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:

КАДРОВІ ТЕХНОЛОГІЇ В СИСТЕМІ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

СТУДЕНТ: Мосійчук Владислав Миколайович _____
(підпис)

КЕРІВНИК: к.держ.упр., доц. 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 Мосійчуку Владиславу Миколайовичу

Тема роботи: «КАДРОВІ ТЕХНОЛОГІЇ В СИСТЕМІ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА», затверджена наказом по університету № 170 від «11» жовтня 2021 р.

1. **Термін здачі** студентом оформленої роботи «___» _____ 20___ р.
2. **Об'єкт дослідження:** система управління інформаційною безпекою підприємства.
3. **Предмет дослідження:** кадрові технології в системі управління інформаційною безпекою підприємства.
4. **Мета дослідження** полягає у вивченні кадрових технологій в системі управління інформаційною безпекою підприємства.
5. **Перелік питань, які мають бути розроблені:**

5.1 З’ясувати роль і види кадрових технологій у СУІБ підприємства.

5.2 Дослідити кадрові аспекти діяльності посадових осіб і підрозділів компанії у сфері інформаційної безпеки.

5.3 Вивчити технології підбору й відбору персоналу та встановити їх специфіку у сфері інформаційної безпеки.

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

Науковий керівник _____ Т.М. Мужанова
підпис

Завдання прийнято до виконання _____ В.М. Мосійчук
підпис

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

КАЛЕНДАРНИЙ ПЛАН
виконання дипломної роботи
студентом МОСІЙЧУКОМ Владиславом Миколайовичем

Дата видачі завдання: «16» вересня 2021 р.

№ з/п	Етапи дипломної роботи	Термін виконання етапів	Примітка
1.	Визначення об’єкта, предмета, мети та завдань дослідження.	16.09.2021	
2.	Збір та аналіз літератури.	28.09.2021	
3.	З’ясування ролі і видів кадрових технологій у СУІБ підприємства.	12.10.2021	
4.	Дослідження кадрових аспектів діяльності посадових осіб і підрозділів компанії у сфері інформаційної безпеки.	26.10.2021	
5.	Вивчення технологій підбору й відбору персоналу та встановлення їх специфіки у сфері інформаційної безпеки.	09.11.2021	
6.	Формулювання висновків до роботи.	23.11.2021	
7.	Оформлення роботи.	07.12.2021	
8.	Оформлення презентації.	14.12.2021	
9.	Отримання рецензії на роботу.	24.12.2021	
10.	Захист у ДЕК.	__.01.2022	

Студент В.М. Мосійчук
(підпис)

Науковий керівник Т.М. Мужанова
(підпис)

РЕФЕРАТ

Дипломна робота присвячена дослідженню кадрових технологій в системі управління інформаційною безпекою підприємства. Робота складається зі вступу, трьох розділів, що містять 12 рисунків, висновків та списку використаних джерел з 44 найменувань. Загальний обсяг роботи становить 86 аркушів, 5 з яких займає список використаних джерел.

Об'єктом дослідження є система управління інформаційною безпекою підприємства.

Предметом дослідження є кадрові технології в системі управління інформаційною безпекою підприємства.

Метою роботи є вивчення кадрових технологій в системі управління інформаційною безпекою підприємства.

Для цього у роботі використані методи аналізу, синтезу, класифікацій та порівняння, узагальнення, положення системного і комплексного підходів до управління інформаційною безпекою, теорії управління персоналом, зокрема підбору й відбору, тестування персоналу.

Як результат у роботі з'ясовано роль і види кадрових технологій у СУІБ підприємства; досліджено кадрові аспекти діяльності посадових осіб і підрозділів компанії у сфері інформаційної безпеки; вивчено технології підбору й відбору персоналу та встановлено їх специфіку у сфері інформаційної безпеки.

Галузь застосування. Розроблені підходи можуть бути використані у ході вибору та впровадження кадрових технологій у рамках системи управління інформаційною безпекою підприємства, зокрема при підборі та відборі кандидатів на зайняття вакантних посад, а також у процесі визначення та розподілу повноважень служб інформаційної безпеки та управління персоналом щодо роботи з персоналом у сфері інформаційної безпеки підприємства.

Ключові слова: СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА, КАДРОВІ ТЕХНОЛОГІЇ (ТЕХНОЛОГІЇ УПРАВЛІННЯ ПЕРСОНАЛОМ), КАДРОВІ ТЕХНОЛОГІЇ В СИСТЕМІ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА, ВІДБІР І ПІДБІР ПЕРСОНАЛУ У ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

ЗМІСТ

ВСТУП

Актуальність теми. Статистика інцидентів інформаційної безпеки свідчить про потужний вплив «людського» чинника на стан захищеності інформаційного середовища підприємства. Сьогодні саме персонал найчастіше є джерелом порушень інформаційної безпеки, які є наслідком непрофесійності, халатності або навмисних злих намірів безвідповідальних або невдоволених працівників. Крім того, одним із слабких місць у системі управління інформаційною безпекою є процедури наймання працівників, які часто не дають змоги виявити недостойних або зловмисних кандидатів.

З огляду на зростання числа внутрішніх загроз інформаційній безпеці сучасне підприємство має приділяти велику увагу роботі з персоналом шляхом використання різноманітних кадрових технологій, а дослідження передових технологій управління персоналом та встановлення їх специфіки у сфері інформаційної безпеки є актуальним науковим завданням.

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. З’ясувати роль і види кадрових технологій у СУІБ підприємства.

2. Дослідити кадрові аспекти діяльності посадових осіб і підрозділів компанії у сфері інформаційної безпеки

3. Вивчити технології підбору й відбору персоналу та встановити їх специфіку у сфері інформаційної безпеки.

Об’єкт дослідження - система управління інформаційною безпекою підприємства. **Предмет дослідження** – кадрові технології в системі управління інформаційною безпекою підприємства.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу, синтезу, класифікацій та порівняння, узагальнення, положення системного і комплексного підходів до

управління інформаційною безпекою, теорії управління персоналом, зокрема підбору й відбору, тестування персоналу.

Наукова новизна одержаних результатів. У роботі досліджено кадрові технології, які можуть бути успішно впроваджені в системі управління інформаційною безпекою підприємства, зокрема новітні підходи до підбору й відбору, а також різнопланового тестування кандидатів на зайняття вакантних посад у сфері інформаційної безпеки.

Практичне значення одержаних результатів. Застосування отриманих напрацювань на практиці дасть змогу зменшити ризики інформаційній безпеці підприємства, пов’язані з персоналом, зокрема запобігти працевлаштуванню фахівців у сфері інформаційної безпеки, які не володіють належними професійними характеристиками та особистими якостями, шляхом застосування новітніх технологій підбору й відбору, а також тестування потенційних кандидатів на вакантні посади.

Розділ 1.

КАДРОВІ ТЕХНОЛОГІЇ У СУІБ ПІДПРИЄМСТВА

1.1 Принципи та етапи СУІБ

У нинішніх умовах впровадження забезпечення надійного захисту інформації та засобів їх обробки є обов’язковим завданням управління підприємством. Найбільш ефективним і визнаним на світовому рівні засобом є впровадження системи управління інформаційною безпекою (СУІБ).

Відповідно до основоположного стандарту ISO 27001 [6], який регламентує ці питання, СУІБ є невід’ємною частиною корпоративної системи управління, яка має на меті проектування, впровадження, контроль, підтримку та вдосконалення заходів у сфері інформаційної безпеки. Основою функціонування СУІБ є ризико-орієнтований підхід, тобто спрямування зазначених заходів на запобігання реалізації загроз інформаційній безпеці підприємства [9]. Основними складовими СУІБ є політика, дії з планування, організаційні структури, повноваження, процеси, процедури і ресурси.

Відповідно до класичного бачення СУІБ спрямована на забезпечення таких властивостей інформації, яка підлягає захисту: конфіденційності, доступності для авторизованих користувачів, цілісності інформації та пов'язаних з нею процесів (створення, введення, обробки і виведення), запобігання несанкціонованого доступу до носіїв інформації тощо [16]. СУІБ має запобігти випадкам реалізації як зовнішніх загроз (розголошення, витік, несанкціонований доступ), так і виникненню внутрішніх загроз спотворення, модифікація, втрати критичної інформації.

Передумовою ефективності СУІБ є дотримання низки вимог, серед яких, зокрема, узгодженість з бізнес-стратегією компанії; підтримка та зацікавленість з боку керівництва; безперервність управлінських процесів; чіткий розподіл повноважень і встановлення персональної відповідальності; забезпечення

оптимального балансу між можливостями, продуктивністю і витратами на СУІБ, тобто економічна доцільність [16]; законність заходів ІБ; безперервність реалізації та вдосконалення засобів та методів ІБ; комплексність використання всього арсеналу наявних засобів захисту у всіх підрозділах фірми та на всіх етапах процесів захисту [43].

У технічному контексті СУІБ має здійснюватися відповідно до принципів безперервності захисту, гнучкості управління і застосування, відкритості алгоритмів і механізмів захисту [1, 5]. Важливим є забезпечення неможливості уникнути засобів захисту; неможливості переходу в небезпечний стан; мінімізації привілеїв; ешелонованості захисту; різноманіття захисних засобів; керованості ІС; прозорості для авторизованих користувачів; рівностійкості ланок (стійкість захисту визначається стійкістю найслабшої його ланки) [44].

Таким чином, під інформаційною безпекою далі розумітимемо стан захищеності інформаційних ресурсів, технологій їх формування та використання, а також прав суб'єктів інформаційної діяльності [43]. У цьому контексті варто зазначити, що:

1. об'єктом захисту є непросто інформація як певні дані, а інформаційний ресурс, тобто інформація, яка зберігається на матеріальних носіях (документи, е-реєстри, бази даних, хмарні сховища тощо), право на доступ до якої закріплено за її власником або розпорядником відповідно до законодавства;

2. інформаційна безпека користувачів передбачає захищеність їхніх прав на доступ до інформаційних ресурсів для задоволення власних інформаційних потреб;

3. беручи до уваги принцип економічної доцільності захисту підлягає тільки та інформація, розголошення (витік, втрата тощо) якої неминуче призведе до матеріальних, фінансових, репутаційних або інших втрат для підприємства [37].

Як зазначено вище, найбільш відомим варіантом реалізації моделі управління інформаційною безпекою підприємства є підхід Міжнародної організації зі стандартизації (ISO), яка є автором сімейства стандартів ISO 27к, які власне і присвячені зазначеному питанню.

Для опису життєвого циклу СУІБ (як і, як і життєвого циклу будь-якої іншої системи управління) прийнято використовувати PDCA-модель (Рис.1.1).

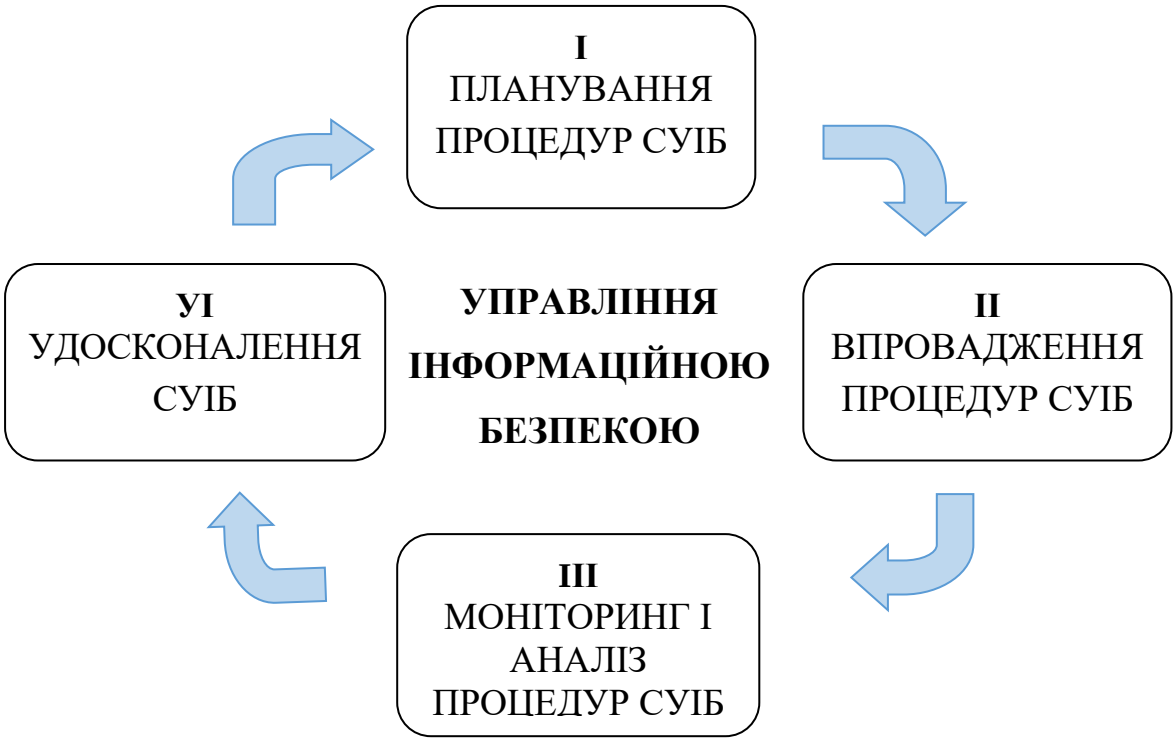

Рис. 1.1. Етапи СУІБ підприємства

Усі процедури СУІБ повинні послідовно проходити такі чотири етапи: планування, впровадження, моніторинг і аналіз, удосконалення. Кожен етап характеризується виконанням різноманітних процедур.

Опишемо послідовно етапи функціонування СУІБ, починаючи із створення системи.

1. Планування процедур СУІБ:

- рішення щодо створення СУІБ керівництвом компанії;
- вибір області дії системи;
- інвентаризація та класифікація інформаційних активів;
- оцінка рівня захищеності інформаційної системи (ІС) – визначення вразливостей та загроз ІБ;
- аналіз інформаційних ризиків;
- розробка Положення про застосування;
- вибір заходів щодо зниження інформаційних ризиків;

- розробка бази нормативних документів ІБ.

2. Впровадження процедур СУІБ:

- впровадження заходів щодо зниження інформаційних ризиків;
- визначення методів оцінки ефективності впроваджених заходів;
- підвищення кваліфікації співробітників компанії у галузі ІБ;
- використання системи управління інцидентами ІБ.

3. Моніторинг та аналіз процедур СУІБ:

- регулярні перевірки ефективності процедур системи управління;
- регулярний перегляд результатів аналізу інформаційних ризиків;
- реєстрація записів системи управління з метою оцінки її ефективності.

4. Удосконалення СУІБ:

- виконання коригувальних та превентивних дій;
- забезпечення ефективності вжитих заходів, удосконалення СУІБ [6].

Зупинимося докладніше на деяких процедурах СУІБ, які зазвичай викликають найбільші складнощі.

Вибір області дії

Загалом СУІБ поширюється на всю ІБ компанії. Однак використання даної системи управління - досить складний процес, тому, зазвичай, компанії вибирають один з критичних бізнес-процесів або автоматизованих систем і впроваджують управлінські процедури, а потім поширюють їх на інші процеси компанії.

Зазначимо, що в рамках сфери дії СУІБ потрібно визначити такі активи:

- інформаційні ресурси;
- засоби зберігання та обробки інформації;
- програмне забезпечення;
- користувачів ІС;
- допоміжні послуги та системи життєзабезпечення [32].

Класифікація інформаційних активів компанії

Рівень необхідної безпеки залежить від ступеня критичності інформації для компанії, оскільки нелогічно витрачати на захист інформації $100, якщо сама інформація коштує $10.

Оцінку критичності інформації проводять, як правило, за трьома критеріями - конфіденційності, цілісності та доступності, тобто для кожної інформації потрібно визначити збитки, які зазнає компанія при її розголошенні, модифікації або неможливості отримати до неї доступ. Основна складність цього процесу полягає в тому, що оцінку критичності активів повинні проводити співробітники, які працюють з інформацією, а вони часто не знають, як це зробити, або не хочуть відволікатися від своєї основної діяльності. З метою спрощення цього процесу розробляються методики оцінки критичності, різні форми заповнення результатів. Таким чином, цей процес може вимагати багато часу та уваги до виконавців робіт.

Хоча інвентаризація та класифікація інформаційних ресурсів – це внутрішній процес компанії, загальноприйнятою практикою є запрошення сторонніх консультантів. Це допомагає заощадити кошти і, головне, час, оскільки сторонні консультанти вже мають досвід подолання труднощів, які можуть виникнути у процесі інвентаризації та класифікації.

Ефективність процедур СУІБ

Після проведення аналізу ризиків, вибору та впровадження контрзаходів необхідно оцінити їх ефективність. Зазвичай ефективність впроваджених засобів захисту визначається за допомогою повторного аналізу ризиків. Необхідно зрозуміти, наскільки дійсно знизився ризик. Враховуючи, що заходами зниження ризиків можуть бути не лише окремі програмні чи апаратні рішення (наприклад, антивірус), а й різні заходи (наприклад, регулярне резервне копіювання інформації). Щоб оцінити ефективність цих заходів, треба знати, чи виконуються необхідні дії відповідно до вказівок і який внесок у безпеку вони роблять.

Для прикладу розглянемо процес моніторингу журналів системних подій. Адміністратор безпеки повинен регулярно (не рідше двох разів на тиждень) аналізувати журнал, виявляти найбільш критичні події, визначати їх причини та

способи усунення. Перевіркою виконання процесу моніторингу можуть бути записи, тобто адміністратор повинен фіксувати факт виконання моніторингу та його результати. Крім того, необхідно регулярно перевіряти дії адміністратора, наприклад, за допомогою різних тестів або інших методів.

Побудова СУІБ відповідно до вимог загальновизнаного міжнародного стандарту ISO/IEC 27001:2013 надає можливість комплексного захисту всіх форм та засобів обробки інформації з метою забезпечення її конфіденційності, цілісності та доступності.

Ключовими плюсами стандарту ISO/IEC 27001: 2013 є:

- може бути застосованим до будь-яких організацій;
- не має галузевої специфіки і застосовується до організацій будь-якого розміру.
- не нав’язує засоби та заходи захисту.

Стандарт визначає систему управління, у межах якої захист інформації будується з урахуванням оцінки ризиків. У цьому організація має самостійно визначити методику оцінки ризиків і рівень ризиків, які є для неї прийнятним. Це дозволяє визначити ключові напрями забезпечення ІБ, витрачати ресурси тільки на ті організаційні й технічні заходи захисту, які дійсно дозволять знизити ризики бізнесу, пов’язані з порушенням ІБ критичних активів.

- Забезпечує відповідність ІБ цілям бізнесу та передбачає постійне вдосконалення СУІБ.

Стандарт розроблений на базі відомого стандарту на системи менеджменту якості – ISO 9001, і включає до обов’язкових вимог наявність таких процесів, як навчання персоналу, внутрішні аудити, аналіз з боку керівництва, управління коригуючими та попереджувальними діями, що забезпечує можливість проведення періодичного контролю відповідності реалізованих захисних заходів цілям і вимогам як підрозділи ІБ, а й бізнесу загалом.

