МІНІСТЕРСТВО ОСВІТИ ТА 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:

ФОРМУВАННЯ ЛОЯЛЬНОСТІ ПЕРСОНАЛУ ЯК СКЛАДОВА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

СТУДЕНТ: Матковський Богдан Юрійович _____
(підпис)

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

НОРМОКОНТРОЛЕР: к.т.н., доц. Дзюба Тарас Михайлович _____
(підпис)

Київ – 2021

«ЗАТВЕРДЖУЮ»
Завідувач кафедри УІКБ
_____ С.В.Легомінова
«_____»_____ 2020 р.

ЗАВДАННЯ

на дипломну роботу

студенту Матковському Богдану Юрійовичу

Тема роботи: «ФОРМУВАННЯ ЛОЯЛЬНОСТІ ПЕРСОНАЛУ ЯК СКЛАДОВА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ», затверджена наказом по університету № 230 від «13» жовтня 2020 р.

1. **Термін здачі** студентом оформленої роботи «___» _____ 20___ р.
2. **Об'єкт дослідження:** забезпечення інформаційної безпеки організації.
3. **Предмет дослідження:** формування лояльності персоналу як складова забезпечення інформаційної безпеки організації.
4. **Мета дослідження** полягає у вивченні засад формування лояльності персоналу як складової забезпечення інформаційної безпеки організації.
5. **Перелік питань, які мають бути розроблені:**

5.1 Вивчити характеристики персоналу як об’єкта забезпечення інформаційної безпеки організації.

5.2 Проаналізувати сутність поняття лояльності персоналу та підходи до її оцінювання в контексті інформаційної безпеки.

5.3 З’ясувати роль методів мотивації і стимулювання у формуванні лояльності персоналу з інформаційної безпеки.

6. **Дата видачі завдання «**16» вересня 2020 р.

Науковий керівник _____ Т.М. Мужанова
підпис

Завдання прийнято до виконання _____ Б.Ю. Матковський
підпис

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

КАЛЕНДАРНИЙ ПЛАН
виконання дипломної роботи
студентом МАТКОВСЬКИМ Богданом Юрійовичем

Дата видачі завдання: «16» вересня 2020 р.

№ з/п	Етапи дипломної роботи	Термін виконання етапів	Примітка
	Визначення об'єкта, предмета, мети та завдань дослідження.	16.09.2020	
	Збір та аналіз літератури.	28.09.2020	
	Вивчення характеристик персоналу як об'єкта забезпечення інформаційної безпеки організації.	12.10.2020	
	Аналіз сутності поняття організаційної лояльності персоналу й підходів до її оцінювання в контексті інформаційної безпеки.	26.10.2020	
	Встановлення ролі методів мотивації і стимулювання у формуванні лояльності персоналу з інформаційної безпеки.	09.11.2020	
	Формулювання висновків за результатами проведеного дослідження.	23.11.2020	
	Оформлення роботи.	07.12.2020	
	Оформлення презентації.	14.12.2020	
	Отримання рецензії на роботу.	25.12.2020	
	Захист у ДЕК.	__.01.2021	

Студент Б.Ю. Матковський
(підпис)

Науковий керівник Т.М. Мужанова
(підпис)

РЕФЕРАТ

Дипломна робота присвячена дослідженню засад формування лояльності персоналу як складової забезпечення інформаційної безпеки організації. Робота складається зі вступу, трьох розділів, що містять 11 рисунків, висновків та списку використаних джерел з 46 найменувань. Загальний обсяг роботи становить 81 аркуш, з яких 5 аркушів займає список використаних джерел.

Об'єктом дослідження є забезпечення інформаційної безпеки організації.

Метою роботи є вивчення засад формування лояльності персоналу як складової забезпечення інформаційної безпеки організації.

Для цього у роботі використані методи аналізу, синтезу, класифікацій та порівняння, теорій менеджменту персоналу й інформаційної безпеки, прикладні методи оцінювання персоналу.

Як результат у роботі досліджено характеристики персоналу як об'єкта забезпечення інформаційної безпеки організації; проаналізовано сутність поняття лояльності персоналу та підходи до її оцінювання в контексті інформаційної безпеки; з'ясовано роль методів мотивації і стимулювання у формуванні лояльності персоналу з інформаційної безпеки.

Галузь застосування. Розроблені підходи можуть бути використані при організації та впровадженні комплексу заходів, спрямованих на формування лояльності персоналу у контексті забезпечення інформаційної безпеки організації.

Ключові слова: ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ, ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ З ВИНИ ПЕРСОНАЛУ, ЛОЯЛЬНІСТЬ ПЕРСОНАЛУ, ОЦІНЮВАННЯ ЛОЯЛЬНОСТІ ПЕРСОНАЛУ, СТИМУЛЮВАННЯ Й МОТИВАЦІЯ ПЕРСОНАЛУ.

ЗМІСТ

ВСТУП

Актуальність теми. Сьогодні в умовах досить агресивного інформаційного середовища, як у технічному, так і в соціальному планах, кожній організації чи підприємству для ефективної діяльності та досягнення своєї місії необхідно створити надійну систему забезпечення інформаційної безпеки, яка здійснюватиме запобігання і протидію різноманітним інформаційним загрозам.

Оскільки, за даними статистики, близько 80% суб'єктів правопорушень у сфері інформаційної безпеки є працівниками організації, важливим напрямом роботи з персоналом є виховання надійного і відданого трудового колективу, розвиток корпоративної культури інформаційної безпеки, формування відповідального ставлення до роботи та дотримання вимог захисту інформації. Досягнення цих завдань у сфері інформаційної безпеки забезпечується у рамках реалізації комплексу заходів з метою формування організаційної лояльності персоналу.

З огляду на це тема дипломної роботи є актуальною, а використання її результатів сприятиме зменшення кількості порушень з боку персоналу зокрема і підвищенню рівня інформаційної безпеки організації загалом.

Мета і завдання дослідження. **Мета роботи** полягає у вивченні засад формування лояльності персоналу як складової забезпечення інформаційної безпеки організації.

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

1. Вивчити характеристики персоналу як об'єкта забезпечення інформаційної безпеки організації.

2. Проаналізувати сутність поняття лояльності персоналу та підходи до її оцінювання в контексті інформаційної безпеки.

3. З'ясувати роль методів мотивації і стимулювання у формуванні лояльності персоналу з інформаційної безпеки.

Об'єкт дослідження - забезпечення інформаційної безпеки організації.

Предмет дослідження - формування лояльності персоналу як складова забезпечення інформаційної безпеки організації.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу, синтезу, класифікацій та порівняння, теорій менеджменту персоналу й інформаційної безпеки, прикладні методи оцінювання персоналу.

Наукова новизна одержаних результатів. Розроблені підходи можуть бути використані при організації та впровадженні комплексу заходів, спрямованих на формування лояльності персоналу у контексті забезпечення інформаційної безпеки організації.

Практичне значення одержаних результатів. Застосування напрацювань дасть змогу здійснити обґрунтований вибір методів і засобів роботи з персоналом з інформаційної безпеки, допоможе підібрати ефективні методи як оцінювання наявного рівня лояльності персоналу, так і заходи для формування високолояльного трудового колективу організації як запоруки належного забезпечення організаційної інформаційної безпеки.

РОЗДІЛ 1
ПЕРСОНАЛ ЯК ОБ'ЄКТ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

1.1. Основи забезпечення інформаційної безпеки організації

Будь-яка організація є засобом задоволення потреб і досягнення певних цілей суспільства, соціальних груп та окремих осіб. Виступаючи засобом виживання людини й колективу організації, зацікавлених сторін, організація має забезпечувати безпеку своїх членів в умовах наявності різноманітних чинників ризику, що становлять загрози її існуванню та цілісності. Це обумовлює необхідність забезпечення діяльності з підвищення захищеності життєво важливих інтересів організації та її членів. В умовах інформаційного суспільства особливо важливого значення набуває проблема інформаційної безпеки організації.

Людина, прагнучи підвищити ступінь своєї захищеності від негативного впливу інформаційних чинників, так змінила умови свого життя, що вони самі стали джерелом небезпек. Соціальне середовище сьогодні не володіє такими якостями як визначеність, стабільність та прозорість, що характерні для стану інформаційної безпеки. Водночас, постійно зростають обсяги інформації, що пов'язано з необхідністю її обробки, зберігання та передачі. Додатковим чинником загроз стало переведення переважної частини інформації в електронну форму, а використання глобальної та локальних мереж створює якісно нові загрози конфіденційній інформації. Саме тому забезпечення інформаційної безпеки стає ключовим завданням кожної організації.

Незважаючи на наявність багатьох розробок у сфері інформаційної безпеки, в науковій літературі немає єдиної позиції щодо змісту понять «інформаційна безпека» та «інформаційна безпека організації».

Розглянемо основні з представлених підходів, застосовуючи різні дефініції для рівня організації (Таблиця 1.1.).

Таблиця 1.1.

Визначення поняття «інформаційна безпека організації»

стан захищеності життєво важливих інтересів організації, за якого запобігається нанесення шкоди через: – неповноту, несвоєчасність та недостовірність інформації; – негативний інформаційний вплив; – негативні наслідки застосування інформаційних технологій; – несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації
стан захищеності потреб в інформації організації та зацікавлених сторін, за якого забезпечується їхнє існування та прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз.
стан захищеності організації від інформаційних загроз, який визначається рівнем реальної або потенційної шкоди, заподіяної внаслідок деструктивного інформаційного впливу або порушення безпеки інформації.
стан захищеності організації від зовнішніх та внутрішніх небезпек і загроз, який базується на діяльності організації та залучених суб'єктів з виявлення (вивчення), запобігання, послаблення, ліквідації і відбиття небезпек і загроз, здатних завдати завдати неприйнятної шкоди.
стан захищеності інформаційних інтересів та потреб організації, при якому забезпечується її функціонування та прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз
стан захищеності інформаційного середовища організації, за якого забезпечується її формування, використання й розвиток незалежно від впливу внутрішніх та зовнішніх інформаційних загроз.
стан інформованості, який визначає ступінь адекватності сприйняття організацією і, як наслідок, - обґрунтованість прийнятих рішень і дій.
суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи організації.
збереження конфіденційності, цілісності та доступності інформації (доступність - це властивість бути досяжним і придатним до використання в інформаційному середовищі; цілісність - властивість захищеності точності і повноти даних; конфіденційність - властивість захищеності інформації від несанкціонованого використання).

Виходячи з вищенаведених визначень «інформаційної безпеки», під забезпеченням інформаційної безпеки організації розумітимемо цілеспрямовану діяльність її органів і посадових осіб з використанням дозволених методів і засобів по досягненню стану захищеності інформаційного середовища організації та забезпечення його нормального функціонування і динамічного розвитку.

Пріоритетними напрямами забезпечення інформаційної безпеки організації є:

– захист організації від деструктивних інформаційних впливів;

– захист від несанкціонованого впливу інформації, яка належить організації (комерційної таємниці, інших видів інформації обмеженого доступу) або перебуває у її розпорядженні (персональні дані). Особливого значення набуває збереження в таємниці комерційно важливої інформації, що дозволяє успішно конкурувати на ринку товарів і послуг);

– захист інформаційної інфраструктури організації від руйнівних впливів (випадкових або навмисних, природного або штучного характеру);

– забезпечення цілісності та доступності інформації або інформаційних послуг, надійності як технічних, так і програмних засобів, що реалізують процеси збирання, зберігання й обробки інформації.

Життєво важливим є комплексний підхід до забезпечення інформаційної безпеки організації, який на практиці включає сукупність напрямів, різноманітних методів, засобів і заходів, що допомагають вирішувати завдання інформаційної безпеки.

Основними принципами забезпечення інформаційної безпеки на основі вивчення джерел [20,21,29,30] є:

- узгодженість з бізнес-завданнями і стратегією організації;

- наявність усвідомленої згроди й зобовязань з боку керівництва організації;

- економічна обгрунтованість (баланс між можливостями, продуктивністю і витратами);

- безперервність (циклічність) процесу забезпечення інформаційної безпеки;

- гнучкості управління і застосування;

- чіткий розподіл повноважень і персональна відповідальність;.

Важливою для ефективного забезпечення інформаційної безпеки є узгодженість та взаємозв'язок цієї відносно вузьконаправленої концепції не тільки з загальноорганізаційною стратегією, але і з програмами внутрішнього контролю й аудиту організації, менеджменту персоналу, вдосконалення і управління IT-системами організації, моделями загальноорганізаційного управління ризиками, а також її відповідність внутрішній нормативній базі, що визначає ролі та організаційні політики [29].

