звернення: 25.11.2021)
17. Кавун С., Носов В., Мажай О. Інформаційна безпека. Навчальний посібник. Ч.1, Харків: Вид. ХНЕУ, 2008. 352 с.
18. Коваленко Ю. Забезпечення інформаційної безпеки на підприємстві. Економіка промисловості. 2010. № 3. С. 123-129. URL: http://nbuv.gov.ua/j-pdf/econpr_2010_3_20.pdf (дата звернення: 25.11.2021)
19. Конеев И., Беляев А. Информационная безопасность предприятия. СПб. : БХВ-Петербург, 2003. 747 с.

20. Коптелов А., Беркович В. Построение эффективной системы управления информационной безопасностью компании. URL: http://businessprocess.narod.ru/index18.htm (дата звернення: 25.11.2021)
21. Лукацкий А. Новые подходы к обеспечению информационной безопасности сети. URL: https://compress.ru/article.aspx?id=11178 (дата звернення: 25.11.2021)
22. Менеджмент: конспект лекцій з дисципліни. URL: http://library.if.ua/book/58/4101.html (дата звернення: 25.11.2021)
23. Методика организации контрольно-пропускного режима на предприятии (организации). URL: http://ntagil.org/bezopas/info.php?SECTION_ID=1216 (дата звернення: 25.11.2021)
24. Обеспечение информационной безопасности организации. URL: http://www.iccwbo.ru/blog/2016/obespechenie-informatsionnoy-bezopasnosti/ (дата звернення: 25.11.2021)
25. Організаційні основи захисту інформації на підприємстві. URL: http://bezopasnik.org/article/19.htm (дата звернення: 25.11.2021)
26. Организация внутриобъектового и пропускного режимов на предприятии. URL: http://www.безопасник.рф/article/15.htm) (дата звернення: 25.11.2021)
27. Ортинський В.Л., Керницький І.С., Живко З.Б. Економічна безпека підприємств, організацій та установ. К.: Правова єдність, 2009. 544 с.
28. Осовська Г.В., Осовський О.А. Основи менеджменту: Підручник. Видання 3-є, перероблене і доповнене. К.: «Кондор», 2006. 664 с.
29. Островерхова Г. Сутність та структура організаційного забезпечення інноваційної діяльності. URL: http://eprints.kname.edu.ua/29738/1/45.pdf (дата звернення: 25.11.2021)
30. Романов О. Организационное обеспечение информационной безопасности: Учеб. пособие. М.: Издательский центр «Академия», 2008. 192 с. URL: http://www.academia-moscow.ru/ (дата звернення: 25.11.2021)

31. Сафронов А., Плачинда О., Венедиктов Ю. Применение организационно-технических методов для развития системы информационной безопасности организации. Праці Одеського політех. ун-ту. 2011. Вип. 1(35). С.262-266.
32. Сороковская А. А. Информационная безопасность предприятия : новые угрозы и перспективы. URL: http://nbuv.gov.ua/portal/Soc_Gum/ Vchnu_ekon/2010_2_2/032-035.pdf (дата звернення: 25.11.2021)
33. Системы SOAR. URL: https://www.securityvision.ru/blog/soar-sistemy/ (дата звернення: 25.11.2021)
34. Системы класса Security Governance, Risk Management and Compliance: применение и основные функции. URL: https://www.securityvision.ru/products/sgrc/ и(дата звернення: 25.11.2021)
35. Шевченко С. Формування системи управління інформаційної безпеки підприємства. URL: http://kneu.edu.ua/.../ec.../ShevchenkoS.rtf.docx (дата звернення: 25.11.2021)
36. Шопін А. Інформаційна безпека як фактор забезпечення конкурентоспроможності підприємства. URL: http://repository.hneu.edu.ua/ (дата звернення: 25.11.2021)
37. Шушурихин В. Что такое Центр информационной безопасности (SOC). URL: https://itglobal.com/ru-ru/company/blog/soc-security-operations-center/ (дата звернення: 25.11.2021)
38. Ярочкин В. Информационная безопасность: Учебник для студентов вузов. М.: Академический Проект; Гаудеамус, 2-е изд. 2004. 544 с.
39. IBM Internet Security Systems IBM ISS Overview. URL: https://www.ibm.com/ jm/download/IBM_ISS_Overview.pdf (дата звернення: 25.11.2021)
40. What is MDR? URL: https://medium.com/cycraft/ what-is-managed-detection-and-response-952a37eca4a6 (дата звернення: 25.11.2021)
41. 2021 Must-Know Cyber Attack Statistics and Trends. URL: https://www.embroker.com/blog/cyber-attack-statistics/ (дата звернення: 25.11.2021)