Серед переваг, які отримують організації після впровадження системи управління інформаційною безпекою та проходження сертифікаційного аудиту на відповідність вимогам стандарту ISO/IEC 27001:2013, слід зазначити:

- підвищення довіри клієнтів, партнерів та інших заінтересованих сторін за рахунок підтвердження відповідності певному рівню захищеності інформації;
- зміцнення іміджу організації на внутрішньому та зовнішньому ринку;
- підвищення стабільності функціонування організації та рівня керованості;
- інтеграція процесів управління інформаційною безпекою у загальну систему корпоративного управління організації;
- чітке визначення ролей та відповідальності щодо забезпечення інформаційної безпеки для всіх залучених осіб;
- адекватність обраних захисних заходів реальним загрозам інформаційній безпеці;
- регулярна незалежна оцінка діючої системи управління інформаційною безпекою;
- запобігання та/або зниження шкоди від інцидентів інформаційної безпеки;
- зниження операційних витрат та виключення «перехресного» фінансування в рамках єдиної системи управління інформаційною безпекою;
- покращення:
- взаємодії між бізнес-сектором, ІТ та ІБ;
- у забезпеченні безперервності бізнес-процесів;
- методів забезпечення інформаційної безпеки, що застосовуються, з урахуванням практик, що підтвердили свою ефективність (best practice);
- у забезпеченні прозорості управління інформаційної безпеки організації для керівництва організації;
- рівня відповідності управління інформаційною безпекою організації світових практик управління;
- в ефективності використання часу та ресурсів;

- полегшення впровадження інших стандартів у сфері забезпечення інформаційної безпеки (наприклад, PCI DSS) та у сфері систем управління (наприклад, ISO/IEC 20000-1, ISO 22301);
- підвищення компетентності персоналу у сфері інформаційної безпеки та зниження впливу людського чинника на бізнес-процеси організації [32].

Крім того, після впровадження в організації СУІБ відповідно до вимог стандарту ISO/IEC 27001: 2013 переваги також набувають:

- контрагенти організації за рахунок гарантії виконання передбачених законодавством норм і вимог, що висуваються самими контрагентами, з інформаційної безпеки;
- власники та інвестори організації за рахунок зростання конкурентоспроможності організації на вітчизняних та міжнародних ринках; підвищення інвестиційної привабливості організації; збільшення вартості нематеріальних активів; збільшення частки ринку та поліпшення результатів діяльності організації; підвищення капіталізації організації; збільшення шансів на перемогу у тендерах та конкурсах;
- співробітники ІБ-служби організації за рахунок зниження кількості питань та специфічних вимог у сфері інформаційної безпеки з боку клієнтів організації (завдяки наявності визнаного сертифіката відповідності, виданого незалежною організацією).

1.2 СУІБ у системі управління підприємством

Сьогодні переважаючою є позиція, відповідно до якої СУІБ є невід'ємною частиною інтегрованої системи управління компанією, яка складається з кількох рівнів управління: стратегічного, корпоративного, керування та забезпечення [34] (Рис. 1.2).

Розглянемо кожен із рівнів докладніше.

Стратегічний рівень. На цьому рівні визначається набір регламентуючих документів (міжнародних стандартів), на основі яких відбуватиметься побудова

інтегрованої системи управління підприємством, а також описуються вимоги до неї та політика.

Корпоративний рівень. На цьому рівні визначаються цілі, які описуються у вигляді політик, корпоративних стандартів та процедур для спеціалізованих систем управління, в тому числі системи управління IT-сервісами (ISO 20000), системи управління забезпеченням безперервності бізнесу (BS 25999), а також СУІБ (ISO 27001).

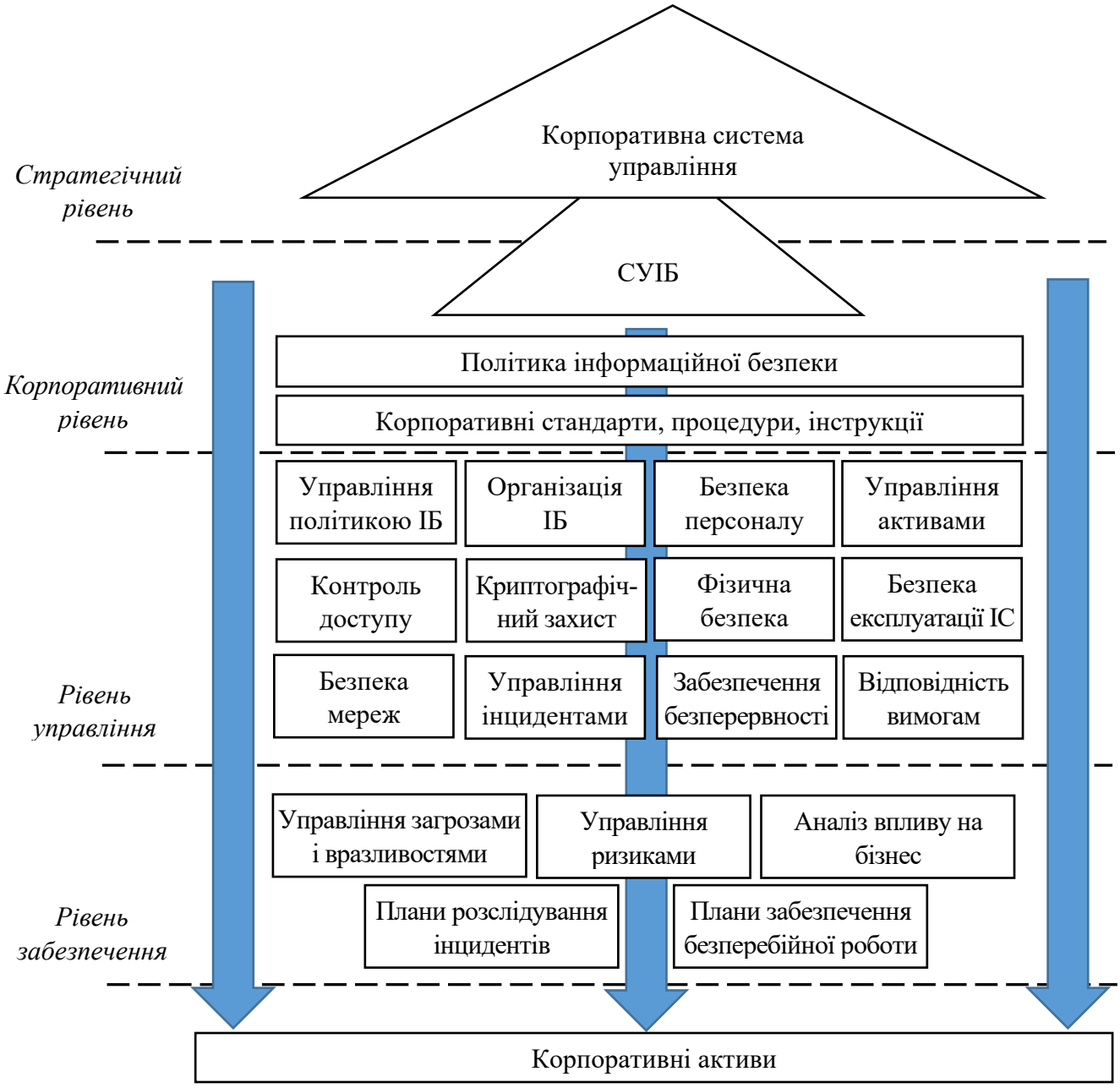

Рис. 1.2. Рівні управління інформаційною безпекою у системі управління підприємством

Рівень керування. На цьому рівні проводиться конкретизація цілей, визначених на корпоративному рівні, та визначається набір правил та дій щодо досягнення поставлених цілей.

Рівень забезпечення. На цьому рівні здійснюється реалізація організаційних і технічних заходів, спрямованих на досягнення певних цілей та зниження ризиків, що впливають на активи.

Інформація та інформаційні системи є життєво важливими активами будь-якої конкурентоспроможної організації. Неправомірні або випадкові дії щодо знищення, зміни, блокування, копіювання та розповсюдження інформації призводять до серйозних матеріальних або репутаційних збитків для організації, її контрагентів та підконтрольних організацій.

Інформація може бути представлена у різних формах: в електронному вигляді на серверах та персональних комп'ютерах, що передається по обчислювальних мережах; на паперових носіях; у вигляді усного мовлення та ін.

Проект із впровадження системи управління інформаційною безпекою з наступним виходом на сертифікацію складається з наступних етапів:

1. Проведення аналізу розбіжностей діючих процесів управління інформаційною безпекою організації з вимогами стандарту ISO/IEC 27001: 2013 та розробка Плану впровадження системи управління інформаційною безпекою;

2. Визначення та документування Області застосування системи управління інформаційною безпекою організації;

3. Розробка/доопрацювання комплекту документації системи управління інформаційною безпекою відповідно до вимог стандарту ISO/IEC 27001: 2013;

4. Проведення оцінки ризиків інформаційної безпеки в рамках затвердженої сфери застосування системи управління інформаційною безпекою та вибір засобів та заходів захисту інформації, що найбільш відповідають актуальним ризикам інформаційної безпеки;

5. Реалізація за нашою участю та під нашим контролем узгодженого Плану впровадження системи управління інформаційною безпекою, включаючи впровадження процесів забезпечення інформаційної безпеки;

6. Впровадження з нашою участю та під нашим контролем вибраних засобів та заходів захисту інформації;

7. Підтвердження коректності реалізації узгодженого Плану впровадження системи управління інформаційною безпекою у ході передсертифікаційних перевірок спільно із співробітниками організації;

8. Сертифікація системи управління інформаційною безпекою на відповідність вимогам стандарту ISO/IEC 27001:2013 [3].

Як відзначено вище, важливою передумовою ефективного захисту інформаційних активів є комплексне використання всього арсеналу наявних засобів ІБ у рамках єдиної керованої системи - СУІБ. Залежно від масштабу та виду діяльності компанії структура її СУІБ може бути різною, виходячи з економічної доцільності. Однак обов'язковими видами заходів ІБ мають бути такі:

1. правовий захист (юридична служба або окремий фахівець з юридичних питань у галузі ІБ та дотичних сферах);

2. організаційний захист (підрозділ управління/забезпечення/організації ІБ у складі фахівців управлінського профілю, охорони та режиму, що взаємодіють з відділом кадрів);

3. інженерно-технічний захист (служба ІТ та захисту інформації, які включають фахівці різного профілю: програмісти, інженери, криптографи, тестувальники, аналітики тощо), які взаємодіють із функціональними підрозділами підприємства) [35].

Керівником напряму забезпечення ІБ є директор з інформаційної безпеки на рівні заступника керівника фірми з безпеки, який керує й координує зусилля начальників зазначених служб.

Функціонально СУІБ будується у вигляді «концентричних» контурів захисту, що перекриваються (Рис. 1.3), по відношенню до зовнішніх загроз, в центрі яких перебуває об'єкт захисту. При цьому «зовнішнім» контуром є контур правового захисту, що забезпечує законність та правомірність як самого об'єкта, так і заходів щодо його захисту.

Наступний у напрямку до центру є контур організаційного захисту, що забезпечує порядок доступу до об'єкта, який безпосередньо захищається «внутрішнім» контуром інженерно-технічного захисту шляхом контролю та запобігання витоку, несанкціонованому доступу, модифікації та втраті даних [37].

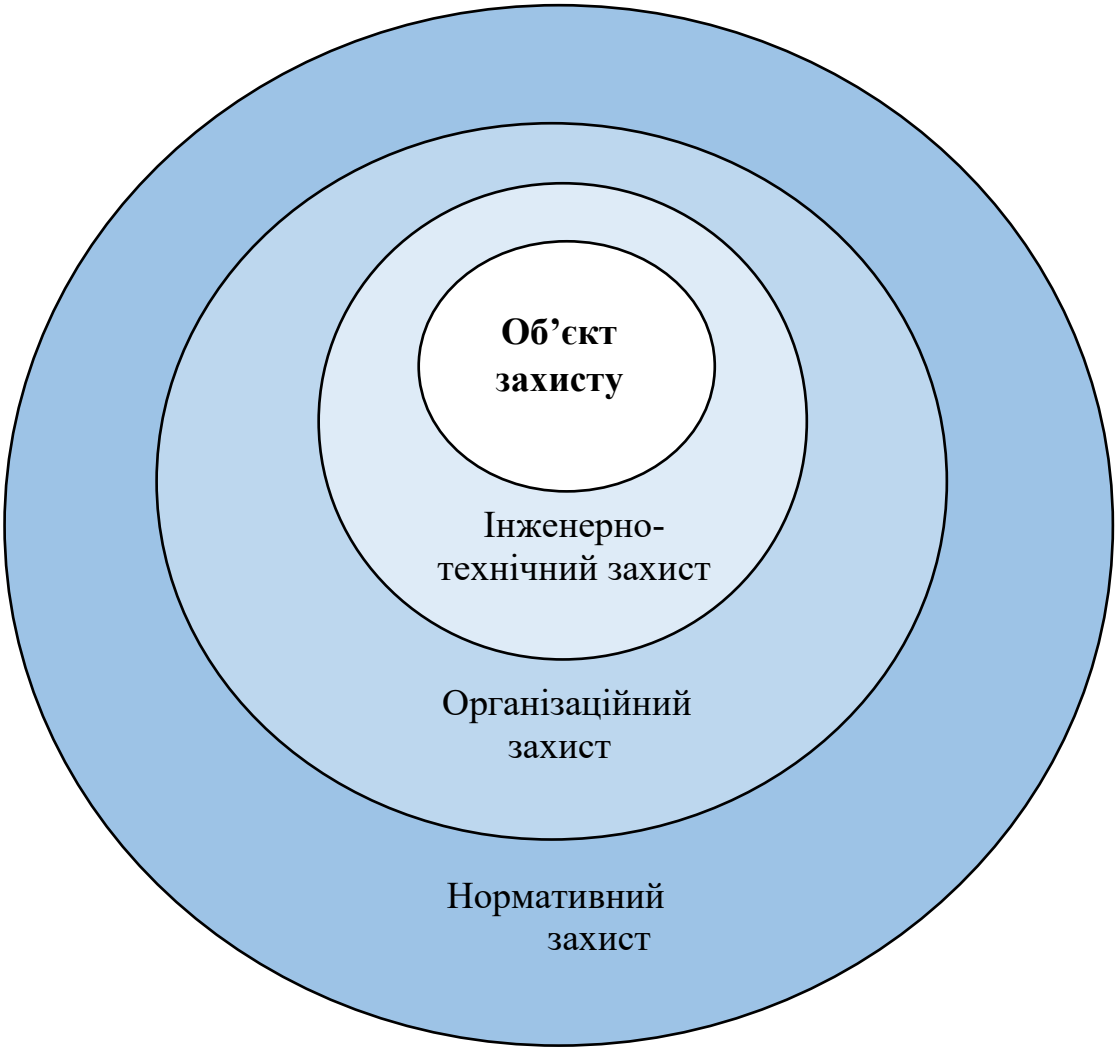

Рис. 1.3. Контури захисту об’єкта ІБ

Така побудова СУІБ дозволяє суттєво локалізувати технічний захист та скоротити витрати на нього внаслідок правової «селекції» об'єктів захисту та організації обмеженого доступу до них. Реалізація процесу ІБ у кожному із зазначених контурів відбувається приблизно за такими етапами:

1. Визначення об'єктів ІБ (обов’язок щодо захисту інформаційних ресурсів; їх вартісна оцінка, тривалість життєвого циклу та траєкторія у функціональних підрозділах компанії).

2. Виявлення загроз: джерел загроз (конкурентів, злочинців, персоналу тощо); мети загроз (ознайомлення, модифікація, знищення тощо); потенційних каналів реалізації загроз (розголошення, витік, НСД тощо).

3. Визначення необхідних заходів захисту (нормативних, організаційних, інженерно-технічних, фізичних).

4. Оцінка економічної доцільності й ефективності обраних заходів.

5. Впровадження запланованих заходів з урахуванням вироблених критеріїв (пріоритетів).

6. Доведення вжитих заходів до працівників, залучених у роботу з конфіденційними відомостями, та фахівців дотичних сфер, контроль за їх дотриманням і усунення (запобігання) наслідків загроз [37].

Описаний вище процес по суті є процесом управління інформаційною безпекою об'єкта і реалізується системою управління, що включає в себе крім самого керованого (захищеного) об'єкта, засоби контролю за його станом, механізм порівняння поточного стану з необхідним і формувач впливів, що управляють, для локалізації та запобігання шкоди внаслідок загроз . Критерієм управління у разі доцільно вважати мінімум інформаційного збитку при мінімальних витратах на ОБІ, а метою управління - забезпечення необхідного стану об'єкта у сенсі захищеності.

Поєднуючи при створенні СУІБ різні принципи управління в кожному окремому контурі захисту об'єкта можна досягти оптимального співвідношення її вартості й ефективності.

У процесі створення СУІБ доцільно взяти до уваги кращі світові стандарти і практики, зокрема рекомендації експертів Інституту програмування Університету Карнегі-Меллон, відповідно до яких ознаками ефективного управління інформаційною безпекою компанії є такі:

СУІБ охоплює все підприємство, включаючи усі його ієрархічні і горизонтальні організаційні структури, виробничі й технологічні процеси, інформаційно-телекомунікаційні та інші системи, продукти, політики та

процедури, інформаційні ресурси, а також персонал компанії, залучених працівників, партнерів і клієнтів.

Керівники компанії усвідомлюють необхідність ІБ, постійно публічно просувають ідеї захисту та безпечного поводження з інформацією, розуміють і визнають свою відповідальність і підзвітність у сфері ІБ. Управлінська діяльність із захисту інформації здійснюється на основі аналізу ризиків, нормативно закріплена в політиках, корпоративних стандартах і процедурах, має належне фінансове забезпечення, підтримується адекватними методами контролю й аудиту. Керівництво найвищого рівня несе відповідальність у випадку реалізації ризиків інформаційної безпеки.

Управління інформаційною безпекою є обов'язковим елементом системи управління компанією як безпосередня передумова досягнення стратегічних бізнес-цілей, виконання тактичних завдань і планів управління підприємством, а також забезпечення відповідності нормативних та законодавчим вимогам. Керівники усіх рівнів розуміють роль системи управління інформаційної безпеки як чинника успішного функціонування та розвитку бізнесу.

Активності з управління інформаційною безпекою розглядають як обов'язковий елемент видатків на ведення бізнесу або пряму інвестицію у його розвиток, а не як додаткову статтю витрат (за наявності ресурсів) чи видатки за залишковим принципом. Видатки на інформаційну безпеку визначаються на найвищому рівні корпоративного управління і йдуть у поєднанні із стратегією розвитку підприємства. Зміни фінансування можливі лише у випадках необхідності вдосконалення окремих бізнес-процесів, а керівники володіють відповідними засобами контролю.

Основою СУІБ є обробка ризиків, яка базується на розрахунках видатків на забезпечення достатнього рівня захищеності інформаційних активів відповідно до рівнів прийнятності ризиків, зокрема недотримання нормативних вимог, допущення технічних аварій та переривання в роботі ІТКС, негативного впливу на імідж компанії та втрати репутації, фінансових і матеріальних збитків

внаслідок реалізації інформаційних ризиків як зовнішніх (загрози), такі внутрішніх (вразливості) [35].

Повноваження і зони відповідальності персоналу з інформаційної безпеки, насамперед керівного, чітко розподілені, забезпечено дію принципу персональної відповідальності. Ключовими посадовими особами у сфері забезпечення інформаційної безпеки є директор з інформаційної безпеки (CISO), директор з питань IT (CIO), керівники відділів безпеки, управління ризиками та інших підрозділів за наявності. Зазначені посади можуть займати тільки висококваліфіковані фахівці із значним практичним досвідом роботи за фахом.

В компанії розроблена і впроваджена політика ІБ, яка відповідає специфіці і вимогам бізнесу, є актуальною і добре структурованою, доведена до відома всіх працівників. Дотримання положень і вимог політики безпеки на підприємстві забезпечується відповідними організаційними і технічними заходами, а також через використання механізмів мотивування і санкцій.

На виконання заходів із забезпечення інформаційної безпеки виділяються необхідні обсяги коштів на постійній основі. Стабільне фінансування створює можливості для того, щоб підтримувати ефективне функціонування системи управління інформаційної безпеки, забезпечувати її удосконалення за потреби.