У контексті реалізації принципу безперервності забезпечення інформаційної безпеки фахівці вважають доцільним використання моделі (Рис.1.1.), яка складається з таких етапів:

– усвідомлення потреби в захисті інформації та постановка завдань;

– збір та аналіз даних про стан інформаційної безпеки в організації;

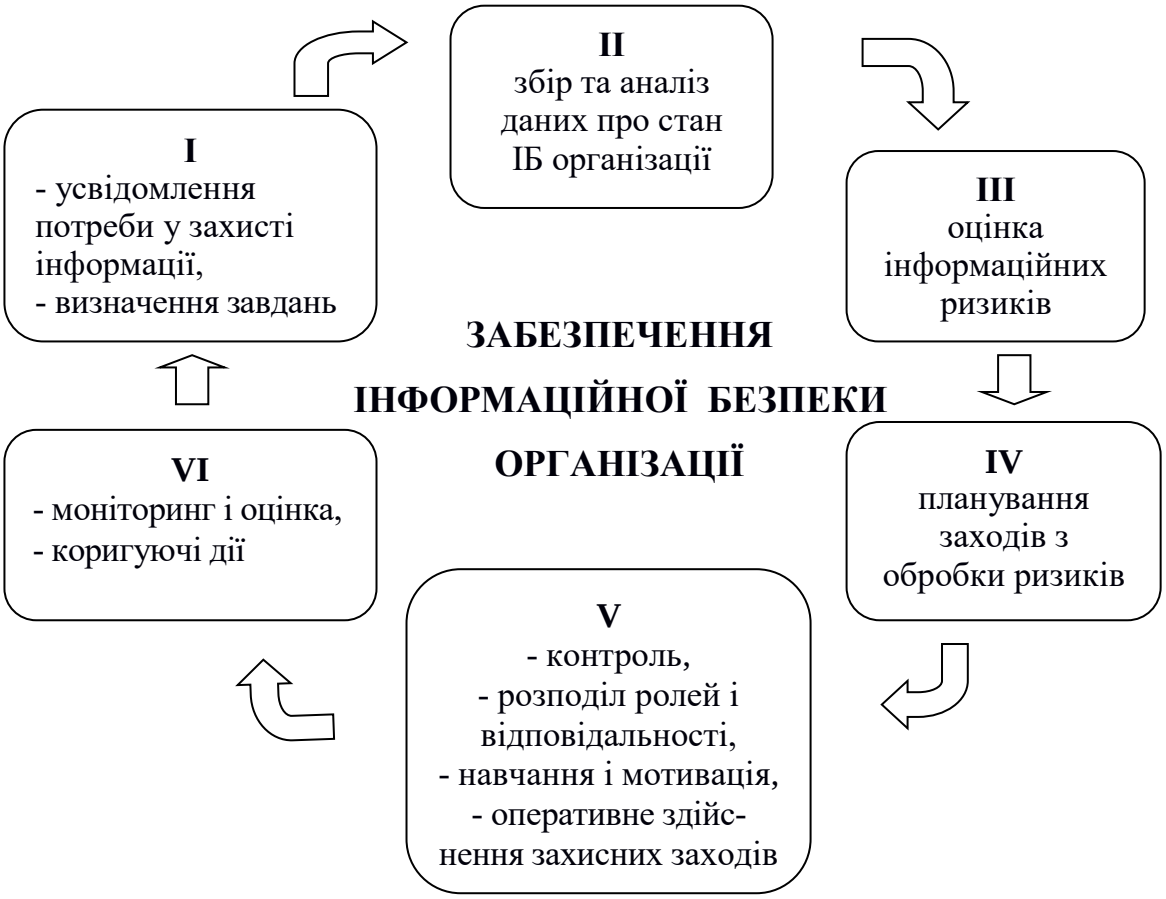

Рис. 1.1. Цикл забезпечення інформаційної безпеки організації

– оцінка інформаційних ризиків;

– планування заходів з обробки ризиків;

– реалізація і впровадження відповідних заходів, розподіл ролей і відповідальності, навчання і мотивація персоналу тощо;

– моніторинг функціонування механізмів контролю, оцінка їх ефективності та відповідні коригуючі дії.

Виходячи з того, що сьогодні щораз більше організацій по всьому світу прагнуть сертифікувати свої системи забезпечення (управління) інформаційної безпеки відповідно до міжнародного стандарту ISO / IEC 27001, основою для побудови ефективного підходу до забезпечення інформаційної безпеки може бути модель PDCA [21], що за загальною логікою відповідає попередньо представленій моделі:

– Plan (Планування) - фаза розробки політики забезпечення інформаційної безпеки та інших нормативних документів (політик нижчого рівня, інструкцій, процедур тощо), визначення цілей, процесів та процедур, суттєвих для управління ризиками та вдосконалення інформаційної безпеки, щоб одержати результати, які відповідають загальним політикам та цілям організації;

– Do (Виконання) - етап реалізації та впровадження політики інформаційної безпеки, процесів, відповідних заходів та процедур;

– Check (Перевірка) - фаза оцінювання результативності й ефективності забезпечення інформаційної безпеки, вимірювання продуктивності процесів згідно з політикою, цілями і практичним досвідом, звітування керівництву про результати для подальшого перегляду;

– Act (Покращення) - виконання коригувальних і превентивних дій на підставі результатів внутрішніх перевірок і перегляду з боку керівництва або іншої суттєвої інформації для досягнення постійного вдосконалення системи забезпечення інформаційної безпеки організації.

Комплексність забезпечення інформаційної безпеки організації досягається за рахунок узгодженого й послідовного використання різних заходів правового, організаційного, програмно-технічного, фізичного і навіть морального впливу (Рис.1.2.) [34].

Структура, послідовність і зміст заходів, їх взаємозв'язок залежать від об'єму і цінності інформації, що захищається, характеру можливих загроз інформаційної безпеки, ступеню запланованого захисту і його вартості.

Рис. 1.2. Види заходів забезпечення інформаційної безпеки.

Нормативно-правові засоби забезпечення інформаційної безпеки включають міжнародні та національні стандарти у зазначеній сфері; законодавство, постанови й укази органів виконавчої влади держави; галузеві та регіональні нормативи й технічні специфікації; політики, положення, інструкції та інші документи організації, які регламентують правила поводження з інформацією обмеженого доступ і встановлюють санкції за їх порушення на корпоративному рівні.

Організаційні засоби забезпечення інформаційної безпеки використовують для вирішення завдань щодо функціонування інформаційно-телекомунікаційних систем організації; використання корпоративних інформаційних ресурсів та систем; діяльності персоналу з інформаційної безпеки тощо.

До організаційних засобів відносять розробку вимог та правил обробки інформації в інформаційно-телекомунікаційних системах; підбір, оцінювання й підготовку персоналу, що задіяний у сфері інформаційної безпеки, створення умов для дотримання працівниками вимог безпеки та уникнення зловживань; організацію пропускного режиму й охорони; облік та роботу з документами й носіями конфіденційної інформації; розмежування доступу (паролів, повноважень тощо); здійснення контролю за роботою користувачів і персоналу; сертифікацію технічних і програмних засобів, їх перевірку на відповідність вимогам захисту.

Серед програмно-технічних засобів інформаційної безпеки можна назвати безліч програм та пристроїв апаратного забезпечення, які самостійно або в поєднанні з іншими здійснюють захист інформаційних активів та ІТКС організації, зокрема засоби обох видів, що унеможливлюють витік, знищення та блокування інформації, забезпечують дотримання цілісності та режиму доступу до конфіденційних даних: ідентифікацію й автентифікацію користувачів; гарантують розмежування доступу до інформаційних ресурсів та систем, контроль цілісності й забезпечення конфіденційності даних; здійснюють аудит подій в ІТКС, резервне копіювання активів та елементів ІТКС тощо.

Фізичні засоби становлять сукупність різноманітних механічних, електричних і електромеханічних пристроїв або споруд, призначених для створення фізичних перешкод за потенційними напрямами проникнення і доступу порушників (кодові замки, турнікети, системи пожежно-охоронної сигналізації, посилені огорожі тощо).

Особливу роль відіграють морально-етичні засоби, до яких відносять цінності і традиції, правила і норми поведінки, що існують у суспільстві, галузі чи на рівні окремої організації і стосуються питань трудової діяльності, взаємовідносин у колективі, між керівниками і підлеглими, методів вирішення

спірних ситуацій, безпечної поведінки, тощо. Ці норми можуть бути неписаними (загальновизнані норми чесності, корпоративної відданості тощо) або формалізованими у вигляді кодексу поведінки, зводу правил чи приписів.

Відповідно до іншого підходу [20] методи забезпечення інформаційної безпеки організації є такими:

- фізичне перешкоджання доступу зловмисника до інформації та засобів її обробки;

- управління доступом до всіх ресурсів ІТКС організації, яке включає ідентифікацію користувачів, персоналу і ресурсів ІТКС; автентифікацію об'єкта або суб'єкта за представленим ідентифікатором; перевірку повноважень (відповідність встановленому регламенту таких параметрів як дата, час, обєкти і процедури доступу); ведення обліку усіх звернень до критичних інформаційних активів та засобів їх обробки; реагування на несанкціоновані дії (попередження, відключення, відтермінування або відмова в доступі);

- криптографічне закриття інформації в ІТКС організації (маскування);

- створення умов обробки, зберігання та передачі інформації, за яких мінімізується можливість несанкціонованого доступу (регламентація);

- створення середовища, в якому користувачі та персонал дотримуються вимог інформаційної безпеки з огляду на настання матеріальної, адміністративної або навіть кримінальної відповідальності у випадку їх порушення (примус);

- формування атмосфери, в якій користувачі й персонал не порушують встановлені вимоги інформаційної безпеки, оскільки слідують морально-етичних нормам, діючим в організації (спонукання).

Перелічені методи забезпечення інформаційної безпеки реалізуються за допомогою вже традиційних і раніше перелічених апаратних, програмних, програмно-апаратних, криптографічних, фізичних, організаційних, законодавчих та морально-етичних засобів.

Апаратні засоби захисту (самостійні електронні, електромеханічні та інші пристрої або пристрої, безпосередньо вбудовані в ІТКС) мають на меті забезпечення внутрішнього захисту структурних елементів засобів і систем

обчислювальної техніки: процесорів, терміналів, периферійного обладнання, ліній зв'язку тощо.

Програмні засоби, які є найбільш поширеним видом захисту, виконують логічні й інтелектуальні функції захисту і є складовими програмного забезпечення корпоративних ІТКС або засобів, комплексів і систем апаратури контролю. Цим засобам притаманні такі характеристики як універсальність, гнучкість, можливість вдосконалення, простота реалізації.

Програмно-апаратні засоби захисту поєднують взаємопов'язані і нероздільні програмні (мікропрограмні) й апаратні частини.

Криптографічні засоби захищають інформаційні ресурси та засоби їх обробки й передачі шляхом перетворення інформації (шифрування).

Фізичні засоби захисту (автономні пристрої і системи) призначені для зовнішньої охорони території об'єктів, захисту корпоративних ІТКС.

Організаційні засоби включають організаційно-правові й організаційно-технічні засоби, спрямовані на регламентацію поведінки користувачів і персоналу.

Законодавчими засобами є нормативно-правові акти держави, які регламентують правила використання, обробки та передачі інформації, в тому числі обмеженого доступу і визначають відповідальність за їх порушення.

Засоби морально-етичного впливу є норми, традиції, правила, сформовані в суспільстві, територіальній громаді, колективі або інших групах людей. Прикладом можу слугувати Кодекси професійної поведінки членів галузевих профспілок або фахових асоціацій на рівні держави або регіону.

На думку авторів даної концепції, всі зазначені засоби захисту можуть бути формальними, тобто виконувати захисні функції за наперед встановленою процедурою без участі людини, і неформальними, які визначаються цілеспрямованою діяльністю організації або регламентують таку діяльність [20] (Рис. 1.3.).

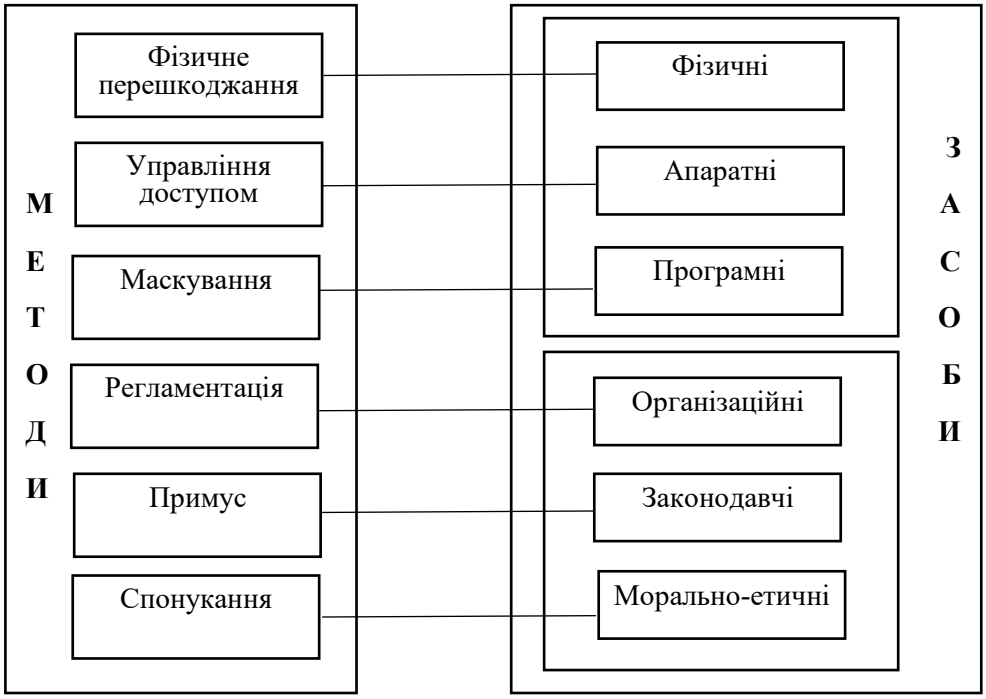

Рис. 1. 3. Методи і засоби забезпечення інформаційної безпеки організації.

1.2. Загрози інформаційній безпеці з вини персоналу

У науковій думці *загрозу* визначають як крайню ступінь небезпеки (безпосередню небезпеку); будь-який потенційно можливий несприятливий вплив, стадію крайнього загострення протиріч, безпосередньо передконфліктний стан тощо.

На думку фахівців з національної безпеки, загроза - це стадія крайнього загострення протиріч, безпосередньо передконфліктний стан, коли в наявності готовність одного із суб'єктів політики застосувати силу стосовно іншого конкретного об'єкта для досягнення своїх політичних та інших цілей. Небезпеку ж розуміють як стадію зародження і насичення протиріч, коли один із суб'єктів політики потенційно може, але ще не готовий застосувати силу або загрозу сили в своїх інтересах.

