МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут захисту інформації

На рецензію
Завідувач кафедри УІКБ
доктор економічних наук, доцент
_____ С.В.Легомінова
«___»_____20__ р.

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

ДИПЛОМНА РОБОТА
на тему:
ЗАСАДИ УПРАВЛІННЯ ПЕРСОНАЛОМ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

СТУДЕНТ: Мосійчук Владислав Миколайович _____
(підпис)

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

НОРМОКОНТРОЛЕР: к.е.н., доцент Мордас Ірина Василівна _____
(підпис)

Київ – 2020

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою
Освітньо-кваліфікаційних рівень – бакалавр
Спеціальність «Кібербезпека»
Спеціалізація «Управління інформаційною безпекою»

«ЗАТВЕРДЖУЮ»

Завідувач кафедри УІКБ
_____ С.В.Легомінова
(підпис)

«___» _____ 2020 р.

ЗАВДАННЯ

на дипломну роботу

студенту Мосійчуку Владиславу Миколайовичу

1. Тема роботи «Засади управління персоналом у сфері інформаційної безпеки», затверджена наказом по університету від «16» березня 2020 р. № 81.

2. Термін здачі студентом оформленої роботи «05» червня 2020 р.

3. Об'єкт дослідження: система управління інформаційною безпекою.

4. Предмет дослідження: засади управління персоналом у сфері інформаційної безпеки.

5. Мета дослідження: вивчення засад управління персоналом у сфері інформаційної безпеки.

6. Перелік питань, які мають бути розроблені:

1. Встановити роль менеджменту персоналу як важливої складової системи управління інформаційною безпекою підприємства.
2. Дослідити напрями управління персоналом з інформаційної безпеки.
3. Визначити шляхи вдосконалення управління персоналом у сфері інформаційної безпеки.

7. Дата видачі завдання «24» лютого 2020 р.

КАЛЕНДАРНИЙ ПЛАН
виконання дипломної роботи
студентом Мосійчуком Владиславом Миколайовичем

Дата видачі завдання: «24» лютого 2020 р.

№ з/п	Етапи виконання дипломної роботи	Термін виконання етапів	Примітка
1.	Визначення об'єкту, предмету, мети та завдань дослідження.	09.03.2020	
2.	Збір та аналіз літератури.	30.03.2020	
3.	Вивчення ролі менеджменту персоналу як важливої складової системи управління інформаційною безпекою підприємства.	16.04.2020	
4.	Дослідження напрямів управління персоналом з інформаційної безпеки	30.04.2020	
5.	Визначення шляхів удосконалення управління персоналом в сфері інформаційної безпеки	15.05.2020	
6.	Формулювання висновків за результатами проведеного дослідження.	22.05.2020	
7.	Оформлення роботи.	29.05.2020	
8.	Оформлення презентації.	05.06.2020	
9.	Отримання рецензії на роботу.	08.06.2020	
10.	Захист в ДЕК.	09.06.2020	

Студент: Мосійчук Владислав Миколайович _____
(підпис)

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

РЕФЕРАТ

Дипломна робота присвячена дослідженню засад управління персоналом у сфері інформаційної безпеки. Робота складається зі вступу, трьох розділів, що містять 10 рисунків та 4 таблиці, висновків, списку використаних джерел із 44 найменувань. Загальний обсяг роботи становить 73 аркуші, з яких 4 аркуші займає список використаних джерел.

Об'єкт дослідження – система управління інформаційною безпекою.

Предмет дослідження – засади управління персоналом у сфері інформаційної безпеки.

Мета дослідження – вивчити засади управління персоналом у сфері інформаційної безпеки.

У дипломній роботі встановлено роль менеджменту персоналу як важливої складової системи управління інформаційною безпекою підприємства. Досліджено напрями управління персоналом з інформаційної безпеки. Визначено шляхи вдосконалення управління персоналом у сфері інформаційної безпеки.

Галузь застосування. Розроблені підходи можуть бути використані при плануванні та реалізації заходів менеджменту персоналу в рамках системи управління інформаційною безпекою підприємства.

Ключові слова: ПЕРСОНАЛ, УПРАВЛІННЯ ПЕРСОНАЛОМ, ІНФОРМАЦІЙНА БЕЗПЕКА, УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ.

ЗМІСТ

ВСТУП

Актуальність теми. Практика та соціологічні дослідження свідчать про великий вплив «людського фактора» на стан інформаційної безпеки підприємства. Саме персонал є основним і найціннішим ресурсом підприємства. Люди у процесі трудової діяльності створюють нові ідеї, роблять відкриття і винаходи, прискорюючи розвиток науково-технічного прогресу. Ефективно та якісно виконуючи свої робочі функції, співробітники підприємства забезпечують прибутковість і зростання бізнесу, формують імідж та репутацію, сприяють конкурентоспроможності компанії на ринку.

Водночас, персонал є основним джерелом втрати цінної і конфіденційної інформації, як навмисно, так і через непрофесійність і халатність. Жодна система захисту не зможе гарантувати безпеку інформації та запобігти її розголошенню без цілеспрямованої і системної роботи з персоналом підприємства.

З огляду на зазначені чинники дослідження засад управління персоналом у сфері інформаційної безпеки, є актуальним науковим завданням.

Мета і завдання дослідження. **Мета роботи** полягає у вивченні засад управління персоналом у сфері інформаційної безпеки.

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

1. Встановити роль менеджменту персоналу як важливої складової системи управління інформаційною безпекою підприємства.
2. Дослідити напрями управління персоналом з інформаційної безпеки.
3. Визначити шляхи вдосконалення управління персоналом у сфері інформаційної безпеки.

Об’єкт дослідження - система управління інформаційною безпекою підприємства.

Предмет дослідження – засади управління персоналом у сфері інформаційної безпеки.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи теоретичного аналізу літератури, управління інформаційною безпекою й теорії менеджменту персоналу, методи аналізу, синтезу та порівняння, соціологічні методи.

Наукова новизна одержаних результатів. Розроблені підходи можуть бути використані при плануванні та реалізації комплексу заходів з менеджменту персоналу у рамках системи управління інформаційною безпекою підприємства.

Практичне значення одержаних результатів. Застосування напрацювань дадуть змогу підприємству здійснити обґрунтований вибір організаційних заходів з метою здійснення ефективного менеджменту персоналу у системі управління інформаційною безпекою підприємства.

РОЗДІЛ 1. Менеджмент персоналу як важлива складова системи управління інформаційною безпекою підприємства

1.1. Основні характеристики системи управління інформаційною безпекою підприємства

У процесі своєї діяльності будь-яке підприємство оперує інформацією як специфічним товаром високої цінності. Володіння інформацією, її оптимальне використання забезпечує ефективне функціонування суб'єкта господарювання як цілісного комплексу.

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

Сучасний діловий світ, представлений головним чином фінансово-інформаційними корпораціями, страждає від інформаційної крадіжки. За даними світової статистики, втрата тільки 20% інформації веде до руйнування 65 % фірм і компаній. Тому інформаційна безпека є одним із найважливіших показників успішної діяльності організації [43].

Інформаційну безпеку підприємства визначають як суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб'єкта господарської діяльності [37].

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

Інформаційна безпека підприємства характеризується конфіденційністю, цілісністю, доступністю та може розглядатися як сукупність таких елементів: безпечні умови функціонування інформаційних технологій, побудова ефективної інфраструктури інформаційного простору, цілісного ринку інформації, створення оптимальних умов для проходження інформаційних процесів.

Метою інформаційної безпеки є збереження цілісності, повноти та точності інформації, мінімізація ризику несанкціонованих змін у інформаційних системах [8].

До основних цілей інформаційної безпеки належать:

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

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

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

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

• збереження конфіденційності документованої інформації відповідно до законодавства [23].

Система управління інформаційною безпекою (СУІБ) - це частина загальної системи управління підприємства, що базується на аналізі ризиків і призначена для проектування, реалізації, контролю, супроводу та вдосконалення заходів в області інформаційної безпеки [13]. Цю систему складають організаційні структури, політика, дії з планування, обов'язки, процедури, процеси і ресурси.

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

Система управління інформаційною безпекою повинна забезпечувати досягнення таких цілей як забезпечення конфіденційності критичної інформації, запобігання несанкціонованого доступу до критичної інформації, цілісності інформації та пов'язаних з нею процесів (створення, введення, обробки і виведення) і ряду інших цілей [18].

Якісне управління інформаційною безпекою базується на таких принципах як узгодженість з бізнес-завданнями і стратегією підприємства; високий рівень керованості; адекватність інформації, яка використовується і генерується; ефективність - оптимальний баланс між можливостями, продуктивністю і витратами СУІБ; безперервність управління.

Крім того СУІБ створюється на стику двох методологічних підходів:

- комплексного, відповідно до якого управління ІБ має бути всеосяжним, охоплювати всі компоненти ІС і враховувати всі актуальні фактори формування ризиків, що діють в інформаційній системі підприємства та за її межами;

- процесного, який пов'язує процеси управління в замкнутий цикл планування, впровадження, перевірки, аудиту та коригування, і підтримка нерозривному зв'язку між етапами циклу, що дозволяє зберігати і постійно підвищувати якість СУІБ [41].

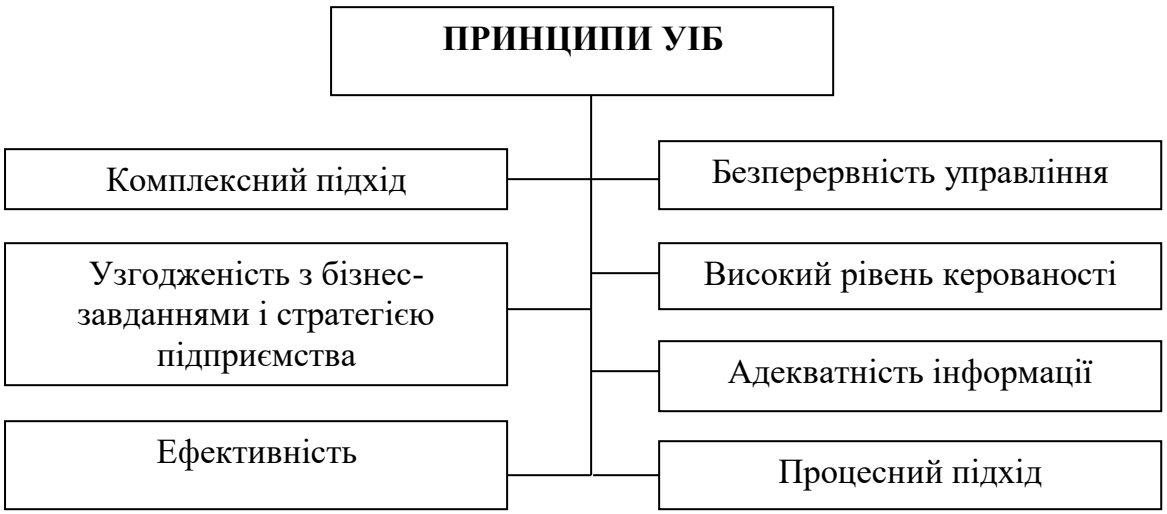

Рис. 1.1. Принципи управління інформаційною безпекою.

У технічному контексті управління інформаційною безпекою має здійснюватися відповідно до принципів безперервності захисту, розумної достатності, гнучкості управління і застосування, відкритості алгоритмів і механізмів захисту, простоти застосування захисних заходів і засобів [1].

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

Управління інформаційною безпекою - це циклічний процес (Рис. 1.1.), що включає:

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

Рис. 1.2. Цикл управління інформаційною безпекою підприємства.

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

Відповідно до основоположного стандарту у сфері інформаційної безпеки ISO / IEC 27001 основою для побудови системи управління інформаційною безпекою є PDCA модель [13], що за загальною логікою відповідає попередньо представленій моделі:

- Plan (Планування) - фаза створення СУІБ, створення переліку активів, оцінки ризиків та вибору заходів;
- Do (Дію) - етап реалізації та впровадження відповідних заходів;

- Check (Перевірка) - фаза оцінки ефективності та продуктивності СУІБ. Зазвичай виконується внутрішніми аудиторами.
- Act (Покращення) - виконання превентивних і коригувальних дій.

За способами здійснення всі заходи і засоби у межах СУІБ поділяють на нормативно-правові; організаційні; програмно-технічні; фізичні; морально-етичні (Рис. 1.3.) [44].

Рис. 1.3. Основні засоби управління інформаційної безпеки підприємства.

До нормативно-правових засобів управління інформаційною безпекою належать діючі в державі закони, укази, положення, інструкції та інші нормативні акти, які регламентують правила роботи з інформацією обмеженого доступу і відповідальності за їх порушення. Цим вони перешкоджають несанкціонованому використанню інформації і стримують потенційних порушників.

Організаційні заходи управління інформаційною безпекою підприємства регламентують процеси функціонування ІС; використання ресурсів ІС; діяльність персоналу служби інформаційної безпеки на підприємстві; порядок роботи користувачів з ІС з метою зменшити або цілком виключити можливість реалізації загроз безпеці.

Організаційні заходи включають:

- розробку вимог і правил роботи з інформацією в ІС;
- порядок дій при проектуванні та налаштуванні об'єктів ІС;
- заходи управління персоналом до прийняття на роботу (підбір і підготовка нового персоналу, ознайомлення з вимогами до роботи з конфіденційною інформацією та мірами відповідальності за їх порушення), під

час роботи (контроль і мотивування працівників до дотримання вимог інформаційної безпеки) та по завершенню працевлаштування;

- організацію пропускного і внутрішнього режимів;

- формування і дотримання засад обліку, зберігання, використання та знищення документів і носіїв з конфіденційною інформацією;

- розподіл реквізитів розмежування доступу (паролів, повноважень тощо);

- організацію контролю за роботою користувачів і персоналу;

- сукупність організаційних дій при проектуванні, розробці, ремонті та модифікації устаткування і ПЗ (сертифікація технічних і програмних засобів, перевірка на відповідність вимогам захисту, документальна фіксація дій тощо).

До програмно-технічних засобів інформаційної безпеки відносяться різні електронні пристрої та спеціальні програми, які реалізують самостійно або в комплексі з іншими засобами такі способи захисту, що унеможливлюють витік, знищення та блокування інформації, порушення цілісності та режиму доступу до неї [1]: ідентифікацію і аутентифікацію суб'єктів ІС; розмежування доступу до ресурсів ІС; контроль цілісності даних; забезпечення конфіденційності даних; аудит подій, що відбуваються в ІС; резервування ресурсів і компонентів ІС.

Фізичні засоби передбачають використання різноманітних механічних, електричних і електромеханічних пристроїв або споруд, призначених для створення фізичних перешкод на можливих шляхах проникнення і доступу порушників (огорожа, двері-пастки, турнікети, кодові замки, системи охоронно-пожежної сигналізації та відеоспостереження, детектори руху, засоби біометричного контролю тощо).

До морально-етичних засобів належать норми поведінки, які традиційно складаються в процесі інформатизації та комп’ютеризації усіх сфер життєдіяльності суспільства. Ці норми бувають як неписаними (загальновизнані норми чесності, корпоративної відданості), так і оформленими в окремий звід правил чи приписів.

Крім цього, дії, орієнтовані на забезпечення інформаційної безпеки, можуть бути охарактеризовані цілим рядом параметрів, що відображають, крім напрямків, орієнтацію на об'єкти захисту, характер загроз, способи дій, їх поширеність, охоплення і масштабність (Рис 1.4.).

Так, за характером загроз захисні дії інформаційної безпеки орієнтовані на захист інформації від розголошення, витоку і несанкціонованого доступу.