Важливою передумовою успішності СУІБ є поінформованість і належна професійна підготовка персоналу: усі працівники, задіяні у сфері інформаційної безпеки або ті, що мають володіти відповідними знаннями і навичками із захисту інформації на своїх робочих місцях, ознайомлені зі своїми безпосередніми обов’язками щодо підтримання достатнього рівня захисту і безпечного поводження з цінними інформаційними активами та засобами їх обробки.

Важливими у цьому контексті є мотивованість персоналу і дотримання встановлених правил безпеки, які мають бути інтегровані у корпоративну культуру. Навчання і підвищення кваліфікації з питань захисту інформації здійснюється на постійній основі і відповідати запитам інформаційної безпеки.

Вимоги ІБ є обов’язковими елементами усіх етапів життєвого циклу ПЗ, починаючи від придбання чи розробки, тестування, впровадження в дію, технічний супровід і виведення з експлуатації та знищення.

ІБ підприємства має реалізуватися на плановій, керованій і вимірюваній основі. Заходи інформаційної безпеки є невід’ємною частиною оперативного і довготермінового планування, елементом бюджетного планування. Цілі і завдання інформаційної безпеки мають бути досяжними і вимірюваними, їх досягнення контролюється на основі використання відповідних методик оцінювання - метрик.

Аудит інформаційної безпеки є засобом визначення відповідності реальних заходів запланованим, виявлення прогалин у системі управління інформаційною безпекою, забезпечення неперервності бізнес-процесів підприємства. Досягнення встановленого рівня забезпечення ІБ є ознакою належної роботи керівників та рядових фахівців. Наявність ефективної системи управління інформаційною безпекою є великим плюсом для ділової репутації компанії і налагодження надійних і довгострокових відносин з партнерами і клієнтами [35].

Для виявлення слабких місць СУІБ та подальшого її удосконалення підприємство проводить регулярні аудити – перевірки, які дозволяють оцінити рівень захисту і є підставою внесення коректив у корпоративні заходи безпеки. Завдяки проведенню незалежних перевірок компанія зможе підтримувати прийнятний рівень інформаційної безпеки.

1.3 Технології роботи з персоналом у СУІБ

На виконання вимог стандарту ISO/IEC 27001 у стандарті ISO/IEC 27002 організаціям та підприємствам рекомендовано формалізувати і структурувати процеси управління інформаційною безпекою за наступними блоками [7]:

- розробка політики безпеки;
- організація інформаційної безпеки;

- організація управління внутрішніми активами та ресурсами, що становлять основу ключових бізнес-процесів;
- *захист персоналу та зниження внутрішніх загроз;*
- фізична безпека та безпека навколишнього середовища;
- управління засобами зв'язку та експлуатацією обладнання;
- управління та контроль доступу;
- розробка та обслуговування апаратно-програмних систем;
- управління безперервністю бізнес-процесів;
- забезпечення відповідності вимогам стандарту та дотримання правових норм щодо безпеки.

Як бачимо одним із обов'язкових елементів управління інформаційною безпекою є робота з персоналом з метою зниження ризиків внутрішніх порушень інформаційної безпеки.

На основі вивчення теорії управління персоналом [14, 22, 27] виділимо такі основні напрями роботи з персоналом, задіяним у СУІБ підприємства (Рис.1.4.):

- планування чисельності та професійно-кваліфікаційної структури персоналу відповідно до економічної доцільності та потреб у забезпеченні інформаційної безпеки підприємства;
- аналіз робіт і формування вимог до працівників з урахуванням принципу мінімізації загроз несанкціонованого доступу до інформації працівників, які не мають на це дозволу;
- професійний підбір і відбір персоналу з використанням традиційних кадрових процедур та методик психологічної оцінки, а також різних форм перевірки особистісних та професійних якостей претендента;
- виробнича і соціальна адаптація новоприйнятих працівників, що включає проведення комплексу занять практичного характеру, інструктажів, тренінгів з питань інформаційної безпеки та захисту інформації;
- чіткий розподіл і передача повноважень відповідно до вимог обмеженого доступу працівників до конфіденційної інформації;

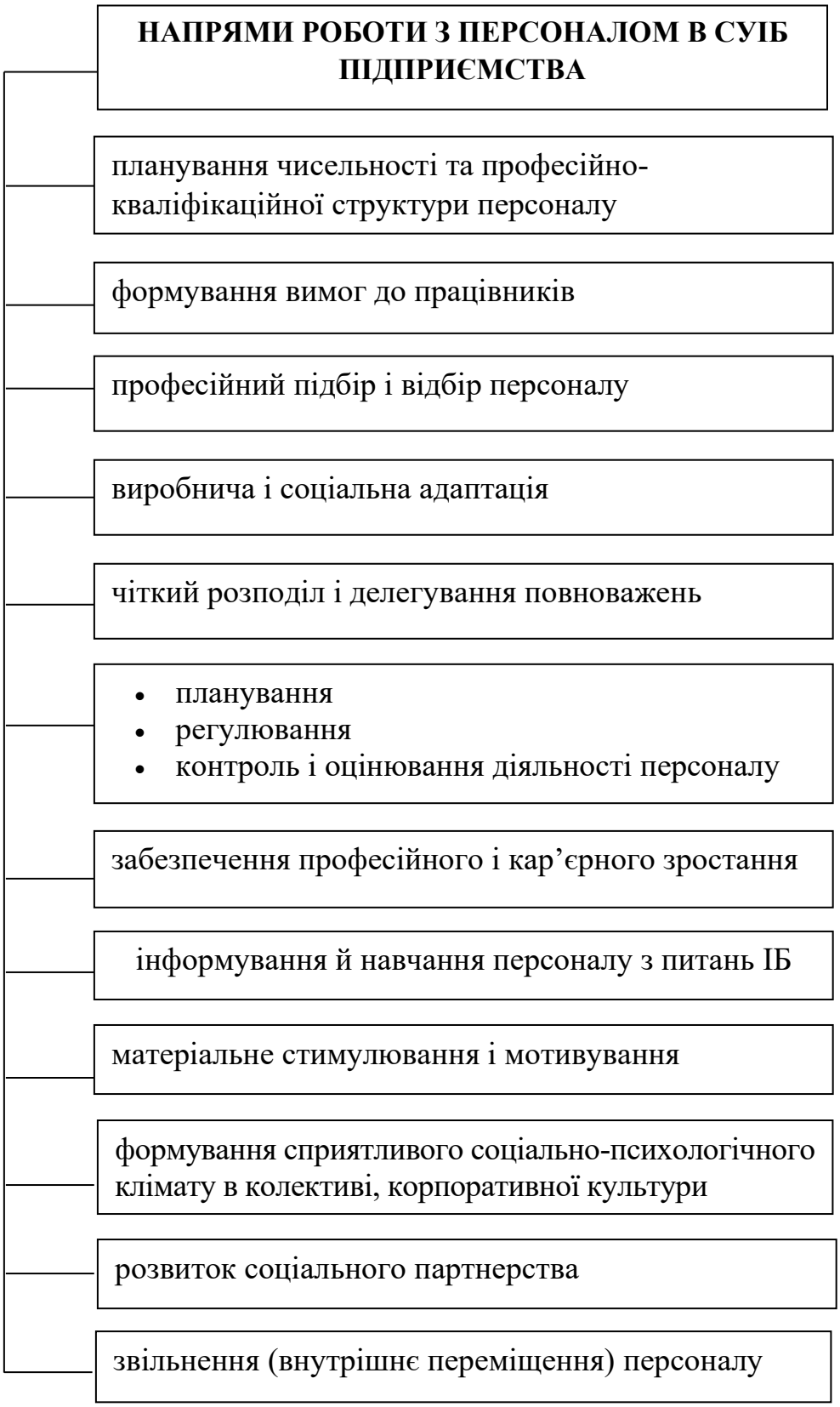

Рис. 1.4. Напрями менеджменту персоналу в СУІБ підприємства

- планування та регулювання трудової діяльності персоналу, здійснення контролю й оцінювання праці як окремих працівників, так і проектних команд, колективів функціональних підрозділів;

- забезпечення професійного та кар’єрного розвитку персоналу, що працює у системі управління інформаційною безпекою;
- інформування й навчання працівників, залучених до роботи з конфіденційними даними, засобами їх обробки та передачі, а також усього колективу підприємства з питань інформаційної безпеки;
- застосування ефективних систем матеріального і морального стимулювання праці з метою не тільки формування лояльності працівників до своєї компанії, але запобігання порушенням інформаційної безпеки;
- розвиток соціального партнерства в компанії, що передбачає налагодження конструктивних відносин та атмосфери взаєморозуміння між власниками, топ-менеджментом підприємства та його трудовим колективом;
- підтримання сприятливого соціально-психологічного клімату в колективі, формування корпоративної відданості й культури, в тому числі культури інформаційної безпеки;
- звільнення (або переміщення на інші посади) персоналу з дотриманням спеціальних процедур тощо.

Таким чином, можна говорити про використання в управлінні інформаційною безпекою підприємства низки технологій управління персоналом (кадрових технологій). Під кадровою технологією розумітимемо набір операцій і процедур впливу на персонал підприємства, які дозволяють забезпечити укомплектування необхідною кількістю працівників з очікуваними професійними й особистісними характеристиками, досягти оптимальної продуктивності праці і, в кінцевому рахунку, гарантувати ефективне функціонування бізнесу.

Однак, застосування технологій управління персоналом в СУІБ підприємства має свої особливості. З огляду на високу ціну пошкодження, втрати чи витоку конфіденційної інформації управління персоналом має допомагати у виконанні низки важливих завдань інформаційної безпеки.

Для зменшення ризиків нанесення шкоди інформаційним активам підприємства з боку персоналу особливого значення набувають: формування

стабільного трудового колективу і подолання плинності кадрів; посилений контроль і ускладнена процедура оцінювання персоналу перед працевлаштуванням та під час роботи; встановлення персональної відповідальності й чіткий розподіл обов'язків із захисту інформації; нормативне закріплення вимог та обмежень щодо нерозголошення інформації; забезпечення високого рівня обізнаності й належної кваліфікації персоналу з інформаційної безпеки; формування ефективної системи мотивування персоналу, формування лояльного, відданого колективу тощо [19, 41].

На основі вивчення традиційних підходів до управління персоналом та врахування його специфіки у сфері інформаційної безпеки запропоновано схему застосування кадрових технологій для мінімізації та/або нейтралізації ризиків інформаційній безпеці, пов’язаних з персоналом (Рис.1.5).

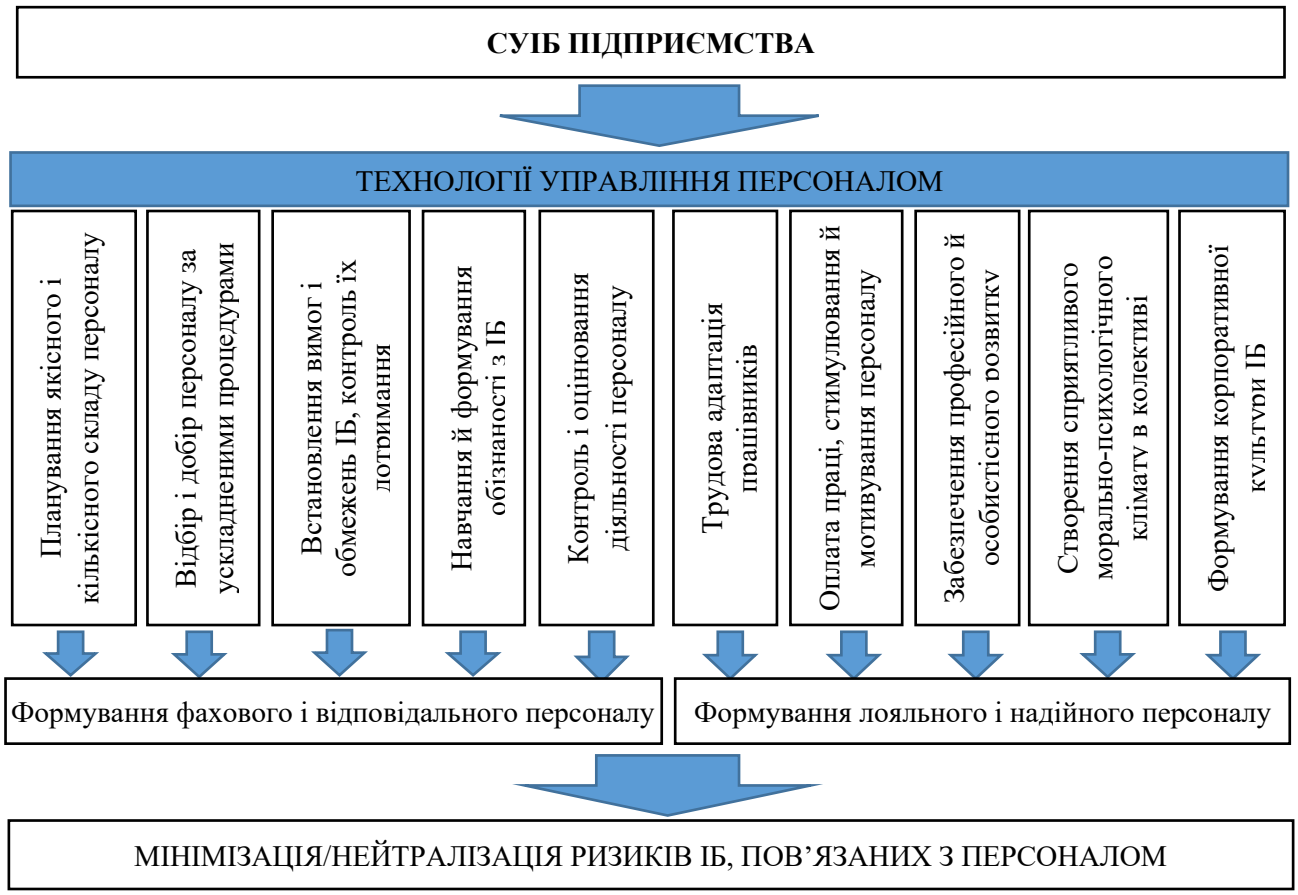

Рис.1.5. Схема застосування кадрових технологій у забезпеченні інформаційної безпеки

Таким чином, основні технології управління персоналом, які використовують як засоби забезпечення інформаційної безпеки підприємства,

можна умовно поділити на два блоки: перший блок включає кадрові технології, які забезпечують формування кваліфікованого і відповідального персоналу через переважно (але не виключно) використання адміністративних засобів впливу; другий – технології формування лояльного і надійного персоналу, реалізація яких частіше здійснюється економічними та психологічними методами.

Висновки до розділу 1

Встановлено, що основою функціонування системи управління ІБ є ризико-орієнтований підхід, тобто спрямування зазначених заходів на запобігання реалізації загроз інформаційній безпеці підприємства. Основними складовими СУІБ є політика, дії з планування, організаційні структури, повноваження, процеси, процедури і ресурси. Життєвий цикл СУІБ включає такі етапи: планування, впровадження, моніторинг і аналіз, удосконалення. Кожен етап характеризується виконанням різноманітних процедур.

Побудова СУІБ здійснюється відповідно до вимог міжнародного стандарту ISO/IEC 27001:2013, який забезпечує можливість комплексного захисту всіх форм та засобів обробки інформації підприємства з метою забезпечення її конфіденційності, цілісності та доступності.

СУІБ є невід’ємною частиною інтегрованої системи управління компанією, яка складається з кількох рівнів управління: стратегічного, корпоративного, керування та забезпечення. Важливою передумовою ефективного функціонування СУІБ є поєднання заходів правового, організаційного та інженерно-технічний захисту.

Функціонально СУІБ будується у вигляді «концентричних» контурів захисту, що перекриваються, по відношенню до зовнішніх загроз, в центрі яких перебуває об'єкт захисту. При цьому «зовнішнім» контуром є контур правового захисту, що забезпечує законність та правомірність заходів. Наступний у напрямку до центру є контур організаційного захисту, що забезпечує порядок доступу до об'єкта, який безпосередньо захищається «внутрішнім» контуром інженерно-технічного захисту

шляхом контролю та запобігання витоку, несанкціонованому доступу, модифікації та втраті даних.

Одним із основних напрямів СУІБ є управління персоналом. На основі вивчення традиційних підходів до управління персоналом та врахування його специфіки у сфері ІБ запропоновано схему застосування кадрових технологій для мінімізації та/або нейтралізації ризиків інформаційній безпеці, пов’язаних з персоналом. Таким чином, основні технології управління персоналом, які використовують як засоби ІБ підприємства, умовно поділено на два блоки: перший блок включає кадрові технології, які забезпечують формування кваліфікованого і відповідального персоналу через переважно (але не виключно) використання адміністративних засобів впливу; другий – технології формування лояльного і надійного персоналу, реалізація яких частіше здійснюється економічними та психологічними методами.

Розділ 2.
КАДРОВІ АСПЕКТИ ДІЯЛЬНОСТІ ПОСАДОВИХ ОСІБ І ПІДРОЗДІЛІВ КОМПАНІЇ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1 Роль топ-менеджменту підприємства у забезпеченні ІБ

Топ-менеджмент підприємства затверджує й забезпечує реалізацію політики (сформульованою радою директорів), стратегії, бізнес-планів, бюджету та проектів. Топ-менеджмент приймає рішення, які впливають на весь колектив підприємства, а також відповідає за успішність або невдачі компанії.

Сучасні менеджери підприємства найвищого рівня зазвичай мають різні спеціалізації та відповідають за різні напрямки бізнес-діяльності. До кожної позиції висуваються певні професійній, освітні та особистісні вимоги. Серед позицій топ-менеджерів найчастіше виділяють: генерального директора, виконавчого директора, технічного директора, операційного директора, фінансового директора.

Західна концепція управління передбачає наявність таких посадових осіб найвищого управлінського рівня: CEO (Chief Executive Officer) – генеральний директор - головна посадова особа підприємства; CHRO (Chief Human Resources Officer) - директор з персоналу; CIO (Chief Information Officer) - директор з інформаційних технологій; CLO (Chief Legal Officer) – головний юрисконсульт, директор юридичної служби; CSO (Chief Security Officer) - директор із забезпечення безпеки бізнесу, голова корпоративної служби безпеки.

У нинішніх умовах величезного значення технологій захисту інформації практично у кожній компанії середнього і великого бізнесу є посада директора з інформаційної безпеки – CISO, Chief Information Security Officer [8].

Зазначені вище посадові особи є представниками керівництва вищої ланки, яке відповідає за управління підприємством, тобто здійснює вплив на колектив компанії та всі сторони її діяльності з метою отримання максимальних результатів. Керівники вищої ланки приймають або затверджують всі життєво

важливі рішення в діяльності компанії. Робота вищого керівництва передбачає найвищий ступінь відповідальності, великі обсяги і напружений темп.

Топ-менеджери, відповідно до класичної теорії управління виконують такі функції: організація управлінської системи; вибір цілей; прогнозування; планування; акумулювання й аналіз інформації; прийняття рішень; організацію діяльності підлеглих підрозділів; контроль; оцінювання ефективності управління. Деякі фахівців додають до функцій керівництва найвищого рівні функції регулювання і корегування, а також обліку й контролю.

Беручи за основу концепцію дослідників функцій керівника щодо організаційних систем В. Рубахіна й А. Філіппова [40] виділимо такі загальні та спеціальні функції топ-менеджменту з інформаційної безпеки.

Загальні функції:

- прийняття і реалізація загально-корпоративних рішень у сфері ІБ;
- встановлення мети й основних завдань діяльності підприємства щодо забезпечення ІБ, прогнозування розвитку системи забезпечення ІБ компанії на коротко- та довготерміновий періоди;
- формування лояльного, надійного і працездатного колективу фахівців із захисту інформації та ІБ;
- формування раціональної організаційної структури департаменту/ підрозділу ІБ;
- розподіл функціональних обов'язків, наявних ресурсів і засобів усередині департаменту/підрозділу ІБ;
- розробка і впровадження ефективної організації праці й управління.