Загроза повинна містити в собі два компоненти: наміри і можливість нанесення збитку інтересам безпеки, а небезпека обмежується наявністю тільки однієї з цих компонент. Загроза має персоніфікований, конкретно-адресний характер, що припускає наявність очевидних суб'єкта (джерела) загрози і об'єкта,

на який спрямована її дію. На відміну від загрози небезпека носить гіпотетичний, часто безадресний характер, її суб'єкт і об'єкт явно не виражені.

Небезпека містить у собі потенційну загрозу заподіяння шкоди тим чи іншим інтересам, для реалізації якої необхідне створення відповідних умов (накопичення можливостей і формування намірів), загроза ж є безпосередня можливість нанесення збитку, від початку здійснення якої її відділяє лише часовий інтервал, необхідний для прийняття рішення про реалізацію загрози.

Незважаючи на наявність різних підходів до визначення поняття «загроза», більшість учених сходяться на думці, що загрози:

– мають динамічний, змінний характер і включають події, зміни або дії;

– спричиняють шкоду або порушення нормального функціонування об’єкта (держави), і як наслідок є причиною збитків та втрат;

– виникають під дією певних чинників (зовнішніх та внутрішніх), і тому потребують комплексу заходів з боку держави для їх нейтралізації та усунення [5].

Під загрозами інформації розуміють потенційні або реально можливі дії стосовно інформаційних ресурсів та засобів їх обробки та передачі, що призводять до неправомірних дій щодо них.

Стандарт ISO 27000 визначає загрозу інформаційній безпеці як потенційну причину неочікуваного інциденту, який може мати наслідком нанесення шкоди системі або організації.

Загроза інформаційній безпеці може спричинити часткову або повну втрату організацією можливості реалізувати свої інтереси в інформаційній сфері, а також призвести до порушення нормального функціонування, руйнації або стримування розвитку технічних об’єктів інформаційної безпеки.

У науці представлено багато підходів до класифікації загроз інформаційній безпеці організації. Зокрема, за джерелами походження загрози бувають природного, техногенного та антропогенного походження; за розміщенням джерела - зовнішні і внутрішні; за намірами впливу - навмисні і випадкові; за рівнем визначеності – закономірні і випадкові; за наслідками – допустимі і неприпустимі; за характером реалізації – реальні і потенційні.

Вартою уваги є примірна класифікація загроз інформаційній безпеці організації, представлена у стандарті ISO 27005 [38] (Таблиця 1.2.).

Таблиця 1.2.

Види загроз інформаційній безпеці згідно зі стандартом ISO 27005.

Тип	**Загрози**
Фізичне пошкодження	Пожежа
	Втрати внаслідок аварій водопостачання
	Забруднення
	Масштабні інциденти
	Пошкодження обладнання або носіїв
	Запилення, корозія, замерзання
Природні явища	Кліматичні явища
	Сейсмічні явища
	Вулканічні явища
	Метеорологічні вища
	Паводок
Порушення роботи систем життєзабезпечення	Збої в роботі систем кондиціонування чи водопостачання
	Припинення електропостачання
	Вихід з ладу телекомунікаційного обладнання
Порушення внаслідок випромінювання	Електромагнітне випромінювання
	Термічна радіація
	Електромагнітна пульсація
	Перехоплення сигналів скомпрометованих внаслідок втручання
	Віддалене стеження
	Підслуховування
	Крадіжка носіїв або документів
Компрометація інформації	Крадіжка обладнання
	Відновлення перероблених або загублених носіїв
	Розкриття інформації
	Поширення інформації з недостовірних джерел
	Підробка апаратного забезпечення
	Підробка програмного забезпечення
	Виявлення місцерозташування

Продовження Табл.1.2.

Технічні збої	Несправність обладнання
	Відмова обладнання
	Перевантаження інформаційних систем
	Відмова програмного забезпечення
	Порушення ремонтопридатності обладнання
Неавторизовані дії	Неавторизоване використання обладнання
	Копіювання програмного забезпеченняз метою шахрайства
	Використання підробного або копійованого програмного забезпечення
	Пошкодження даних
	Нелегальна обробка інформації
Компрометування функцій	Помилки у використанні
	Зловживання правами
	Підробка прав
	Відмова в діях
	Порушення доступності персоналу

На думку науковців [20,21,29,30] джерела походження загроз інформаційної безпеки можна розділити на три групи:

– внутрішні джерела загроз для інформаційної безпеки організації - особи, які мають доступ до корпоративних ІТКС (фаховий та допоміжний персонал, працівників партнерських або аутсорсингових організацій);

– зовнішні джерела загроз для інформаційної безпеки організації - особи, конкуруючі компанії, а також спеціальні розвідувальні організації, які не мають доступу до корпоративних ІТКС;

– джерела загроз для інформаційної безпеки організації, пов'язані з дією природних і техногенних чинників.

Схема джерел загроз інформаційній безпеці організації представлена на Рис. 1.4.

Рис. 1.4. Джерела загроз інформаційній безпеці.

Розглянемо кожну категорію джерел детальніше.

Внутрішніми джерелами загроз інформаційній безпеці може бути деструктивна діяльність персоналу організації, працівників організацій-підрядників, ділових партнерів, а також клієнтів, які мають санкціонований доступ на територію організації та до його ІТКС. Зазначені особи можуть здійснити такі протиправні дії: надати третім особам несанкціонований доступ до ІТКС віддалено, за допомогою комп'ютерних мереж або безпосередньо на території організації; скопіювати критичну інформацію з метою її подальшої передачі третім особам як на фізичних носіях (паперові документи, мікроплівка, компакт-диски, флеш-карти тощо), так і за допомогою комп'ютерних мереж; у протиправний спосіб змінити або видалити інформацію в корпоративних ІТКС.

Причинами зловмисної діяльності персоналу організації й інших осіб, які мають офіційний доступ до критичних об'єктів і ІТКС, є три основні чинники: некомпетентність, халатність і злий умисел.

У першому випадку співробітники компанії або організації-підрядника, ділового партнера або навіть клієнти не мають достатньої підготовки з питань інформаційної безпеки, зокрема не знають своїх обов'язків із забезпечення захисту інформації, вимог і процедур, обов'язкових до виконання.

Як свідчить дослідження SOC Survey 2019, проведене американським Інститутом системного адміністрування, аудиту, мереж і безпеки (The SysAdmin, Audit, Network, Security Institute, SANS) 57,7% опитаних працівників Центрів операцій з безпеки (Security Operations Center, SOC) відзначили, що брак навичок з інформаційної безпеки є першочерговим викликом для корпоративних команд SOC [43].

У разі халатності персоналу причина виникнення загроз інформаційній безпеці полягає не у відсутності спеціалізованих знань, оскільки працівники пройшли навчання і знають свої обов'язки в системі захисту інформації, правила, процедури і вимоги, яких треба дотримуватися. Однак, вони нехтують їх виконанням з різних причин, першою з яких є низький рівень мотивації персоналу внаслідок негативного впливу на співробітників організації внутрішніх і зовнішніх факторів, наприклад незадоволення рівнем оплати праці чи ставленням керівництва. Результати дослідження компанії Bitdefender (Bitdefender Hacked Off! Survey) показали, що у 2017 році п'ята частина зареєстрованих порушень інформаційної безпеки відбулися внаслідок халатності персоналу, у 2018 році цей показник незначно зріс до 21%, а у 2019 знову зупинився на позначці у 20% [40].

За наявності злого умислу працівник компанії, організації-підрядника, ділового партнера або клієнт свідомо здійснює шкідливу для організації діяльність (так званий інсайд або шкідливий інсайд), яка може бути викликана бажанням помститися за реальні чи уявні образи, отримати матеріальну або грошову вигоду, тиском з боку третіх осіб, як правило конкурентів або зловмисників. Як свідчить статистика шкідливий інсайд є однією з найбільш серйозних і широко поширених загроз для інформаційної безпеки організації. Так, результати досліджень телекомунікаційної компанії Verizon показали, що у 2019 році 34% випадків порушень, пов’язаних з даними, сталися із залученням інсайдерів [39].

До *зовнішніх джерел* загроз інформаційній безпеці відносять діяльність осіб, які не є працівниками організації і не мають офіційного доступу до його території, приміщень та корпоративних ІТКС. Така деструктивна діяльність може включати

хакерські атаки, різні види шахрайства, несанкціоновані дії з даними за допомогою технічних засобів або фізичного доступу.

Хакерські атаки мають на меті переважно отримання доступу до ІТКС підприємства чи організації, втручання в її роботу й отримання доступу до критичної інформації для її подальшого копіювання, зміни або знищення.

Хакери використовують різноманітні підходи і методи, які постійно вдосконалюються, зокрема злом системи доступу, впровадження шкідливого програмного забезпечення, використання вразливостей у системі захисті ІТКС. Низка досліджень, проведених різними компаніями, показали, що 64% організацій постраждали внаслідок кібератак. 59% компаній зіткнулися із зараженнями зловмисним ПЗ та деструктивною діяльність ботнетів, а 51% мали досвід атак відмови в обслуговуванні [45].

Як показує практика, у понад 50% успішних хакерських атак на ІТКС організацій хакери мали спільників серед співробітників атакований організації.

Шахрайство відносно співробітників організації з метою отримання конфіденційної інформації є дуже поширеним видом протиправних дій у сфері інформаційної безпеки. Шахрайські дії можуть бути реалізовані різними методами. Шахраї, які не застосовують технічні засоби, використовують різні маніпулятивні прийоми у безпосередньому спілкуванні з персоналом організації, наприклад техніку «за хвостом». У випадку телефонного шахрайства зловмисник може представитися другом, партнером, замовником, використовуючи заздалегідь зібрану інформацію жертву. Мабуть, найбільш поширеним видом шахрайства є його Інтернет-різновид, де для виманювання конфіденційної інформації використовують фейкові сайти, за допомогою засобів інтернет-спілкування встановлюють довірчі відносини з працівником, спонукають особу до скачування шкідливого ПЗ. Так, за останні роки 62% організацій стали жертвами фішингових атак та інших методів соціальної інженерії.

Для здійснення несанкціонованого отримання інформації за допомогою технічних засобів використовують засоби підслуховування і стеження (лазерні мікрофони, відеокамери, тепловізори), системи радіоперехоплення. З цією ж

метою встановлюють спеціальні пристрої («жучки») на території організації та на об'єктах його ІТКС.

Несанкціонований доступ до конфіденційної або чутливої інформації за допомогою засобів фізичного доступу передбачає протиправне проникнення сторонніх осіб на територію, що охороняється, та в закриті для загального доступу місця зберігання інформації і має на меті її викрадення на різних носіях залежно від форми представлення даних (папір, мікроплівка, цифрові носії).

До *інших джерел* загроз інформаційній безпеці відносять джерела, не пов'язані з діяльністю людей, або пов'язані з нею опосередковано, зокрема аварії та надзвичайні ситуації як природного походження (повені, землетруси, буревії, блискавки), так і техногенного характеру (пожежі, перебої в електроживленні, контакти електроніки з агресивними речовинами тощо). Крім аварій і надзвичайних ситуацій до інших джерел загроз природного походження також відносять пошкодження внаслідок деструктивного впливу на інформацію та засоби її обробки представників флори і фауни.

Відповідно до наукових джерел та міжнародних стандартів [6,20,21,30,40] загрози інформаційній безпеці у контексті захисту інформації можна згрупувати у чотири блоки:

– внесення несанкціонованих змін в інформацію, внаслідок чого можуть виникнути помилки і збої в діяльності організації, а також привести до фінансових або репутаційних втрат;

– несанкціоноване видалення інформації, в результаті чого організація повністю або частково втрачає важливі дані. Факт знищення інформації легше виявити, ніж її зміну, однак, наслідки такого інциденту можуть бути більш значними з огляду на втрати тієї чи іншої категорії критичних або чутливих даних (конструкторська розробка або персональні дані клієнтів).

– недозволене копіювання інформації може призвести до ознайомлення з критичною інформацією конкуруючих компаній, що надасть їм конкурентну перевагу над власником інформації. Також це може привести до нанесення збитку

третім особам (ті ж персональні дані, зокрема дані щодо банківських рахунків і карток);

– блокування доступу до інформації для авторизованих користувачів може здійснюватися з використанням програмних або апаратних засобів і призвести до збоїв у функціонуванні організаційних або технологічних процесів, ускладнень або неможливості трудової діяльності колективу організації.

2.3. Напрями роботи з персоналом у сфері інформаційної безпеки

Розглянемо джерела загроз інформаційній безпеці у контексті ролі персоналу організації у реалізації загроз з цих джерел. Так, загрози, спрямовані із внутрішніх джерел, реалізують працівники організації, при чому такі загрози взагалі не можуть виникати без їх участі.

Загрози із зовнішніх джерел, які, за винятком різних видів шахрайства, по суті є обманом персоналу організації, можуть реалізуватися без його безпосередньої й усвідомленої участі. Але, як свідчить практика [42], у більшості випадків такі загрози були успішно реалізовані саме завдяки участі працівників організації, яка стала жертвою інформаційної атаки.

Загрози, спричинені природними і техногенними факторами виникають без участі персоналу, однак саме персонал забезпечує ефективну протидію таким загрозам та мінімізацію їхніх наслідків.

Проаналізувавши типологію загроз та їхніх джерел, з одного боку, та види активностей із забезпечення інформаційної безпеки організації, спрямованих на персонал організації, доцільно виділити такі три основні напрями роботи з персоналом:

1. Навчання персоналу з питань інформаційної безпеки та дотичних сфер.

2. Мотивація і, як наслідок, формування і підтримання високого рівня організаційної прихильності (лояльності).

3. Контроль персоналу.