За способами дій їх можна поділити на попередження, виявлення, виявлення, припинення і відновлення збитку чи інших збитків.

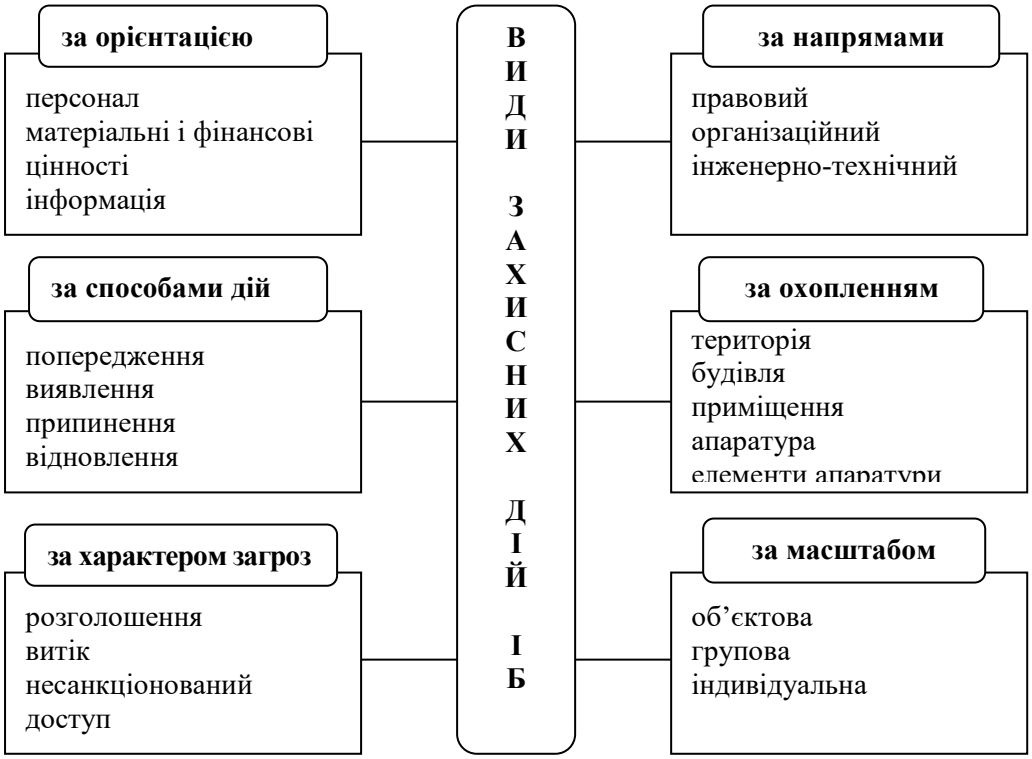

Рис. 1.4. Види захисних дій у сфері інформаційної безпеки.

За охопленням захисні дії інформаційної безпеки можуть бути орієнтовані на територію, споруди, приміщення, апаратуру або окремі елементи апаратного забезпечення.

Масштабність захисних заходів інформаційної безпеки характеризується як об'єктовий, груповий або індивідуальний захист [44].

1.2. Персонал як джерело загроз інформаційній безпеці

Сьогодні безсумнівним є той факт, що саме люди є основним і найціннішим ресурсом підприємства. Адже, персонал створює нові ідеї, робить відкриття і винаходи, тим самим прискорюючи розвиток науково-технічного прогресу. Ефективно та якісно виконуючи свої робочі функції, співробітники підприємства забезпечують прибутковість і зростання бізнесу, формують імідж та репутацію, сприяють конкурентоспроможності компанії на ринку.

Водночас, персонал є основним джерелом втрати цінної і конфіденційної інформації. У сучасних підприємницьких структурах практично кожен співробітник стає носієм цінних відомостей, які становлять інтерес для конкурентів і кримінальних структур.

Людський фактор лежить в основі управління інформаційною безпекою будь-якого підприємства: якщо окремий співробітник не виправдає довіри, не буде відданим інтересам підприємства, усвідомлено не дотримуватиметься встановлених правил інформаційної безпеки та захисту інформації, то жодна ефективна система захисту не зможе гарантувати безпеку інформації та запобігти її розголошенню.

Говорячи про персонал, науковці часто відзначають важливість врахування в процесі управління також і інших, близьких категорій, т.зв. «оточуючих підприємство людей», до яких відносять:

• співробітників інших фірм - посередників, виробників комплектуючих деталей, торгових фірм, рекламних агентств тощо);

• співробітників державних установ, до яких підприємство звертається відповідно до закону - податкових та інших інспекцій, органів місцевого самоврядування, правоохоронних органів тощо;

• журналістів засобів масової інформації, які співпрацюють з підприємством;

• відвідувачів підприємства, працівників комунальних служб, поштових службовців, працівників служб екстремальної допомоги тощо;

• сторонніх осіб, які працюють або проживають поряд з будівлею або приміщеннями підприємства, вуличних перехожих;

• родичів, знайомих і друзів всіх зазначених вище осіб.

Перераховані особи в тій чи іншій мірі є або можуть стати в силу обставин джерелами конфіденційних відомостей. Кожне із джерел, особливо те, що стало ним випадково, може стати небезпечним для підприємства в результаті несанкціонованого розголошення (оголошення) відомостей, що захищаються.

Найбільш обізнані в секретах підприємства перший керівник, його основний заступник, їх референти і секретарі, працівники служби конфіденційної документації [38].

Отже, персонал підприємства, що володіє цінною і конфіденційною інформацією, працює з конфіденційними справами і базами даних, є найбільш обізнаним і часто досить доступним джерелом для зловмисника, який бажає отримати необхідні йому відомості.

Наскільки актуальна проблема захисту інформації від загроз з боку персоналу, можна також побачити на прикладі даних, опублікованих Computer Security Institute (Сан-Франциско, штат Каліфорнія, США), згідно з якими порушення захисту комп'ютерних систем відбувається з таких причин:

- помилки персоналу (недостатній рівень кваліфікації) – 55%;
- цілеспрямовані дії персоналу – 20%;
- несанкціонований доступ – 2%
- дія вірусів – 3%;
- технічні відмови апаратури мережі – 20%.

Таким чином, однією з потенційних загроз для інформації в інформаційних системах слід вважати цілеспрямовані або випадкові деструктивні дії персоналу (людський фактор), оскільки вони становлять 75% усіх випадків [12].

З огляду на актуальність проблем безпеки персоналу проводиться багато соціологічних опитувань і наукових досліджень у цій сфері. Розглянемо результати деяких з них.

Говорячи про види протиправних дій у сфері інформаційної безпеки з боку персоналу підприємства, фахівців визначають такі їх види:

– крадіжка конфіденційної інформації – працівник може скопіювати інформацію на портативні пристрої, чи на зовнішні носії, опублікувати її на веб-сайті, відправити за помилковим поштовим індексом. Може реалізовуватися через помилку працівника або через його навмисні дії;

– порушення авторських прав на інформацію - здійснення несанкціонованого копіювання авторського документу чи його частини, шифрування документу з власним паролем, підробка реквізитів іншого працівника чи компанії. Найчастіше реалізується через навмисні дії персоналу;

– шахрайство - спотворення фінансової документації, перевищення повноважень під час роботи з базами даних, модифікація важливих даних. Реалізується через навмисні дії задля досягнення певної мети;

– саботаж інформації - реалізується навмисно задля досягнення певної мети чи для помсти [11].

Аналізуючи чинники виникнення внутрішніх загроз, серед основних науковці виділити такі:

- непрофесійність, низька фахова підготовка працівників;
- психологічні та комунікативні особливості працівників, зокрема психологічна готовність (схильність) працівника до зловживання службовим становищем;
- сумнівні зв’язки, вчинки, захоплення;
- особисті фінансові труднощі, неможливість задоволення життєвих потреб своїх та сім’ї;
- низький стан виховної та профілактичної роботи в організації;
- недосконала система заробітної плати та стимулювання праці персоналу;
- порушення правил роботи з персоналом, невідповідність кадрової політики умовам роботи в організації;
- відсутність нормативної бази організації, яка б установлювала режими діяльності та правила поведінки персоналу;
- низький стан трудової та виробничої дисципліни, слабка вимогливість керівного складу;
- відсутність належного контролю дій персоналу з боку керівництва;
- неефективна персональна робота з кадрами;
- нездоровий діловий клімат у колективі підприємства [6].

Цікавими також є відомості щодо оцінки різних мотиваційних факторів, що впливають на дії персоналу, отримані в результаті опитування ВД "Коммерсантъ" спільно з Harvard Business School і Вищою школою економіки (Таблиця 1.1.).

Якщо відкинути деякі мотивації очевидного особистісного характеру, то на перші місця претендують такі незадоволені людські мотивації, як - заробітна плата, цікава робота, кар'єрні перспективи, перспективи професійного зростання, репутація компанії [7].

Таблиця 1.1.

Фактори, які впливають на лояльність персоналу підприємства.

Росія	Фактор	США
1	Матеріальна винагорода	4
2	Цікава робота	1
3	Кар’єрне зростання	2
4	Перспективи професійного росту	8
5	Репутація компанії	10
6	Психологічна атмосфера в колективі	7
7	Умови роботи	5
8	Корпоративна культура	9
9	Особистість керівника	3
10	Поведінка керівника	6

За підсумками інших соціологічних досліджень відзначено, що причина витоку інформації найчастіше криється в недбалості перших осіб організації. Наприклад, у приватних фірмах більше 75% відповідальних співробітників, приймаючи відвідувачів, не вважають за необхідне прибирати конфіденційні документи зі столу або ж вимикати комп'ютер. Це призводить до втрати до 30% оперативної інформації.

За даними дослідження, проведеного італійськими психологами, тільки 25% службовців фірми - дійсно надійні люди, ще стільки ж очікують зручного випадку для розголошення конфіденційної інформації, а 50% будуть діяти залежно від обставин [20].

Дослідження показали, що основними умовами, що сприяють неправомірному оволодінню інформацією, є:

- Розголошення (зайва балакучість співробітників) - 32%;

- Здійснення несанкціонованого доступу внаслідок підкупу і схиляння до співпраці з боку конкурентів і злочинних угрупувань - 24%;

- Відсутність на фірмі належного контролю і жорстких умов забезпечення інформаційної безпеки - 14%;

- Традиційний обмін виробничим досвідом - 12%;

- Безконтрольне використання інформаційних систем - 10%;

- Наявність передумов виникнення серед співробітників конфліктних ситуацій, а також відсутність високої трудової дисципліни, психологічна несумісність, випадковий підбір кадрів, слабка робота кадрів по згуртуванню колективу - 8% [31].

Також встановлено, що забезпечення ефективного захисту комерційної таємниці фірми та інших видів конфіденційної інформації залежить від стабільності кадрового складу [39].

Серед форм і методів недобросовісної конкуренції на персонал спрямовані, зокрема, такі:

- погрози фізичної розправи над керівниками фірми та провідними фахівцями (22%);

- підкуп співробітників з метою копіювання інформації (24%), проникнення в бази даних (18%), отримання конфіденційних документів (10%), підслуховування телефонних розмов і переговорів у приміщеннях (5%), а також обмеження доступу до інформації, дезінформування [31].

У науці виділяють дві форми співпраці персоналу з субєктами, які зацікавлені в отриманні конфіденційної інформації підприємства: усвідомлену і неусвідомлену. До усвідомленої співпраці працівника підприємства зі зловмисником можна віднести:

• ініціативне співробітництво працівника підприємства з метою помсти керівництву або колективу підприємства, а також з причини підкупу, регулярної оплати постійних послуг, і психічної нестійкості;

• формування спільності - зловмисник і його спільник, помічник, який працює на основі переконання в справедливості поглядів зловмисника, дружніх та інших відносин, взаємодопомоги тощо.

• співробітництво на основі особистого переконання працівника у протиправних діях керівництва підприємства або їх моральному розкладанні;

• схиляння (примус, спонукання) до співпраці шляхом обманних дій, зміни поглядів або моральних принципів шляхом переконання, вимагання, шантажу, використання негативних рис характеру, фізичного насильства.

Найбільш частим, досить небезпечним і таким, що важко виявляється є використання співробітника підприємства для неусвідомленої співпраці:

• переманювання цінних і обізнаних фахівців обіцянкою кращої матеріальної винагороди, кращими умовами праці та іншими перевагами («крадіжка мізків»);

• створення ілюзії прийому співробітника на високооплачувану роботу в конкуруючу фірму, вивідування в процесі співбесіди необхідних конфіденційних відомостей і потім відмова в прийомі;

• вивідування цінної інформації у співробітника підприємства за допомогою підготовленої системи запитань на наукових конференціях, зустрічах з пресою, на виставках, в особистих бесідах у неслужбовій обстановці;

• підслуховування і записування на диктофон розмов співробітників підприємства в службових і неслужбових приміщеннях, в процесі переговорів і прийомі відвідувачів, в транспорті, на банкетах, в домашній обстановці, при спілкуванні з друзями та знайомими;

• прослуховування службових та особистих телефонів співробітників підприємства; перехоплення телексів, телеграм, факсів, повідомлень по електронній пошті, відкриття та ознайомлення зі службовою та особистою кореспонденцією керівництва підприємства співробітниками (іноді за сприяння секретаря);

• отримання зловмисником від співробітника потрібної інформації, коли співробітник знаходиться в стані алкогольного сп'яніння, під дією наркотиків, психотропних препаратів, навіювання, гіпнозу, приведення зловмисником співробітника в несвідомий стан, що не дозволяє адекватно оцінювати свої дії і легко змінює переконання [19].

У результаті незнання правил інформаційної безпеки та захисту інформації конфіденційна інформація несанкціоновано розголошується на загальнодоступних наукових семінарах, виставках, офіційних і неофіційних зустрічах і презентаціях, особливо колегам по професії і журналістам.

Дуже небезпечні особи, які були звільнені з підприємства і володіють її конфіденційною інформацією [38].

У результаті узагальнення вище наведених даних, варто виділити такі види чинників, які створюють підґрунтя для порушень інформаційної безпеки з боку персоналу підприємства:

- власне персонал (його особисті та професійні якості, психологічні особливості, кваліфікація, досвід, матеріальний стан тощо);
- недостатньо успішна робота з кадрами підприємства;
- деструктивна діяльність конкурентів (Рис. 1.5.).

Також, на нашу, думку, доцільно згадати чинники неправомірних дій персоналу, які залежать від зовнішнього середовища компанії, наприклад, відсутність законодавчого регулювання певних питань, пов'язаних, наприклад, з появою нових технологій, а відповідно і їх зловживання, нестабільна соціально-економічна чи політична ситуація в державі, соціальні заворушення, військові конфлікти тощо.

Рис. 1.5. Чинники порушення інформаційної безпеки з боку персоналу підприємства.

Таким чином, встановлено, що з огляду на вирішальний вплив людського фактора та зростання пов'язаних з ним загроз інформаційній безпеці успішний менеджмент персоналу є ключовим чинником забезпечення інформаційної безпеки підприємства.

1.3. Менеджмент персоналу в системі управління інформаційною безпекою

Враховуючи той факт, що 75% усіх випадків потенційних загроз для інформаційної безпеки підприємства становлять цілеспрямовані або випадкові деструктивні дії персоналу, система управління інформаційною безпекою повинна насамперед ґрунтуватися на виборі і застосуванні ефективних методів менеджменту персоналу.

Людський фактор завжди був і є одним із найважливіших чинників зростання ризиків для будь-якої організації, оскільки більшість інцидентів відбуваються саме з вини співробітників. Відповідно до даних Антирейдерського союзу підприємців України 82% загроз реалізується власними співробітниками фірми або за їх прямої чи опосередкованої участі; тільки 1% загроз інформаційній безпеці мають випадковий характер [16].