Спеціальні функції:

Планово-економічна функція включає:

- визначення потреби в людських, матеріальних і фінансових ресурсах для забезпечення ефективного функціонування системи забезпечення ІБ, контроль за їх наявністю та використанням - за погодженням з керівником підприємства;

- затвердження нормативних документів у сфері ІБ підприємства й контроль дотримання задекларованих у них вимог;
- планування й загальна координація діяльності департаменту/ підрозділу ІБ, а також усіх функціональних підрозділів компанії у частині дотримання вимог ІБ з метою забезпечення ефективного використання людських, матеріальних і технічних ресурсів;
- прогнозуванням потенційних «прогалин» - вразливостей у корпоративній системі забезпечення ІБ і плануванням заходів для їх усунення

Кадрова функція передбачає такі види діяльності:

- планування й комплектування кадрів у сфері ІБ та загальним керівництвом департаментом/підрозділом ІБ щодо виконання ними своїх функціональних обов'язків;
- забезпечення обізнаності, навчання й підвищення кваліфікації працівників департаменту/підрозділу ІБ, а також усіх функціональних підрозділів підприємства з питань ІБ та захисту інформації;
- розробка і впровадження заходів морального й матеріального стимулювання працівників, формування лояльного колективу фахівців з ІБ;
- організація моніторингу й оцінювання діяльності персоналу, задіяного у сфері забезпечення ІБ.

Технолого-управлінська функція охоплює:

- визначення завдань і оцінювання професійної/виробничої діяльності із забезпечення ІБ;
- визначення способів і засобів виконання завдань із забезпечення ІБ відповідно до можливостей колективу (кількості і кваліфікації спеціалістів, часу, матеріального й технічного (програмно-апаратного) забезпечення;
- прийняття рішень за напрямом забезпечення ІБ, визначення завдань керівнику департаменту/підрозділу ІБ, контроль їх виконання з термінами;
- оцінювання ефективності і своєчасності виконання поставлених завдань із забезпечення ІБ, підбиття підсумків, коригування завдань.

Як бачимо із перелічених функцій топ-менеджера підприємства управлінську діяльність можна розглядати як системну діяльність із управління персоналом, яка передбачає інтеграцію індивідів шляхом ознайомлення працівників із загальними завданнями, цілями, визначення засобів та умов їх досягнення, а також завдяки плануванню, координації спільної праці, обліку і контролю; комунікацію всередині колективу і з вищими ланками управління; навчання й виховання (і, як наслідок, забезпечення кваліфікованим і лояльним персоналом).

На основі положень міжнародного стандарту ISO 27001 можна зробити висновок, що основними показниками ефективної діяльності керівництва підприємства, в тому числі директора з ІБ, є такі:

a) наявність корпоративної політики ІБ, встановлення цілей та ведення діяльності із забезпечення ІБ, які відображують цілі бізнесу;

b) впровадження корпоративного підходу до забезпечення ІБ з дотриманням основних правил проектування, реалізації, супроводження, моніторингу і вдосконалення діяльності у сфері ІБ відповідності із культурою компанії;

c) офіційна та загальновідома підтримка та зобов’язання керівництва усіх рівнів щодо забезпечення ІБ;

d) усвідомлення необхідності і глибоке розуміння вимог ІБ, оцінювання й управління ризиками ІБ як запорука запобіжного характеру діяльності із захисту інформації та дотичних дій;

e) розроблення і розподіл ролей і відповідальностей щодо забезпечення ІБ;

f) розповсюдження настанов щодо політики ІБ та стандартів всім керівникам, працівникам підприємства та іншим зацікавленим сторонам;

g) забезпечення належного фінансування діяльності із забезпечення ІБ;

h) забезпечення відповідних поінформованості, навчання та освіти фахівців із захисту інформації та ІБ, а також усього трудового колективу з питань ІБ;

i) розробка і впровадження ефективного процесу управління інцидентами ІБ;

j) впровадження системи вимірювань, яка використовується для оцінювання результативності забезпечення ІБ і пропозицій зворотного зв’язку для вдосконалення [6] (Рис. 2.1).

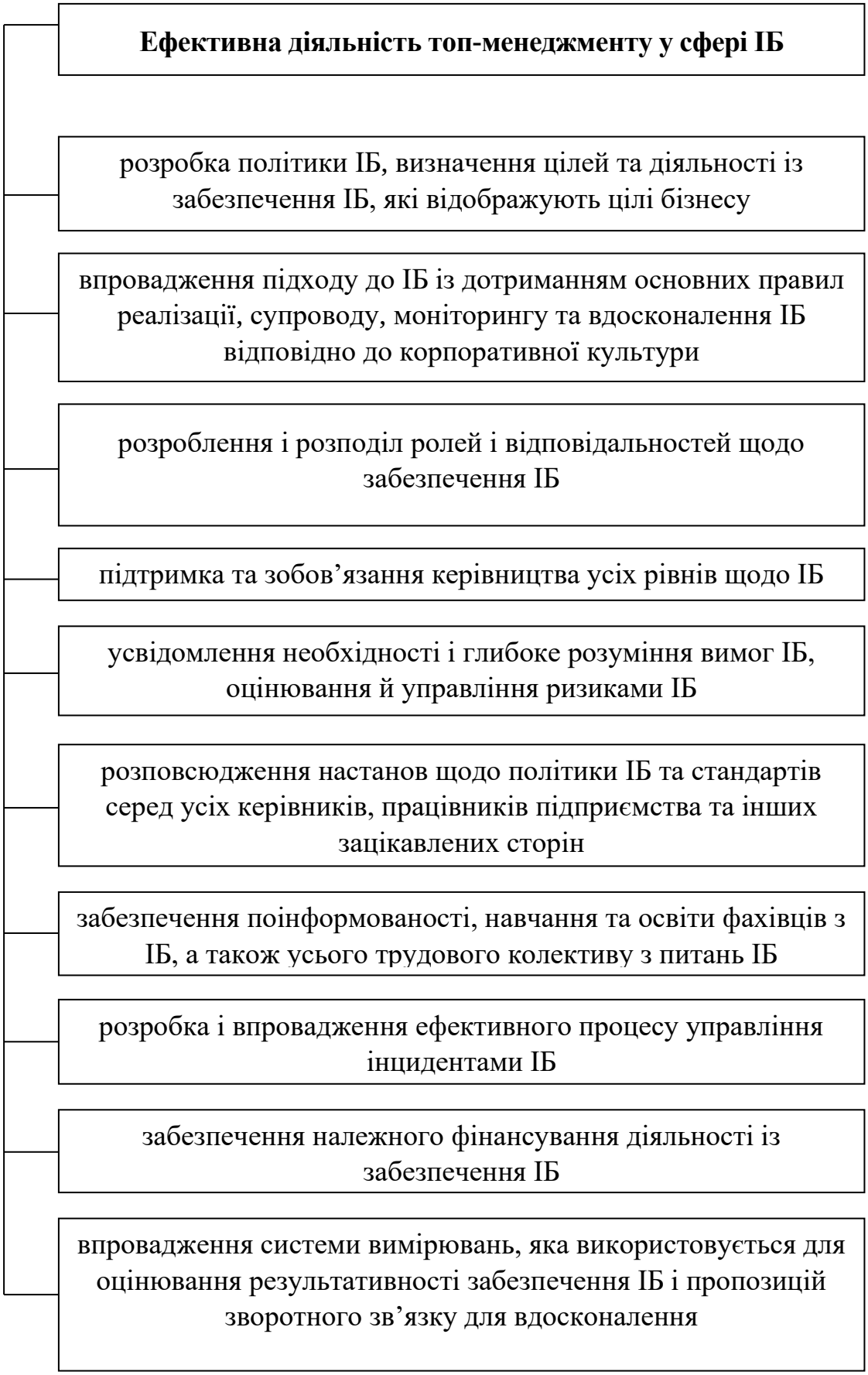

Рис.2.1. Показники ефективності топ-менеджменту у сфері ІБ.

Підводячи підсумок, варто наголосити на визначальній ролі директора з інформаційної безпеки у забезпеченні ефективного захисту інформаційних активів та корпоративних ІТКС. Водночас безсумнівним є той факт, що успішна реалізація комплексу різнопланових заходів у сфері ІБ не є можливою без виведення питань забезпечення ІБ на рівень бізнес-підрозділів та топ-менеджменту, а також зосередження й координування зусиль усіх перелічених на початку посадових осіб найвищого рівня: генерального директора, директора з персоналу, директора з ІТ, голова корпоративної служби безпеки, директора з інформаційної безпеки.

2.2 Напрями роботи служби ІБ з персоналом

Роль кадрової безпеки в СУІБ підприємства пов’язана із зниження ризиків та загроз, пов'язаних з недоброякісною роботою й поведінкою персоналу, його інтелектуальним потенціалом та трудовими відносинами загалом.

Зокрема, в СУІБ підприємства кадрові технології забезпечують наймання й утримання психологічно придатного до роботи з конфіденційною інформацією, висококваліфікованого та надійного персоналу.

Психологічна придатність до роботи визначається властивостями психіки працівника, що дозволяють безпомилково та впевнено виконувати свої трудові та службові функції, не наражаючи на ризик підприємство. Особливо важливим є збереження працездатності в умовах високого рівня відповідальності та напруженості, тривалих стресів, фізичних та психологічних перевантажень, які характерні для галузі інформаційної безпеки та захисту інформації.

Професійна придатність фахівців з інформаційної безпеки забезпечується рівнем знань, кваліфікації та досвіду, можливістю постійно оновлювати й вдосконалювати свої компетентності відповідно до розвитку ІТ, наявністю професійних якостей, розвиненою професійною культурою.

Особистісна придатність характеризується надійністю й відданістю працівника своїй компанії, його лояльність з позиції оцінки власних особистих моральних якостей, соціального оточення [12].

Служба інформаційної безпеки підприємства саме і повинна забезпечити виконання завдань щодо наймання психологічно придатного, висококваліфікованого та надійного персоналу й забезпечення його результативної та якісної роботи з конфіденційною інформацією. Служба інформаційної безпеки має надавати допомогу керівництву та кадровим підрозділам краще пізнати працівників і передбачити їх дії.

Світова статистика свідчить про те, що близько 80% шкоди матеріальним активам організацій завдає їх власний персонал. За останні 20 років близько 100 банків США зазнали краху через шахрайство персоналу. У вітчизняному бізнесі ситуація є аналогічною. Саме тому топ-менеджерам необхідно мати якомога більш повне уявлення про якість «людського капіталу», який є носієм конфіденційної корпоративної інформації.

Основними умовами ефективності роботи з персоналом є узгодженість діяльності служби ІБ за різними напрямами (внутрішня безпека, інформаційна безпека, правова безпека, технічний захист тощо) і тісний контакт з іншими структурними підрозділами (відділом кадрів, юридичним відділом, службою економічної безпеки) [20].

Завдання служби ІБ - з одного боку, виявляти осіб, схильних до порушень інформаційної безпеки, шахрайства, недобросовісної роботі та інше, з іншого - сприяти створенню єдиної команди перевірених старанних фахівців. Для цього проводяться організаційні та організаційно-технічні заходи, використовуються особисті спостереження і бесіди, а також результати інформаційно-аналітичної роботи.

Вибудовуючи свою діяльність в компанії таким чином, служба ІБ має проводити її принципово і компетентно через здійснення організаційних та організаційно-технічних заходів (Рис. 2.2).

Організаційні заходи з питань інформаційної безпеки, що проводяться в компанії, включають:

- організацію і проведення процедур добору та відбору кандидатів на зайняття вакантних посад у сфері інформаційної безпеки;
- регламентацію внутрішньо-корпоративних процедур захисту інформації та поводження з її носіями, в тому числі розробку нормативних документів (політик, положень, процедур, інструкцій, а також розпорядчих документів);
- організацію контролю за діяльністю персоналу компанії у сфері інформаційної безпеки;

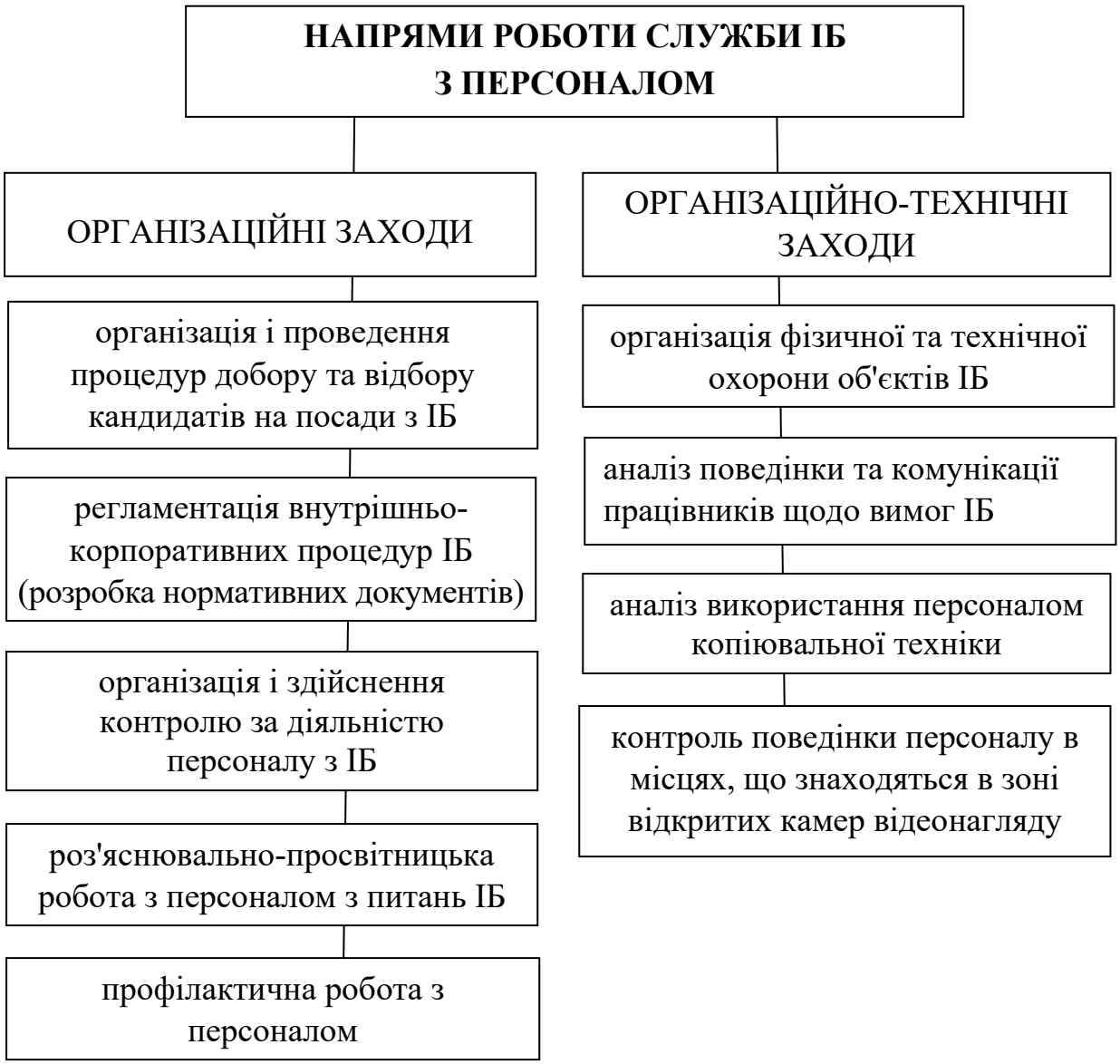

Рис. 2.2. Напрями роботи служби ІБ з персоналом

- роз'яснювально-просвітницьку роботу з працівниками усіх підрозділів підприємства з питань захисту інформації (проведення занять по збереженню комерційної таємниці, правил безпечної поведінки і використання інформаційних систем та ресурсів компанії, методів зловмисної поведінки у сфері інформаційної безпеки, в т. ч. соціальної інженерії тощо);
- профілактичну роботу зі співробітниками (виявлення осіб, схильних до порушень інформаційної безпеки, роз'яснення наслідків неправомірних дій).

Організаційно-технічні заходи з питань інформаційної безпеки включають:

- організацію фізичної та технічної охорони об'єкта (в т. ч. контрольно-пропускного режиму (вхід-вихід персоналу та зовнішніх осіб) і внутрішнього режиму (режим роботи співробітників, дотримання обмежень, пов’язаних з використанням конфіденційних відомостей та засобів їх обробки, запобігання витоку інформації технічними каналами тощо);
- аналіз поведінки та комунікації працівників з питань інформаційної безпеки (використання електронної пошти, відвідування Інтернет-ресурсів, спілкування у соцмережах та месенджерах, зміст переговорів через службові телефони, вивчення зв'язків між співробітниками тощо);
- аналіз використання копіювальної техніки (з метою запобігання витоку інформації, що становить конфіденційну інформацію);
- контроль поведінки персоналу в місцях, що знаходяться в зоні відкритих камер відеоспостереження [20].

Особисті спостереження і бесіди дозволяють вивчити: особистісні особливості працівників компанії; особливості психологічного клімату в колективі; ступінь задоволеності співробітників умовами праці, заробітною платою тощо.

Мета інформаційно-аналітичної роботи служби ІБ з персоналом - виявлення позитивних і негативних моментів, пов'язаних з поведінкою працівників. Інформаційно-аналітична діяльність складається з двох етапів:

- збір та обробка інформації;

- аналіз і оцінка отриманих відомостей для прийняття оперативних управлінських рішень.

Накопичення інформації про конкретного працівника починається з моменту вивчення його особистості при прийомі на роботу і триває безперервно протягом усієї його трудової діяльності в компанії. Розпорядок робочого дня співробітника, особливості його поведінки під час спілкування з колегами та партнерами, у ході організації заходів захисту інформації, підготовки і введення в дію нормативних та розпорядчих документів є предметом постійної уваги з боку відповідальних фахівців служби ІБ.

Дуже корисну інформацію про працівників компанії можна отримати при проведенні неофіційних заходів (свята, вечори відпочинку, екскурсії, культурні та спортивні заходи). За таких обставин можна об’єктивно оцінити мікроклімат в колективі, рівень інтелекту й культури, особисту поведінка співробітників.

Отримані в результаті таких спостережень відомості щодо працівників, задіяних у забезпеченні інформаційної безпеки, формалізують, складаючи довідки або інші аналітичні документи, які долучають до особової справи співробітника. Це дозволяє систематизувати роботу з даними. Аналогічні довідки можуть складатися на основі контролю за виконанням працівником його професійних та посадових обов’язків. У них фіксують факти прояву з боку працівника недбалості при виконанні посадових обов'язків, прийняття непрофесійних, хибних рішень, порушень дисципліни, нечесності тощо або навпаки: свідчення високих результатів у роботі, сумлінність при виконанні своїх обов'язків, високі особисті якості (порядність, чесність, відповідальність, виваженість тощо). Аналітична інформація повинна містити висновки, отримані в результаті оцінки встановлених фактів [20].

У нинішніх умовах на допомогу у вирішенні питань інформаційно-аналітичної роботи, пов’язаної з діяльністю й поведінкою персоналу, приходять спеціальні програмні засоби, наприклад:

- системи запобігання втраті даних (Data Loss Prevention - DLP). DLP-системи забезпечують контроль усіх видів комунікацій працівника (електронна

пошта, веб-трафік, месенджери, хмарні додатки, обмін інформацією між робочими станціями, переносні носії, засоби бездротового доступу тощо) [10];

- системи аналітики поведінки користувачів (User Behaviour Analitics - UBA). Завдяки моніторингу різних джерел (журналів серверних і мережевих компонентів, журнали систем аутентифікації і безпеки, кінцевих станцій, переписки у соцмережах, месенджерах і через е-пошту) UBA-системи виявляють випадки крадіжки даних, компрометації облікових даних, зловживання привілеями, аномальної поведінки працівників [21]
- системи управління інформацією та подіями безпеки - (Security Information and Event Management - SIEM), які також зосереджуються на аналізі даних і подій з файєрволів, операційних та інших систем, різних реєстраційних журналів, щоб встановити випадки підозрілих дій і поведінки з боку персоналу [28].