Унаслідок зіставлення встановлених джерел загроз інформаційній безпеці організації, ролі персоналу в реалізації загроз і напрямки роботи з персоналом, можна представити таку схему зв'язку джерел загроз інформаційній безпеці та напрямків роботи з персоналом з метою їх запобігання і протидії [6] (Рис. 1.5.).

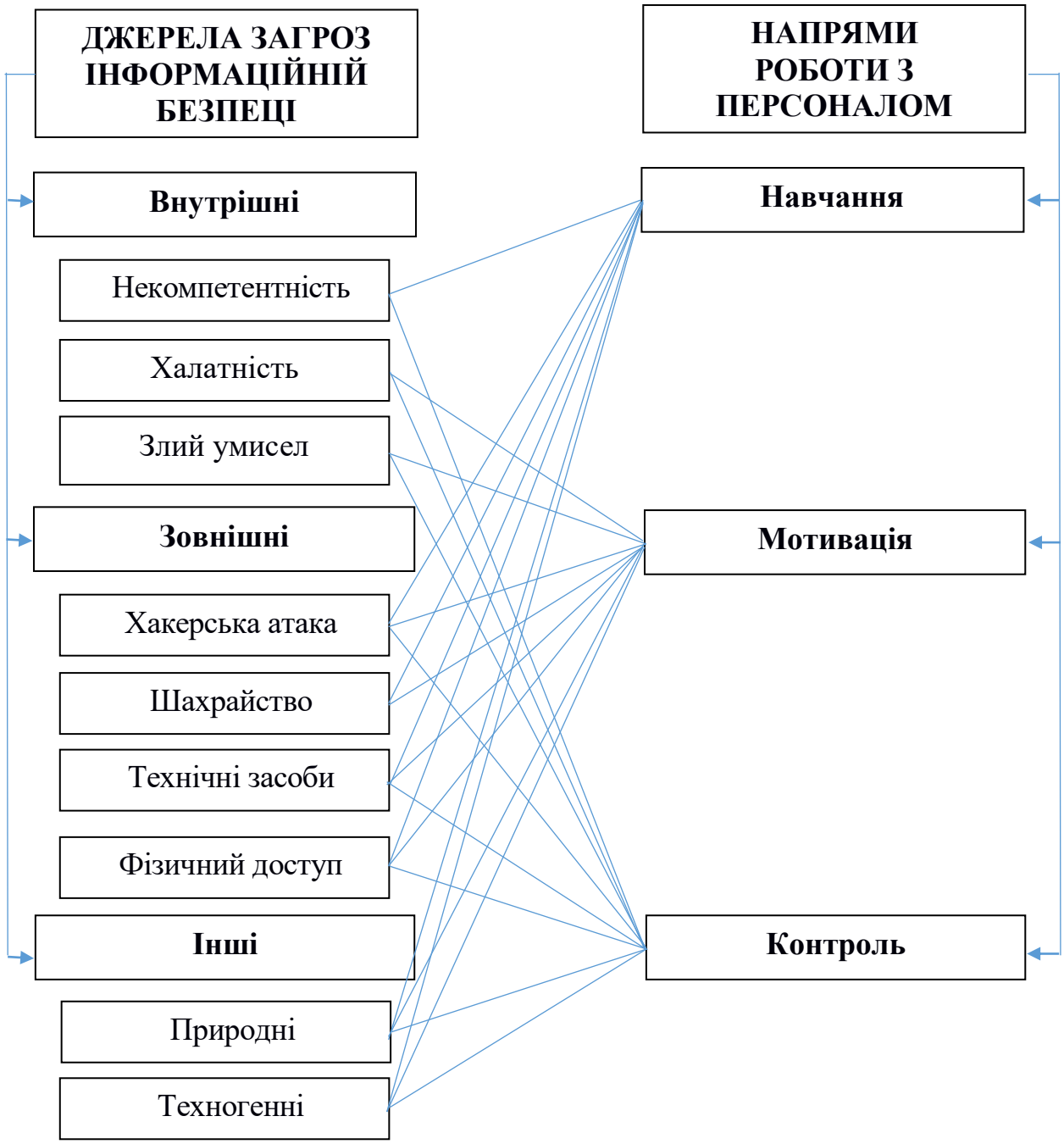

Рис. 1.5. Зв'язок джерел загроз ІБ з напрямами роботи з персоналом з метою їх запобігання й протидії.

Розглянемо представлену схему, яка встановлює напрями роботи з персоналом з огляду на запобігання різним типам загроз інформаційній безпеці, докладніше.

Внутрішні загрози.

Як засвідчив аналіз, для запобігання випадкам некомпетентності персоналу основними заходами є: навчання працівників процедурам, правилам і принципам інформаційної безпеки та контроль успішності засвоєння отриманих знань. У таких випадках можна використовувати різноманітні методи навчання, серед яких зовнішні (проходження курсів, освітніх та професійних програм на базі зовнішніх установ – закладів освіти, спеціалізованих сертифікованих організацій начального спрямування), так і внутрішні (тренінги на робочому місці, вивчення кращого досвіду більш професійно підготовлених колег, наставництво тощо) [2].

Для протидії випадкам халатного ставлення працівників до виконання своїх професійних обов'язків необхідно: забезпечити проведення заходів з формування й підтримки високого ступеня вмотивованості персоналу щодо виконання процедур, правил і принципів інформаційної безпеки, а також контролювати стан і якість виконання професійних функцій.

Як відомо, велике значення для формування надійного персоналу відіграють засоби матеріального стимулювання, насамперед належна оплата праці, достатній соціальний захист та медичне страхування, психологічна допомога. Водночас, обов'язковим елементом є заходи мотивування персоналу, наприклад залучення підлеглих до обговорення поточних питань, а також прийняття стратегічних рішень, справедливе оцінювання досягнутих результатів й відповідне заохочення, кар'єрне зростання і професійний розвиток, заохочення ініціативи та творчого підходу до виконання поставлених завдань [25].

Виявляти і протидіяти появі навмисних деструктивних намірів у працівників організації необхідно шляхом належного мотивування персоналу з метою зниження ймовірності шкідливого інсайду й контролю діяльності фахівців в інформаційній системі організації для своєчасного виявлення фактів порушень інформаційної безпеки і подальшої їх протидії.

Забезпечити належний контроль за діяльністю персоналу можна у різний спосіб, зокрема через контроль з боку керівника та колег (на Заході, наприклад, широко поширеним є створення спеціальних каналів, наприклад е-пошти, для

повідомлення про випадки порушення безпеки, так звані whistleblowing; регулярні перевірки керівником організації або службою безпеки дотримання співробітниками вимог щодо захисту інформації; самоконтроль співробітників [34]. Не останню роль у забезпеченні якісного контролю відіграє система покарань і штрафів за невиконання вимог інформаційної безпеки. До засобів контролю також можна віднести системи відеонагляду та моніторингу дій працівника в інформаційних системах та мережах.

Зовнішні загрози.

Зовнішні загрози є окремою категорією загроз, які вимагають проведення системних та послідовних дій для зменшення ймовірності та запобігання їх появі. Для протидії хакерським атакам основним завданням є забезпечення якісної професійної підготовки фахівців, володіння методами і засобами захисту інформації в мережевому середовищі; безсумнівною є роль мотивації персоналу, завдяки чому формується відповідальність і небайдужість людей до справ організації та залученість у процес вирішення організаційних проблем, а тим більше зводяться до мінімуму шанси участі співробітників у проведенні зовнішньої хакерської атаки на організацію. Також важливою складовою запобігання участі інсайдерів в хакерських атаках є постійний контроль за діяльністю персоналу, включаючи моніторинг відвідування ними сайтів в мережі Інтернет, установки або спроб встановлень програмного забезпечення, створення і зберігання паролів доступу та інших активностей, не пов’язаних з професійною діяльністю.

У нинішніх умовах постійно зростає кількість випадків шахрайства, спрямованого на персонал організації, які мають на меті вивідування конфіденційних даних, отримання неавторизованого доступу до зон безпеки. З метою їх запобігання необхідно навчати персонал, як розпізнавати спроби застосування методів соціальної інженерії, виявлення шахраїв і уникнення попадання під їхній вплив. Засоби мотивації у таких випадках сприяють зростанню уважності й обережності персоналу при взаємодії з незнайомими або ненадійно ідентифікованими особами.

Для протидії участі персоналу у порушеннях інформаційної безпеки з використанням технічних засобів організація повинна використовувати комплексний підхід, реалізуючи заходи навчання (працівники мають володіти знаннями і навичками протидії технічним засобам незаконного отримання інформації, зокрема знати ознаки, що вказують на їх наявність), підвищення мотивації для підтримки необхідного рівня пильності персоналу та контролю за діяльністю працівників, запобігаючи випадкам пронесення на територію організації технічних засобів збору інформації внаслідок некомпетентності або навмисно.

У контексті запобігання порушення фізичного доступу на територію організації загалом та в зони безпеки зокрема обов’язковими є заходи за трьома переліченими вище напрямами: підготовка співробітників щодо процедур і правил доступу й перебування сторонніх осіб на території організації; мотивування персоналу, що має на меті запобігти випадкам їхнього сприяння стороннім особам в незаконному проникненні на територію організації; контроль за діяльністю й поведінкою працівників для своєчасного виявлення спроб допомоги стороннім особам в незаконному проникненні в зони безпеки.

Випадкові загрози.

Робота з персоналом для запобігання його причетності до виникнення випадкових загроз як природного, так і техногенного характеру, має включати: по-перше, навчання діям в умовах надзвичайних ситуацій природного й техногенного характеру; по-друге, підтримання достатнього рівня мотивації персоналу для виконання ним своїх обов'язків в умовах таких ситуацій; по-третє, здійснення належного контролю за дотриманням персоналом встановлених процедур із запобігання й протидії можливим природним і техногенним загрозам.

Висновки до першого розділу

Встановлено, що забезпечення інформаційної безпеки організації - це цілеспрямована діяльність її органів і посадових осіб з використанням дозволених методів і засобів по досягненню стану захищеності інформаційного середовища організації та забезпечення його нормального функціонування і динамічного розвитку. Важливим напрямом забезпечення інформаційної безпеки організації є створення середовища, в якому користувачі та персонал дотримуються вимог інформаційної безпеки.

Під загрозами інформаційній безпеці розуміють потенційні або реально можливі дії стосовно інформаційних ресурсів організації та засобів їх обробки та передачі, що призводять до неправомірних дій щодо них. Відзначено, що значний вплив на стан інформаційної безпеки мають внутрішні джерела загроз, тобто у більшості випадків персонал організації, який здійснює різноманітні протиправні дії щодо інформації та інформаційних систем організації внаслідок своєї некомпетентності, халатності або злого умислу.

На основі аналізу джерел загроз виділено такі три основні напрями роботи з персоналом з інформаційної безпеки: навчання персоналу з питань інформаційної безпеки; мотивування і, як наслідок, формування високого рівня організаційної лояльності; контроль персоналу. Таким чином, заходи матеріального стимулювання і мотивування персоналу забезпечують запобігання випадкам навмисного чи ненавмисного порушення вимог інформаційної безпеки, зниження ймовірності шкідливого інсайду.

Розділ 2
ОРГАНІЗАЦІЙНА ЛОЯЛЬНІСТЬ ПЕРСОНАЛУ ТА ПІДХОДИ ДО ЇЇ ОЦІНЮВАННЯ В КОНТЕКСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Як показало дослідження джерел загроз інформаційній безпеці та напрямів роботи з персоналом, які запобігають і протидіють різним інформаційним загрозам (внутрішнім, зовнішнім, випадковим), ключового значення для забезпечення інформаційної безпеки організації у сучасних умовах набуває формування й утримання високого рівня організаційної лояльності персоналу.

2.1. Сутність і види лояльності персоналу

У сучасній теорії і практиці управління лояльність персоналу розглядається як один з найважливіших ресурсів організації, обов'язкова умова успішності її діяльності. Саме про це свідчать результати досліджень.

Встановлено, що в організаціях з низьким рівнем плинності кадрів, а отже з високим рівнем лояльності співробітники на 51% рідше звільняються і на 27% менше прогулюють роботу. Водночас персонал цих організацій працює в середньому на 12% ефективніше, ніж аналогічні за родом діяльності групи нелояльних працівників [4,10].

За підсумками досліджень скандинавської консалтингової компанії Forespring, яка спеціалізується на проблемах лояльності працівників і клієнтів, встановлено, що лояльність працівників позитивно впливає на лояльність клієнтів, а лояльність клієнтів робить позитивний вплив на прибутковість. Доведено, що у разі зростання лояльності персоналу в даному кварталі на 1%, лояльність клієнтів у тому ж кварталі збільшується на 1,25%. За умови підвищення рівня лояльності клієнтів на 1% прибуток компанії в наступному кварталі збільшується на 0,885%.

Згідно з результатами міжнародних досліджень компанії FleetBoston Financial Corp. збільшення лояльності працівників на 1% може дати $11 мільйонів річного

доходу і економить від $ 15 до $ 19 мільйонів при наймі та навчанні тільки в межах одного напряму діяльності [11].

Отже, очевидною є важливість цілеспрямованої роботи щодо формування лояльності співробітників.

За кордоном лояльність персоналу, її наслідки та визначальні чинники стали однією з актуальних тем досліджень організаційної поведінки ще з 70-х рр. XIX ст. На сьогодні, однак, єдиного підходу до розуміння суті поняття лояльності персоналу не було сформовано.

В іноземній літературі для позначення даного феномена використовується термін organizational commitment. В російсько- та україномовних інтерпретаціях зустрічаються різні поняття (лояльність, відданість, прихильність), які ми будемо використовувати як синоніми.

Розглянемо основні підходи до розуміння терміну «лояльність персоналу» на основі вивчення наукових публікацій [8,19,27, 37].

Загалом у науковій думці представлено дві протилежні концепції феномену «лояльність персоналу».