З огляду на зазначені чинники питання управління персоналом, робота якого пов'язана з обробкою, зберіганням і використанням конфіденційних відомостей, документів і баз даних, в даний час все більшою мірою в стратегічному і прикладному аспектах входить в число головних при вирішенні проблем інформаційної безпеки. При цьому варто пам'ятати, що персонал підприємства сьогодні є найважливішим його ресурсом. Кадри не тільки вирішують все, але можуть і позбавити всього.

Управління персоналом у сфері інформаційної безпеки має на меті мінімізувати ризики порушення працівниками вимог і запобігти виникненню передумов для таких дій шляхом формування корпоративної відданості персоналу інтересам підприємства, і усвідомленого дотримання ним встановлених правил захисту інформації. Якщо окремий співробітник не виправдає довіри, то жодна ефективна система захисту не зможе гарантувати безпеку інформації та запобігти її розголошенню.

З метою запобігання та протидії негативному впливу людського фактора у рамках СУІБ підприємства має здійснюватися низка організаційних заходів по роботі з персоналом, задіяним у роботі з конфіденційною інформацією. Такі заходи можна розділити на кілька груп:

• проведення ускладнених аналітичних процедур відбору і прийому нових працівників, а також порядку звільнення персоналу;

• документування добровільної згоди працівника про нерозголошення конфіденційних відомостей та зобов'язань дотримуватися правил безпечного поводження з інформацією;

• постійне і послідовне інструктування і навчання співробітників практичним діям із захисту інформації;

• контроль за виконанням персоналом вимог щодо захисту інформації, стимулювання відповідального ставлення до збереження конфіденційних

відомостей;

• формування корпоративної культури безпеки, мотивування працівників в матеріальний та нематеріальний спосіб з метою забезпечення їх лояльності до підприємства.

Ефективне управління персоналом - життєво обумовлена стратегічна функція, яка є важливою гарантією не тільки того, що підприємство буде успішним і прибутковим, але й того, що завдання забезпечення інформаційної безпеки будуть виконані своєчасно і якісно.

Принципи, покладені в основу ефективного управління персоналом, досить різноманітні. Вони носять багаторівневий характер і поширюються на різні сфери діяльності (управління працею в масштабах усього суспільства, галузі, підприємства, окремого працівника).

Система управління персоналом підприємства, задіяним у сфері інформаційної безпеки, має здійснюватися у відповідності як з загальними *принципами управління персоналом*, так і зі спеціальними принципами, які відображають специфіку роботи корпоративної СУІБ.

Загальну схему зазначених принципів показано на рис. 1.6.

Серед, *загальних принципів* управління персоналом виділяють, зокрема, принцип *науковості*, що означає використання науково обґрунтованих методів та засобів у процесі здійснення управління персоналом підприємства.

Дуже важливим для ефективного менеджменту персоналу є принцип *системності*, який обумовлює необхідність реалізації системного підходу в управлінні підприємством як цілісним соціальним організмом.

Принцип *плановості* вимагає, щоб усі процеси, процедури, операції, дії, що відбуваються на підприємстві з відтворення та використання персоналу, виробництво та праця на кожному робочому місці відбувались на планомірній основі. Відсутність планомірності, неузгодженість окремих планів або їхніх складових спричиняють порушення ритму виробництва, втрати робочого часу та інших ресурсів, погіршення якості продукції та послуг тощо.

Принцип *адаптивності* означає пристосовуваність системи управління персоналом до швидко змінних оточуючих підприємство умов, а відповідно і цілей, завдань бізнесу.

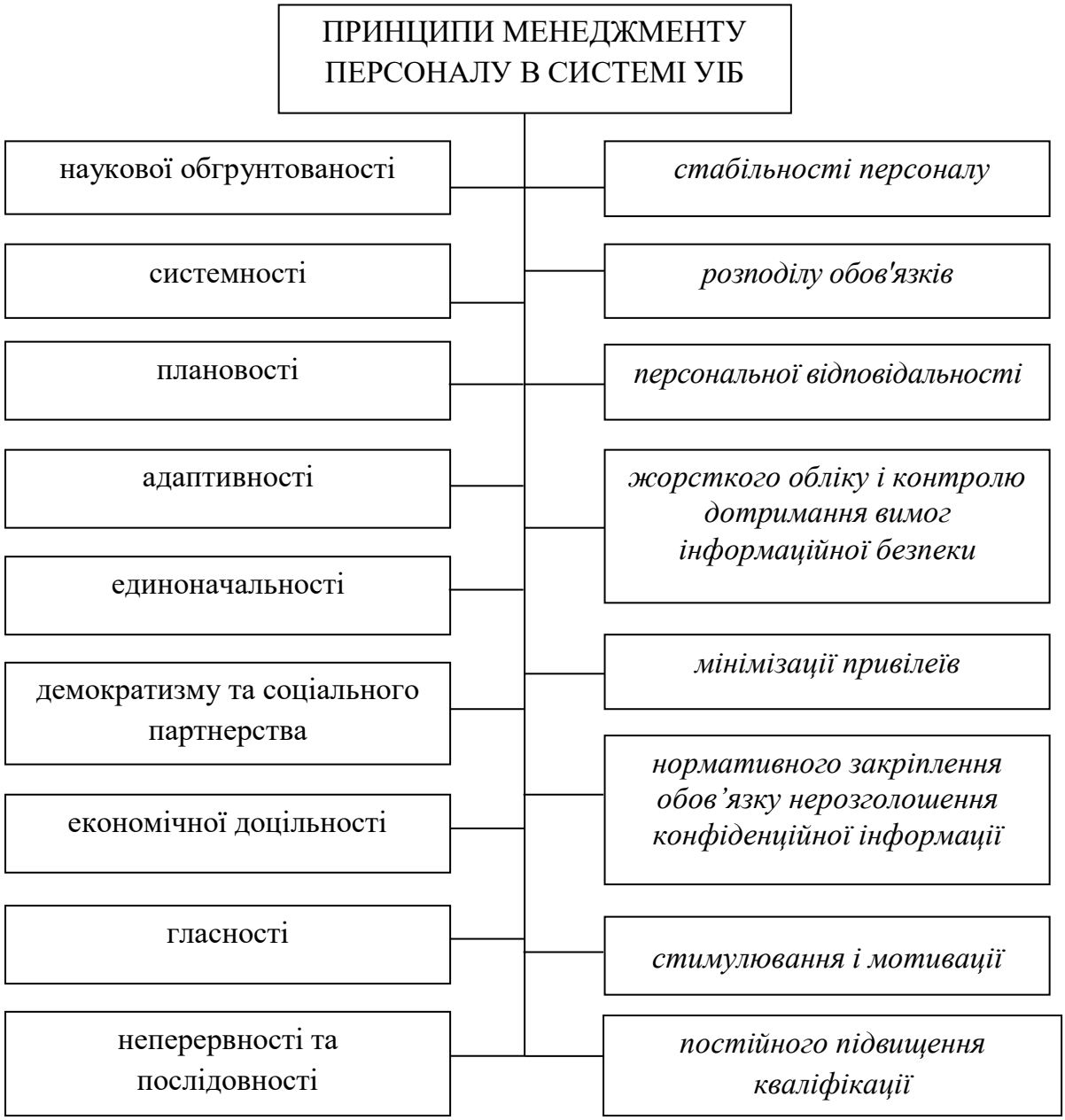

Рис.1.6. Принципи менеджменту персоналу в СУІБ підприємства.

Принцип *єдиноначальності* відображає необхідність чіткого розподілу повноважень між керівниками та структурними підрозділами по вертикалі й горизонталі, адміністративну підпорядкованість кожного працівника і структурної ланки лише одному керівникові, який несе за них персональну відповідальність.

Принцип *соціального партнерства* врівноважує принцип єдиноначальності і акцентує, що між соціальними партнерами (найманим персоналом і роботодавцем) має бути досягнуто взаєморозуміння і балансу інтересів отримання взаємовигідних кінцевих результатів.

Принцип оптимального поєднання *централізації і децентралізації* управління – забезпечує, щоб стратегічні рішення приймалися централізовано, а прийняття оперативних - делегувалися нижчому рівню управління.

Принцип *демократизму* вимагає оптимального поєднання єдиноначальності, персональної відповідальності керівника за стан справ у підрозділі, яким він керує, з участю найманих працівників у формуванні стратегії та політики менеджменту персоналу, прийнятті оперативних рішень, виявленні резервів підвищення ефективності виробництва тощо.

Запорукою ефективної системи співпраці між колективом і власником, керівником підприємства є принцип *гласності*, який зобов'язує до належного інформування колективу і окремих працівників щодо політики, принципів і методів підбору кадрів, перспектив підвищення матеріального добробуту тощо;

Принцип *економічної ефективності* вимагає ретельного обґрунтування інвестицій у розвиток персоналу, витрат на оплату праці та утримання робочих місць, інших прямих і непрямих витрат з огляду на їх віддачу, окупність.

Принцип *економічної зацікавленості* полягає в необхідності створення гнучкої системи стимулів, яка спонукала б керівників і весь персонал працювати з повною віддачею творчого потенціалу на благо організації, а отже, кожного працівника і суспільства. Водночас, не слід забувати про велику роль не матеріальних факторів у мотивуванні персоналу [24].

Принцип *пропорційності* відображає необхідність дотримання конкретних пропорцій між різними функціональними групами працівників за чисельністю, кваліфікацією і обсягами виконуваних робіт з метою своєчасного, якісного, узгодженого здійснення всіх виробничих і управлінських функцій;

Сприяє успішному розвитку кадрової системи підприємства принцип *збалансованості* за віковим критерієм, оскільки таким чином забезпечується поєднання досвідчених працівників із молодими кадрами, систематичне поповнення управлінських кадрів за рахунок перспективних працівників;

Принцип *поєднання вимогливості, контролю роботи працівників із повагою* до них. Контроль і оцінювання службової діяльності не повинні принижувати гідність працівника, їхні завдання полягають у підвищенні ефективності праці, мотивуванні працівників.

Принцип створення умов для постійного *підвищення професійної*

кваліфікації та кар'єрного зростання кадрів на основі обґрунтованих критеріїв оцінки їхньої діяльності та особистих якостей.

Принцип *ротації кадрів* реалізується у цілеспрямованому горизонтальному і вертикальному переміщенні працівників з метою ефективного використання їхніх знань і навичок, управління кар'єрами.

Управління персоналом підприємства має здійснюватися на засадах *послідовності, безперервності та узгодженості, врахування об'єктивних закономірностей розвитку* виробничих та невиробничих систем підприємства.

Для системи менеджменту персоналу підприємства у сфері інформаційної безпеки характерні також спеціальні принципи, зокрема:

- принцип *стабільності персоналу,* який формує орієнтацію працівників на лояльність до організації і довгострокову роботу. Подолання плинності кадрів підвищує ефективність роботи і зменшує ризики витоку інформації.
- принцип *підбору і добору кадрів* за спеціальною процедурою, яка передбачає оцінювання претендентів не тільки за діловими і моральними якостями, а і з урахуванням їх професійної та психологічної придатності для роботи з конфіденційною інформацією;
- принцип *розподілу обов'язків* - розподіляти ролі й відповідальність так, щоб одна людина не могла порушити критично важливий для організації процес;
- принцип *мінімізації привілеїв* пропонує виділяти користувачам тільки ті права доступу, які необхідні їм для виконання службових обов'язків, і таким чином зменшити збиток від випадкових або навмисних некоректних дій.
- принцип *персональної відповідальності* керівництва і персоналу;
- принцип *нормативного закріплення обов'язку працівника щодо нерозголошення конфіденційної інформації;*
- принцип здійснення *жорсткого обліку та контролю* за використанням та зберіганням, знищенням працівником конфіденційної інформації.

Особливо важливого значення набуває принцип *стимулювання і мотивації* працівників, задіяних у системі інформаційної безпеки підприємства як засобів забезпечення стабільності персоналу і зменшення ризиків витоку інформації.

Необхідним є також забезпечення принципу регулярного *підвищення кваліфікації персоналу*, задіяного у роботі з конфіденційною інформацією, через проведення тренінгів, інструктажів, стажувань з актуальних питань у цій сфері.

До основних *напрямів менеджменту персоналу*, задіяного у системі управління інформаційною безпекою підприємства, належать (Рис.1.7.):

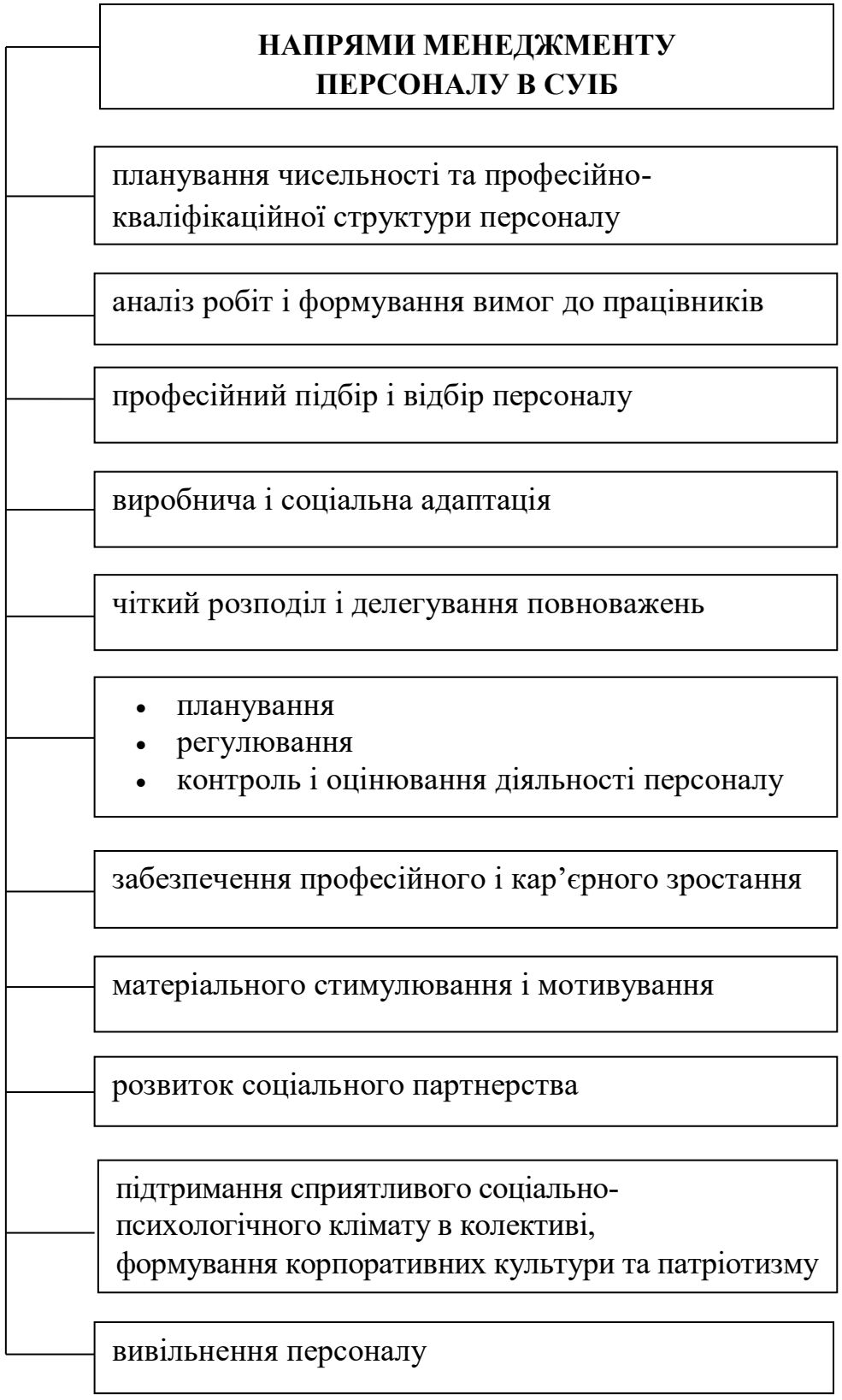

Рис.1.7. Напрями менеджменту персоналу в СУІБ підприємства.