У роботі з персоналом служба ІБ має враховувати вплив зовнішніх і внутрішніх факторів, які можуть відображатися на діяльності компанії як позитивно, так і негативно.

До зовнішніх чинників відносять: соціально-економічні (покращення або погіршення соціально-економічної ситуації в державі, соціальні зміни, зростання напруги в суспільстві, рівень безробіття й оплати праці тощо); політичні (дестабілізація політичної ситуації, конфлікти в суспільстві, нормативно-правові зміни або корупція).

До внутрішніх чинників належать: погіршення організації управлінськими процесами в компанії, стиль керівництва (переважання авторитарних підходів, небажання з’ясовувати реальний стан справ тощо), особливості внутрішньо-корпоративної культури.

У ході виявлення випадків неадекватної поведінки працівника компанії під час виконання ним службових обов'язків, у відносинах з колегами співробітник служби ІБ має звертати особливу увагу на такі факти: порушення режиму трудового дня (невмотивовані запізнення на роботу, відлучення в робочий час, вихід на роботу у позаробочий час, затримки на роботі); схильність до азартних

ігор; зловживання алкоголем, наркотична залежність; наявність серйозних особистих проблем, стресів.

Про можливі «фактори ризику» для компанії можна говорити в тому випадку, коли в поведінці працівника спостерігається: інтерес до кола виробничих і фінансових питань компанії, які не входять до його функціональних обов'язків; невиправдано часті дзвінки і контакти з організаціями та особами, не пов'язаними діловими відносинами з компанією; ведення в робочий час будь-яких справ, що не входять в функціональні обов'язки; помітні зміни в стилі спілкування з колегами, поява невпевненості, страху; використання в неробочий час обладнання, розмножувальної техніки в особистих цілях; ознаки раптового погіршення матеріального становища співробітника, різке збільшення його особистих витрат, що не відповідає офіційним доходам (придбання дорогих товарів, нерухомості тощо) [20].

Одна з форм роботи служби ІБ - вивчення взаємовідносин між керівниками структурних підрозділів ІТ та захисту інформації і підлеглими. У компанії повинні бути розроблені форми контролю за роботою співробітників - картки оцінки праці (своєчасність, якість роботи, творчий підхід, ініціативність, самостійність у прийнятті рішень). Різко негативна або завищена оцінка діяльності працівників вимагає додаткового вивчення і виявлення причин.

Завдяки інформації, отриманій від довірених осіб і в особистих бесідах, співробітники служби ІБ можуть вивчати психологічний клімат в колективі, ставлення персоналу до різних форм стимулювання праці тощо. Про свої спостереження служба ІБ інформує керівництво компанії.

Велика увага при роботі з персоналом служба ІБ має приділяти питанням забезпечення захисту конфіденційної інформації, яка належить або обробляється компанією, а її витік може завдати шкоди бізнес-інтересам. З огляду на це безпосереднім обов’язком служби ІБ є розробка корпоративної політики ІБ, нормативних документів і переліку відомостей, що відносяться до різних видів інформації обмеженого доступу, положення про систему доступу до таких документів, а також порядок обліку, зберігання і організації роботи з ними.

Представник служби ІБ бере безпосередню участь у процесі добору й відбору претендентів на зайняття вакантних посад у сфері ІБ та захисту інформації, зокрема надає перелік вимог до потенційного кандидата (освіта, досвід, особисті та професійні якості), вивчає документи, надані кандидатом, проводить співбесіду з фахових питань, за потреби збирає інформацію про зазначену особу щодо наявності судимості чи фінансових проблем.

При прийомі на роботу нових співробітників представник служби ІБ проводить інструктаж на робочому місці, знайомить їх з правилами роботи з документами, що містять конфіденційну інформацію, організовує підписання новопризначеним працівником зобов'язання про нерозголошення конфіденційних відомостей, доступ до яких буде отримано у ходів професійної діяльності, у контракті або трудовій угоді [42].

Контролюючи дотримання працівниками компанії встановленого порядку забезпечення ІБ, вимог захисту конфіденційної інформації, служба ІБ виявляє факти їх порушення. Для цього використовуються організаційні, технічні заходи, а також робота з довіреними особами. Аналізуючи причини витоку інформації, служба ІБ пропонує способи їх усунення, а також виявляє осіб, які можуть сприяти такому витоку або прямо передавати конфіденційну інформацію підприємства конкурентам.

Здійснюючи організаційно-технічні заходи роботи з персоналом служба ІБ має регламентувати і контролювати дотримання персоналом вимог користування Інтернетом і локальною мережею компанії. Доцільно підготувати інструкцію про порядок їх використання, в якій регламентувати допуск співробітників, передбачити закриття доступу окремим користувачам при їх переміщеннях, звільненні тощо, а також при нецільовому використанні Інтернету та локальної мережі.

Кожна компанія також визначає власні корпоративні правила використання електронної пошти, що доводиться до персоналу у вигляді розпоряджень, інструкцій. Завдання служби ІБ у співпраці з ІТ-відділом полягає у фіксації спроб

та випадків витоку конфіденційної інформації через використання спеціальних програмних та апаратних засобів.

Служба ІБ бере активну участь у запобіганні й вирішенні конфліктних ситуацій між керівниками і підлеглими, між інтересами співробітників і компанії. Обов’язком служби безпеки є об'єктивна їх оцінка і пошук компромісів між сторонами, що має на меті зниження ризиків порушень інформаційної безпеки компанії, а в кінцевому рахунку – уникнення потенційних збитків компанії від дій нелояльного персоналу [20].

Підсумовуючи, варто відзначити, що служба ІБ здійснює не тільки регламентуючі та контролюючі функції, але також сприяє формуванню в колективі обстановки довіри та взаєморозуміння, надає підтримку працівникам з усіх проблемних питань, забезпечує справедливу оцінку праці і можливості кар'єрного і професійного зростання для сумлінних і відповідальних працівників.

2.3 Роль кадрової служби в забезпеченні ІБ

Забезпечення інформаційної безпеки компанії - результат злагодженої роботи багатьох служб, в першу чергу, служби інформаційної безпеки і служби персоналу. Завдяки злагодженій роботі насамперед цих двох служб має здійснюватися розгляд кожного кандидата на зайняття вакантної посади у сфері інформаційної безпеки, кожного фахівця із захисту інформації та інших дотичних професій як джерело ризику, потенційної загрози.

Ризики з боку персоналу можуть бути пов'язані як з умисним нанесенням шкоди, так і внаслідок низької кваліфікації, халатності чи необережності. Потенційно небезпечними є також і занадто кваліфіковані для займаної ними посади працівники, які не можуть застосувати свої високі знання і навики, що призводить до невдоволення роботою та умовами праці.

На виникнення ризиків інформаційній безпеці з боку персоналу впливає відсутність чітко і однозначно закріплених юридичних правовідносин,

неадекватна оцінка результатів праці, неефективне прогнозування та недостатній контроль лояльності та надійності кадрів.

З точки зору забезпечення ІБ діяльність служби управління персоналом (УП) включає такі аспекти: повноваження, взаємодія, комунікації, моніторинг, управління конфліктами й контроль [33].

Повноваження. Сучасна служба персоналу є одним із найважливіших ресурсів щодо забезпечення конкурентоздатності компанії на ринку. Ключові співробітники служби персоналу наділяються відповідними повноваженнями, які повинні бути не тільки надані, але публічно делеговані і зафіксовані документально. Дуже важливими для ефективного функціонування служби УП є підтримка керівництва компанії, проведення узгодженої та послідовної політики забезпечення інформаційної безпеки на всіх рівнях управління, надання фахівцям служби УП доступу до необхідних корпоративних ресурсів: планів стратегічного розвитку компанії, інформаційних масивів і баз даних (в тому числі і конфіденційного характеру), аналітичних та звітних матеріалів.

Фінансування служби УП здійснюється як з урахуванням витрат на реалізацію програм роботи з персоналом (залучення кваліфікованих кадрів, навчання, оцінка, розвиток, кадрові ротації, управління лояльністю тощо), так і на заходи щодо забезпечення кадрових аспектів ІБ підприємства.

Служба УП бере безпосередню участь в розробці документаційного забезпечення ІБ. Керівник служби відповідає за наявність необхідних регламентів і процедур, їх функціональність і відповідність чинним нормативно-правовим актам. Існує ряд обов'язкових документів, безпосередньо пов'язаних з ІБ компанії: трудовий договір або контракт, угода про нерозголошення конфіденційної інформації, правила внутрішнього трудового розпорядку та режиму контролю доступу, політики та процедури, інша нормативна документація у сфері ІБ.

Служба УП займається документування дисциплінарної практики на підприємстві, в тому числі в підрозділах захисту інформації та ІБ. Крім того, служба УП має право на пряму або опосередковану участь у роботі по створенню

іншої документації, пов'язаної з ІБ, наприклад, пакета документів, що регламентують питання охорони конфіденційної інформації, або положення про внутрішній канал зворотного зв’язку, по якому будь-який співробітник компанії може анонімно вказати на потенційні або реальні порушення ІБ, що ведуть до втрат і збитків [40].

Взаємодія. Діяльність служби УП є результативною у сфері ІБ завдяки постійної і послідовної взаємодії з іншими підрозділами. У зв’язку з цим на підприємстві має бути регламентовано і описано розподіл прав і обов'язків між співробітниками служби УП та їх колегами зі служби ІБ та інших відділів. Документально це може бути закріплено в положенні про взаємодію в галузі забезпечення ІБ, де визначаються: порядок взаємодії служб на різних етапах роботи із забезпечення ІБ, з питань виділення коштів, порядок узгодження при прийнятті рішень, ступінь доступності для окремих категорій фахівців внутрішньої інформації і рівень її конфіденційності, відповідальність конкретних посадових осіб тощо.

Взаємодія служби УП і служби ІБ має бути тісною, постійною і взаємодоповнюючою.

На думку фахівців, основними напрямами взаємодії цих двох служб є:

- відбір і проведення перевірок кандидатів на зайняття вакантних посад, а також внутрішніх претендентів на посади, що звільняються;
- розробка програм забезпечення фізичної безпеки персоналу, внутрішнього режиму роботу на об’єктах інформаційної безпеки;
- організація інформування, навчання та розвитку персоналу;
- реалізація процедур звільнення працівників;
- оцінка лояльності й надійності як кандидатів, так і діючих співробітників у сфері ІБ;
- розгляд випадків нанесення шкоди компанії і введення санкції щодо порушників з числа персоналу та інші [33].

Обов’язковою передумовою успішної співпраці служби УП і служби ІБ є підтримання оперативного зв'язку між керівниками двох служб. Важливу роль у процесах взаємодії відіграє вище керівництво компанії.

У ході проведенні «поглиблених» перевірок кандидатів на зайняття вакантних посад у сфері ІБ представники обох зазначених підрозділів беруть участь у таких заходах:

- перевірка наданих документів (диплом, паспорт) на справжність;
- виявлення фактів судимості, серйозних адміністративних стягнень, розшукових справ щодо кандидата через облікові реєстри МВС;
- перевірка рекомендацій з місць попередньої роботи через служби безпеки компаній;
- перевірка реєстрації за місцем проживання (перебування);
- вивчення кредитної історії через служби безпеки або кредитні відділи банків;
- встановлення фактів наявності зв'язків у кримінальному середовищі (в т.ч. через родичів і членів сім'ї);
- перевірка наявності нерухомого та рухомого майна, зокрема на відповідність заявленим даним;
- виявлення фактів участі в капіталі організацій - юридичних осіб, в т.ч. назви таких установ;
- перевірка членства в некомерційних організаціях - фондах, товариствах, асоціаціях, громадських організаціях [42].

Необхідним елементом співпраці служб УП та ІБ є організація взаємодії із залученими фахівцями з навчання та розвитку персоналу, оскільки зазвичай для проведення корпоративних тренінгів і семінарів компанії запрошують бізнес-тренерів, консультантів з консалтингових фірм, психологів, інших фахівців. Працівники служби УП займаються організацією навчальних та тренінгових заходів, проведенням оцінювання якості навчання та ступеня засвоєння персоналом вивчених матеріалів та оволодіння необхідними навичками.

У ході організації та проведення навчальних заходів фахівці обох служб мають можливість вирішити й додаткові завдання: виявити найбільш яскравих, активних учасників тренінгу і потенційних лідерів, оцінити рівень компетентності керівника відділу як формального лідера, а також загальний психологічний клімат в колективі.

У ході здійснення повноважень із забезпечення ІБ у частині роботи з персоналом служби УП та ІБ взаємодіють також і з профспілковими організаціями з питань відображення в колективних договорах прав і обов'язків працівників компанії у сфері забезпечення ІБ, участі профспілкового комітету в процедурах звільнення тощо.

Комунікації. Важливою складовою діяльності служби УП у галузі ІБ є налагодження постійних, конструктивних, результативних, безпечних і довірчих комунікацій:

- вертикальних – з керівництвом підприємства;
- горизонтальних – з представниками функціональних підрозділів (служби ІБ, ІТ-підрозділу, юридичного, економічного відділів, профспілками тощо);
- зовнішніх - з представниками інших організацій, партнерів та клієнтів.

Насамперед варто виділити можливість виходу служ УП та ІБ на керівництво компанії в разі отримання інформації про порушення в системі ІБ. Цей вихід повинен бути прямим (тобто без посередників), оперативним і навіть екстреним за потреби.

Для отримання «гарячої» інформації про потенційних та діючих працівників служби підтримують тісні контакти з органами внутрішніх справ (наявність судимості), військкоматами (військовий облік), банківськими установами (кредитні історії). Співпраця з рекрутинговими й кадровими агентствами дозволяє перевіряти кандидатів з точки зору безпеки, необхідної кваліфікації, репутації, надійності, затребуваності кандидатів на ринку праці. Так, наприклад, можна замовити послугу, за якою компанію повідомлять, що конкуренти «замовлять» переманити їхнього ключового фахівця [33].

Моніторинг. Служба УП здійснює організацію постійного спостереження за змінами певних параметрів, отримання, систематизація та ретельний аналіз даних, пов’язаних із забезпеченням ІБ підприємства Моніторинг усіх доступних каналів інформації - одна з найважливіших функцій служби персоналу при забезпеченні ІБ компанії.

Моніторинг каналів неофіційною (кулуарної) інформації - завдання, яке має бути чітко визначеним, зрозумілим і забезпечене ресурсами (люди, час, обладнання, приміщення). Контроль неформальних інформаційних потоків здійснюється різними способами, а за його результатами можуть бути визначені загальний стан мотивації персоналу і випадки підозрілої поведінки, рівень довіри до керівництва, виявлені неформальні лідери груп, факти і конкретні винуватці внутрішніх порушень, прояви недбалості. Контроль «чуток» - важливе завдання в контексті забезпечення ІБ компанії.

Практика використання різних джерел надходження внутрішньої інформації показує, що найбільш результативними для виявлення порушень ІБ і зловживань виявляються приватні повідомлення працівників через канали зворотного зв'язку від персоналу (гаряча телефонна лінія, внутрішня електронна пошта або ящик для листів). Організація і підтримка функціонування яких, а також обробка інформації, що надходить, є спільним завданням служб УП й ІБ компанії.

З точки зору ІБ, обов'язковим є моніторинг рівнів лояльності як кандидатів на вакансії, так і працівників компанії, що дозволяє встановити ступінь задоволеності персоналу роботою та психологічним кліматом в колективі, а також з'ясувати їхнє ставлення до керівництва і компанії.

Основними засобами такого моніторингу є опитувальники й анкети. Однак, щоб контролювати питання ІБ, недостатньо одноразових опитувань, необхідно регулярно відстежувати ситуацію, аналізувати отримані результати і обов'язково відстежувати динаміку змін. Таким чином, формується уявлення про психологічне благополуччя і лояльність співробітників. Крім того, відстеживши зміни лояльності окремих працівників і підрозділів компанії, можна своєчасно

розробити заходи для корекції ситуації і вдосконалення існуючої системи мотивації персоналу.

Важливу роль у забезпеченні ІБ відіграє моніторинг ринку праці у цій сфері. Адже тільки володіючи актуальною інформацією щодо наявних вакансій з ІБ, рівня безробіття, динаміки зміни рівнів середніх зарплат по ключових позиціях галузі, умов праці, які пропонують конкуренти, компанія зможе залучити й утримати найкращих фахівців із захисту інформації. Кадрові прорахунки в таких випадках часто призводять до великих збитків, поразки масштабних проектів або упущеної вигоди.

Моніторинг змін у законодавстві служба УП проводить спільно з юридичним відділом. Недотримання нормативних вимог через їх незнання призводить до прямих фінансових і репутаційних втрат для бізнес-інтересів компанії [33].

Управління конфліктами. Участь у запобіганні та вирішенні конфліктів є обов’язком не тільки служби УП, але й усіх лінійних менеджерів. Конфлікти між фахівцями у сфері ІБ є предметом діяльності фахівців з УП та ІБ, які мають володіти знаннями технологій запобігання й вирішення конфліктів.

Конфлікти традиційно поділяють на організаційні та міжособистісні. Обидва типи конфліктів можуть приводити або до розвитку (конструктивні), або до руйнування (деструктивні) людських відносин і компанії загалом. До потенційно конфліктних моментів відносять: незадоволеність персоналу умовами праці, рівнем оплати, результатами атестації, можливостями для кар'єрного зростання тощо. Часто виникають конфлікти з приводу невиконання правил внутрішнього трудового розпорядку, вимог посадових інструкцій, зобов'язань про нерозголошення конфіденційної інформації. Постійно призводить до напруженості і проблем конфлікт інтересів - використання працівниками ресурсів компанії в особистих цілях, встановлення приватних відносин з конкурентами.

Невирішені конфлікти небезпечні, оскільки є причиною відволікання від роботи, виникнення тривалих стресів, негативних емоцій, внаслідок чого падає

продуктивність праці, погіршується морально-психологічний клімат в колективі , знижуються трудова мотивація і лояльність до компанії. У важких випадках конфліктні ситуації можуть привести до порушень вимог ІБ, недбалості, а іноді й цілеспрямованого шкідництва з боку персоналу.

Контроль. Встановивши корпоративні політики і вимоги ІБ, служба УП спільно зі службою ІБ контролюють їх виконання: перевіряють дотримання режиму роботи з конфіденційною інформацією, вимоги її захисту, результативність роботи персоналу. Завдяки контрольним заходам можна виявити і вирішити проблему до того, як вона призведе до незворотних негативних наслідків.

Ефективність контролю залежить від дотримання низки принципів: систематичність, безперервність (попередній, поточний, підсумковий, далі - повторення циклу), оперативність, своєчасність, ретельність, об'єктивність, різноманітність за формами (перевірка, письмовий звіт, контрольний журнал, особиста бесіда, нарада). Постановка конкретних короткочасних завдань допомагає зробити контроль реальним і створює певний стандарт, щодо якого можна вимірювати результати.

Особливу увагу необхідно звертати на дотримання співробітниками правил внутрішнього трудового розпорядку і режиму роботи з конфіденційною інформацією, вимог політик та інструкцій з ІБ, зобов'язань про нерозголошення конфіденційної інформації тощо.

За результатами контрольних заходів приймаються управлінські рішення: позитивні (оголосити подяку, преміювати) і негативні (зробити зауваження, оголосити догану, накласти штраф, звільнити). При цьому треба пам'ятати, що дисциплінарне стягнення може призвести до формування ворожого ставлення до компанії, і навіть в певному сенсі «навчає» того, як наступного разу проблему «замаскувати» [33].