Поведінковий підхід розглядає лояльність персоналу як джерело організаційної безпеки або поведінку на благо компанії, в якій співробітники дотримуються правил і норм, обережно ставляться до свого робочого місця. У такому разі лояльність проявляється через прагнення працівника належати до своєї компанії, а також продовжувати працювати в ній.

Одним з засновників цього підходу є соціолог Г. Беккер, який стверджує, що лояльність персоналу є наслідком діяльності, що виникає через вкладення в компанію або через скорочення будь-яких можливостей в матеріальному, професійному або кар'єрному плані.

На думку колективу науковців у складі Сіміларлі, Вінера і Варді, лояльність – це тоді, коли працівник продовжує сприяти організації, бо вважає, що повинен вести себе таким чином, оскільки це є його «правом» і «очікуваною поведінкою».

Російський дослідник А. Килимов у своїх роботах зазначає, що лояльність персоналу складається з двох елементів: професійної придатності й надійності.

Він вважає, що про лояльність працівника можна говорити тільки після того, як він пропрацює достатній час в організації і матиме повне уявлення про організаційну культуру.

К. Харський також є прихильником цієї точки зору. На його думку, лояльність працівника характеризується почуттям гордості і відданості, здатністю й готовністю змиритися з одними вимогами і глибоко прийняти інші, прагненням зберегти своє робоче місце, бажанням зробити свою роботу найкращим чином й усвідомлено дотримуватися прийнятих правил.

Установочний підхід під лояльністю розуміє емоційну прихильність персоналу до організації, яка формується через набір таких елементів: попередній досвід роботи, особистісні характеристики співробітника і сприйняття організації, які призводять до позитивного ставлення до організації і, в результаті цього – до організаційної лояльності.

Досить широке поняття лояльності в рамках установчого підходу належить Л. Портеру і його співавторам, які вважають, що лояльність – це готовність співробітника докладати значних зусиль в інтересах організації і прийняти її основні цілі та цінностей.

Під лояльністю вони мають на увазі ступінь ідентифікації працівника зі своєю організацією та його залученість у трудову діяльність. У свою чергу, ідентифікація та залученість передбачають наявність трьох взаємопов'язаних характеристик: віри в цілі і завдання своєї організації, згоди здійснювати зусилля від її імені, а також бажання відчувати приналежність до організації [8].

Н. Янс запропонував своє визначення, відповідно до якого лояльність є певним мірилом сприйняття працівником цінностей і цілей своєї організації, розглядаючи власні організаційну роль та внесок у досягнення організаційних цінностей і цілей.

Відомі дослідники проблем лояльності персоналу Д. Мейер та Н. Аллен вважають, що лояльність складається з трьох компонентів: афективної (емоційної прихильності), продовженої (втрати співробітника, пов'язані зі звільненням) і нормативної (відчуття зобов'язань у стосунку до організації).

Афективна лояльність характеризується певним ступенем ідентифікації працівника з організацією, його любові й гордості за свій фах або компанію, а також залученістю і прихильністю до організації. У цьому випадку співробітник по справжньому зацікавлений у досягненні поставлених перед ним завдань і залишається працювати у своїй організації, тому що дійсно цього хоче.

Продовжена (розрахункова) лояльність означає, що працівник пов'язує необхідність працювати в організації насамперед з тим, що припинення роботи призведе до певних втрат, наприклад зміни професії або організації, втрати статусу, припинення відносин з колегами тощо.

Нормативна лояльність виражається через почуття боргу: працівник вважає себе зобов'язаним перед організацією, наприклад, за навчання, набутий досвід або допомогу в вирішенні певних особистих проблем. У такому разі особа переконана у правильності своїх дій і не змінює місце роботи. Згідно з моральними нормами працівник залишається в організації, оскільки вважає, що повинен так вчинити.

С. Гордейко визначає лояльність персоналу як готовність співробітників розділяти місію і цінності компанії, формувати свої особисті цілі і завдання відповідно до них.

Згідно з баченням В. Доміняка, лояльність - це доброзичливі, відкриті і шанобливі відносини між працівниками організації та з іншими особами; прагнення досягти встановлених мети і завдань організації, дотримання встановлених норм і правил щодо всіх суб'єктів, пов'язаних з організацією.

М. О'Меллі, відповідаючи на запитання «Як залучити й утримати талановитих співробітників за допомогою побудови тривалих відносин» будує свою модель лояльності, яка складається з п'яти елементів:

– відповідність і приналежність до організації (потреба бути прийнятим) - відчуття своєї значимості і збігання власних інтересів та цінностей з цінностями й інтересами організації;

– статус та індивідуальність (потреба в повазі), пов’язані з гордістю співробітника з приводу своєї приналежності до організації;

– довіра і взаємність (потреба в безпеці) означає усвідомлення працівником, що організація враховує і дбає про його інтереси;

– емоційна винагорода (потреба в розвитку) - відчуття задоволення від роботи в організації та діяльності, якою займається працівник;

– економічна взаємозалежність (потреба в коштах) відображає рівень відповідності одержуваної винагороди, заробітної платою рчікуванням працівника [19].

На основі підходів Мейєра-Аллен та О'Меллі російські вчені М. Магура і М. Курбатов висунули своє бачення класифікації лояльності. На їх думку, лояльність буває: справжньою, коли працівник максимально проявляє перераховані вище характеристики і не висуває жодних вимог до своєї організації; прагматичною, коли працівник зіставляє й порівнює свій внесок в організацію та свої вигоди взамін; вимушеною, коли працівник не має можливості знайти інше місце роботи.

Вартою уваги є класифікація лояльності, запропонована К. Харським [36], який розглядає даний феномен як функцію двох чинників: локусу контролю, що дозволяє локалізувати причини ставлення працівника до своєї організації (цінності й особистісні особливості працівника або особливості організації) та локусу часу, що має на увазі можливість оцінювання передбачуваної зміни ставлення працівника до своєї організації, що, в свою чергу, дозволяє спрогнозувати рівень його лояльності.

Завдяки цим двом атрибутам, К. Харський сформулював свою модель лояльності, виділивши чотири її крайніх типи:

– «ветеран» - є найбільш надійним типом, основою якого є система цінностей і світогляд особи. Цей тип лояльності утворюється внаслідок попереднього досвіду працівника і його внутрішньої мотивації (внутрішній локус контролю);

– «мрійник» - тип, властивий засновникам організації і працівникам, які працювали в організації з моменту її створення. Лояльність такого типу визначається внутрішнім локусом контролю і зосереджена на майбутніх очікуваннях;

– «спадкоємець» - тип лояльності, яка заснована на зовнішніх мотиваторах і попередньому досвіді. Працівник, який відноситься до цього типу, найбільше піддатливий до переконання або примусу з боку зовнішнього середовища, не приймає власних рішень;

– «зомбі» - у працівника даного типу лояльність формується через майбутнє і зовнішній локус контролю. Тому це є найбільш слабкий і нестабільний тип лояльності, який легко сформувати, надавши привабливий образ майбутнього.

Також К. Харський запропонував авторський підхід до рівнів лояльності персоналу, визначивши 7 рівнів (Таблиця 2.1.).

Таблиця 2.1.

Рівні лояльності персоналу

	№	Рівень	Ознаки
НЕЛОЯЛЬНИЙ ПРАЦІВНИК	1	демонстративна нелояльність	споживацьке ставлення і пріоритет власної вигоди, нехтування правилами організації, сарказм і обман у твердженнях, пов'язаних з організацією, які негативно впливають на інших працівників, руйнуючи їх прихильність організаційним цінностям.
	2	прихована нелояльність	бездоганне виконання правил і норм організації, однак формально і через страх бути покараним або бажання отримати винагороду, створення й розповсюдження чуток, підштовхування інших працівників до критики організації.
	3	нульова лояльність	індиферентна налаштованість по відношенню до організації: у деяких випадках – лояльна поведінка, в інших – прояви нелояльності; найбільш непередбачуваний стиль поведінки, який залежить від того, під чий вплив така особа потрапила при працевлаштуванні на роботу в організацію.

Продовж. Таблиці 2.1.

ЛОЯЛЬНИЙ ПРАЦІВНИК	4	лояльність на рівні зовнішніх атрибутів	бажання носити, тримати при собі символи своєї організації (фірмовий одяг, речі, які їх містять), а також поведінка у відповідності з організаційними правилами; демонстрація лояльної організаційної поведінки, небажання відкрито проявляти ознаки нелояльності.
	5	лояльність на рівні поведінки	дотримання встановлених організацією норм, правил, традицій; схильність наслідувати прийняту в організації поведінку; добровільна і натхненна участь у заходах компанії; прагнення розвивати свої професійні компетенції, однак відсутність бажання до самопожертви і змін всередині організації.
	6	лояльність на рівні переконання	максимально ефективна трудова діяльність, відповідальне ставлення до виконання своїх обов'язків, ініціативність, неприпустиме ставлення до будь-яких порушень організаційних норм з боку колег; почуття причетності й готовність розділити проблеми організації.
	7	лояльність на рівні ідентичності	повне ототожнення себе з організацією; відданість, незалежна від матеріальної складової чи критики організації з боку інших працівників; максимальна вмотивованість і найвища продуктивність.

У вітчизняній літературі з питань лояльності персоналу представлено підхід, відповідно до якого лояльність буває раціональною, емоційною, нормативною і вимушеною (див. Рис.2.1) [18]. Першу можна вважати найбільш конструктивною, останню - найменш.

Рис. 2.1. Види лояльності

Раціональна лояльність. Її поява пов’язана з процесами усвідомленого розуміння працівника, який поділяє організаційні цінності й норми, вважає їх своїми власними, отримує задоволення від своєї праці і несе відповідальність за її результати, оскільки переконаний, що від досягнення цілей організації залежить досягнення його власних цілей. Зрозуміло, що це той тип, до якого потрібно прагнути, а організація має докладати зусилля для його формування.

Емоційна лояльність. Такий тип лояльності характеризується наявністю у працівника таких почуттів щодо своєї організації як: радість і задоволення від приналежності до неї, виконання своєї професійної діяльності, роботи з колегами. Однак, незважаючи на щирість цих емоцій, вони є рухливими, ситуативними і часто недовговічними. Тому особа, чия відданість організації базується на тезі «мені тут подобається», не є надійною.

Нормативна лояльність базується на конструкті «повинен» і часто притаманна керівникам або працівникам, які давно працюють в організації, тому проявляють відданість загальній справі, повагу до організаційних правил і традицій.

Вимушена лояльність. Основний мотив такої людини «мені тут комфортно». Працівнику з таким типом лояльності зручно працювати в організації, водночас він радо покинув би організацію, але не робить цього, бо більше нікуди піти, йому лінь або боязко шукати щось краще. Такий тип вид лояльності не є конструктивним і має бути змінений.

2.2. Підходи до оцінювання організаційної лояльності персоналу

Вивчаючи феномен лояльності персоналу організації, вітчизняні та зарубіжні вчені презентують різні підходи до її оцінювання. У науковій літературі можна зустріти три найбільш відомі моделі організаційної лояльності: одномірна модель Л.Портера (R. Mowday, L. Porter, R. Steers, 1982), трикомпонентна модель Дж.Мейера і Н.Аллен (J.Meyer, N.Allen, 1991).

Однією з найбільш поширених методик самооцінювання є опитувальник організаційної лояльності Л. Портера (Organizational Commitment Questionnaire - OCQ).

Опитувальник Л. Портера містить перелік тверджень, що відображають можливе ставлення особи до організації, в якій вона працює. Розглянемо варіант зазначеного опитувальника, розробленого російськими вченими під керівництвом В. Доміняка [14].

Відповідаючи на запитання, працівник має вказати ступінь своєї згоди або незгоди з кожним твердженням, вибравши за семибальною шкалою один із варіантів відповіді:

1 - абсолютно не згоден;

2 - не згоден;

3 - скоріше не згоден;

4 - не маю певної думки;

5 - скоріше згоден;

6 – згоден;

7 - абсолютно згоден .

Перелік тверджень:

1. Я готовий працювати понаднормово на благо організації.
2. Я розповідаю моїм друзям про те, як добре працювати в організації.
3. Я не дуже відданий організації.
4. Я згоден майже на будь-яку роботу для того, щоб залишитися в організації.
5. Я вважаю, що мої цінності і цінності організації дуже схожі.
6. Я пишаюся тим, що можу сказати: «Я - частина організації».
7. Аналогічну роботу я можу виконувати в іншій організації не гірше, ніж у нинішній.
8. Заради організації я готовий підвищувати продуктивність своєї праці.
9. Навіть незначного зменшення моєї заробітної плати було б достатньо, щоб я звільнився з організації.

10. Я радий, що вибрав саме цю організацію з тих, які розглядав при працевлаштуванні.
11. Відданість організації навряд чи обіцяє багато переваг.
12. Часто мені важко погодитися з політикою організації щодо її працівників.
13. Я дійсно дбаю про долю організації.
14. Для мене це найкраща з усіх організацій, в яких я працював.
15. Рішення про роботу в організації було помилкою з мого боку.

У методиці використовується 7-бальна шкала, при цьому для пунктів 1, 2, 4, 5, 6, 8, 10, 13 і 14: абсолютно не згоден – 1; не згоден – 2; скоріше не згоден – 3; не маю певної думки – 4; скоріше згоден – 5; згоден – 6; абсолютно згоден – 7.

Для пунктів 3, 7, 9, 11, 12, 15: абсолютно не згоден – 7; не згоден – 6; скоріше не згоден – 5; не маю певної думки – 4; скоріше згоден – 3; згоден – 2; абсолютно згоден – 1.

Всі значення додають і ділять на 15 (тобто вираховується середнє арифметичне).