- 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;
- 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 делегування повноважень з урахуванням вимог обмеженого доступу працівників до конфіденційної інформації;
- планування та регулювання трудової діяльності персоналу, контроль і оцінювання діяльності трудових колективів і кожного працівника;
- забезпечення професійного та кар'єрного розвитку персоналу, що працює у системі управління інформаційною безпекою;
- застосування ефективних систем матеріального і морального стимулювання праці як засобів формування корпоративної відданості працівників;
- розвиток соціального партнерства в організації;
- підтримання сприятливого соціально-психологічного клімату в трудовому колективі, виховання у працівників корпоративного патріотизму і культури;
- вивільнення персоналу відповідно до спеціальних процедур тощо.

Необхідними компонентами менеджменту персоналу, який працює з конфіденційною інформацією, є також навчання співробітників щодо порядку роботи з конфіденційними відомостями, в тому числі психологічна підготовка з метою протистояння методам «соціальної інженерії».

Висновки до першого розділу

З'ясовано, що система управління інформаційною безпекою - це частина загальної системи управління підприємства, що базується на аналізі ризиків і

призначена для проектування, реалізації, контролю, супроводу та вдосконалення заходів в області інформаційної безпеки.

За способами здійснення всі заходи і засоби у межах СУІБ поділяють на нормативно-правові; організаційні; програмно-технічні; фізичні; морально-етичні. До організаційних заходів відносять, серед інших, заходи з управління персоналом.

Як показує практика, саме люди є основним і найціннішим ресурсом підприємства. Водночас, вони є основним джерелом втрати цінної і конфіденційної інформації. Дослідження засвідчили, що цілеспрямовані або випадкові деструктивні дії персоналу становлять 75% усіх випадків порушення інформаційної безпеки. Таким чином, управління персоналом, що працює з конфіденційною інформацією, набуває все більшого стратегічного значення при вирішенні проблем інформаційної безпеки.

У результаті дослідження визначено види протиправних дій у сфері інформаційної безпеки з боку персоналу: крадіжка конфіденційної інформації; порушення авторських прав на інформацію; шахрайство; саботаж інформації, а також чинники, які створюють підґрунтя для порушень інформаційної безпеки з боку персоналу: власне персонал (його особисті та професійні якості, психологічні особливості, кваліфікація, досвід, матеріальний стан тощо); недостатньо успішна робота з кадрами підприємства; деструктивна діяльність конкурентів.

Управління персоналом у сфері інформаційної безпеки має на меті мінімізувати ризики порушення працівниками вимог і запобігти виникненню передумов для таких деструктивних дій шляхом: 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; 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 делегування

повноважень з урахуванням вимог обмеженого доступу працівників до конфіденційної інформації; планування та регулювання трудової діяльності персоналу, контроль і оцінювання діяльності трудових колективів і кожного працівника; забезпечення професійного та кар'єрного розвитку, навчання і підвищення кваліфікації персоналу, що працює у системі управління інформаційною безпекою; застосування ефективних систем матеріального і морального стимулювання праці як засобів формування корпоративної відданості працівників; розвиток соціального партнерства; підтримання сприятливого соціально-психологічного клімату в трудовому колективі, виховання у працівників корпоративного патріотизму і культури; вивільнення персоналу відповідно до спеціальних процедур тощо.

РОЗДІЛ 2. Напрями управління персоналом з інформаційної безпеки

2.1. Засади наймання працівників, задіяних у сфері інформаційної безпеки

Один з найбільш важливих етапів у роботі з персоналом підприємства – процес набору й відбору можливих кандидатів для призначення на посади, пов’язані з конфіденційною інформацією.

Процес наймання починається з пошуку й добору осіб, які відповідають вимогам. Пошук кандидата на знову створювану або вакантну посаду на підприємстві не повинен носити безсистемний характер. Крім очікування на кандидатів, які відгукнуться на оголошення про вакансію, варто використовувати інші методи підбору потенційних фахівців, зокрема пошук кандидатів з числа працівників підприємства, особливо якщо мова йде про керівника або спеціаліста високого рівня.

Цей метод дає можливість просувати перспективних працівників по службових сходах і зацікавлювати їх роботою, виховувати відданість справам підприємства. Можна запрошувати на посаду особу, яка раніше працювала на підприємстві і добре себе зарекомендувала. Перевагою цього методу є те, що про кандидата досить багато відомо і не доводиться «купувати кота в мішку». Такий підхід є найбільш надійним при підборі кандидата на посаду, пов'язану з володінням цінною і конфіденційною інформацією.

Водночас, слід пам’ятати, що без припливу нових людей колектив втрачає свої новаторські якості, перспективи залучення нових ідей, пропозицій, що визначатимуть нові перспективи розвитку.

Можливим є пошук кандидатів серед студентів і випускників навчальних закладів, встановлення зв'язків з підрозділами вузів, зайнятими працевлаштуванням випускників. Можна мати досить повну інформацію про професійні та особисті якості студентів. Дуже ефективно вести пошук (навіть на середніх курсах) найбільш здібних студентів, залучати їх в процесі навчання до роботи на підприємстві, оплачувати їх працю і, можливо, фінансувати навчання у вузі, платити стипендію.

Одним із методів пошуку потенційних працівників є звернення в державні та приватні бюро, агентства з найму робочої сили, біржі праці, організації з працевлаштування осіб, звільнених за скороченням штатів, працевлаштування молоді, колишніх військовослужбовців тощо. Подібні агентства пропонують досить великий контингент потенційних працівників, ведуть цілеспрямований пошук висококваліфікованих фахівців, організовують перепідготовку фахівців за індивідуальними замовленнями.

Підбір кандидатів за рекомендаціями співробітників підприємства також є доцільним, оскільки зазвичай такі рекомендації є відповідальними і виваженими. Адже особам, які рекомендують кандидатів, у подальшому доведеться з ними працювати [17].

Зазначені напрями пошуку кандидатів на посади, пов'язані з володінням конфіденційною інформацією, як правило, дозволяють вибрати необхідних працівників з ряду осіб, які виявили бажання зайняти вакантну посаду.

Починаючи пошук кандидатів на зайняття вакантної посади у підрозділи інформаційної безпеки, захисту інформації, конфіденційного діловодства та інших, робота яких пов'язана з володінням конфіденційною інформацією, варто приділити особливу увагу формуванню вимог до потенційного працівника.

При підборі кандидатів оцінюється відповідність кожного з них таким основним вимогам:

- за рівнем підготовки та кваліфікації, наявності необхідного досвіду роботи;
- за морально-діловими і особистісними якостями;
- за ступенем відповідальності за прийняті управлінські та виконавські рішення (залежно від займаної посади).

При підборі кандидатів для призначення на посади, пов’язані з конфіденційною інформацією, в обов’язковому порядку враховується рівень кожної конкретної посади з точки зору прийняття та реалізації управлінських рішень, виконання організаторських функцій і завдань повсякденної діяльності підприємства. Виходячи з названих критеріїв, дані посади поділяють на такі групи:

- посади керівників підприємства (керівник підприємства, представництва, філії);

- посади заступників керівника;
- посади керівників структурних підрозділів;
- посади керівників служб безпеки та їх заступників;
- посади співробітників служб безпеки підприємства;
- посади співробітників підприємства, які здійснюють на постійній основі роботу з конфіденційною інформацією у відповідних структурних підрозділах.

При підборі кандидатів для призначення на перераховані посади додатково враховується обсяг і важливість відомостей конфіденційного характеру, до яких допускаються працівники, що займають ці посади [29].

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

- проведення ускладнених аналітичних процедур при прийомі на роботу;
- документування добровільної згоди особи не розголошувати конфіденційні відомості й дотримуватися правил забезпечення безпеки інформації;
- інструктування і навчання щодо практичних дій у сфері інформаційної безпеки.

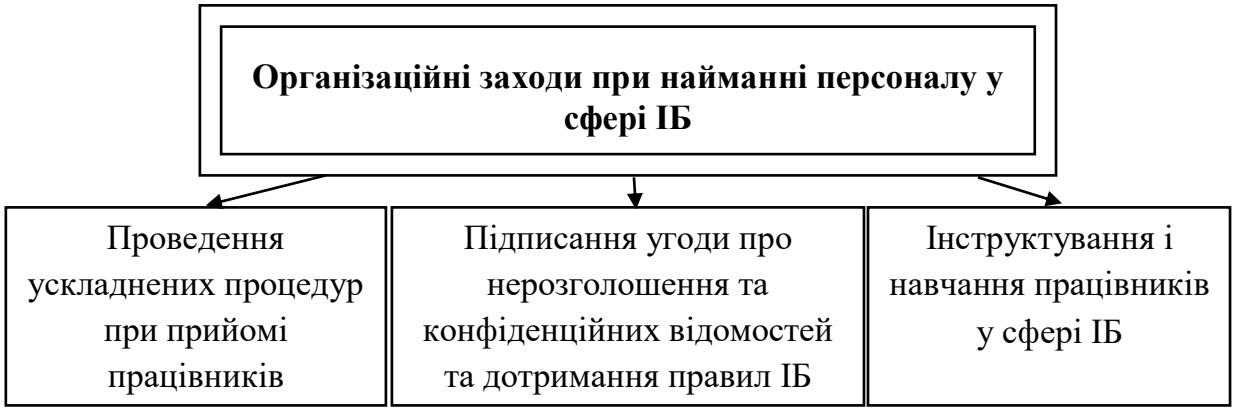

Рис. 2.1. Організаційні заходи при найманні персоналу у сфері інформаційної безпеки.

Технологічний ланцюжок підбору й добору співробітників, що працюватимуть з конфіденційною інформацією, складається з таких етапів:

• підбір передбачуваного кандидата (кандидатів) для прийому на роботу або переведення, отримання резюме;

• вивчення резюме (і особової справи, якщо кандидат працює на підприємстві) керівництвом підприємства, структурного підрозділу та службою персоналу, виклик для бесіди підходящих кандидатів;

• інформування кандидатів, що працюють на підприємстві, про їх майбутні посадові обов'язки, пов'язані з конфіденційною інформацією підприємства;

• знайомство (попередня співбесіда) керівництва підприємства, структурного підрозділи і служби персоналу з кандидатами, які не працюють на підприємстві; бесіда з ними, уточнення окремих положень резюме; відповіді на питання про майбутню роботу; вивчення отриманих від кандидата рекомендаційних листів;

• заповнення кандидатами, які не працюють на підприємстві, і подання до відділу кадрів усіх необхідних документів;

• оновлення матеріалів особової справи потенційного кандидата, що працює на підприємстві; отримання уявлення про переведення на нову посаду від керівника структурного підрозділу;

• співбесіда кандидатів з працівником відділу кадрів за поданими документами, при необхідності підтвердження тих чи інших відомостей поданням додаткових документів;

• опитування співробітником відділу кадрів авторитетних для підприємства осіб, які особисто знають кандидата на посаду, протоколювання опитування;

• співбесіда експертів з кандидатами з метою визначення їх особистих і моральних якостей, а для непрацюючих на підприємстві співробітників додатково – професійних здібностей; розгляд медичної довідки;

• за необхідності - тестування та анкетування кандидатів [17].

При бесідах і співбесідах з кандидатами на посаду в області інформаційної безпеки та захисту інформації переслідуються такі цілі:

- виявити реальну причину бажання кандидата працювати в даній компанії;
- виявити можливих зловмисників або спробувати побачити слабкості кандидата як людини, які можуть сприяти шпигунству;
- переконатися, що кандидат не приніс з собою конфіденційну інформацію іншого підприємства чи організації, яку хоче таємно використовувати;
- переконатися в добровільній згоді кандидата дотримуватися правил захисту інформації та мати певні обмеження у професійному й особистому житті.

Працівник кадрового органу також запитує необхідні довідки та документи, знайомить претендента зі змістом договору (контракту) про оформлення допуску конфіденційної інформації. Особливу увагу секретар-референт повинен звертати 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 громадянина (на фотографії окуляри, борода, перука – тільки при постійному носінні), відповідність форми бланка документа роками їх використання, відсутність підчисток, незавірених виправлень, спроб заміни аркушів, фотографій тощо.

Усі печатки повинні відповідати назвам тих організацій, які видали документ. Наприклад: трудова книжка повинна відповідати встановленій формі або мати напис «дублікат», містити запис про звільнення з останнього місця роботи, завірений печаткою.

При якихось сумнівах особу просять подати дублікати зіпсованих документів, завірити виправлення. Документи, що викликали явний сумнів, повертаються громадянину, і одночасно йому відмовляється у розгляді питання про прийом на роботу.

Тільки після ретельного аналізу поданих документів з кандидатами на посаду проводиться співбесіда [30].

Співбесіди з кандидатами на посаду переслідують такі цілі:

• виявити реальну причину бажання працювати саме на цьому підприємстві;

• виявити можливих зловмисників або спробувати побачити слабкості кандидата як людини, які можуть провокувати злочинні дії;

• переконатися, що кандидат не має наміру використовувати в роботі секрети організації, в якій він раніше працював;

• переконатися в добровільній згоді кандидата дотримуватися правил захисту інформації та мати певні обмеження в професійному та особистому житті [38].

Зокрема, опитувальники для співбесіди складаються таким чином, щоб з'ясувати причини звільнення кандидата з колишнього місця роботи, джерело інформації про вакансії на даному підприємстві, наявність досвіду роботи з

конфіденційною інформацією, стосунки в сім'ї, рівень добробуту, житлові умови, культурний рівень кандидата тощо.

Крім традиційних кроків для більше повного ознайомлення з особистістю кандидата можна також скористатися послугами органів внутрішніх справ: довідатися про наявність (відсутність) судимості кандидата й про осіб, що перебувають у розшуку.

Можливим є також перевірка на поліграфі, хоча проведення такого тестування пов’язано з певними складнощами. Застосування поліграфа в Україні не узаконено, але й не заборонено. Небезпідставно керуючись даним принципом, керівники багатьох організацій вважають застосування поліграфа цілком виправданим і корисним [14].

Важливу роль відіграє перевірка психологічних особливостей потенційного працівника у сфері інформаційної безпеки, яка має на меті:

• виявлення судимостей, що мали місце раніше, злочинних зв'язків, кримінальних нахилів;

• визначення можливих злочинних нахилів, схильності кандидата до вчинення протиправних дій, зухвалих і необдуманих вчинків у випадку формування в його оточенні певних обставин;

• встановлення факторів, що свідчать про морально-психологічну ненадійність, нестійкість, уразливість кандидата тощо.

На думку фахівців, претендент на зайняття вакантної посади, що передбачає роботу з конфіденційною інформацією, має володіти низкою особистих якостей. Встановлено також перелік характеристик, небажаних для працівника, задіяного у сфері інформаційної безпеки (Таблиця 2.1).

Очевидно, що при вмілому поєднанні традиційних і психологічних кадрових методів аналізу можна з певною мірою вірогідності прогнозувати поведінку співробітників в різних, у тому числі екстремальних, ситуаціях.