Підсумовуючи, представимо напрями співпраці служби УП і служби ІБ (Рис. 2.3).

Рис. 2.3. Напрями взаємодії служби управління персоналом і служби інформаційної безпеки

Таким чином, завдання фахівців служби УП в контексті забезпечення ІБ є досить різноманітними і передбачають, з одного боку, виконання завдань із своєчасного виявлення недбалих або зловмисних працівників, з іншого – завдання з формування довірчих відносин з персоналом, підвищення лояльності працівників, розбудову корпоративної культури ІБ і впровадження прогресивних норм поведінки і праці у галузі ІБ.

Висновки до розділу 2

Встановлено, що сьогодні практично у кожній компанії середнього і великого бізнесу є посада директора з інформаційної безпеки, який у співпраці з

іншими посадовими особами найвищого рівня забезпечує успішне планування й реалізацію комплексу різнопланових заходів у сфері ІБ.

Відповідно до міжнародного стандарту 27001 основними показниками ефективної діяльності топ-менеджменту компанії у сфері ІБ є: наявність корпоративної політики ІБ, встановлення цілей та ведення діяльності із забезпечення ІБ відповідно до цілей бізнесу; впровадження загально-корпоративного підходу до забезпечення ІБ; підтримка та зобов'язання керівництва щодо забезпечення ІБ; розуміння вимог ІБ, оцінювання й управління ризиками ІБ; розподіл ролей і відповідальностей щодо забезпечення ІБ; розповсюдження настанов щодо політики ІБ та стандартів серед персоналу; забезпечення належного фінансування діяльності із забезпечення ІБ; забезпечення відповідних поінформованості, навчання та освіти персоналу з питань ІБ; впровадження ефективного процесу управління інцидентами ІБ.

Служба інформаційної безпеки підприємства забезпечує виконання завдань щодо наймання висококваліфікованого, психологічно придатного та надійного персоналу й забезпечення його результативної і якісної роботи з конфіденційною інформацією.

Вибудовуючи свою роботу з персоналом компанії, служба ІБ має проводити її принципово і компетентно через здійснення організаційних та організаційно-технічних заходів. Організаційні заходи з питань ІБ включають: організацію і проведення процедур добору та відбору кандидатів на зайняття вакантних посад у сфері інформаційної безпеки; регламентацію внутрішньо-корпоративних процедур захисту інформації та поводження з її носіями; організацію контролю за діяльністю персоналу компанії у сфері ІБ; роз'яснювально-просвітницьку і профілактичну роботу з персоналом підприємства з питань ІБ. До організаційно-технічних заходів служби ІБ відносять: організацію фізичної та технічної охорони об'єктів ІБ і внутрішнього режиму; аналіз поведінки та комунікації працівників з ІБ; аналіз використання копіювальної техніки; контроль поведінки персоналу в місцях, що знаходяться в зоні відкритих камер відеоспостереження.

Дослідження показало важливу роль служби управління персоналом у впровадженні заходів у сфері ІБ. Основними напрямами діяльності служби управління персоналом у співпраці зі службою ІБ є: розробка документаційного забезпечення ІБ; інформування, формування підтримки керівництва з питань ІБ; підтримка контактів з державними органами, банками, кадровими й рекрутинговими агентствами; наймання персоналу, проведення «поглиблених» перевірок кандидатів; організація інформування й навчання персоналу з питань ІБ; контроль дотримання норм ІБ, розгляд випадків дисциплінарних стягнень; оцінювання результативності праці, відповідності посаді; управління лояльністю персоналу; запобігання й вирішення конфліктів; моніторинг усіх доступних каналів інформації з ІБ, в т.ч. зворотного зв'язку від персоналу.

Розділ 3.
ТЕХНОЛОГІЇ ПІДБОРУ Й ВІДБОРУ ПЕРСОНАЛУ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1 Методи підбору працівників, задіяних у сфері інформаційної безпеки

Наймання персоналу, насамперед, пов’язані з такими поняттями, як підбір і відбір персоналу.

Підбір персоналу – визначення кандидатів посади, у тому числі організація відбиратиме найбільш підходящих неї співробітників.

Відбір персоналу – вивчення професійних, психологічних характеристик людини, щоб зрозуміти його придатність для даної посади та роботи, а також вибір найкращого з-поміж претендентів за критеріями кваліфікації, досвіду, особистих якостей, інтересів компанії та співробітника [11]. При прийомі працювати кожне підприємство використовує різні технології та методи добору та відбору персоналу.

Пошук та підбір персоналу завжди грали ключову роль у процесі управління персоналом як провідна частина організаційного функціонування підприємства, а також як важливий компонент діяльності із запобігання та зменшення загроз інформаційній безпеці з боку працівників. Сьогодні ці процеси стають усе більш значущими, оскільки в умовах дедалі більшої конкуренції організації все частіше розглядають своїх працівників як джерело конкурентної переваги.

Методи підбору персоналу різняться залежно від середовища, в якому він відбуватиметься. Відповідно до цієї ознаки виділяють внутрішньо-організаційний і зовнішній підбір персоналу.

Внутрішньо-організаційний підхід передбачає підбір працівників з урахуванням внутрішнього кадрового резерву компанії, а зовнішній - залучення необхідних працівників із інших джерел.

Внутрішній підбір працівників відіграє важливу у роль у найманні персоналу з інформаційної безпеки і передбачає заповнення насамперед посад високого професійного або управлінського рівня, оскільки зменшує шанси найняти незнайому, а, отже, недостатньо вивчену особу на посади з високим рівнем доступу до конфіденційної інформації. У таких випадках керівництво насамперед звертає увагу на вже існуючий кадровий резерв.

Крім того, такий спосіб підбору персоналу є досить ефективним з кількох причин. По-перше, він не вимагає додаткового фінансування для проведення процедур з підбору персоналу. По-друге, працівники компанії вже добре відомі для керівництва та мали можливість продемонструвати свої навички та вміння і тим самим показати свій потенціал ефективності. Третім позитивним моментом є те, що процес адаптації працівника до нової посади буде легшим у порівнянні з працівником, що прийшов ззовні, оскільки колектив у цій організації йому вже знайомий і не буде необхідності інтегруватися в робоче середовище заново.

Тим не менш, важливо зазначити, що підбір персоналу з внутрішнього середовища організації не позбавлений своїх мінусів: вибір потенційних працівників на нову посаду обмежений існуючим трудовим резервом і позбавляє роботодавця можливості залучити «свіжі уми», тобто людей ззовні, які можуть продемонструвати якісно новий підхід до вирішення поставлених завдань [11].

До внутрішнього підбору персоналу також відносять підбір персоналу за рекомендаціями працюючих співробітників. Переваги цього методу аналогічні попередньому, у той час як недоліком є те, що запропоновані кандидати незнайомі керівництву, і їхню кваліфікацію необхідно перевірити. До того ж працівник компанії може рекомендувати знайому особу на зайняття вакантної посади не тому, що він є кваліфікованим професіоналом і своєю працею сприятиме покращенню функціонування організації, а виходячи із власних корисливих цілей.

Зовнішній підбір персоналу також має низку позитивних і негативних аспектів. Основною перевагою використання цього методу є те, що організації, залучаючи до процесу пошуку потенційних кандидатів, наприклад, рекрутингові

агентства, звільняють себе від необхідності самостійно цим займатися, а, навпаки, мають можливість брати участь у фінальному етапі вибору серед кандидатів, рекомендованих на посаду, що успішно пройшли всі етапи відбору. Такий стан справ, безумовно, економить час організації, необхідний для проведення усіх процедур.

Водночас, такий метод підбору персоналу передбачає великі матеріальні витрати, оскільки послуги рекрутингових агентств є досить дорогими. Також існує ризик, що рекрутинговий агент може скласти хибний образ бажаного фахівця і підібрати непідходящих кандидатів.

Досить ефективним зовнішнім способом підбору персоналу є використання можливостей Інтернету й соціальних мереж, де існує велика кількість сайтів, на яких можна розмістити оголошення про пошук співробітників та наявність існуючих вакансій. Як свідчить практика, розміщені там оголошення зазвичай знаходять миттєвий відгук. Водночас, організації доведеться витратити багато часу для того, щоб впоратися з усім масивом заявок, що надійшли, і відібрати необхідних кандидатів [11].

Можна виділити такі методи, з яких менеджери з персоналу ведуть пошук необхідних кандидатур на вакантні посади [11, 13] (Рис. 3.1):

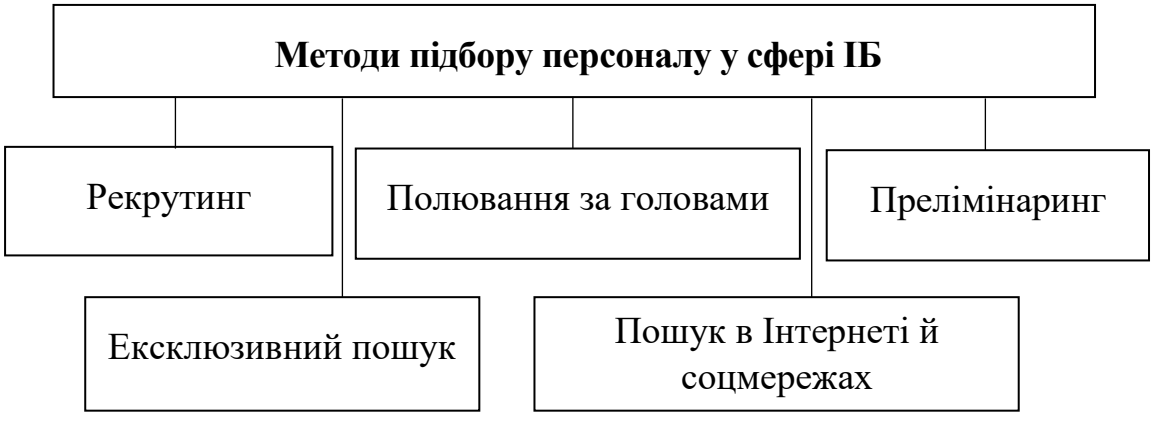

Рис. 3.1. Методи підбору персоналу у сфері ІБ

1. Рекрутинг (англ. recruiting) як метод пошуку персоналу застосовується, як правило, до кадрів середньої та нижчої ланки. Метою рекрутингу є залучення контингенту, який перебуває у вільному пошуку роботи. Основною перевагою використання зазначеного способу є економія часу роботодавця за рахунок

попередньої фільтрації потоку кандидатів і як наслідок – прискорений пошук необхідних кандидатів. З точки зору застосування кількісних методів, рекрутинг, що проводиться кадровими агентствами, які мають велику базу резюме, а також володіють статистикою проходження випробувального терміну працівниками, рекомендованими клієнтам, дає можливість моделювати ймовірність проходження випробувального терміну і працевлаштування на основі аналізу інформації, вказаної в резюме.

2. Ексклюзивний пошук (англ. exclusive search) – прямий та цілеспрямований пошук, спрямований на формування вищої управлінської ланки, а також представників дефіцитних або унікальних професій. Мета методу – залучення як працюючих фахівців, так і осіб, які перебувають у процесі пошуку роботи. Найчастіше до цього методу вдаються, якщо в організації мають на меті знайти людей, здатних здійснити ключовий вплив на ефективність функціонування компанії.

Зазвичай пошук фахівців рідкісного профілю доцільно здійснювати із залученням рекрутингового агентства, оскільки, найімовірніше, ексклюзивний пошук виявиться ефективним, більше того, як і в попередньому випадку, рішення про рекомендацію співробітника кадровим агентством може спиратися на результати кількісного моделювання ймовірності проходження випробувального терміну і зайняття вакантної посади.

3. Метод полювання за головами (англ. head hunting) передбачає пошук конкретних досвідчених і висококваліфікованих фахівців, які працюють на іншу компанію і не мають наміру змінювати робоче місце, та їх переманювання в зацікавлену організацію, що є одним із методів конкурентної боротьби.

Залучити такого працівника на посаду є складним завданням, оскільки для успішного переманювання його необхідно «мотивувати» і запропонувати вигідніші умови, ніж на місці існуючої роботи. Крім того, працівники часто не вітають зміну місця праці через багато причин соціального характеру (усталений колектив, сприятливий психологічний клімат, визнання, стабільність тощо). Також метод переманювання вимагає тривалого часу та великих

фінансових вкладень. По перше, якщо організації, що здійснює пошук на вакантне місце, необхідно знайти підходящого фахівця конкурентів, по друге, переконати його змінити місце праці.

4. Прелімінаринг (англ. preliminaring) має на меті залучення на вакантні посади перспективних молодих фахівців (студентів та випускників вузів) за допомогою виробничої практики та стажування. Підбираючи фахівців у такий спосіб організація розраховує, що молоді активні працівники будуть здатні зробити значний внесок у її функціонування та розвиток. Також даний метод передбачає проведення безкоштовних тренінгів для випускників, молодих та початківців. Зазначений метод у разі успішного застосування має на увазі проходження спеціалістом усіх наступних етапів просування, починаючи з профорієнтації та адаптації молодого спеціаліста та закінчуючи роботою на посаді керівника вищої ланки управління [11].

Очевидною перевагою прелімінарингу є те, що під час проведення практики, стажування чи безкоштовного тренінгу організація має можливість оцінити потенційних кандидатів та створити базу кандидатів на майбутнє.

Разом з тим, даний метод не позбавлений певних недоліків. На думку багатьох компаній, отримання «неготового» співробітника, який не володіє відповідними спеціальними навичками та вміннями – витрата сил та втрата ефективності діяльності організації. Однак, є компанії, які віддають перевагу студентам і випускникам, оскільки доучують їх «під себе», оскільки для організації, в якій ефективно налагоджено процес навчання та адаптації нових співробітників, це не є проблемою.

5. Інтернет-пошук (англ. internet search) – пошук кандидатів на вакантну посаду за допомогою спеціалізованих сайтів в Інтернеті та соціальних мереж. Перевага електронних засобів пошуку фахівців полягає насамперед у базі, що постійно поповнюється (тут знаходяться найбільш свіжі та актуальні вакансії та резюме), повідомлення про вакансію великого кола шукачів роботи, а також у можливості їх оперативного відгуку на оголошення. Витрати часу на подання інформації тут дуже низькі. Багато сайтів, у яких компанії купують пакет послуг

щодо розміщення вакансій, самостійно розміщують оголошення, а відповідальний менеджер слідкує за тим, щоб оновлення з'являлися на сайті.

Серед недоліків електронного пошуку персоналу відзначають наявність у базі великої кількості резюме низької якості. За твердженням фахівців з підбору персоналу, 8 із 10 резюме автоматично йдуть у кошик, оскільки не відповідають рівню компанії.

Сьогодні більшість працедавців сходяться на думці, що знайти висококваліфікованого спеціаліста за допомогою лише Інтернету складно. Знайти в Інтернеті досвідченого програміста практично не реально. Сайти для працевлаштування є досить ефективним інструментом для закриття стартових (асистенти, молодші спеціалісти) та масових позицій (наприклад, системні адміністратори). Водночас в Інтернеті можна знайти розумного і перспективного фахівця нижчої ланки і дати йому можливість навчитися і зробити кар'єру в організації [30].

Найбільш відомими сайтами з пошуку роботи та публікації вакансій в Україні є: Work.ua, Rabota.ua, UA.Jooble.org, Trud.com, Superjob.ua та інші. Серед топових вітчизняних рекрутерів, зацікавлених у пошуку кваліфікованих фахівців, популярною є ділова соціальна мережа LinkedIn.com.

Найбільшими майданчиками для працевлаштування в Європі є: https://layboard.com, рекрутингова платформа jobandtalent.com, професійна соціальна мережа viadeo.com (схожа на LinkedIn), система пошуку роботи Adzuna, фріланс - біржа Fiverr, ресурс пошуку роботи для студентів і випускників вишів Graduateland.

У США діють найбільші у світі сайти розміщення й пошуку вакансій для працевлаштування, зокрема Monster.com, Craigslist, Indeed, CareerBuilder та Careerjet [17].

Соціальні мережі найчастіше використовують для пошуку фахівців із вузькою спеціалізаціями. Для цього розміщують оголошення у спільнотах за інтересами, наприклад, за IT-фахівцями йдуть на англомовний ресурс GitHub, де можна переглянути профіль IT-фахівця та його досвід у вигляді реалізованих

проектів. Водночас такий метод має один істотний мінус: роботодавець може отримати занадто багато нерелевантних відгуків.

Розглянувши вищевказані методи підбору персоналу, які вважають скоріше традиційними, варто згадати нетрадиційні способи пошуку працівників на вакантні посади, зокрема:

- пошук необхідних кандидатів на конференціях тематичного характеру та на різноманітних професійних виставкових заходах;
- розсилання запитів електронною поштою в Інтернеті потенційно зацікавленим кандидатам (спам);
- залучення до процесу підбору персоналу особистого штату співробітників, мотивованого грошовими преміями за успішний пошук спеціалістів;
- залучення кандидатів певних спеціальностей із провінційних регіонів з більш низьким рівнем життя.

Також фахівці виділяють інші джерела пошуку та залучення персоналу, серед яких: розміщення інформації про вакансії у друкованих ЗМІ щодо пошуку роботи; на об’єктах зовнішньої реклами та реклами у громадському транспорті (за допомогою радіо, у салонах та вагонах громадського транспорту, зовнішня реклама на транспортних засобах); проведення власної «кампанії» (реклама на чеках, пакетах, у торговій точці) [11].

Підсумовуючи, варто зауважити, що набираючи персонал у сферу інформаційної безпеки, багато підприємств віддають перевагу набору всередині своєї компанії. По перше, такий метод пошуку персоналу зменшує ризики наймання ненадійних або навіть зловмисних працівників. По друге, просування по службі своїх працівників коштує керівництву дешевше. Крім того, це підвищує зацікавленість діючих працівників у продуктивній та відданій праці з перспективою подальшого кар’єрного або професійного зростання, посилює лояльність працівників, покращує моральний клімат у колективі.

3.2 Особливості відбору працівників у сфері ІБ

Другим етапом процесу наймання персоналу є підбір кандидатів, які максимально відповідають вимогам посади й очікуванням роботодавця.

Відбір персоналу полягає у вивченні професійних, психологічних характеристик людини, щоб зрозуміти його придатність для даної посади та роботи, а також вибір найкращого з-поміж претендентів за критеріями кваліфікації, досвіду, особистих якостей, інтересів компанії та співробітника. При прийомі працювати кожне підприємство використовує різні технології та методи добору та відбору персоналу.

Стандартна процедура відбору персоналу включає кілька етапів:

- Попередній добір претендентів;
- Проведення первинної співбесіди;
- Оцінювання претендентів;
- Перевірка наданої документації, збирання та перевірка рекомендацій;
- Медичний огляд (за потреби);
- Проведення підсумкової співбесіди;
- Прийняття остаточного рішення щодо працевлаштування;
- Підписання трудового договору [24].

Говорячи про методи відбору персоналу, варто відзначити, що вони бувають традиційними і нетрадиційними [11, 13] (Табл. 3.1).

Таблиця 3.1.

Методи відбору персоналу

Традиційні	Нетрадиційні
аналіз резюме кандидатів телефонне інтерв'ю психологічне тестування професійне тестування співбесіда групова співбесіда	відбір за компетенціями стресове інтерв'ю бізнес-кейси

Традиційними методами відбору персоналу є:

- аналіз резюме кандидатів,
- телефонне інтерв'ю,
- психологічне тестування,
- професійне тестування,
- співбесіда,
- групова співбесіда.

Аналіз резюме кандидатів передбачає вивчення характеристик кандидатів, які вони повідомили себе. Зазвичай воно відбувається до реального знайомства з людиною. Як можна зрозуміти, це далеко не найефективніший спосіб, тому що не все представлене у резюме може відповідати дійсності.