Ще однією відомою методикою є шкала організаційної лояльності (Organizational Commitment Scale - OCS-93), розроблена Дж. Мейером і Н. Аллен, яка базується на моделі організаційної лояльності. Відповідно до зазначеної моделі є три компоненти лояльності, що дозволяють пояснити зв'язки між працівником і організацією, завдяки яким знижується ймовірність добровільного звільнення працівника з організації:

– емоційна прихильність до організації - «афективна лояльність»;

– усвідомлення витрат, пов'язаних зі звільненням з організації - «продовжена лояльність»;

– відчуття зобов'язань перед організацією - «нормативна лояльність».

Підшкала афективної (емоційної) лояльності (Affective Commitment Scale - ACS) вимірює ступінь ідентифікації, залученості і емоційної прихильності працівника до організації. Підшкала продовженої лояльності (Continuous Commitment Scale - CCS) - ступінь усвідомлення працівником того, як витрати, що асоціюються з припиненням зв’язків з організацією, пов'язують його з

організацією. Підшкала нормативної лояльності (Normative Commitment Scale - NCS) - ступінь відчуття працівником зобов'язань перед організацією. На думку авторів методики, вимірювання кожного компонента є незалежним і відносно не пов'язаним між собою.

Анкета-опитувальник Дж. Мейера і Н. Аллен передбачає визначення опитуваним ступеня його згоди або незгоди з кожним твердженням цифрою від 1 до 7 (де 1 - абсолютно не згоден, а 7 - повністю згоден):

1. Я був би радий до виходу на пенсію працювати в нинішній організації.

2. Зараз я бачу необхідність продовжувати працювати в цій організації.

3. Я не відчуваю ніяких зобов'язань щодо цієї організації.

4. Я сприймаю проблеми своєї організації як свої власні.

5. Зараз мені було б важко піти з нинішньої організації, навіть якщо б я цього хотів.

6. Зараз я не відчуваю вправі залишити свою організацію, навіть якби це було вигідно для мене.

7. У мене немає відчуття приналежності до моєї організації.

8. Якщо я зараз піду з організації, в моєму житті багато чого зруйнується.

9. Якби я зараз звільнився зі своєї організації, то почувався б винним.

10. Я не відчуваю теплих почуттів по відношенню до моєї організації.

11. Мені здається, що у мене дуже мало перспектив працевлаштування, щоб розглядати можливість звільнення з нинішньої організації.

12. Ця організація заслуговує моєї відданості.

13. Я не відчуваю себе членом колективу в моїй організації.

14. Я розглядав би можливість іншого місця роботи, якби не отримував так багато від своєї організації.

15. Зараз було б неправильно піти з цієї організації, оскільки я маю зобов'язання перед іншими людьми.

16. Моя організація багато значить для мене особисто.

17. Я втратив би багато можливостей, звільнившись зі своєї організації.

18. Я багато чим зобов'язаний нинішній організації.

Результати виявляють три типи прихильності (за вказаними вище підшкалами).

Для кожної підшкали потрібно додати оцінки відповідно до ключа і знайти середнє арифметичне. Оцінки за твердженнями, зазначеним буквою R, інвертується, тобто замість 7 ставимо 1, замість 6 - 2, 5 - 3 і так далі.

Для підшкали афективної (емоційної) лояльності сумуємо оцінки за номерами питань: 1 + 4 + 7R + 10R + 13R + 16. Для підшкали продовженої лояльності: 2 + 5 + 8 + 11 + 14 + 17. Для підшкали нормативної лояльності: 3R + 6 + 9 + 12 + 15 + 18 [1].

На основі аналізу різних підходів до визначення і вивчення лояльності, а також різних моделей лояльності В. Доміняк виділив основні принципи, що лежать в основі розуміння організаційної лояльності, серед них принципи:

– когнітивної відповідності: поведінка пересоналу і його установки що до організації в процесі узгодження взаємно зміцнюються;

– зниження витрат, заснований на усвідомленні працівником своїх інвестицій в організацію і можливих альтернатив. Зміна місця праці означатиме відмову від існуючих вкладень і переваг і потребу у повторному їх накопиченні.

– взаємних переваг як для працівника, так і для організації;

– особистого досвіду, що базується на когнітивній та емоційній оцінці особистого досвіду за такими критеріями як справедливість і підтримка в організації, власна компетентність і значущість;

– виконання зобов'язань по відношенню до організації, які розглядаються як продукт соціалізації (особисті цінності) і результат інвестицій в працівника (обов’язок);

– задоволення потреб персоналу;

– поділяння і / або схвального сприйняття цілей і цінностей організації.

Науковець наголошує, що організаційна лояльність розглядається як стійке утворення і багато в чому визначається взаємністю: тобто не тільки ставленням працівника до організації, але й навпаки [26].

Російська дослідниця С. Баранська [3] пропонує оцінювати лояльність персоналу за підходом, відповідно до якого розглянуто таку типологію лояльності персоналу:

– організаційна лояльність;

– професійна лояльність;

– лояльність до праці .

Організаційну лояльність розглядають у двох аспектах:

по-перше, як основу благонадійності і безпеки працівників організації (пов'язану з прийняттям і підпорядкуванням персоналу нормам і правилам організації та визнання їх своїми особистими, відсутністю саботажу і проявів нелояльної поведінки, зростання толерантності та зменшення байдужості);

по-друге, як емоційний зв'язок, доброзичливе ставлення і прихильність персоналу до своєї організації. У цьому випадку акцентується на появі у працівників емоцій і почуттів щодо організації: прояви інтересу і занепокоєння станом справ організації, гордість з приводу своєї причетності до колективу та участі у вирішенні організаційних проблем.

Професійна лояльність пов’язана з можливостями професійної самореалізації працівників усередині організації, побудови кар'єри в рамках своєї спеціалізації. Лояльність професії пов'язана з ідентифікацією працівника зі своєю професійною діяльністю, залученістю в неї, прагнення до професійного самовдосконалення, майстерності. При цьому роль власне організації має другорядне значення у стосунку до характеру фахової діяльності.

Лояльність праці базується на сприйнятті трудової діяльності як ключового поняття з особливою цінністю для працівника. Її розглядають також як мотивацію до праці і часто прирівнюють до поняття працьовитості. Для багатьох людей праця, становлячи цінність сама по собі як діяльність, спрямована на суспільне і особисте благо, здатна впливати на ставлення і до організації (як місця трудової активності), і до професії (як спеціалізації праці).

Опитувальник, складений відповідно до зазначеної методики, складається з двох частин по 25 тверджень, що відносяться до згаданих трьох типів лояльності.

Особливістю опитувальника є те, що в першій його частині респондентам пропонують оцінити твердження за 5-бальною шкалою від 1 - «абсолютно не згоден» до 5 - «повністю згоден» з точки зору ставлення до своєї нинішньої організації. Натомість у другій частині анкети ці ж твердження просять оцінити щодо гіпотетичної бажаної організації. Твердження опитувальника сформульовані від третьої особи, щоб підвищити достовірність відповідей та знизити кількість відповідей, які схвалює соціальне середовище опитуваного.

Шкала «Організаційна лояльність» представлена в опитувальнику у вигляді 15 тверджень, що відносяться до трьох субшкал: «гордість за організацію» (твердження № 1, 4, 9, 12, 21); «залучення в організаційні справи» (твердження № 8, 11, 16, 19, 20); «нелояльна поведінка» (твердження № 2, 6, 14, 18, 22.

За шкалами «Лояльність професії» та «Лояльність праці» опитувальник містить по п'ять тверджень відповідно: № 3, 7, 15, 23, 25 та № 5, 10, 13, 17, 24.

Перелік тверджень:

1. Працівники переконані, що працюють в чудовій організації.

2. Будь-який з співробітників з таким же успіхом працював би і в іншій організації.

3. Працівники організації прагнуть удосконалювати свої професійні навички.

4. Для персоналу є очевидною перевага їхньої організації над іншими.

5. Робота є частиною найважливіших речей, які трапляються в житті працівників.

6. Будь-який із співробітників легко залишить роботу в організації за умови наявності вигіднішої пропозиції праці.

7. Професійне зростання - одна з найважливіших цілей роботи персоналу організації.

8. Працівники готові взяти на себе додаткове навантаження задля потреб організації.

9. Репутація організації є бездоганною в очах персоналу.

10. Робота – це те, чим співробітник має займатися більшість свого часу.

11. Працівники відчувають особисту відповідальність за успіхи і провали організації.

12. Якість роботи організації є предметом гордості її співробітників.

13. Щастя в житті персоналу пов’язане, переважно, з роботою.

14. Єдине, що стримує працівників в організації – це складнощі в пошуку нового робочого місця.

15. Співробітники віддають перевагу працювати виключно у своїй професійній сфері.

16. Персонал сприймає проблеми організації як свої особисті.

17. Працівники вважають працю центральним моментом свого життя.

18. Багато робітників вважають, що їхня організація не варта відданості.

19. Працівники активно допомагають організації у вирішенні її проблем.

20. Персонал прагне працювати з повною самовіддачею.

21. Співробітники з гордістю повідомляють, що є частиною своєї організації.

22. У працівників немає відчуття будь-яких зобов'язань перед своєю організацією.

23. Працівники організації відчувають задоволення від роботи за професією.

24. Життя співробітників є найбільш цінним для організації, коли вони заглиблені у роботу.

25. Можливість використовувати свої професійні навички - головне в роботі персоналу.

Твердження № 2, 6, 14, 18, 22 (шкала «Нелояльна поведінка») опитувальника представлені у вигляді інверсій; бали за цими твердженнями зараховуються зі зворотним ключем. У шкалі «Організаційна лояльність» загальний показник дорівнює сумі балів субшкал «Гордість за організацію» (твердження « 1, 4, 9, 12, 21), «Залучення в справи організації» (твердження № 8, 11, 16, 19 , 20), «Нелояльна поведінка» (твердження № 2, 6, 14, 18, 32). Загальний показник шкали «Професійна лояльність» дорівнює сумі балів тверджень № 3, 7, 15, 23, 25, помножених на 3, шкали «Лояльність праці» - сумі балів тверджень № 5, 10, 13, 17, 24, помножених на 3 [3].

2.3. Методика оцінювання лояльності персоналу з інформаційної безпеки

Як відзначалося у першому розділі для забезпечення інформаційної безпеки важливим є здійснення ефективної та послідовної роботи з персоналом за трьома напрямами: належна підготовка працівників, висока мотивація та якісний контроль їхньої праці з боку організації.

Відповідно, оцінювання лояльності персоналу має складатися з трьох блоків:

– оцінювання підготовки у сфері інформаційної безпеки (навчання, підвищення кваліфікації, забезпечення обізнаності з питань інформаційної безпеки);

– оцінювання організаційної прихильності, яке може здійснюватися з використанням однієї з моделей, розглянутих у пункті 2.2. Водночас, бажаним є використання методів оцінювання як суб'єктивних чинників по відношенню до працівника, так і об'єктивних чинників, що впливають на нього або його характеризують;

– оцінювання активності персоналу в інформаційній системі організації.

З цією метою варто використати модель оцінки надійності персоналу в забезпеченні інформаційної безпеки, розроблену дослідником М. Бойдалом, яка представлена на Рис. 2.2. [6].

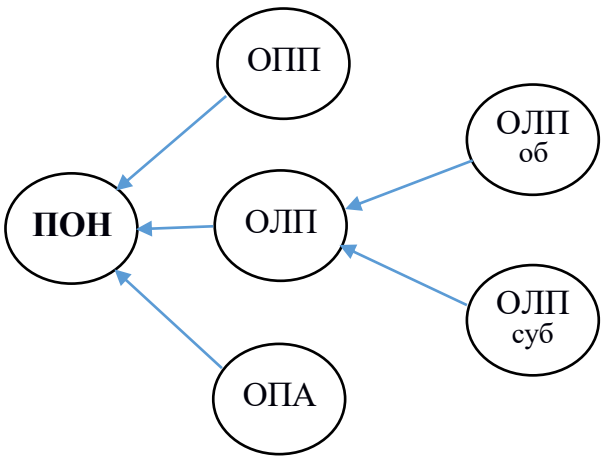

Рис.2.2. Модель оцінювання надійності і лояльності персоналу

Розглянемо її основні елементи.

Підсумкова оцінка надійності працівника (ПОН), яку отримують в результаті оцінювання працівника за трьома зазначеними вище блоками:

1. Оцінка рівня підготовки персоналу в області забезпечення інформаційної безпеки (ОПП), яка проводиться у формі атестації. Форми атестації (письмовий тест, практичні завдання, співбесіда, комбінація різних підходів) обирають відповідно до специфіки організації та контролю процесу навчання персоналу з питань інформаційної безпеки.

Оцінювання рівня підготовки працівника здійснюється за результатами його атестації в рамках навчання політиці інформаційної безпеки. Для розрахунку результатів атестації в розробленій моделі необхідно:

– формалізувати результати атестації (усі результати атестації, які будуть враховуватися при оцінюванні, мають бути приведені в єдиний числовий формат;

– розробити модель, яка забезпечить підсумкову оцінку рівня підготовки працівника за результатами атестації;

– привести чисельні значення оцінок підготовки персоналу до вигляду придатного для обліку в розробленій моделі.

2. Оцінка рівня організаційної лояльності працівника (ОЛП), яка розраховується на основі двох оцінок: за об'єктивними і суб'єктивними чинниками.

Оцінка рівня організаційної лояльності співробітника на підставі об'єктивних факторів (ОЛПоб) передбачає аналіз впливу зовнішніх для особи чинників, що впливають на її організаційну лояльність або дозволяють оцінити її. У рамках оцінки організаційної лояльності враховують дві групи об’єктивних чинників. Перша група включає чинники, що впливають на працівника: оплата праці (відносна заробітна плата по організації та по галузі), міжнаціональна напруга в колективі, національний склад підрозділу й організації загалом. До другої групи відносять чинники, які характеризують діяльність працівника і його ставлення до організації: наявність заохочень та стягнень (абсолютний та відносний рейтинг працівника), залученість в роботу організації, стаж роботи та зміни посади тощо.