Зазвичай відібраним для роботи вважається кандидат, у якого результати аналізу документів, співбесід, перевірок, тестів та психологічного вивчення є несуперечливими, і не містять даних, що перешкоджали б працевлаштуванню.

Після прийняття рішення про наймання єдиного претендента проводять заключну співбесіду з претендентом на посаду з метою отримання від нього принципової згоди на роботу з конфіденційною інформацією. Після цього

новий працівник підписує зобов'язання про нерозголошення таємниці підприємства, зокрема, доступних йому конфіденційних відомостей. Фахівця інформують про характер конфіденційної інформації, з якою він буде працювати, наявності системи захисту цієї інформації і ті обмеження, яких доведеться дотримуватися в позаробочих умовах.

Таблиця 2.1

Бажані та небажані особисті якості персоналу у сфері інформаційної безпеки

Бажані особисті якості	Небажані особисті якості
Порядність, чесність, сумлінність, принциповість	Емоційні розлади
Старанність, дисциплінованість	Неврівноваженість поведінки
Емоційна стійкість	Відчуження від колег по роботі
Прагнення до успіху і порядок у роботі	Розчарування в собі і своїх здібностях
Самоконтроль у вчинках і діях	Ображене самолюбство
Адекватна самооцінка власних можливостей і здібностей	Невдоволення своїм службовим становищем
Помірна схильність до ризику	Надмірно егоїстична поведінка
Вміння зберігати секрети за будь-яких обставин та стану	Відсутність достатньої розсудливості
Тренована увага	Нечесність
Хороша пам'ять, вміння вести порівняльне оцінювання фактів	Небажання і нездатність захищати інформацію
	Фінансова безвідповідальність, бажання отримати гроші без особливих затрат розумових і фізичних сил
	Вживання алкоголю та наркотиків, що призводить до балакучості, необдуманих вчинків, випадкових знайомств, тощо.

Наступними кроками є працевлаштування є:

• проведення керівником структурного підрозділу, керівником служби безпеки і співробітником служби персоналу бесід-інструктажів з працівником,

• ознайомлення претендента з посадовою інструкцією, робочими технологічними інструкціями, інструкцією щодо забезпечення інформаційної безпеки підприємства й іншими аналогічними матеріалами;

• складання проекту контракту, що містить пункт про обов'язок працівника не розголошувати конфіденційні відомості підприємства;

• підписання контракту про тимчасову роботу без права доступу до конфіденційної інформації;

• складання та підписання наказу про прийом на роботу з випробувальним терміном (або на тимчасову роботу) з оформленням відповідних облікових документів;

• проведення випробувального терміну, під час якого проходить вивчення особистих і професійних якостей працівника, навчання правилам роботи з конфіденційною інформацією і документами, інструктажі, перевірка знань;

• за результатами роботи співробітника протягом випробувального терміну укладення нового контракт про постійну роботу та видання відповідного наказу або відмова співробітника в роботі;

• оформлення допуску працівника до конфіденційної інформації і документів [38].

Після отримання допуску до конфіденційної інформації співробітник в індивідуальному порядку проходить інструктажі та тренінги щодо правил роботи з документами, базами даних, які будуть йому надані. Результат навчання фіксується у зобов'язанні або контракті. Відмітка засвідчується підписами керівника служби безпеки та співробітника.

2.2. Заходи регламентації доступу та контролю щодо персоналу, який працює з конфіденційною інформацією

Допуск та доступ персоналу до конфіденційної інформації

Регламентація доступу персоналу до конфіденційних відомостей, документів і баз даних є однією з центральних проблем системи управління інформаційною безпекою підприємства та захисту інформації.

Регламентація порядку доступу лежить в основі режиму конфіденційності робіт, які виконуються підприємством. Важливо чітко і однозначно визначити: хто, кого, до яких відомостей, коли і як допускає.

Режим – це сукупність обмежувальних правил, заходів, норм, які забезпечують контрольований доступ на певну територію, до приміщень, до інформації та документів. Будь-який режим базується на так званій дозвільній системі. Дозвільна система в загальному вигляді передбачає необхідність отримання спеціального дозволу на здійснення відповідних правових заходів, наприклад на в'їзд в зону обмеженого доступу, на відвідування приміщень підприємства тощо.

Дозвільна (розмежувальна) система доступу в сфері комерційної таємниці – це сукупність правових норм і вимог, що встановлюються першим керівником або колективним органом керівництва підприємством з метою забезпечення правомірного ознайомлення та використання співробітниками підприємства конфіденційних відомостей, необхідних їм для виконання службових обов'язків.

Дозвільна система вирішує такі завдання:

• обмеження і регламентації складу співробітників, функціональні обов'язки яких вимагають знання конфіденційних відомостей та роботи з документами;

• строгого вибіркового і обґрунтованого розподілу документів та інформації між співробітниками;

• забезпечення співробітника всім необхідним для реалізації своїх службових функцій (документами, справами, базами даних, інформацією, технічними засобами тощо);

• безперешкодного проходу співробітника в будівлю підприємства, в конкретне робоче приміщення (режимну зону), до виділеного йому офісного робочого обладнання і комп'ютера;

• виключення можливості для сторонніх осіб несанкціонованого ознайомлення з конфіденційною інформацією в процесі роботи співробітника з документами, справами і базами даних;

• раціональне розміщення робочих місць співробітників, при якому виключалося б безконтрольне використання співробітником інформації, яка підлягає захисту (колективний контроль за роботою співробітників) [17].

Дозвільна система включає в себе дві складові частини: допуск співробітника до конфіденційної інформації і безпосередній доступ цього співробітника до конкретних відомостей.

Під допуском розуміється процедура оформлення права співробітника підприємства або іншої особи на доступ до відомостей (інформації) обмеженого поширення і одночасно правовий акт згоди (дозволу) власника (власника) інформації на передачу її для роботи конкретній особі.

Оформлення допуску, тобто згоди особи на певні обмеження у використанні інформації, завжди носить добровільний характер. Наявність допуску надає співробітнику формальне право працювати зі строго певним колом конфіденційних документів, баз даних та окремих відомостей.

У підприємницьких структурах дозвіл на допуск дає перший керівник підприємства. Дозвіл оформляється відповідним пунктом у контракті (трудовому договорі). Допуск може оформлятися наказом першого керівника із зазначенням типового складу відомостей, з якими дозволяється працювати даному співробітнику або групі співробітників. Допуск може носити тимчасовий характер на період виконання певної роботи і переглядатися при зміні профілю роботи співробітника.

Кінцевою інстанцією, яка вирішує питання про необхідність допуску даній особі, є керівник, який розпоряджається цією інформацією і здійснює за нею контроль.

Доступ - практична реалізація кожним співробітником наданого йому допуском права на ознайомлення і роботу з певним складом конфіденційних відомостей, документів і баз даних. Він санкціонується повноважною посадовою особою (першим керівником, його заступником, керівником підрозділу, служби або напрямки діяльності) стосовно конкретної інформації і конкретного співробітника. Право на видачу такого дозволу строго регламентується.

Дозвіл (санкція) на доступ до конкретної інформації може бути дано за дотримання таких умов:

• наявність підписаного наказу першого керівника про прийом на роботу (переведення, тимчасове заміщення, зміні посадових обов'язків тощо) або призначенні на посаду, у функціональну структуру якої входить робота з конкретною інформацією;

• наявність у підписаному сторонами трудовому договорі (контракті) пункту про збереження таємниці підприємства і підписаного зобов'язання про нерозголошення конфіденційних відомостей, що стали відомими, і дотриманні правил їх захисту;

• відповідність функціональних обов'язків співробітника переданим йому документам і інформації;

• знання співробітником вимог нормативно-методичних документів щодо захисту інформації та збереження таємниці підприємства;

• наявність необхідних умов в офісі для роботи з конфіденційними документами;

• наявність систем контролю за роботою співробітника [38].

Особливість інформаційного обслуговування працівників, які є користувачами конфіденційної інформації полягає в тому, що питання визначення складу необхідної їм інформації вирішуються повноважним керівником, а не самими користувачами. Існує загальне, обов'язкове правило: виконавці, яким документ не адресований керівником, не тільки не мають права доступу до нього, але й не повинні знати про існування такого документа і вихідних даних про нього.

Розмежування доступу грунтується на однозначному розчленуванні інформації за тематичними групами, рівнями конфіденційності цих груп і користувачів, яким ця інформація необхідна для роботи. Завданням процедури розмежування доступу є регламентація мінімальних потреб персоналу в конфіденційних відомостях.

Це дає можливість розділити знання елементів комерційної таємниці серед якомога більшого числа співробітників. Наприклад, бажано, щоб цілком ідею, формулу, конструкцію не знав ніхто, кожен знав би лише свою незначну частину. Дроблення інформації також не дозволяє конкурентам використовувати її за рахунок прийому на роботу звільненого з підприємства співробітника.

Дозвіл на доступ до конфіденційних відомостей є суворо персоніфікованим, тобто керівники несуть персональну відповідальність за правильність виданих ними дозволів на доступ виконавців до конфіденційних відомостей, а особи, які працюють з конфіденційними документами, несуть персональну відповідальність за збереження в таємниці їхнього змісту, збереження носія і дотримання встановлених правил роботи з документами.

Керівник підприємства має право давати дозвіл на ознайомлення з усіма видами конфіденційних документів підприємства всім категоріям виконавців та іншим особам [2].

Отже, процедури допуску та доступу співробітників до конфіденційної інформації завершують процес включення даного співробітника до складу осіб, що реально володіють таємницею підприємства. З цього часу велике значення набуває поточна робота з персоналом, у розпорядженні якого знаходяться цінні та конфіденційні відомості.

Здійснення контролю діяльності персоналу

Однак, поряд з необхідністю формування потужної корпоративної культури підприємства (відносин, соціальних пріоритетів, норм моралі), що забезпечить потрапляння новачків у систему самовідтворюваної суспільної свідомості, важливим є створення ефективної системи контролю, яка б відповідала таким вимогам: регулярність і систематичність, персональна відповідальність працівників [20].

Основними формами контролю якості роботи персоналу, підвищення працівниками своїх професійних знань, у тому числі в частині захисту інформації, можна назвати такі:

• атестація співробітників;

• звіти керівників підрозділів про роботу підрозділів і стан системи захисту інформації;

• регулярні перевірки керівником підприємства або службою безпеки дотримання співробітниками вимог щодо захисту інформації;

• самоконтроль співробітників [38].

Атестація співробітників є однією з найбільш ефективних форм контролю їх діяльності як у професійній сфері, так і у сфері дотримання інформаційної безпеки підприємства. Атестація персоналу - це колективна форма оцінки

професійної придатності працівника, його відповідності займаній посаді. Атестація проводиться періодично (щокварталу, раз на рік і інші терміни).

При проведенні атестації розглядаються такі характеристики співробітника: трудова дисципліна, старанність, працьовитість, відповідальність, вимогливість і принциповість, організованість у роботі, якість і ефективність виконуваної роботи, самостійність і ініціатива, творча діяльність, прогресивність професійних рішень, професійний кругозір, вміння спілкуватися з людьми, організаторські здібності, відданість справі підприємства.

В частині дотримання вимог захисту інформації розглядаються такі характеристики, як знання нормативних та інструктивних документів щодо захисту інформації, вміння застосовувати вимоги цих документів у практичній діяльності, відсутність порушень у роботі з конфіденційними документами, вміння спілкуватися зі сторонніми особами, не розкриваючи секрети підприємства тощо. На основі вивчення цих характеристик формується уявлення про кожного співробітника, його ділові і людські якості.

Варто відзначити можливість використання нетрадиційних методів атестації персоналу з інформаційної безпеки, серед яких: перевірка діяльності робочої групи як основної одиниці та здатності особи працювати в групі, оцінювання працівника його колегами; оцінювання не тільки ефективного виконання робочих функцій працівника, а й його здібностей до професійного розвитку та оволодіння новими знаннями, уміннями і практичними навичками; метод «360° атестація», коли працівник оцінюється своїм керівником, своїми колегами рівними за рангом.

Популярним в процесі проведення атестації персоналу на зарубіжних підприємствах є застосування психологічних методів оцінки. Спеціальні центрами оцінки персоналу компаній створюють спеціальні програми оцінки потенціалу своїх працівників за допомогою психологічних методів. Однак, психологічні оцінки працівників у процесі атестації персоналу повинні доповнювати експертні оцінки [25].

Одна з форм контролю - заслуховування керівників структурних підрозділів та керівника служби безпеки на нараді у першого керівника підприємства про стані системи захисту інформації та виконанні її вимог

співробітниками підрозділів. Одночасно на нараді приймаються рішення за фактами порушення співробітниками цієї системи.

Формою контролю є також регулярні перевірки виконання працівниками (у тому числі тими, що показують високі результати роботи) правил роботи з конфіденційною інформацією, документами і базами даних. Перевірки проводяться керівниками структурних підрозділів та напрямків діяльності підприємства, заступниками першого керівника, працівниками служби безпеки. Одночасно з дотриманням співробітником правил роботи з конфіденційними документами перевіряється наявність у цього співробітника документів, носіїв інформації, справ, магнітних носіїв інформації, які закріплені за ним; електронних масивів інформації, виробів та інших елементів, що становлять таємницю підприємства.

Перевірки можуть бути плановими, позаплановими (раптовими). Позапланові перевірки проводяться при виникненні найменшої підозри про розголошення або витік інформації.

Самоконтроль співробітників підприємства полягає в перевірці самими керівниками і виконавцями повноти і правильності виконання ними діючих інструктивних положень, а також негайного інформування безпосереднього керівника і службу безпеки про факти втрати документів, втрати з будь-якої причини цінної інформації, розголошенні особисто або іншими співробітниками відомостей, що становлять таємницю підприємства, порушенні співробітниками порядку захисту інформації [38].

У разі встановлення фактів невиконання співробітниками вимог щодо захисту інформації до них повинні в обов'язковому порядку і своєчасно застосовуватися заходи осуду і покарання відповідно до правил внутрішнього трудового розпорядку: оголошення догани, пониження в посаді, позбавлення премії, відсторонення від роботи з конфіденційною інформацією, звільнення.

Факт втрати інформації виявляється в основному за допомогою аналізу публікацій, реклами, виставкових та інших матеріалів фірм-конкурентів. В цьому випадку аналізуються картки обліку обізнаності співробітників в таємниці підприємства і виявляється коло співробітників, які володіють втраченої інформацією. Аналіз ведеться в рамках службового розслідування.

Службове розслідування організовується за фактами розголошення або витоку інформації, втрати документів і виробів, іншим грубих порушень правил захисту інформації.

Питання про покарання винних осіб ставиться тільки після завершення службового розслідування, міра покарання визначається особисто першим керівником підприємства. При підтвердженні факту передачі співробітником інформації сторонній особі підприємство повинна звернутися до суду для винесення рішення про відшкодування матеріальних збитків від крадіжки інформації [38].

Отже, рекомендовані напрямки і методи поточної роботи з персоналом підприємства дозволяють організувати ефективну систему зацікавленої участі співробітників в забезпеченні безпеки фірмових секретів, постійного контролю за роботою персоналу з конфіденційною інформацією та своєчасного виявлення спроб зловмисника заволодіти інтелектуальною власністю підприємства.

2.3. Форми і методи навчання персоналу з інформаційної безпеки

Одним із важливих напрямів поточної роботи з персоналом, що володіє конфіденційною інформацією, є навчання і систематичне підвищення кваліфікації співробітників.