Телефонне інтерв'ю – це розмова з претендентом після аналізу резюме. Використовується для доповнення інформації, безпосереднього знайомства з кандидатом. Мінус тут у тому, що інтерв'ю проводиться телефоном, і, швидше за все, після розмови багато нових відомостей про кандидата навряд чи можна отримати.

За допомогою психологічних тестів визначається характер особи, стиль поведінки, психологічний портрет. Цей спосіб вважається допоміжним при відборі персоналу, оскільки є тести, які підходять не для кожної людини.

Професійне тестування, на відміну психологічного, є дуже важливим, значимим і, ймовірно, найбільш дієвим методом в оцінюванні кандидата на вакантну посаду. Воно допомагає визначити професійні знання, уміння й навички, рівень фахової компетентності претендента.

Співбесіда є дуже популярним методом знайомства й оцінювання претендентів а у будь-якій сфері діяльності. Рекрутер оцінює рівень освіти, професіоналізм, досвід, психологічні характеристики кандидата, встановлює значимість і бажання кандидата зайняти вакантну посаду. На співбесіді потрібно ставити конкретні питання, щоб отримати найточнішу інформацію. Вони мають бути пов'язані безпосередньо з новим місцем роботи, а також з

бажаною посадою. Адже, саме за підсумками співбесіди найчастіше приймається рішення про «відсівання» небажаних кандидатів.

Метод співбесіди має важливу перевагу над іншими методами. Це можливість оцінити поведінку кандидата наживо: жести, міміку, пози, інтонацію голосу тощо, скласти його психологічний та емоційний портрет. На перший погляд може здатися, що для організації, що займається відбором персоналу, такий метод не є трудомістким. Однак для проведення ефективної співбесіди з позитивними результатами, а саме – вибором кращого кандидата, необхідна серйозна підготовка до її проведення. Зокрема, необхідно сформувати попередній список питань для того, щоб ставити тільки необхідні питання, виявити наявність в кандидата конкретних якостей і здібностей. Крім того, особа, яка проводить співбесіду має бути кваліфікованою і володіти необхідними навичками спілкування й аналізу відповідей кандидата.

Окремим видом безпосереднього спілкування є групова співбесіда, яка передбачає одночасне оцінювання кількох претендентів на посаду. Цей метод має на меті створення некомфортної для учасників психологічної ситуації, щоб встановити, як вони будуть поводитися і взаємодіяти в колективі [11].

Нетрадиційними методами відбору персоналу є:

- відбір за компетенціями,
- стресове інтерв’ю,
- бізнес-кейси.

За допомогою відбору за компетенціями проводиться аналіз відповідності дійсних компетенцій здобувача з тими, які необхідні для роботи на посаді. Це встановлюється з досвіду. Спосіб є дієвий та досить ефективним за умови правильного застосування.

Стресове інтерв’ю має на меті створення для кандидата психологічно некомфортної ситуації для того, щоб простежити за його реакцією та подальшими діями. Такий метод перевірки доречно використовувати при відборі на посади, робота на яких дійсно вимагає високого рівня стресостійкості.

Бізнес-кейси використовують додатково до співбесіди, щоб зрозуміти, як особа поведеться у певній ситуації, проявить притаманні їй професійні й особисті якості, зокрема встановлюючи та вирішуючи прикладну проблему за фахом. Цей спосіб може бути корисним та ефективний при найманні досвідчених спеціалістів.

З огляду на те, що кожен із перелічених методів має свої переваги та недоліки, доцільно поєднувати використання декількох методів у залежності від ситуації, виду посади, специфіки підприємства тощо.

При підборі найбільш підходящих претендентів на зайняття вакантної посади застосовують низку загальних критеріїв, серед них: орієнтованість підбору на особистість конкретної особи; детальне і, за потреби, поглиблене вивчення біографії кандидата; вибір кандидата, який найбільше відповідає критеріям посади й підприємства; володіння кандидатом спеціальними знаннями, навичками, відповідними діловими якостями; наявність практичного досвіду роботи; здатність до проявлення ініціативи і творчого підходу, співпраці й роботи в колективі; наявність особистісного потенціалу й бажаних для конкретної посади особистих якостей; позитивний морально-психологічний стан кандидата і любов до своєї професії [13].

Говорячи про успішність застосування технологій підбору персоналу, слід зазначити, що існують різні труднощі, які знижують їх ефективність. Наприклад, не кожен співробітник відділу управління персоналом може правильно оцінити претендента на вільну вакансію. Часто HR-фахівці оцінюють претендентів через призму одного, найважливішого на їх думку критерію, неправильно тлумачать результати відбору, а іноді просто не мають чіткого уявлення і розуміння, яким має бути конкретний фахівець, що від нього вимагається, які завдання він вирішуватиме і які функції виконуватиме. Для зменшення ризиків виникнення таких ситуацій у процесі відбору найбільш підходящих кандидатів на зайняття вакантних посад обов’язково мають брати участь лінійні менеджери, які краще знають специфіку конкретної професії чи посади.

На основі вивчення засад наймання персоналу [11, 13, 24, 29] виділимо такі етапи процесу підбору і відбору персоналу у сфері ІБ (Рис. 3.2):

Рис. 3.2. Етапи процесу підбору й відбору персоналу у сфері ІБ

1. Визначення реальних потреб у працівниках і критеріїв їх оцінювання;

2. Вироблення стратегії пошуку й наймання персоналу, що узгоджується з корпоративною стратегією управління;

3. Встановлення вимог до претендентів на зайняття конкретних вакантних посад (кваліфікаційних вимог, а також особистісних і ділових якостей, необхідних для ефективного виконання передбаченої роботи);

4. Розробка комплексу процедур пошуку і наймання персоналу, форм документів, правил набору персоналу, вибір методів вивчення й оцінювання претендентів, визначення рівня оплати праці за посадами, вибір способів мотивації і перспектив кар'єрного просування;

5. Пошук джерел заповнення вакантних посад і прийнятних методів залучення кандидатів, які відповідають встановленим критеріям;

6. Здійснення практичних дій з підбору і відбору персоналу, формування резерву кандидатів на вакантні посади, визначення сукупності методів відбору кадрів, які дозволяють здійснити поглиблене вивчення й оцінку кандидатів на зайняття вакантних посад у сфері ІБ;

7. Встановлення випробувального терміну і проведення випробування, щоб об'єктивно оцінити придатність обраних осіб для роботи на конкретних посадах;

8. Підписання угод про нерозголошення конфіденційної інформації та дотримання інших вимог та обмежень ІБ та підписання контрактів з новопризначеними працівниками;

9. Створення максимально комфортних умов для адаптації нових працівників до роботи на посадах уз ІБ в компанії.

Організаційні заходи при підборі персоналу, що одержує доступ до конфіденційної інформації, можна розділити на кілька груп:

- проведення ускладнених аналітичних процедур при прийомі і звільнення співробітників;
- документування добровільної згоди особи не розголошувати конфіденційні відомості й дотримуватися правил забезпечення ІБ;
- інструктування і навчання працівників практичним діям із захисту інформації [31].

У ході попередньої бесіди з кандидатом можуть уточнюватися питання, які враховуються при оформленні матеріалів на допуск до конфіденційної інформації, а саме щодо: попередньої роботи кандидата з конфіденційними документами, секретними виробами, на режимних об’єктах, а також взяття зобов’язань щодо нерозголошення конфіденційних відомостей.

Співбесіди з кандидатами на посади в галузі ІБ мають на меті:

- встановити реальну причину бажання кандидата працювати на даному підприємстві;
- виявити можливих зловмисників або спробувати побачити слабкі сторони кандидата, які можуть сприяти шпигунству;
- переконатися, що кандидат не приніс з собою конфіденційну інформацію іншої компанії, яку хоче таємно використовувати;
- досягти добровільної згоди кандидата дотримуватися правил ІБ та мати певні обмеження у професійному та особистому житті у зв’язку із зайняттям відповідної посади.

Також кандидата просять надати необхідні довідки та документи, знайомлять зі змістом угоди (контракту) про нерозголошення конфіденційної інформації.

У процесі відборі кандидатів на посади у сфері ІБ особливу увагу звертають на аналіз достовірності та правильності оформлення персональних документів: відповідність прізвищ, імен та по батькові, інших персональних даних, наявність у документах необхідних відміток і записів, ідентичність фотокарток і особи кандидата, відсутність підчисток, незавірених виправлень, спроб заміни аркушів, фотографій, відповідність печаток назвам тих організацій, які видали документи тощо. У випадку виникнення сумнівів кандидата просять подати дублікати зіпсованих документів, завірити виправлення. У крайніх випадках кандидату повертають сумнівні документи й відмовляють у конкурсі на зайняття вакантної посади [42].

Підсумовуючи, варто наголосити, що кваліфікований та ефективний відбір і підбір персоналу має враховувати специфіку галузі, самого підприємства, а

також особливості сфери ІБ. Це означає, що для успішного наймання персоналу необхідно обирати й поєднувати найбільш підходящі підходи, методи вивчення й оцінювання претендентів на зайняття вакантних посад, залучати до цього процесу не тільки фахівців служби управління персоналом, але й лінійних менеджерів з ІБ, застосовувати методи поглибленої перевірки кандидатів для мінімізації ризиків подальших порушень ІБ з їх вини.

3.3 Тестування персоналу при прийомі на роботу

Як відзначалося вище, важливим і високо ефективним методом перевірки й відбору персоналу є оцінювання різних характеристик потенційних працівників. Залежно від вакансії, обсягу відповідальності та потенційного доступу співробітника до важливих корпоративних активів використовують оцінювання трьох рівнів: поверхневе, середнє та глибоке [31].

1. Поверхневе, яке може включати співбесіду з кандидатами (можливо з тестуванням), перевірку справжності документів, що підтверджують особу, які зазвичай проводять фахівці відділу управління персоналом. Поверхневої перевірки недостатньо для кандидатів, які матимуть доступ до комерційної таємниці чи інших видів конфіденційної інформації.

2. Оцінювання середнього рівня, крім поверхневої перевірки передбачає визначення справжності пакета документів, даних про наявність вищої освіти, підтвердження наведених у документах даних із попередніх місць роботи. Обов'язковим у такому випадку є проведення тестування на професійну придатність, тип особистості. Такий підхід не може гарантувати, що кандидат успішно впорається зі своїми посадовими обов'язками, проте дозволяє відсіяти недобросовісних і нечесних претендентів.

3. Поглиблене оцінювання кандидатів проводиться спільно фахівцями HR-відділу та служби ІБ. У його процесі збирають додаткові відомості про кандидата, відгуки від колишнього керівництва, подають запити щодо наявності недобросовісної кредитної історії, судимостей, перебування на психіатричному

обліку у відповідні державні органи, банківські установи та медичні заклади. Можливим є використання нетрадиційних методів оцінювання (за фотографією, голосом, почерком (графо-ассесмент), а також перевірка на поліграфі [11].

З огляду на високий ступінь відповідальності, доступ до конфіденційної інформації та засобів її обробки претенденти на посади у сфері ІБ перед прийняттям на роботу мають проходити поглиблене оцінювання різними методами.

Популярним і широко застосовуваним методом оцінювання є тестування, яке може бути як письмовим, так і усним.

За змістом тести для кандидатів на зайняття вакантних посад, у тому числі у сфері ІБ, поділяють на тести, які оцінюють:

• професійні знання та навички (містять перелік запитань або ситуацій, для відповіді чи вирішення яких необхідно застосувати знання за фахом);

• загальні та спеціальні здібності (наприклад, перевіряють на здатність до концентрації уваги, стресостійкість тощо);

• інтелектуальний рівень – зазвичай для такої перевірки використовують стандартний тест IQ Айзенка або його скорочений варіант;

• мотиваційний та емоційний профілі кандидата, інші його особистісні характеристики. Зазвичай для такої перевірки застосовуються стандартні опитувальники, наприклад, за методиками Херцберга чи Рисса [26].

Тестування при прийомі на роботу використовують для «відсівання» кандидатів, які не відповідають визначеним критеріям. За допомогою анкет та опитувальників, крім перелічених вище показників, можна визначити особливості мислення кандидата, його цінності й мотиватори, здібності до навчання, термін адаптації, лідерські якості. сумісність кандидата із майбутніми колегами та багато іншого.

Для того, щоб анкетування було успішним і об’єктивним необхідно заздалегідь визначитися з метою оцінки, скласти перелік обов'язкових якостей та навичок ідеального кандидата і лише після цього обирати методики й анкети, які

дозволять ці якості оцінити. Також важливо враховувати специфіку діяльності компанії та сфери ІБ.

На думку фахівців-психологів, фахівець з ІБ має володіти такими особистими якостями як порядність, чесність, принциповість і сумлінність, старанність, дисциплінованість, стресостійкість, уміння працювати в команді. Також претенденту мають бути характерні самоконтроль у вчинках і діях, правильна самооцінка власних можливостей і здібностей, помірна схильність до ризику, вміння зберігати секрети, тренована увага та хороша пам'ять, здібності до порівняльної оцінки фактів тощо.

Натомість не сприяють збереженню таємниць такі особисті якості: емоційна неврівноваженість, розчарування в собі і своїх здібностях, невдоволення своїм службовим становищем, нечесність, ображене самолюбство, надмірно егоїстична поведінка, недостатня розсудливість, фінансова безвідповідальність [2, 4].

Питання під час тестування можуть бути типовими, адаптованими чи індивідуальними. Головне, щоб вони відповідали основній сфері діяльності компанії та конкретній посаді.

Для того, щоб з'ясувати відомості про попередній досвід кандидата, фахівці рекомендують використовувати принцип STAR (Рис. 3.3).

Рис. 3.3. Схема методики STAR.

Дана методика включає поведінкові питання і відповіді на них за таким шаблоном:

1. Ситуація: кандидату пропонують детальний опис конкретної робочої ситуації, в якій йому потрібно здійснити певні кроки для вирішення проблеми чи досягнення бажаного стану.

2. Завдання: кандидату встановлюють завдання, які він має здійснити для досягнення мети.

3. Дії: кандидат має докладно описати послідовність дій, щоб досягти поставленої мети, в тому числі йому необхідно зазначити конкретні етапи й особистий внесок у спільну справу.

4. Результат: кандидат має описати результати своїх дій, розповісти про свою відповідальність та вплив на ситуацію, дати відповіді на запитання про досягнення й уроки для себе внаслідок виконання завдання [23].

Варто відзначити, що тести бувають вербальними і невербальними. Вербальні варіанти передбачають роботу особи, що проходить оцінювання, зі словами - вони більш чутливі до рівня освіти, мовної культури кандидатів. Невербальні тести містять інформацію, представлену у вигляді відповідних графіків, картинок, креслень. Невербальних завдань менше ніж вербальних, тому їх використовуються тільки в певних випадках і часто застосовують в оцінці претендентів з порушенням слуху або мови.

При підборі й оцінювання кандидатів на зайняття вакантних посад у будь-яких сферах використовують багато різноманітних видів тестів. Розглянемо основні з них, які можуть застосовуватися для оцінювання фахівців з ІБ.

➤ Логічні тести при прийомі на роботу призначені для визначення абстрактно-логічного мислення кандидата. У логічному тесті застосовуються спеціальні схеми вибудуваних у ряд зображень геометричних фігур. Завдання тестованого логічно правильно продовжити цей ряд.

➤ Числові тести є найпоширенішим способом перевірки здібностей кандидата, цей тест використовують частіше ніж інші. У числовому тесті перевіряється здатність аналізувати графічну та табличну інформацію,

обчислювати відсотки, конвертувати валюту, складати пропорції, обчислювати коефіцієнти.

➤ Вербальні тести використовуються багатьма компаніями. Даний тест визначає здатність людини до сприйняття та аналізу вербальної інформації, можливості робити висновки. У тесті особа знайомиться із текстом, на підставі аналізу якого має відповісти на запитання-твердження: «Правда», «Брехня» або «Мало інформації».

У якості прикладу згаданих трьох видів тестів можна навести логічні, числові та вербальні тести компанії Kenexa – міжнародного розробника програм та тестів для управління персоналом, у тому числі для його підбору. Зазначені види тестів виконані за стандартами розробників SHL, Talent Q, Kenexa, Ontarget [39].

➤ Тести на рівень інтелекту (IQ) та емоційного інтелекту (EQ). Найбільш популярними опитувальниками рівня інтелекту є психологічний тест коефіцієнта інтелекту англійського психолога Г. Айзенка й тест «Стандартизований багатофакторний метод дослідження особистості (MMPI), який базується на авторській методиці російської дослідниці Л. Собчик. Водночас, треба пам’ятати, що відповіді тестів на IQ досить складно інтерпретувати, що є причиною помилок HR-фахівців в оцінці кандидатів. Крім типового IQ-тесту у процесі перевірки кандидатів на вакантні посади рекомендують паралельно використовувати інші методи оцінки.

Оцінювання емоційного інтелекту є потрібним і важливим, особливо при перевірці спеціалістів, які працюватимуть з людьми. Але, як і у випадку з будь-яким іншим тестом, варто підтвердити результати оцінки шляхом використання додаткових методик. Доцільно проводити експрес-діагностику емоційного інтелекту під час співбесіди з кандидатами.

➤ Психологічні тести. Психологічні методики на співбесіді застосовують рідко, зазвичай, коли оцінюють претендентів на посади, для яких потрібні працівники з певними властивостями характеру. У сфері ІБ працівники мають володіти, зокрема такими рисами як: стресостійкість, уважність та мотивація.

За потреби оцінити рівень психологічної стійкості кандидата використовують, наприклад, опитувальник американських психіатрів Холмса та Раге, які розробили оціночну шкалу стресових подій. На підставі свого дослідження вони склали шкалу, в якій кожній важливій життєвій події відповідає певна кількість балів залежно від ступеня її стресогенності. Такий тип тестування на інтерв'ю допомагає HR-фахівцю визначити соціальну поведінку, особистісні характеристики та здатність до адаптації кандидата на посаду.

До психологічних відносять також тести на уважність та мотивацію. Перші мають на меті встановити здатність особи до зосередженої і тривалої роботи, другі - виявити справжні мотиви здобувача, пов’язані з отриманням нової посади.

➤ Тести на здатність до навчання - використовують, якщо потрібно зрозуміти, як краще розвивати працівника й будувати з ним комунікацію. Одну з відомих методик розробили британські психологи П. Хоні та А. Мамфорд, яка дозволяє виявити стиль навчання, близький кандидату і, як наслідок, передбачити його поведінку на роботі.

Автори виділили чотири стилі навчання: прагматик, мислитель, теоретик та діяч. Наприклад, кандидат зі стилем мислителя обережний, спостерігає, а не діє, небагатослівний у дискусіях. Кандидат-діяч, навпаки, спочатку робить, а потім думає, товариський. Ці визначення дуже зручно використовувати для з'ясування схильностей людини.

Цікавим є те, що компанія CISCO перед початком своїх тренінгів проводить тестування їхніх учасників за методикою Хоні-Мамфорда, щоб модифікувати навчання під потреби й особливості слухачів [38].

Крім того, результати тесту можна використовувати для перевірки відповідності психологічного портрета особи та бажаної вільної посади.

➤ Особистісні тести. Щоб скласти повний портрет претендента, варто визначити його особистісні характеристики. Тут можуть бути використані, наприклад: колірна діагностика Люшера, який передбачає, що вибір кольору нерідко відображає спрямованість особи на певну діяльність, настрій,

функціональний стан і найбільш стійкі риси особистості; психодіагностичний тест «Плями Роршаха», під час якого випробовуваному пропонується повідомити власні асоціації, пов’язані з десяти симетричними відносно вертикальної осі чорнильними плямами. Тест заснований на припущенні, що те, що особа «бачить» у плямі визначається особливостями її власної особистості; проектний тест Маркерта, що складається з восьми абстрактних фігурок, кожна з яких символізує певний стан людини, і дозволяє виявляти слабо усвідомлювані спонукання, оцінювати актуальні емоційні стани і шукати способи набуття психологічної «рівноваги»; тест фрустраційних реакцій Розенцвейга, призначений для діагностики особливостей поведінки особи в ситуаціях фрустрації. Він дозволяє виявити індивідуальні способи подолання перешкод і емоційного ставлення до них, визначити характер вербального реагування на труднощі, оцінити дії особи за параметром конструктивності.