Оцінка рівня організаційної лояльності співробітника на підставі суб'єктивних чинників (ОЛПсуб) включає оцінку чинників, які характеризують ставлення співробітника до організації, колег і керівників.

Для їх оцінки використовують одну з моделей оцінки організаційної лояльності, представлених у п.2.2.

3. Оцінку підозрілої активності (ОПА), здійснюють шляхом врахування специфічних чинників, які можуть бути ознакою діяльності персоналу, спрямованої проти організації.

До таких чинників відносять обсяг обміну інформацією з глобальною мережею Інтернет, локальною корпоративною мережею, знімними носіями інформації. Так, тривожним сигналом може служити різка зміна обсягу такого обміну інформацією. Для обліку обсягу інформаційного обміну персоналу з мережею Інтернет в моделі застосовують параметр відносного середнього обсягу інформаційного обміну.

Про деструктивну діяльність працівника може свідчити також зміна кількості запитів в локальній мережі, особливо за темами, що не стосуються до професійних або службових обов'язків працівника. Водночас, при оцінці рівня інформаційного обміну важливо враховувати специфіку роботи конкретного працівника, що може значно впливати на обсяги його інформаційного обміну.

Враховуючи той факт, що крім навмисної шкідливої діяльності персоналу щодо організації можливим є також нанесення збитку інформаційної системі внаслідок випадкових помилок, рекомендують розглядати у якості специфічних факторів показник кількості і тяжкості помилок, скоєних співробітником під час професійної діяльності.

Коефіцієнти Nопп, Nолп, Nпа описують внесок кожної групи чинників у підсумкову оцінку працівника. Коефіцієнти Nоб і Nсуб представляють роль оцінок об'єктивних і суб'єктивних факторів у загальній оцінці організаційної лояльності співробітника [6].

Розроблена модель дозволяє проводити багатофакторне, різнопланове оцінювання лояльності персоналу в контексті забезпечення інформаційної

безпеки організації. Модель враховує рівень підготовки персоналу, компенсуючи недоліки психологічних моделей оцінки організаційної лояльності, і бере до уваги специфічні ознаки, які вказують на підозрілу діяльність працівників для здійснення шкідливих інсайдерських дій або використання службового положення з деструктивною метою.

Відповідно до розглянутої моделі, оцінювання лояльності персоналу в забезпеченні інформаційної безпеки організації здійснюється у кілька етапів, схема яких представлена на Рис.2.3.

Розглянемо сутність кожного з етапів.

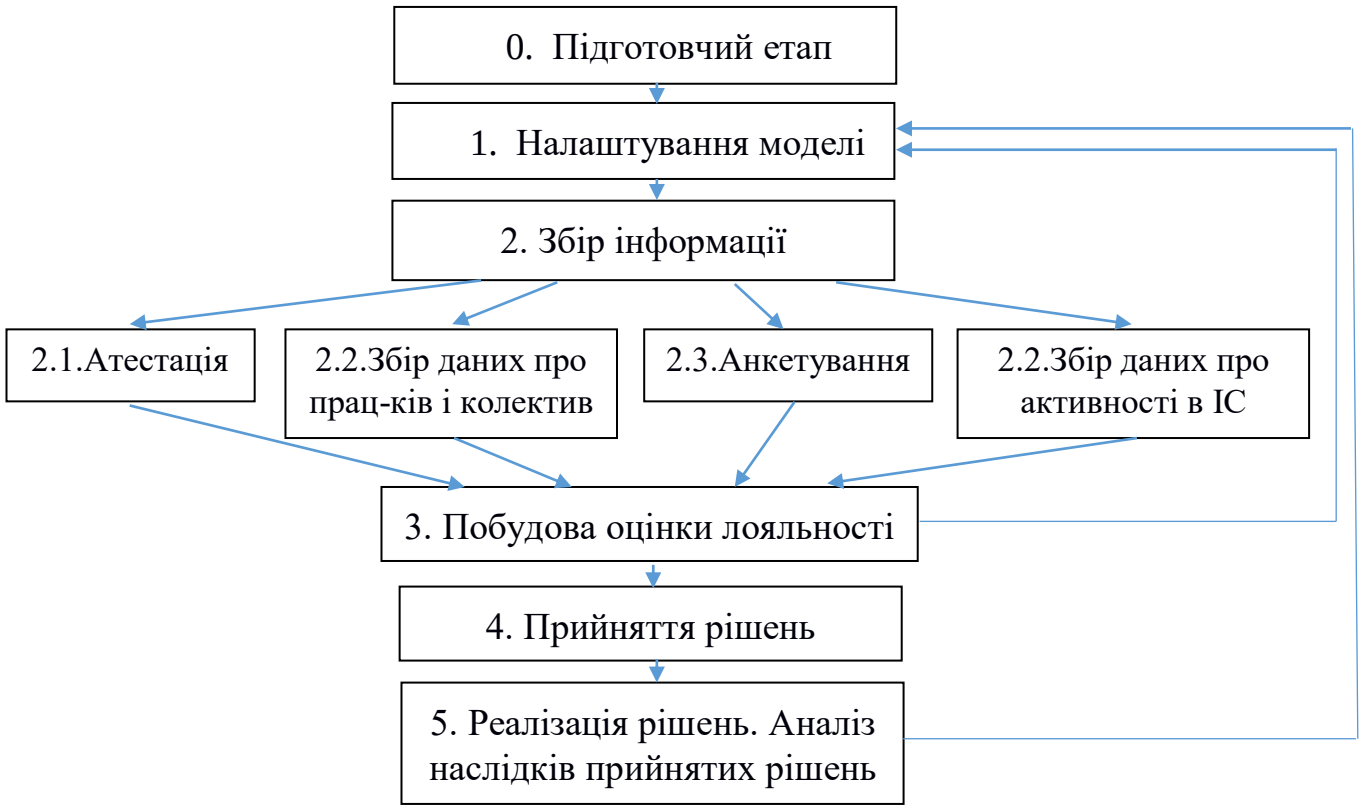

Рис.2.3. Схема проведення оцінки персоналу

Підготовчий етап. Здійснюється збір і аналіз інформації про організацію та персонал для подальшої коригування моделі оцінювання з урахуванням встановлених особливостей організації.

I. Етап налаштування, а за необхідності й модифікації моделі на основі отриманих даних про організацію та її персонал.

II. Етап збирання інформації про персонал організації з метою подальшого оцінювання його лояльності. Цей етап включає: атестацію персоналу для

визначення рівня підготовки з питань інформаційної безпеки; збирання даних про колектив і співробітників для побудови оцінки організаційної лояльності (вибір інформації, яка буде використана в процесі оцінювання, здійснюється з масиву статистичної інформації про персонал, зібраної за попередній період); проведення анкетування працівників для побудови оцінки організаційної лояльності; збір інформації про потенційно шкідливі дії співробітників.

III. Етап побудови оцінки лояльності. На третьому етапі здійснюють розрахунок оцінок лояльності працівників, а за потреби можливе додаткове налаштування моделі оцінки. У випадку внесення значних коректив процес оцінювання запускають з початку.

ІУ. *Етап прийняття рішень за результатами оцінювання* щодо заходів підвищення рівня лояльності як персоналу організації загалом, так окремих ненадійних співробітників.

У. *Етап реалізації рішень за результатами оцінювання*. На останньому етапі проводять впровадження прийнятих рішень, а також збір і аналіз інформації про зміну ситуації в організації в результаті їх реалізації. Далі процес оцінювання лояльності персоналу продовжується з першого етапу циклу [6].

Таким чином, представлена методика оцінювання лояльності персоналу включає в себе врахування й оцінювання низки чинників, які свідчать про рівень компетентності працівників у сфері інформаційної безпеки, їх загальнотрудову та фахову діяльність і ставлення до своєї організації, що відіграє важливу роль для виявлення загроз інформаційній безпеці.

Застосування даної методики на практиці має носити систематичний і регулярний характер. Конкретні періоди проведення опитувань і збору контрольних даних визначають відповідно до специфіки організації, пам’ятаючи, що вони не мають відбуватися занадто рідко, щоб отримані результати можна було ефективно застосовувати для підвищення лояльності персоналу, а також не дуже часто, щоб накопичувався достатній обсяг потрібної для оцінювання інформації, а тестування й перевірки не викликали зайвих негативних емоцій у працівників.

Висновки до другого розділу

Як показало дослідження, ключового значення для забезпечення інформаційної безпеки організації у сучасних умовах набуває формування й утримання високого рівня організаційної лояльності персоналу.

Аналіз наукової літератури показав наявність двох основних підходів до розуміння лояльності персоналу: поведінкового та установочного. Відповідно до поведінкового підходу лояльність розглядають як джерело організаційної безпеки або поведінку на благо компанії, в якій співробітники дотримуються правил і норм, обережно ставляться до свого робочого місця. Прихильники установочного підходу під лояльністю розуміють емоційну прихильність персоналу до організації, яка формується через попередній досвід роботи, особистісні характеристики співробітника і позитивне сприйняття організації. Також виділяють раціональну, нормативну, емоційну і вимушену лояльність.

Вивчення феномену лояльності персоналу засвідчило існування різних наукових підходів до її оцінювання, з яких розглянуто одномірну модель Л. Портера, трикомпонентну модель Дж. Мейера і Н. Аллен, а також модель С. Баранської, відповідно до якої організаційну лояльність розглянуто як поєднання організаційної, професійної лояльності та лояльності до праці.

Для оцінювання лояльності персоналу з інформаційної безпеки доцільно використовувати модель оцінки лояльності (надійності) персоналу, згідно з якою підсумкова оцінка лояльності працівника є сумою оцінок 1) рівня підготовки персоналу з інформаційної безпеки, 2) рівня організаційної лояльності працівника та 3) підозрілої активності персоналу, спрямованої проти організації.

Розглянута схема оцінювання лояльності персоналу включає підготовчий етап, етап налаштування, збирання інформації, побудови оцінки лояльності, а також етапи прийняття рішень за результатами оцінювання та їх реалізації. Дана модель дозволяє проводити багатофакторне оцінювання лояльності персоналу в контексті забезпечення інформаційної безпеки організації.

РОЗДІЛ 3
МЕТОДИ СТИМУЛЮВАННЯ Й МОТИВАЦІЇ У ФОРМУВАННІ ЛОЯЛЬНОСТІ ПЕРСОНАЛУ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

З огляду на наявність великого різноманіття загроз інформаційній безпеці організація, яка прагне зберегти конкурентну позицію на ринку та досягти успіхів у розвитку власного бізнесу, має забезпечити реалізацію комплексу заходів з управління персоналом. Відповідно до розглянутого вище підходу основними напрямами роботи з персоналом у сфері забезпечення інформаційної безпеки є навчання, мотивація та контроль.

Водночас, як свідчить практика, саме заходи мотивування працівників, які на сьогодні є основною передумовою створення й підтримки лояльного кадрового потенціалу організації, показують високу результативність у запобіганні та протидії порушенням інформаційної безпеки з вини персоналу.

Аналіз наукових джерел та результатів досліджень персоналу засвідчив, що основними причинами високої мотивації працівників є як чинники матеріального характеру (справедлива заробітна плата, наявність необхідного матеріального забезпечення для здійснення професійної діяльності, можливості для кар'єрного розвитку), так і нематеріальні мотиви (любов до своєї роботи, хороші відносини з колегами, справедлива оцінка праці з боку керівництва, усвідомлення власної ролі у досягненні місії організації тощо).

3.1. Матеріальне стимулювання персоналу: досвід європейських країн

За оцінкою економістів, понад 60% приросту продуктивності праці забезпечують здобутки технічного прогресу. Саме впровадження інновацій, інтенсифікація виробництва і, як результат, підвищення ефективності виробництва і продуктивності праці призводять до зростання прибутків. Водночас, важливим чинником підвищення продуктивності праці, який, до того ж не вимагає великих капіталовкладень є мотивація праці [17].

Науковці давно встановили, якими є найбільш дієві засоби матеріального стимулювання персоналу. Серед них, насамперед заробітна плата, а також різні додаткові фінансові винагороди. Узагальнений перелік таких засобів представлений на Рис. 3.1.

Рис. 3.1. Засоби матеріального стимулювання персоналу

Варто відзначити, що у сучасних умовах для фахівців сфери IT та інформаційної безпеки засоби матеріального стимулювання відіграють провідну роль. З огляду на велику потребу в технічних кадрах, розміри різних видів матеріальної винагороди для цієї категорії працівників є значно вищими, ніж у більшості інших сфер.

У розвинених країнах накопичений великий досвід застосування найрізноманітніших систем оплати праці. Системи окремих країн Європи характеризуються такими рисами. Так, для Швеції характерна солідарна система заробітної плати; у Німеччині переважають додаткові методи стимулюванням зростання продуктивності, а також використання державних гарантій; Великобританії притаманний підхід, відповідно до якого оплата праці здійснюється за індивідуальними контрактами; у Франції діє принцип індивідуалізації заробітної плати; в Нідерландах віддають перевагу вилаті пільг і компенсацій; в Італії виплачують колективні й індивідуальні надбавки до галузевої тарифної ставки і надбавки в зв'язку зі зростанням вартості життя. Одночасно у всіх системах оплати праці спостерігається загальна націленість на підвищення ефективності виробництва.

Основні характеристики моделей матеріального стимулювання праці в країнах Європи представлено на Рис. 3.2.

Розглянемо концепції мотивації персоналу, які застосовуються в країнах Західної Європи.