Мета професійного навчання персоналу полягає у:

– підтриманні необхідного рівня кваліфікації працівників підприємства;

– підвищенні конкурентоспроможності підприємства, на основі застосування знань, професійного досвіду та ефективних методів організації праці;

– створенні сприятливих умов для професійного зростання, самореалізації співробітників в ринкових умовах на основі підвищення мотивації, використанні новітніх засобів, програм і технологій професійного навчання;

– підвищенні рівня компетенції і професіоналізму працівників та ефективного їх використання, відповідно до запитів бізнесу;

– вдосконаленні професійних навичок та вмінь, які необхідні для ефективної діяльності;

– підготовці персоналу до ротаційного переміщення [24].

Безперервне і послідовне навчання працівників компанії сьогодні є необхідним для виживання бізнесу, оскільки швидкі зміни технологій та інформатизація усіх сфер діяльності вимагають постійного оновлення знань і навичок персоналу. Внаслідок зростання конкуренції підприємство може зайняти і утримати переважаючу позицію на ринку насамперед завдяки володінню новими знаннями і вміннями, носіями яких є його персонал. Також варто відзначити, що для фірми більш ефективним і економічно вигідним є підвищення віддачі від уже працюючих співробітників на основі їхнього безперервного навчання, ніж залучення нових працівників.

Виділяють такі основні види професійного навчання персоналу:

1) первинна професійна підготовка працівників (надання базових знань по конкретній спеціальності);

2) перепідготовка працівників (навчання працівників, яке полягає в набутті нових знань для оволодіння новою професією);

3) підвищення кваліфікації працівників (покращення умінь та навичок, які були набуті в процесі роботи) [9].

Процес навчання і підвищення кваліфікації співробітників підприємства з питань інформаційної безпеки та захисту інформації також повинен бути постійним, оскільки система управління інформаційною безпекою підприємства вимагає регулярного оновлення та видозміни.

Навчання співробітника починається з моменту проведення співбесіди з ним при прийомі на роботу і підписання ним зобов'язання про нерозголошення таємниці і закінчуючи моментом звільнення і підписання цією особою зобов'язання про неприпустимість використання конфіденційних відомостей в чиїхось цілях.

Навчання співробітників може починатися також з моменту початку роботи колективу над новою ідеєю, оціненої в якості фірмового секрету, роботи з використанням ноу-хау і т.п. Звичайна періодичність навчання для працюючих співробітників один раз на 3-5 років, як правило, після атестації або переукладання контракту [38].

Навчання і підвищення кваліфікації персоналу у сфері інформаційної безпеки організовується за кількома основними блоками:

- характер і склад конфіденційної інформації;

- порядок роботи з конфіденційними відомостями і документами;
- структури системи захисту, вимоги і правила захисту конфіденційної інформації, в тому числі інтелектуальної власності;
- потенційні загрози конфіденційним відомостям, канали їх об'єктивного поширення та канали втрати, методів роботи зловмисників;
- способи виявлення і запобігання неправомірним діям інших працівників;
- загальні та спеціальні методи розпізнавання шахрайських дій з боку третіх осіб (партнерів, клієнтів, постачальників тощо);
- колективні й індивідуальні дії в екстрених ситуаціях.

Навчання і підвищення кваліфікації співробітників передбачає набуття та підтримання на високому рівні виробничих навичок роботи з конфіденційною інформацією, психологічне виховання співробітників і виховання глибокої переконаності в необхідності виконання вимог щодо захисту будь-якої інформації з обмеженим доступом, що є власністю підприємства. Персонал повинен отримати знання щодо оцінки важливості тих чи інших відомостей для зміцнення престижу підприємства та її фінансової стабільності, а значить, і для благополуччя кожного співробітника.

Загалом методи навчання персоналу поділяють на дві великі групи: навчання на робочому місці та поза ним. Детальніша інформація представлена у Таблиці 2.2. [4].

Також важливим напрямом навчання персоналу є самостійна підготовка.

Окремим напрямом навчання та підвищення кваліфікації може бути розвиток у персоналу компанії навичок протидії методам т.зв. соціальної інженерії (даний підхід також іноді називають "соціотехніки"). Використання для незаконного проникнення в інформаційні системи методів соціальної інженерії пов'язано з "людським фактором", який являє собою сукупність певних психологічних схильностей і особливостей мислення і поведінки, які властиві практично всім людям.

Таблиця 2.2.

Методи навчання персоналу

Навчання на робочому місці	Навчання поза робочим місцем
Адаптація нових працівників, аналіз робочих дій і процедур Інструктаж на робочому місці Наставництво Розширення кола обов'язків Передача повноважень (делегування) Демонстрація прийомів роботи Передача досвіду Ротація Чергування робочих операцій Метод ускладнених завдань Навчальне заміщення Спеціальний набір завдань Підготовка і розвиток команди Консультування	Лекції, семінарські і практичні заняття Дискусії і обговорення Дистанційне навчання Ознайомлення з передовим досвідом Розгляд практичних ситуацій (кейсів) Ділові ігри Моделювання ситуацій Семінари, виставки, симпозіуми Тренінги Рольові ігри Самостійне навчання Участь у виставках і інших заходах Участь у навчальних програмах Участь у проектах

До числа таких схильностей і особливостей можна віднести:

• нездатність адекватно оцінити небезпеку в деяких ситуаціях;

• специфічне ставлення до подій, які відбуваються рідко (притуплення уваги);

• надмірна довіра і покладання на засоби автоматизації;

• піддатливість маніпулюванню, заснована, наприклад, на бажанні допомогти людям (у тому числі і незнайомим) або на надмірній довірі до людей, одягнених у спеціальну уніформу тощо.

Саме з використанням деяких психологічних особливостей такого роду здійснюються найбільш успішні (для нападників) проникнення в корпоративні інформаційні системи. Прикладами таких проникнень є ситуації, коли зловмисник:

• здійснює телефонний дзвінок, представляється адміністратором і, пославшись на певні обставини (такі як збій в системі), просить повідомити йому пароль;

• приходить в офіс в спеціальній уніформі (наприклад, у формі співробітника компанії, що займається обслуговуванням і ремонтом комп'ютерів) і просить надати йому доступ до інформаційної системи;

• надсилає повідомлення електронною поштою від імені адміністратора інформаційної системи або керівництва підприємства і просить повідомити пароль або вчинити певні дії [2].

Методика навчання включає в себе:

• спеціалізовані програми навчання для забезпечення лекційних курсів і практичних занять;

• проведення лекцій, семінарів та співбесід як загального ознайомлювального плану, так і за конкретними напрямками захисту; тестування співробітників;

• вирішення ситуаційних завдань, пов'язаних з виконанням необхідних вимог по захисту конфіденційної інформації;

• ситуаційні тренінги щодо дій персоналу в екстремальних ситуаціях;

• проведення ділових ігор із застосуванням навчальних методів протидії задумам зловмисника.

Дуже важливо зробити процес навчання індивідуалізованим. У процесі навчання співробітник повинен отримати тільки ті знання, які йому необхідні для роботи. Інформація, що повідомляється в процесі навчання співробітників, є строго конфіденційною. Конспекти, записи співробітники роблять у спеціальних зошитах, які зберігаються відповідно до загального порядку роботи з конфіденційними документами.

Після закінчення навчання проводиться перевірка засвоєння співробітниками отриманих знань бажано шляхом тестування або рішення ситуаційної задачі. Співробітники, які не пройшли перевірку знань, від роботи з конфіденційною інформацією відсторонюються.

Одночасно з навчанням проводять регулярні наради-інструктажі з співробітниками. У процесі інструктажу:

• до відома співробітників доводяться зміни і доповнення, внесені в діючі нормативно-методичні документи щодо захисту інформації, накази і вказівки керівництва підприємства в галузі інформаційної безпеки;

• співробітників інформують про конкретні загрози інформації, канали витоку інформації, дії зловмисників, прийняті додаткові заходи щодо захисту інформації;

• аналізуються випадки порушення правил захисту інформації співробітниками, повідомляється про факти втрати конфіденційної інформації з вини співробітників.

Інструктаж, так само як і навчання, проводиться індивідуально, інформація, яка оприлюднюється під час інструктажу, не підлягає розголошенню. Наради-інструктажі проводяться, як правило, за необхідності [38].

Отже, обов'язковою і першорядною частиною поточної роботи з персоналом має стати навчання і підвищення кваліфікації співробітників щодо правил роботи з конфіденційною інформацією, документами і базами даних. Важко говорити про ефективність роботи з персоналом, якщо співробітники не мають достатньо твердих уявлень про систему захисту конфіденційної інформації, методи протидії зловмисникам.

Висновки до другого розділу

Встановлено, що одним із найбільш важливих етапів у роботі з персоналом у сфері інформаційної безпеки є набір і підбір можливих кандидатів для призначення на посади, пов’язані з конфіденційною інформацією. Основними вимогами до цього процесу є використання різних методів пошуку кандидатів, в тому числі розгляд кандидатів з числа працівників підприємства, залучення студентів і випускників навчальних закладів, використання послуг державних і приватних бюро, агентств з найму робочої сили, бірж праці тощо, підбір кандидатів за рекомендаціями співробітників підприємства.

При підборі кандидатів оцінюється рівень підготовки та кваліфікації, наявність необхідного досвіду роботи; морально-ділові й особистісні якості; ступінь відповідальності за прийняті управлінські та виконавські рішення (залежно від займаної посади).

Організаційні заходи при найманні персоналу, що одержує доступ до конфіденційної інформації, включають: проведення ускладнених аналітичних процедур при прийомі; документування добровільної згоди особи не

розголошувати конфіденційні відомості й дотримуватися правил забезпечення безпеки інформації; інструктування і навчання щодо практичних дій у сфері інформаційної безпеки.

Поточна робота з персоналом у сфері інформаційної безпеки включає заходи з отримання й забезпечення допуску й доступ працівників до конфіденційної інформації.

Дозвільна система забезпечує обмеження і регламентації складу співробітників, функціональні обов'язки яких вимагають знання конфіденційних відомостей та роботи з документами; строгий вибірковий і обґрунтований розподіл документів та інформації між співробітниками; надання співробітнику всього необхідного для реалізації ним службових функцій (документами, справами, базами даних, інформацією, технічними засобами тощо); безперешкодний прохід працівника в режимну зону; виключення можливості для сторонніх осіб несанкціонованого ознайомлення з конфіденційною інформацією в процесі роботи персоналу з документами, справами і базами даних; колективний контроль за роботою співробітників.

Важливим напрямом роботи з персоналом є здійснення контролю за його діяльністю у сфері інформаційної безпеки, основними формами якого є: атестація; звіти керівників підрозділів про роботу підрозділів і стан системи захисту інформації; регулярні перевірки керівником підприємства або службою безпеки дотримання працівниками вимог щодо захисту інформації; самоконтроль співробітників.

Одним із важливих напрямів поточної роботи з персоналом, що володіє конфіденційною інформацією, є навчання і систематичне підвищення кваліфікації, метою якого є: підтримання необхідного рівня кваліфікації працівників; підвищення конкурентоспроможності підприємства, на основі застосування знань, професійного досвіду та ефективних методів організації праці; створення сприятливих умов для професійного зростання, самореалізації персоналу на основі підвищення мотивації; підвищення рівня компетенції і професіоналізму працівників та ефективного їх використання, відповідно до запитів підприємства; вдосконалення професійних навичок та вмінь, які необхідні для ефективної діяльності у сфері інформаційної безпеки.

Навчання і підвищення кваліфікації персоналу у сфері інформаційної безпеки може проводитися за такими основними напрямами: характер і склад конфіденційної інформації; порядок роботи з конфіденційними відомостями і документами; структура системи захисту, вимоги і правила захисту конфіденційної інформації, в тому числі інтелектуальної власності; потенційні загрози конфіденційним відомостям, канали їх об'єктивного поширення та канали втрати, методи роботи зловмисників; способи виявлення і запобігання неправомірним діям інших працівників; загальні та спеціальні методи розпізнавання шахрайських дій з боку третіх осіб (партнерів, клієнтів, постачальників тощо); колективні й індивідуальні дії в екстрених ситуаціях.

РОЗДІЛ 3. Шляхи вдосконалення управління персоналом у сфері інформаційної безпеки

3.1. Формування лояльності персоналу як ключовий чинник запобігання порушенням безпеки

Найкращий вибір керівника – це лояльний співробітник. Лояльність – задоволеність співробітника умовами, винагородою, ростом і перспективами, колективом, захистом від зовнішніх погроз. Формування лояльності персоналу є важливим для підприємств, що дбають про довгострокову перспективу розвитку.

Лояльність персоналу розглядають як універсальну за спрямованістю складову кадрової безпеки, тому що ставлення працівника до власної організації чи підприємства є фактором, який або зміцнює, або руйнує систему кадрової безпеки компанії.

Науковці по-різному трактують сутність поняття «лояльність персоналу». Т.Н.Чистякова і Н.В.Мойсєєнко розглядають лояльність персоналу як готовність працівника відповідати корпоративним очікуванням та формувати способи поведінки в межах, заданих організацією або керівництвом; стійкість до провокуючої дії ззовні; дотримання раніше прийнятих домовленостей; внутрішнє схвалення цілей компанії і цінностей, некритичне ставлення до життя в організації. Л.Г.Почебут розглядає лояльне ставлення працівників до організації, з одного боку, як установку, а з другого як мотивацію людини працювати на користь організації, відстоювати її інтереси в різних сферах бізнесу [32].

У широкому розумінні лояльність персоналу можна розглядати як вірність працівника своїй організації чи підприємству. Високий рівень лояльності персоналу є важливим фактором зміцнення кадрової безпеки, оскільки лояльний працівник цінує своє робоче місце саме в цій компанії, проявляє бажання працювати на благо організації, є ініціативним та активним у вирішенні поставлених завдань, сприяє розвитку і підтримці корпоративної культури та відданому ставленню до компанії.

Також лояльність персоналу є «наріжним каменем» у забезпеченні інформаційної безпеки підприємства. Відданий працівник асоціює себе з підприємством, на якому він працює, відчуває себе його частиною, дорожить своїм робочим місцем і дбає про корпоративну безпеку. Так відбувається тому, що підприємство для працівника є джерелом багатьох благ, основою його задоволення умовами роботи, винагородою та внаслідок цього - якістю свого життя. Дотримання вимог інформаційної безпеки є однією з передумов успішного функціонування підприємства і стабільного робочого місця працівника.

Важливість феномена лояльності для бізнесу підтверджується багатьма дослідженнями. За даними американського щорічного довідника WORKUSA Survey, організації з високолояльними співробітниками за три роки принесли своїм акціонерам 112% прибутку, організації з середнім рівнем лояльності співробітників – 90%, а з низькими показниками лояльності – 76% [15]. Отже, більш лояльні працівники працюють краще, що має наслідком отримання більших прибутків.

Працівники з лояльним ставленням до компанії є набагато стійкішими до «спокус»: їх складно переманити в іншу організацію, схилити до співпраці з конкурентами, шахрайства та зловживання повноваженнями. Лояльні співробітники критично ставляться до колег, які порушують правила компанії, тим самим попереджують виникнення внутрішніх загроз кадровій безпеці. Формування лояльного колективу можливе за рахунок розроблення та впровадження на підприємстві системи заходів управління лояльністю [26].

Під управлінням лояльністю персоналу слід розуміти усвідомлений вплив на чинники, що її формують, з метою забезпечення її подальшого розвитку і зміцнення. Система заходів з управління лояльністю персоналу повинна бути зорієнтована на забезпечення сприятливих умов праці, позитивного психологічного клімату в колективі, розвиненої корпоративної культури та ефективної системи мотивації [22] (Рис. 3.1.).

Умови праці – це середовище, обстановка, в якій вона здійснюється, тобто характер устаткування та організації робочих місць, рівень дотримання санітарно-гігієнічних і естетичних норм, психологічний клімат в колективі.