➤ Технічні тести. Претендентам на позиції, пов'язані з механізмами, складним технічним обладнанням, кресленнями або схемами, важливо мати інженерне мислення. Для виявлення й оцінки такого типу мислення застосовують методики Беннета (даний тест призначений для того, щоб оцінювати технічне мислення особи, зокрема його вміння читати креслення, розбиратися в схемах технічних пристроїв і їх роботі, вирішувати найпростіші фізико-технічні завдання, тест просторового мислення (ТПМ), розроблений колективом науковців у складі І. Якіманської, В. Зархіна та Х.-М.Х.Кадаяса.

➤ Професійні тести. Такі методики, як зрозуміло з назви, потрібні для оцінки специфічних для посади знань і навичок. Анкети допомагають швидко визначити повноту та глибину експертизи, рівень кваліфікації спеціаліста. Такі опитувальники можуть бути складені як на рівні компанії, так і з залученням експертів у певній галузі ззовні [36].

Говорячи про професійне тестування фахівців з ІБ, варто перелічити такі напрями знань за профілем, які підлягають перевірці:

- законодавство України з питань ІБ та захисту інформації;

- нормативні документи регулюючих та наглядових органів щодо забезпечення ІБ;
- норми міжнародних стандартів та найкращих практик забезпечення ІБ (ISO 27001, ISO 22301, CobiT, ITIL);
- сучасні загрози та вразливості ІБ;
- технології, методи та засоби захисту інформації (у тому числі на різних рівнях моделі ISO/OSI);
- засади оцінювання ризиків ІБ, основи внутрішнього тестування інфраструктури компанії та складання звітів із зазначенням ступенів ризиків;
- розробка ефективних політик ІБ та інших організаційних документів;
- способи та методи захисту ІТКС (включаючи технології захисту від шкідливого ПЗ і запобігання несанкціонованому доступу, DLP-системи, сканери аналізу захищеності, IDS/IPS, засоби міжмережевого екранування тощо);
- моніторинг подій інформаційної безпеки (DLP, SIEM тощо);
- технології захисту баз даних та систем управління БД;
- адміністрування популярних операційних систем та сервісів.

На нашу думку, для оцінювання кандидатів на зайняття вакантних посад у сфері ІБ доцільно використовувати різні види тестування у залежності від ситуації та специфіки посади. Типовий перелік показаний на рисунку 3.4.

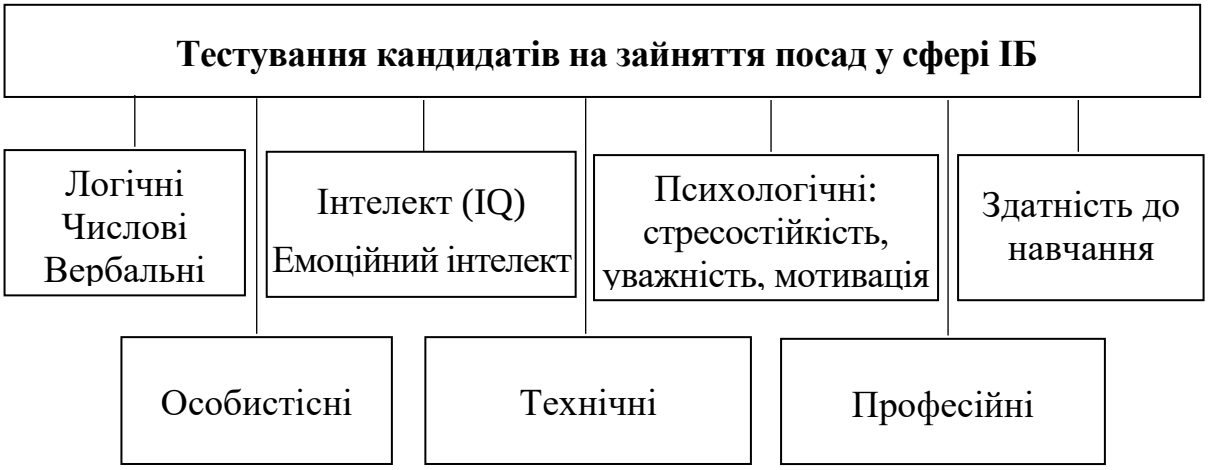

Рис. 3.4. Види тестування кандидатів на зайняття посад у сфері ІБ

Підсумовуючи, варто відзначити, що проведення поглиблених процедур відбору персоналу для роботи у сфері ІБ необхідним є залучення кваліфікованих фахівців: менеджерів з персоналу, психологів, технічних спеціалістів та професіоналів з ІБ та захисту інформації.

На середніх та великих підприємствах часто створюють центри оцінки (ассесмент-центри), в яких працюють спеціально підготовлені оцінювачі (асесори) різного профілю, головним завданням яких є спостереження за поведінкою кандидатів під час проходження тестування та виконання практичних завдань, які зазвичай імітують реальну робочу обстановку. Найважливішим моментом у процесі оцінки є вимірювання можливості виконання кандидатами поставлених завдань.

З огляду на те, що на підготовку власних спеціалістів з оцінювання персоналу необхідно витратити чималу кількість часу і коштів, компанії також користуються одноразовими послугами інших спеціалізованих організацій.

Висновки до розділу 3

Як показало дослідження, наймання персоналу з ІБ, насамперед, пов’язані з такими поняттями як підбір і відбір. Підбір персоналу полягає у пошуку та підборі кандидатів на вакантні позиції в компанії.

Методи підбору персоналу бувають внутрішньо-організаційні і зовнішні. Внутрішньо-організаційний підхід передбачає підбір працівників з урахуванням внутрішнього кадрового резерву організації, а зовнішній - залучення необхідних працівників за допомогою рекрутингових агентств, спеціалізованих сайтів в Інтернеті й соціальних мереж, пошуку перспективних студентів та випускників вишів тощо.

Другим етапом процесу наймання персоналу є відбір кандидатів і полягає у вивченні професійних, психологічних характеристик особи, щоб встановити її придатність для даної посади та роботи, а також вибір найкращого з-поміж

претендентів за критеріями кваліфікації, досвіду, особистих якостей, інтересів компанії та співробітника.

Традиційними методами відбору персоналу є: аналіз резюме, телефонне інтерв'ю, тестування, тестування, співбесіда, групова співбесіда. При підборі персоналу у сфері ІБ обов'язковим є проведення ускладнених аналітичних процедур; документування добровільної згоди особи не розголошувати конфіденційні відомості й дотримуватися правил ІБ; інструктування і навчання працівників практичним діям із захисту інформації.

Встановлено, що високо ефективним методом перевірки й відбору кандидатів на зайняття вакантних посад у сфері ІБ є тестування, яке може включати використання таких видів тестів: логічні, числові, вербальні; тести на інтелект та емоційний інтелект; психологічні (на стресостійкість, уважність, мотивацію); здатність до навчання; особистісні, технічні та професійні (з питань ІБ та захисту інформації).

ВИСНОВКИ

Встановлено, що СУІБ є невід'ємною частиною інтегрованої системи управління компанією, яка складається з кількох рівнів управління: стратегічного, корпоративного, керування та забезпечення. Передумовою ефективного функціонування СУІБ є поєднання заходів правового, організаційного та інженерно-технічного захисту.

Одним із основних напрямів СУІБ є управління персоналом. Основні технології управління персоналом, які використовують як засоби ІБ підприємства, умовно поділено на два блоки: перший блок включає кадрові технології, які забезпечують формування кваліфікованого і відповідального персоналу через переважно (але не виключно) використання адміністративних засобів впливу; другий – технології формування лояльного і надійного персоналу, реалізація яких частіше здійснюється економічними та психологічними методами.

Відповідно до міжнародного стандарту ISO 27001 основними показниками ефективної діяльності топ-менеджменту компанії у сфері ІБ є: наявність корпоративної політики ІБ, встановлення цілей та ведення діяльності із забезпечення ІБ відповідно до цілей бізнесу; підтримка та зобов'язання керівництва щодо забезпечення ІБ; оцінювання й управління ризиками ІБ; розподіл ролей і відповідальностей щодо забезпечення ІБ; забезпечення належного фінансування діяльності із забезпечення ІБ; інформування, навчання та освіта персоналу з питань ІБ; ефективне управління інцидентами ІБ.

Служба ІБ підприємства забезпечує здійснення організаційних та організаційно-технічних заходів. Організаційні заходи з питань ІБ включають: організацію і проведення процедур добору та відбору кандидатів на зайняття вакантних посад у сфері ІБ; регламентацію внутрішньо-корпоративних процедур захисту інформації та поводження з її носіями; організацію контролю за діяльністю персоналу компанії у сфері ІБ; роз'яснювально-просвітницьку і профілактичну роботу з персоналом підприємства з питань ІБ. До організаційно-технічних заходів служби ІБ відносять: організацію фізичної та технічної

охорони об'єктів ІБ і внутрішнього режиму; аналіз поведінки та комунікації працівників з ІБ; аналіз використання копіювальної техніки; контроль поведінки персоналу в місцях, що знаходяться в зоні відкритих камер відеоспостереження.

Дослідження показало важливу роль служби управління персоналом у впровадженні заходів у сфері ІБ. Основними напрямами діяльності служби управління персоналом у співпраці зі службою ІБ є: розробка документаційного забезпечення ІБ; інформування, формування підтримки керівництва з питань ІБ; підтримка контактів з державними органами, банками, кадровими й рекрутинговими агентствами; наймання персоналу, проведення «поглиблених» перевірок кандидатів; організація інформування й навчання персоналу з питань ІБ; контроль дотримання норм ІБ, розгляд випадків дисциплінарних стягнень; оцінювання результативності праці, відповідності посаді; управління лояльністю персоналу; запобігання й вирішення конфліктів; моніторинг усіх доступних каналів інформації з ІБ, в т.ч. зворотного зв'язку від персоналу.

Як показало дослідження, наймання персоналу з ІБ, насамперед, пов’язані з такими поняттями як підбір і відбір. Методи підбору персоналу бувають внутрішньо-організаційні (з кадрового резерву компанії) і зовнішні (за допомогою рекрутингових агентств, спеціалізованих сайтів в Інтернеті й соціальних мереж, пошук перспективних студентів та випускників вишів тощо). Традиційними методами відбору персоналу є: аналіз резюме, телефонне інтерв’ю, тестування, тестування, співбесіда, групова співбесіда.

При відборі й підборі персоналу у сфері ІБ обов’язковим є проведення ускладнених аналітичних процедур; документування добровільної згоди особи не розголошувати конфіденційні відомості й дотримуватися правил ІБ; інструктування і навчання працівників практичним діям із захисту інформації.

Встановлено, що високо ефективним методом перевірки й відбору кандидатів на зайняття вакантних посад у сфері ІБ є тестування, яке може включати використання таких видів тестів: логічні, числові, вербальні; тести на IQ та EQ; психологічні (стресостійкість, уважність); здатність до навчання; особистісні, технічні та професійні (з питань ІБ та захисту інформації).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

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. Астахова Л. Кадровые уязвимости информационной безопасности организации: методика оценки. URL: http://cyberleninka.ru/article/n/problema-identifikatsii-i-otsenki-kadrovyh-uyazvimostey-informatsionnoy-bezopasnosti-organizatsii (дата звернення: 09.12.2021)

3. Внедрение системы управления информационной безопасностью (ISO/IEC 27001:2013). URL: https://www.infosec.ru/uslugi/vnedrenie-sistemy-upravleniya-informatsionnoy-bezopasnostyu-iso-iec-27001-2013/ (дата звернення: 09.12.2021)

4. Вязанкина А., Астахова Л. Методики оценки кадровых рисков и уязвимостей информационной безопасности. https://cyberleninka.ru/article/n/metodiki-otsenki-kadrovyh-riskov-i-uyazvimostey-informatsionnoy-bezopasnosti (дата звернення: 09.12.2021)

5. Домарев В. Безопасность информационных технологий. Методология создания систем защиты. К.: ООО "ТИД "ДС", 2002. 688 с.

6. 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.

7. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT). 2015. 34 с.

8. Естехин В. Роли в ИБ. URL: https://cisoclub.ru/roli-v-ib/ (дата звернення: 09.12.2021)

9. Журавель М. Паршуков С. Проблеми захисту інформації. URL: http://informatika.udpu.org.ua/?page_id=1173 (дата звернення: 09.12.2021)

10. Защита от утечек информации (DLP). URL: http://styletele.com/Solutions/informatsionnaya-bezopasnost/sistemy-dlp/ (дата звернення: 09.12.2021)

11. Зинченко А. Моделирование процессов подбора и оценки персонала. URL: http://www.fa.ru/org/div/uank/autorefs/dissertations/%D0%97%D0%B8%D0%BD%D1%87%D0%B5%D0%BD%D0%BA%D0%BE%20%D0%90.%D0%90.%20(18.02.2016)%20c0a4020b0353bfea4e08f2dec19bc0b3.pdfB.M. (дата звернення: 09.12.2021)

12. Кадровая безопасность как составляющая экономической безопасности организации. URL: https://core.ac.uk/download/pdf/76001638.pdf (дата звернення: 09.12.2021)

13. Караваев В. Технологии найма персонала и их эффективность. URL: https://cyberleninka.ru/article/n/tehnologii-nayma-personala-i-ih-effektivnost (дата звернення: 09.12.2021)

14. Кибанов А., Дуракова И. Управление персоналом организации. Актуальные технологии найма, адаптации и аттестации. М.: КноРус, 2010. URL: http://fptl.ru/files/menedjment/kibanov_ypravlenie-personalom.pdf (дата звернення: 09.12.2021)

15. Комаричева М. Интернет как средство поиска работы и персонала. URL: http://e-koncept.ru/2017/970872.htm. (дата звернення: 09.12.2021)

16. Конеев И., Беляев А. Информационная безопасность предприятия. СПб. : БХВ-Петербург, 2003. 747 с.

17. Кращі сайти для пошуку роботи в СНД, Європі й США. URL: https://profitworks.com.ua/trudoustrojstvo (дата звернення: 09.12.2021)

18. Кузнецова Н. Обеспечение кадровой безопасности как функция управления персоналом. URL: https://cyberleninka.ru/article/n/obespechenie-kadrovoy-bezopasnosti-kak-funktsiya-upravleniya-personalom/viewer (дата звернення: 09.12.2021)

19. Маркіна І., Дячков Д. Основи формування системи менеджменту інформаційної безпеки підприємства. Проблеми і перспективи розвитку підприємництва : зб. наук. пр. ХНАДУ. Харків, 2016. № 3 (14), Т. 1. С. 80-88.

20. Мартыненко И. Организация работы службы безопасности компании с персоналом. URL: https://hrliga.com/index.php?module=profession&op=view&id=465 (дата звернення: 09.12.2021)

21. Матвеев А. Обзор рынка систем поведенческого анализа. URL: https://www.anti-malware.ru/analytics/Market_Analysis/user-and-entity-behavioral-analytics-ubaueba (дата звернення: 09.12.2021)

22. Менеджмент персоналу: Навч. посіб. / В. М. Данюк, В. М. Петюх, С. О. Цимбалюк та ін. К.: КНЕУ, 398 с.

23. Методика STAR для прохождения структурированных собеседований. URL: https://hr-portal.ru/story/metodika-star-dlya-prohozhdeniya-strukturirovannyh-sobesedovaniy (дата звернення: 09.12.2021)

24. Методы и процедуры процесса отбора кандидатов на вакантную должность. URL: http://managment-study.ru/metody-i-procedury-processa-otbora-kandidatov-na-vakantnuyu-dolzhnost.html#ixzz7ESGe7pzW (дата звернення: 09.12.2021)

25. Никишина А. Исследование современных технологий подбора персонала. URL: https://web.snauka.ru/issues/2016/07/70081 (дата звернення: 09.12.2021)

26. Нужно ли проводить тестирование при приеме на работу и зачем? URL: https://hr-portal.ru/article/nuzhno-li-provodit-testirovanie-pri-prieme-na-rabotu-i-zachem (дата звернення: 09.12.2021)

27. Ожиганова М., Хорошко В., Яремчук Ю., Карпінець В. Управління персоналом : навч. посіб. Вінниця : ВНТУ, 2014. 187 с.

28. Онищенко Д. Обзор решений SIEM (Security information and event management). URL: https://habr.com/ru/company/roi4cio/blog/528770/ (дата звернення: 09.12.2021)

29. Основні етапи процесу відбору персоналу, їх характеристика. URL: https://thelib.info/psihologiya/3145098-osnovni-etapi-procesu-vidboru-personalu-ih-harakteristika/ (дата звернення: 09.12.2021)

30. Преимущества и недостатки поиска персонала при помощи job-сайтов. URL: https://www.web-article.com.ua/2012/preimushhestva-i-nedostatki-job-sajtov/ (дата звернення: 09.12.2021)

31. Проверка кандидатов при приеме на работу: актуальные методы в 2022 году. URL: https://spspa.ru/proverka-kandidatov-pri-prieme-na-rabotu-aktualnye-metody/ (дата звернення: 09.12.2021)

32. Рахметов Р. Процессы обеспечения ИБ по стандарту ISO/IEC 27001:2013. URL: https://www.securityvision.ru/blog/protsessy-upravleniya-ib-konspekt-lektsii/ (дата звернення: 09.12.2021)

33. Роль служби персоналу у забезпеченні інформаційної безпеки. URL: https://hrliga.com/index.php?module=profession&op=view&id=109 (дата звернення: 09.12.2021)

34. Романовский С. Инструмент эффективного управления информационной безопасностью. http://lib.itsec.ru/articles2/control/instrument-effektivnogo-upravleniya-ib (дата звернення: 09.12.2021)

35. Русіна Ю., Щеглов І., Русина Ю., Щеглов І. Удосконалення системи управління інформаційною безпекою підприємства. URL: https://www.inter-nauka.com/uploads/public/14791102396895.pdf (дата звернення: 09.12.2021)

36. Сергеева С. Тесты при приеме на работу: как оценить кандидата на вакантную должность. URL: https://www.hr-director.ru/article/66678-testy-priem-na-rabotu-18-m1 (дата звернення: 09.12.2021)

37. Система управления информационной безопасностью коммерческой организации. URL: http://bre.ru/security/571.html (дата звернення: 09.12.2021)

38. Стилі навчання. URL: https://www.cisco.com/c/dam/global/ru_ua/training-events/downloads/anketa_training.pdf (дата звернення: 09.12.2021)

39. Тести Kenexa. URL: https://testonjob.ru/developers-test/kenexa-test/ (дата звернення: 09.12.2021)

40. Функции и структура деятельности руководителя. Свенцицкий А. Организационная психология : учебник для вузов. М.: Изд-во Юрайт, 2015. 504 с.

41. Черниш І., Маховка В., Лобач Л. Управління інформаційною безпекою підприємства в умовах динамічного бізнес-середовища. Економіка і регіон. Полтава: ПНТУ, 2020. Т. (1(76). С. 106-112.

42. Чумарин И. Обеспечение кадровой безопасности компании на этапе подбора кандидатов. URL: https://hrliga.com/index.php?module=profession&op=view&id=272 (дата звернення: 09.12.2021)

43. Ярочкин В. Информационная безопасность: учебник. М.: Фонд "Мир": Акад. проект, 2003. 639 с.

44. Ясенев В., Дорожкин А., Сочков А., Ясенев О. Информационная безопасность: Учебное пособие. Нижний Новгород: Нижегородский госуниверситет им. Н.И. Лобачевского, 2017. 198 с.