Рис.3.1. Чинники формування лояльності персоналу.

Умови праці є одним із чинників забезпечення стабільної продуктивності праці. За сприятливих умов праці працездатність людини підвищується, тому що немає необхідності у витрачанні сил та здоров'я на захист організму від негативного впливу шкідливих та небезпечних виробничих факторів. Шляхом проведених досліджень з'ясовано, що заходи з покращення умов праці підвищують продуктивність праці на 15–20 % [10].

Науково доведено, що комплекс заходів, спрямованих на поліпшення умов праці, сприяє збільшенню її продуктивності, а саме:

– зменшення виробничого шуму до рівня допустимих норм – до 3–15%;

– раціональне забарвлення приміщення – до 25%;

– продумане використання музики – до 12–14%;

– створення раціонального освітлення – до 10–15%;

– правильна організація робочого місця – до 20%;

– оптимальна температури повітря – до 50% [28].

Крім того, безсумнівним є те, що сприятливі умови праці сприяють формуванню лояльності персоналу і формують передумови для стабільності робочої сили на підприємстві, зменшення плинності кадрів. А враховуючи специфіку сфери інформаційної безпеки, це є надзвичайно важливим.

Створення сприятливих умов праці передбачає формування сукупності умов, серед яких:

- організаційно-технічні - враховують особливості конкретної людини і забезпечуються шляхом використання і зручного розміщення меблів, засобів організаційної та обчислювальної техніки з урахуванням вимог ергономіки (науки, що вивчає взаємодію людини і машини в конкретних умовах), технічної естетики та наукової організації праці. Від цього залежить зміст робочих операцій, пози у процесі трудової діяльності, темп праці, відстані і швидкість

переміщень, ергономічні та естетичні умови праці (зручність розташування, форма, розміщення органів управління, кольорове оформлення робочого місця, вплив музики, запахів тощо);

- виробничо-екологічні - сприятливі санітарно-гігієнічні умови праці (температура повітря, його вологість, запиленість, загазованість, рівні шуму, вібрації, освітленості). Нормальними вважаються умови праці з температурою повітря від +18 до +25°С влітку та від +16 до +24°С взимку, вологістю 40-60%, швидкістю потоків повітря до 0,3 м/с / 04, м/с взимку і влітку відповідно [34], рівнем шуму 50-75 децибел [35], освітленістю робочої зони 50 до 750 лк і навколишньої зони від 50 до 500 лк [27];

- соціально-економічні фактори, які впливають на моральну і матеріальну зацікавленість працівника в результатах праці (форми взаємин в колективі, морально-психологічний клімат), а також раціональний режим праці і відпочинку внаслідок ненормованого робочого дня (тривалість робочого дня, регламентованих і нерегламентованих перерв в роботі, відпустки, гнучкі графіки роботи тощо).

Про важливість формування сприятливого психологічного клімату свідчать дані, що внаслідок поганого настрою приблизно в півтора рази знижується ефективність роботи колективу. Загалом на психологічний стан колективу впливають характер працівників, зміст роботи та ставлення до неї виконавців, престижність, розміри винагороди, перспективи кар´єрного та професійного зростання, наявність додаткових переваг, місце та психологічний клімат.

На морально-психологічний клімат колективу можна впливати через сприяння згуртованості колективу; забезпечення сумісності співробітників, які в нього входять; створення позитивної психологічної атмосфери; формування колективної думки і настрою, а також традицій колективу.

Згуртованість колективу досягається через формування ціннісно-цільової і мотиваційної єдності його членів, узгодження індивідуальної поведінки працівників та їх внутрішньо-групових зв´язків, визначення спільної мети, мотиваційної єдності для її досягнення.

Важливою умовою ефективної роботи колективу є сумісність його членів, стабільність і дружність взаємовідносин між ними, які є запорукою успіху

колективної праці. Для досягнення психологічної сумісності учасників спільної діяльності, за якої поведінка і вчинки одного викликають схвалення і позитивні емоції у інших, необхідним є досягнення єдності в розумінні основних цілей колективу і засобів їх досягнення. За таких умов кожен член колективу цікавиться справами і успіхами колег, турбується про престиж своєї групи та докладає значних зусиль для досягнення колективних цілей.

За позитивної психологічної атмосфери в колективі наявне приємне і добровільне спілкування, взаєморозуміння і взаємопідтримка, яке дозволяє ефективно вирішувати службові завдання.

Для хорошого морального клімату характерне переважання таких цінностей як: справедливість, товариськість, принциповість, взаємодопомога, висока свідомість, здатність до співчуття, щирість тощо.

Беззаперечною у формуванні сприятливого морально-психологічного клімату є роль керівника, який володіє великим авторитетом, здатен своїми діями викликати повагу у підлеглих, чітко організувати працю колективу та забезпечити виконання поставлених завдань.

Необхідно залучати працівників до вирішення проблем фірми, це сприятиме тому, що співробітник відчуватиме свою цінність та значимість для компанії. Важливо, щоб працівники могли простежити й переконатися, як відсоток їх особистого внеску в життя компанії оцінюється й винагороджується [32].

Починаючи з адаптації новопризначеного співробітника до нового професійного та соціального оточення, важливим завданням є вироблення і підтримка у персоналу почуття «фірмового патріотизму», гордості за своє підприємство, формування основних засад корпоративної культури.

Корпоративна культура розглядається як система базових передбачень, цінностей і норм організації, що визначає правила поведінки її персоналу, діловий стиль, традиції тощо. Саме ці складові корпоративної культури мобілізують внутрішні ресурси, єднають і мотивують персонал, надають змісту його праці і надихають на максимальну самовіддачу, створюють можливість вирішувати складні завдання, в т.ч. у сфері інформаційної безпеки [40].

Оцінюючи розвиток корпоративної культури України, за результатами соціологічних досліджень, можна стверджувати про таке: 55% сучасних

українських керівників уважають, що в ідеалі корпоративна культура повинна бути на підприємстві: 40% наших підприємців намагаються сформувати її за допомогою західних технологій; 35% визнають потребу в ній, але для цього в них не вистачає ні часу, ні ресурсів; 25% узагалі вважають її непотрібною [42].

Науковці виділяють такі рівні впровадження корпоративної культури на підприємстві.

На адміністративному рівні, який відповідає системі управління підприємством, формується економічна та соціальна поведінка працівників (знання, уявлення, відносини у процесі трудової діяльності, виробництва, обміну, розподілу та споживанні результатів праці).

На професійному рівні, який відповідає результатам системи управління персоналом на підприємстві, створюється структура кадрового складу, професійна забезпеченість, рівень умінь та майстерності персоналу і керівництва.

У сфері управління корпоративну культуру можна назвати «інструментом», за допомогою якого можна керувати персоналом підприємства, підвищувати конкурентоспроможність, якість продукції та послуг і в кінцевому підсумку результативність діяльності підприємства загалом.

Наступний базовий рівень передбачає культивування бажаних відносин, ставлення до колег і керівників, використання корпоративних символів і термінів, заохочення розповідей і висловлювань, які виражають загальні цінності та переконання компанії. Такі методи мають на меті досягти стану, коли працівники свідомо поділяють і розвивають принципи і цінності підприємства.

Останній і найвищий змістовний рівень визначає власне культуру підприємства на основі закладених у психологію людей цінностей, традицій, поведінки, які проявляються підсвідомо та відображаються у діяльності автоматично [33].

Зміцнення лояльного ставлення працівників до організації сприятиме зростанню якості і продуктивності праці, відповідальності співробітників, рівня згуртованості та дисциплінованості трудового колективу, підвищенню трудової мотивації працівників, рівня активності та ініціативи, а також забезпеченню

творчого підходу працівників та адекватної оцінки роботи. За допомогою розробки і реалізації заходів щодо управління лояльністю персоналу на підприємстві вирішується низка важливих завдань, які не лише сприяють зміцненню кадрової безпеки організації, а й підвищують ефективність господарської діяльності компанії в цілому [22].

Як відзначалося, важливу роль у формуванні лояльного працівника відіграють заходи матеріального стимулювання та нематеріальної мотивації працівників.

У системі стимулювання працівників першочерговим стає обґрунтоване й справедливе матеріальне заохочення, достатні соціальний захист та медичне страхування, психологічна допомога. Матеріальні заохочення окремих працівників повинні бути добре обґрунтовані. За життєві незручності, пов'язані зі збереженням комерційної таємниці, співробітникам треба добре платити чи компенсувати психологічне навантаження іншими засобами [3].

Крім матеріального стимулювання обов’язковим елементом є нематеріальна мотивація. Мотивація діяльності людини розуміється як сукупність рушійних сил, спонукають людину до здійснення певних дій. Ці сили знаходяться поза або всередині людини та змушують її усвідомлено, або неусвідомлено робити певні вчинки. Відповідно до цього поточна або профілактична робота з персоналом є обов'язковою складовою частиною запобігання спробам окремих співробітників скористатися в особистих цілях цінною для підприємства інформацією, порушити вимоги інформаційної безпеки підприємства.

До заходів нематеріальної мотивації персоналу відносять, наприклад залучення підлеглих до обговорення поточних питань, а також прийняття стратегічних рішень, справедливе оцінювання досягнутих результатів й відповідне заохочення, просування по службових сходах, підвищення рівня професійної компетентності працівників через навчання та перепідготовку, заохочення ініціативи та творчого підходу до виконання поставлених завдань [21].

Загалом існує багато засобів стимулювання і мотивації персоналу, які можна представити у вигляді таблиці (Таблиця 3.1.).

Таблиця 3.1.

Засоби стимулювання і мотивації персоналу

Зовнішні		*Внутрішні*
Грошові (матеріальні)	*Негрошові (нематеріальні)*	
Заробітна плата	Визнання, похвала, публікації про авторів і створені винаходи у ЗМІ	Самостійність у роботі (автономія)
Премії	Нагороди: грамоти, значки, медалі та інших відзнак, подарунки, пільгові путівки на відпочинок	Досягнення в роботі
Доплати і надбавки	Публічне присудження спеціальних почесних титулів і звань	Особисте та професійне зростання
Участь у прибутках	Присвоєння більш яскравої назви їхній посаді	Змістовність і значимість роботи
Дивіденди	Прийняття в члени винахідницьких клубів, оплата компанією їхнього членства у наукових товариствах	Більша відповідальність
Участь у доходах	Направлення за рахунок компанії у творчі відрядження, на навчання, стажування, виставки тощо, в т. ч. за кордон	
	Оплата участі та проїзду на наукові конференції, в т. ч. за кордон	

Кожен із співробітників підприємства, що працює з конфіденційними документами, повинен перебувати під постійним наглядом керівництва та колективу підприємства, які оцінюють ступінь його лояльності по відношенню до справ підприємства. Зі свого боку підприємство зобов'язане забезпечити будь-якому співробітникові необхідні умови праці та відпочинку, постійно

піклуватися про його добробут, підвищення кваліфікації та підтримці на високому рівні інтересу до виконуваних обов'язків і робіт.

Отже, головним фактором виховання у співробітників лояльності, гордості за компанію, відповідального ставлення до виконання своїх службових обов'язків є перш всього наполеглива робота керівництва й кадрових служб щодо забезпечення сприятливих умов праці, позитивного психологічного клімату в колективі, розвиненої корпоративної культури. Внаслідок впровадження ефективної системи мотивації працівник, який бере участь у справах і прибутках підприємства, задовільняє матеріальні потреби й досягає особистісних і професійних перемог, більш відповідально ставиться до збереження конфіденційності підприємства, суворо дотримується вимог інформаційної безпеки та захисту інформації.

3.2. Рекомендації щодо вдосконалення менеджменту персоналу у сфері інформаційної безпеки

З огляду на зростаючу роль людського фактора для покращення менеджменту персоналу в СУІБ підприємства доцільно здійснення заходів за такими напрямами: організаційні, навчально-методичні, соціально-економічні та інформаційно-психологічні (рис.3.2).

Рис. 3.2. Напрями менеджменту персоналу у системі УІБ підприємства.

Серед *організаційних заходів* виділяють такі, як:

- організація СУІБ підприємства з метою забезпечення її максимальної ефективності та здатності давати адекватну і оперативну відповідь реальним та потенційним загрозам в інформаційній сфері;

- оптимізація структури і складу підрозділів СУІБ, формування системи професійного кадрового менеджменту в СУІБ підприємства;

- проведення спеціальних процедур найму працівників, зокрема з метою «відсівання» невідповідних кандидатів, виявлення психологічних та етичних обмежень будь-якого виду на виконання посадових обов'язків. Так, психологічний відбір дозволяє не тільки з'ясувати морально-етичні якості кандидата, його слабкості, рівень стійкості психіки, але й можливі злочинні схильності, уміння зберігати таємницю;

- визначення повноважень та відповідальності у сфері діяльності з інформації з обмеженим доступом та нормативне закріплення добровільної угоди особи про нерозголошення відомостей обмеженого доступу;

- дотримання правил безпечної роботи з конфіденційною інформацією, навчання й інструктування співробітників щодо практичних дій із захисту інформації;

- здійснення систематичного контролю за роботою персоналу, що працює з конфіденційною інформацією, дотримання порядку обліку, зберігання та знищення документів і технічних носіїв конфіденційної інформації.

Сучасний стан розвитку інформаційного суспільства та ІКТ засвідчує потребу у прискоренні процесу оновлення професійних знань, умінь і навичок кадрів, задіяних у СУІБ підприємства, у відповідності до актуальних вимог системи забезпечення інформаційної безпеки. З огляду на це необхідними *навчально-методичними заходами* є удосконалення системи підготовки, перепідготовки та підвищення кваліфікації кадрів у галузі інформаційної безпеки з посиленням інформаційно-технологічного (урахування розвитку ІКТ, технологій захисту інформації) та інформаційно-психологічного компонентів (розвиток технологій соціальної інженерії та інших засобів деструктивного інформаційно-психологічного впливу на персонал).

Серед основних напрямів менеджменту персоналу у сфері інформаційної безпеки підприємства є удосконалення *інформаційно-психологічних заходів,* які проявляються у двох аспектах:

по-перше, виховання фірмового патріотизму, відданості підприємству з боку його працівників, формування взаємної довіри й атмосфери відкритості

між керівництвом та персоналом підприємства, створення сприятливого психологічного клімату в колективі;

по-друге, формування у персоналу вмінь і навичок розпізнавання та протидії спробам входження в довіру, втягування у недозволену діяльність, здійснення прихованих психологічних впливів чи відкритого тиску з боку зловмисників, за потреби надання психологічної допомоги.

Важливе значення для запобігання інформаційним загрозам мають заходи *мотивації та економічного стимулювання персоналу*, який працює у системі інформаційної безпеки підприємства. Варто застосовувати такі методи стимулювання як справедлива оплата праці, преміювання за виконання додаткових або більш складних завдань, доплати і надбавки, участь у прибутках і доходах, виплата дивідендів. Значною є роль нематеріальних чинників, які дозволяють працівнику задовільнити потреби у визнанні та самореалізації.

Висновки до третього розділу

У результаті дослідження з’ясовано, що лояльність персоналу є ключовим чинником забезпечення інформаційної безпеки підприємства, оскільки дотримання вимог безпеки є однією з передумов успішного функціонування бізнесу і, як наслідок, стабільного робочого місця працівника, завдяки чому забезпечується якість його життя.

Формування лояльного колективу здійснюється за рахунок розроблення та впровадження в організації системи заходів управління лояльністю, які включають забезпечення сприятливих умов праці, позитивного психологічного клімату в колективі, розвиненої корпоративної культури та ефективної системи мотивації.

Встановлено, що створення сприятливих умов праці передбачає формування сукупності організаційно-технічних, виробничо-екологічних соціально-економічних факторів.

На морально-психологічний клімат колективу можна впливати через сприяння згуртованості колективу; забезпечення сумісності співробітників, які

в нього входять; створення позитивної психологічної атмосфери; формування колективної думки і настрою, а також традицій колективу.

Формування корпоративної культури здійснюється на кількох рівнях, починаючи від формування належних норм поведінки персоналу у процесі трудової діяльності, забезпечення володіння працівниками необхідними професійними знаннями, вміннями і навичками, культивування бажаних відносин, ставлення до колег і керівників, заохочення комунікації з метою пропагування й підтримки загальних цінностей, традицій, місії компанії.

Важливу роль у формуванні лояльного працівника відіграють заходи матеріального стимулювання та нематеріальної мотивації працівників. У системі стимулювання працівників першочерговим стає обґрунтоване й справедливе матеріальне заохочення, достатні соціальний захист та медичне страхування, психологічна допомога. Крім цього обов'язковим елементом є нематеріальна мотивація, наприклад залучення підлеглих до обговорення поточних питань, а також прийняття стратегічних рішень, справедливе оцінювання досягнутих результатів й відповідне заохочення, кар'єрний і професійний розвиток шляхом навчання й перепідготовки, заохочення ініціативи та творчого підходу до виконання поставлених завдань.

За підсумками дослідження представлені рекомендації, відповідно до яких для покращення менеджменту персоналу в системі управління інформаційною безпекою підприємства доцільно здійснення комплексу організаційних, навчально-методичних, соціально-економічних та інформаційно-психологічних заходів.

ВИСНОВКИ

З’ясовано, що система управління інформаційною безпекою - це частина загальної системи управління підприємства, що базується на аналізі ризиків і призначена для проектування, реалізації, контролю, супроводу та вдосконалення заходів в області інформаційної безпеки. За способами здійснення всі заходи і засоби у межах СУІБ поділяють на нормативно-правові; організаційні; програмно-технічні; фізичні; морально-етичні. До організаційних заходів відносять, серед інших, заходи з управління персоналом.

У результаті дослідження встановлено, що персонал підприємства є, з одного боку, найціннішим ресурсом підприємства, з іншого – основним джерелом втрати конфіденційної інформації. Також визначено види протиправних дій у сфері інформаційної безпеки з боку персоналу (крадіжка конфіденційної інформації; порушення авторських прав на інформацію; шахрайство; саботаж інформації) і чинники, які створюють підґрунтя для порушень інформаційної безпеки з боку персоналу (власне персонал; недостатньо успішна робота з кадрами підприємства; деструктивна діяльність конкурентів).

Відзначено, що управління персоналом, задіяним у сфері інформаційної безпеки, набуває все більшого стратегічного значення для підприємства і має на меті мінімізувати ризики порушення працівниками вимог безпеки і запобігти виникненню передумов для таких деструктивних дій.

Встановлено перелік напрямів управління персоналом з інформаційної безпеки, серед яких: планування чисельності та професійно-кваліфікаційної структури персоналу; формування вимог до працівників, що мають доступ до конфіденційної інформації; професійний набір і підбір персоналу за ускладненою процедурою; виробнича і соціальна адаптація новоприйнятих працівників; чіткий розподіл і делегування повноважень з урахуванням вимог обмеженого доступу; планування, контроль і оцінювання діяльності персоналу; забезпечення професійного та кар’єрного розвитку, навчання і підвищення кваліфікації персоналу, що працює у системі управління інформаційною безпекою; застосування засобів матеріального стимулювання і нематеріальної мотивації праці; підтримання сприятливого соціально-психологічного клімату в трудовому колективі; формування корпоративної культури тощо.

З’ясовано, що одним із найбільш важливих етапів у роботі з персоналом у сфері інформаційної безпеки є набір і підбір можливих кандидатів для призначення на посади, пов’язані з конфіденційною інформацією. Організаційні заходи при найманні персоналу, що одержує доступ до конфіденційної інформації, включають: проведення ускладнених аналітичних процедур при прийомі; документування добровільної згоди особи не розголошувати конфіденційні відомості й дотримуватися правил безпеки інформації; інструктування і навчання щодо практичних дій у сфері інформаційної безпеки.

Поточна робота з персоналом у сфері інформаційної безпеки включає забезпечення допуску та доступу працівників до конфіденційної інформації. Такі заходи передбачають обмеження складу співробітників, функціональні обов'язки яких вимагають знання конфіденційних відомостей та роботи з документами; обґрунтований розподіл документів та інформації між співробітниками; надання співробітнику всього необхідного для реалізації ним службових функцій; безперешкодний прохід працівника в режимну зону; виключення можливості для сторонніх осіб несанкціонованого ознайомлення з конфіденційною інформацією; колективний контроль.

Важливим напрямом роботи з персоналом є здійснення контролю за його діяльністю у сфері інформаційної безпеки, основними формами якого є: атестація; звіти керівників підрозділів про роботу підрозділів і стан системи захисту інформації; регулярні перевірки керівником підприємства або службою безпеки дотримання працівниками вимог щодо захисту інформації; самоконтроль співробітників.

Управління персоналом у сфері інформаційної безпеки передбачає наявність обов’язкової навчальної складової, метою якої є: підтримання необхідного рівня кваліфікації працівників; створення сприятливих умов для професійного зростання, самореалізації персоналу на основі підвищення мотивації; підвищення рівня компетенції і професіоналізму працівників та ефективного їх використання відповідно до запитів підприємства; вдосконалення професійних навичок та вмінь, які необхідні для ефективної діяльності у сфері інформаційної безпеки.

У результаті дослідження з’ясовано, що ключовим чинником забезпечення інформаційної безпеки підприємства є лояльність персоналу, завдяки якій

зростає рівень дотримання вимог безпеки з боку персоналу. Формування лояльного колективу здійснюється за рахунок розроблення та впровадження системи заходів управління лояльністю, які включають забезпечення сприятливих умов праці, позитивного психологічного клімату в колективі, розвиненої корпоративної культури та ефективної системи мотивації персоналу.

За підсумками дослідження представлені рекомендації, відповідно до яких для покращення менеджменту персоналу в системі управління інформаційною безпекою підприємства доцільно здійснення комплексу організаційних, навчально-методичних, соціально-економічних та інформаційно-психологічних заходів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аникин И. В., Глова В. И., Нейман Л. И., Нигматуллина А.Н. Теория информационной безопасности и методология защиты информации : учеб. пособие. Казань : Изд-во КГТУ им. А.Н. Туполева, 2008. 280 с.

2. Анисимов А. Менеджмент в сфере информационной безопасности: Учебное пособие. URL: http://www.intuit.ru/studies/courses/563/419/lecture/9580 (дата звернення: 29.05.2020)

3. Аніловська Г.Я. Інформаційна безпека підприємства в умовах використання сучасних інформаційних технологій. URL: http://www.nbuv.gov.ua /portal/chem_biol/nvnltu/18_9/270_Anilowska_18_9.pdf (дата звернення: 29.05.2020)

4. Балабанова Л.В., Сардак О.В. Управління персоналом: навч. посіб. – К.: Центр учбової літератури, 2011. - 468 с.

5. Балашов Ю. Оценка персонала - основа кадровой политики зарубежных фирм. URL: http://www.kapr.ru/articles/2003/9/1793.html (дата звернення: 29.05.2020)

6. Будник М. М., Тимофєєв Д. С. Внутрішні загрози інформаційної безпеки та заходи по їх мінімізації. Інформаційні технології. Безпека та зв'язок : матеріали IV всеукраїнської науково-практичної конференції (29 листопада 2012 р., м. Дніпропетровськ). Д. : Державний ВНЗ «Національний гірничий університет», 2012. 51 с.

7. Гаврюшин Е. Человеческий фактор в обеспечении безопасности конфиденциальной информации. URL: http://bre.ru/security/16248.html (дата звернення: 29.05.2020)

8. Герасименко О. В., Козак А. В. Інформаційна безпека підприємства: поняття та методи її забезпечення. URL: http://intkonf.org/ken-gerasimenko-ov-kozak-avinformatsiyna-bezpeka-pidpriemstva-ponyattyata-metodi-yiyi-zabezpechennya (дата звернення: 29.05.2020)

9. Горохівська Н. Формування системи професійного навчання працівників організації.

10. URL: http://dspace.tneu.edu.ua/jspui/bitstream/316497/29871/1/213.PDF (дата звернення: 29.05.2020)

11. Гринюк Т. Ю. Сучасні проблеми поліпшення умов праці на підприємстві. Психолого-педагогічні основи гуманізації навчально-виховного

процесу в школі та ВНЗ : зб. наук. пр. Рівне. 2014. Вип. 1. С. 121-127. URL: http://nbuv.gov.ua/UJRN/Ppog_2014_1_20 (дата звернення: 29.05.2020)

12. Єжова Л.Ф. Корченко А.О., Мачалін І.О., Скачек Л.М., Хорошко В.О. Управління інформаційною безпекою. В 2-х томах. Видання друге, доповнене та перероблене. Київ, 2011. 348 с.

13. Журавель М. Паршуков С. Проблеми захисту інформації. URL: http://informatika.udpu.org.ua/?page_id=1173 (дата звернення: 29.05.2020)

14. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2005, MOD). ГСТУ СУІБ 1.0/ISO/IEC 27001:2010. К.: Національний банк України, 2010. 49 с.

15. Кавун С.В., Носов В.В., Мажай О.В. Інформаційна безпека. Навчальний посібник. Ч.1. Харків: Вид. ХНЕУ, 2008. 352 с.

16. Коваленко Д. В. Методологічні основи соціологічного виміру лояльності персоналу організації. “Соціологія майбутнього: науковий журнал з проблем соціології молоді та студентства”, 2010. № 1. С.13-20

17. Коваленко Ю. Забезпечення інформаційної безпеки на підприємстві. Економіка промисловості. 2010. № 3. С. 123-129. URL: http://dspace.nbuv.gov.ua/xmlui/handle/123456789/24811 (дата звернення: 29.05.2020)

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

19. Коптелов А., Беркович В. Построение эффективной системы управления информационной безопасностью компании. URL: http://businessprocess.narod.ru/index18.htm (дата звернення: 29.05.2020)

20. Кузнецов, И. Н. Бизнес-безопасность. 4-е изд. Москва :Дашков и К, 2016. 416 с. URL: https://znanium.com/catalog/product/430343 (дата звернення: 29.05.2020)

21. Лапина Н., Копейкин Г.Психологические аспекты информационной безопасности организации. URL: https://www.beltim.by/wiki/articles/psikhologicheskie-aspekty-informatsionnoy-bezopasnosti-organ/ (дата звернення: 29.05.2020)

22. Лисенко М. С. Механізм забезпечення кадрової безпеки підприємств. Формування ринкових відносин в Україні. 2008. № 7. С. 137-140.

23. Маренич А.І., Мехеда Н.Г. Виявлення та запобігання загроз кадровій безпеці. Фінансовий простір. 2011. № 3 (3). С. 127-132.

24. Мельник С., Цуп М. Інформаційна безпека як складова економічної безпеки підприємства. URL: http://nauka.kushnir.mk.ua/?p=66146 (дата звернення: 29.05.2020)

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

26. Мехеда Н. Г., Коломієць О. Складові забезпечення кадрової безпеки. URL: http://www.rusnauka.com/1_NIO_2012/Economics/9_98644.doc.htm (дата звернення: 29.05.2020)

27. Мехеда Н. Г., Кулик А. Вплив фактора лояльності персоналу на рівень кадрової безпеки організації. URL: http://www.rusnauka.com/7_NITSB_ 2012/ Economics/10_102819.doc.htm (дата звернення: 29.05.2020)

28. Наказ Міністерства будівництва, архітектури та житлово-комунального господарства України від 15 травня 2006 р. № 168 Державні будівельні норми України. Природне і штучне освітлення ДБН В 2.5-28:2018. URL: https://dreamdim.ua/wp-content/uploads/2018/12/DBN-V2528-1.pdf (дата звернення: 29.05.2020)

29. Никифоренко В.Г. Управління персоналом Навчальний посібник. Одеса: Атлант, 2013. 275 с.

30. Ожиганова М. І., Хорошко В. О., Яремчук Ю. Є. та ін.Управління персоналом : навч. посіб. URL: http://posibnyky.vntu.edu.ua/abooks/petr/ Управління%20персоналом %20%20ніткі/p7.html

31. Ортинський В. Л., Керницький І. С., Живко З. Б. та ін. Контроль персоналу. Економічна безпека підприємств організацій та установ : навч. посіб. К., 2009. URL: http://pidruchniki.com/ 1734030851318/ekonomika/ kontrol_personalu (дата звернення: 29.05.2020)

32. Основы информационной безопасности: учеб. пособие / А.Н. Данилов, С.А. Данилова, А.А. Зорин. Пермь: Изд-во Перм. гос. техн. ун-та, 2008. 556 с.

33. Пилат Н. І. Лояльність персоналу в умовах мотивації професійної діяльності. «Проблеми сучасної психології». 2010. №10. С.601-612.

34. Полянська А.С. Дюк О.М.. Формування моделі корпоративної культури в діяльності вітчизняних підприємств. Причорноморські економічні студії.

2018. Вип. 27(2). С. 9-16. URL: http://nbuv.gov.ua/UJRN/bses_2018_27(2)__4 (дата звернення: 29.05.2020)

35. Постанова Міністерства охорони здоров'я України та Головного державного санітарного лікаря України від 01.12.99 Санітарні норми мікроклімату виробничих приміщень ДСН 3.3.6.042-99. URL: https://zakon.rada.gov.ua/rada/show/va042282-99 (дата звернення: 29.05.2020)

36. Постанова Міністерства охорони здоров'я України та Головного державного санітарного лікаря України від 1.12.1999 р. № 37 Санітарні норми виробничого шуму, ультразвуку та інфразвуку ДСН 3.3.6.037-99. URL: https://zakon.rada.gov.ua/rada/show/va037282-99 (дата звернення: 29.05.2020)

37. Скиба Б. Ю., Курбатов Б. А. Руководство по защите от внутренних угроз информационной безопасности. М.: Изд-во Питер, 2008. 320 с.

38. Сороковская А. А. Информационная безопасность предприятия : новые угрозы и перспективы. URL: http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2010_2_2/032-035.pdf (дата звернення: 29.05.2020)

39. Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации. М.: ИНФРА-М, 2001. 304 с.

40. Столяров Н. Зарубежный опыт защиты информации в процессе организации работы с кадрами (на примере США).

URL: http://bre.ru/security/19485.html (дата звернення: 29.05.2020)

41. Тарасова О.В., Марінова С.С. Корпоративна культура як інструмент ефективного менеджменту підприємства. Економіка харчової промисловості. 2013. № 3. С. 28-32. URL: http://nbuv.gov.ua/UJRN/echp_2013_3_8 (дата звернення: 29.05.2020)

42. Управление информационной безопасностью. URL: http://www.arinteg.ru/articles/upravlenie-informatsionnoy-bezopasnostyu-26728.html (дата звернення: 29.05.2020)

43. Шевченко В. С. Визначення впливу корпоративної культури на діяльність підприємства. Комунальне господарство. 2011. Вип. 14. С. 160–165.

44. Шопін А. Інформаційна безпека як фактор забезпечення конкурентоспроможності підприємства. URL: http://repository.hneu.edu.ua/ (дата звернення: 29.05.2020)

45. Ярочкин В. Информационная безопасность: Учебник для студентов вузов. М.: Академический Проект; Гаудеамус, 2-е изд. 2004. 544 с.