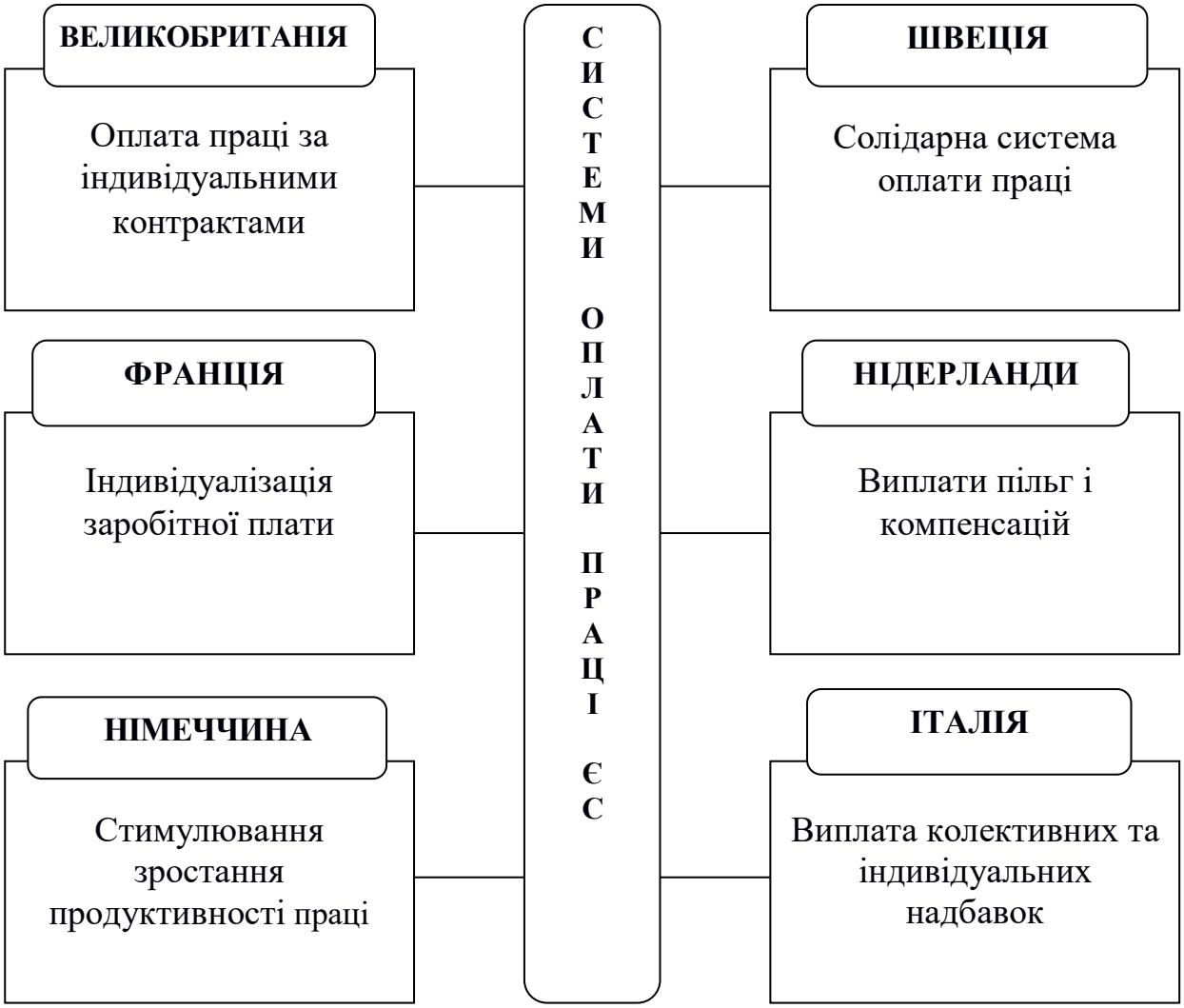

Рис. 3.2. Системи оплати праці в країнах Європи.

Британська модель стимулювання персоналу

Британська модель мотивації праці включає використання двох систем оплати праці: грошової та акціонерної, кожна з яких сповідує принцип залежності зарплати персоналу від загального прибутку підприємства. Також поширеною є схема «рухливої» зарплати, яка змінюється відповідно до зміни рівня доходів компанії. Норма щодо обов'язку компанії виплачувати працівникам частку прибутку фіксується в колективному договорі між працедавцями і працівниками.

Відповідно до пайової моделі участі трудового колективу в капіталі компанії, яка також застосовується на практиці, працівники викуповують часку акцій і отримують дохід по акціях у вигляді відсотків або долю прибутку. У такому випадку сукупний дохід працівника становить суму у розмірі посадового окладу, премії відповідно до рівня ефективності праці та відсотків від прибутку компанії в залежності від розміру вкладеного капіталу. Відсоток прибутку працівника у прибутку компанії становить в межах 3-8% окладу, а заробітна плата є на 4% нижчою, ніж у компаніях з іншим підходом до оплати праці [16].

Загалом впровадження такої моделі мотивації мало наслідком збільшення кількості робочих місць у Великобританії на 13% [23].

Пайова участь персоналу в прибутках компанії сприяє формуванню високої вмотивованості працівників від найнижчого до найвищого рангу щодо підвищення результативності трудової діяльності, посилення непідробного інтересу до розвитку бізнесу і створення сприятливого психологічного клімату в колективі. Для працедавців це також вигідно, оскільки дозволяє підвищити оплату праці, не збільшуючи виробничих витрат.

Німецька модель мотивації персоналу

Сучасна модель мотивації працівників, поширена в Німеччині, базується на понятті економічної свободи: врахування суспільних інтересів і визначення ролі особистості в економічній системі. Тобто, працівник, усвідомлюючи і реалізуючи свої власні інтереси, пов’язані з трудовою діяльністю, водночас несе особисту відповідальність за свою працю перед суспільством.

Зазначений економічний підхід передбачає створення рівних умов життя для кожного жителя Німеччини, незалежно від його можливостей і здатності виживати в ринкових умовах. Завдяки такому підходу корпоративні моделі мотивації поєднуються з державною системою соціальної справедливості, внаслідок чого створюються умови, за яких будь-який працівник не боїться залишитися без засобів до існування й постійного доходу.

Фахівці вважають німецьку модель, яка поєднує державні соціальні гарантії і корпоративні засоби стимулювання праці, оптимальним зразком гармонійної

реалізації економічних теорій. Також у структурі заробітної плати німці роблять значний акцент на отриманні додаткової платні за суміщення професій і ширшу відповідальність, наприклад за організацію роботи та її якість, забезпечення функціонування обладнання, високий рівень психологічної напруги тощо.

Французька модель мотивації персоналу

У Франції мотивація персоналу базується на стратегічному плануванні, принципах вільної конкуренції та лояльному оподаткуванні. Французи негативно ставляться до понаднормової роботи. Так, стандартний робочий тиждень у Франції на п'ять годин коротше, ніж у більшості країн Європейського Союзу, тобто становить 35 годин замість 40.

Нормою вважається отримання працівником додаткових «бонусів» від роботодавця: оплати курсів підвищення кваліфікації та корпоративної медичної страховки, допомоги в погашенні іпотеки, фінансування обідів за рахунок компанії тощо. Найкращим стимулом є гнучкий графік або дистанційна робота, яка відкидає потребу бути присутнім на робочому місці.

Система оплати праці у Франції включає два напрямки:

- індексацію зарплат в залежності від зростання цін, яка закріплюється в колективних договорах і контролюється профспілками, та
- індивідуалізацію оплати праці відповідно до освіти, кваліфікації, якості роботи, рівня мобільності співробітника.

Нарахування індивідуалізованих зарплат відбувається за трьома схемами: по-перше, встановлення розміру зарплати в залежності від кількості відпрацьованого часу, участі в житті компанії та ефективності праці працівника; по-друге, чітке встановлення розміру окладу та премії, величина яких відрізняється в залежності від продуктивності праці; по-третє, застосування таких форм як участь в прибутку, покупка акцій підприємства, виплата премій за результатами продажів. Водночас мінімальна зарплата індексується як і раніше.

У Франції в рамках індивідуалістичного підходу представлені такі форми оплати праці, які можуть поєднуватися:

- оплата за індивідуальний виробіток;

- зарплата, що містить гарантований мінімум (зазвичай 80%) і змінну частину (близько 20%, але може сягати від 10 до 50%);

- заробітна плата з фіксованою частиною у залежності від кваліфікації, а змінною - від результатів роботи колективу і від успіхів самого працівника [17].

Така форма індивідуалізації заробітної плати може використовувати всі види додаткових надбавок, наприклад, виплати натуральними товарами чи придбання акцій підприємства. За умови індивідуалізації заробітної плати її розмір залежить від особистого внеску працівника у виробництво, а не від його статусу.

Перевага французької системи мотивації в частині, яка стимулює підвищення продуктивності і якості праці, полягає в «саморегуляції» розміру заробітної плати відповідно до фінансового стану підприємства.

Шведська модель мотивації персоналу

Своя система стимулювання персоналу сформована у Швеції, де широко використовують методи преміювання і заохочення успішної виробничої діяльності на рівні колективу. У зв'язку з цим змінна частина заробітної плати, пов'язана з груповими результатами діяльності, збільшується, а відрядні форми оплати втрачають своє значення.

Контроль за дотриманням вимог до оплати праці здійснюють профспілки Швеції. Вони дбають, щоб під час переукладання колективних трудових договорів працедавці дотримувалися двох ключових принципів: рівність зарплат на аналогічних посадах і скорочення розриву між максимальною і мінімальною зарплатою.

Так звана солідарна система оплати праці у Швеції покликана вирішити комплекс завдань:

- стимулювати оновлення матеріально-технологічної бази і впровадження на виробництві інновацій;
- забезпечити соціальну підтримку незахищених верств населення;
- стимулювати ринкову конкуренцію;
- забезпечити рівність зарплат за рівноцінну працю [23].

Завдяки активній позиції профспілок Швеції власники компаній з низьким прибутком не можуть занижувати зарплати персоналу, відповідно вони змушені підвищувати рентабельність підприємств шляхом модернізації виробництва.

Важливим для забезпечення соціальної справедливості є дотримання в Швеції принципу скорочення розриву між високооплачуваними і низькооплачуваними фахівцями, який реалізується у вигляді системи однорівневого підвищення оплати праці. Такий підхід сприяє усередненню розміру зарплат, внаслідок чого мінімальні зарплати підвищуються, а максимальні - стримуються. При переукладання колективних трудових договорів профспілки забезпечують нормативне закріплення зобов'язань працедавців щодо прискорення зростання заробітної плати низькооплачуваних працівників. Подібна тактика спрямована на розвиток висококваліфікованих фахівців у всіх сферах економіки.

Голландська модель мотивації персоналу

Основою матеріального стимулювання в Нідерландах є пільги і компенсації. У випадку, коли працівник відлучається з роботи для вирішення особистих питань (відвідати лікаря або сходити в банк), працедавець платить за цей час в повному обсязі. Якщо працівник хворіє і залишається на лікарняному більше трьох місяців, власник фірми надає йому в якості компенсації додатковий день до оплачуваної відпустки.

Також у формуванні заробітної плати в багатьох європейських країнах часто використовують і систему заслуг. Ця система оцінювання праці спрямована на встановлення диференційованої заробітної плати працівникам однакової кваліфікації, але з різними показниками якості роботи. Чинники, за якими оцінюють працівника, можуть бути як виробничими, так і особистісними. Методи оцінки заслуг працівників різноманітні: анкетування, рейтингова і експертна оцінка, віднесення працівників за результатами оцінки їх роботи до окремих груп.

Загалом багато розвинених країн поступово відмовляються від традиційних форм оплати праці на основі оцінювання індивідуальних результатів праці, оскільки складно виміряти особистий внесок окремого робітника в загальний

виробничий процес. Крім того, сьогодні на перший план виходять завдання щодо стимулювання кооперації всередині трудового колективу і формування колективної відповідальності.

Аналіз методів матеріального стимулювання, якими користуються вітчизняні підприємства й організації, показав, що вони орієнтуються в більшій мірі на результативність праці, при цьому ігнорують якість роботи, кваліфікацію та професійну майстерність працівників. При цьому майже не застосовується участь у прибутках та капіталі, що є дуже популярним методом в інших країнах [22].

3.2. Методи нематеріальної мотивації працівників

Крім матеріального стимулювання обов'язковим елементом забезпечення ефективної роботи персоналу та формування його лояльності організації є нематеріальна мотивація.

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 [31]. Загалом існуючі методи нематеріальної мотивації персоналу поділяють на зовнішні і внутрішні (Таблиця 3.1.).

Відповідно до теорії Маслоу, нижчі потреби людини задовольняє матеріальна мотивація [13], яка є короткотерміновою. Отже, підвищення заробітної плати або інших грошових заохочень лише на короткий час може підвищити ефективність праці персоналу. У той час, як нематеріальна мотивація спрямована на задоволення вищих потреб особи (прагнення до професійного й особистісного розвитку, реалізації потенціалу, самоповаги і поваги з боку оточуючих) і здатна спонукати працівників до якіснішої й результативнішої роботи упродовж тривалого часу.

Таблиця 3.1.

Засоби мотивації персоналу

Зовнішні	*Внутрішні*
Визнання, похвала, публікації про авторів і створені ними винаходи у ЗМІ	Самостійність у роботі (автономія)
Нагороди: грамоти, значки, медалі, інші відзнаки, подарунки, пільгові путівки на відпочинок	Досягнення в роботі
Публічне присудження спеціальних почесних титулів і звань	Особисте та професійне зростання
Надання більш поважної назви посаді	Змістовність і значимість роботи
Членство у винахідницьких клубів, наукових товариствах (за кошти організації)	Більша відповідальність
Направлення за рахунок організації 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	

Правильне використання методів нематеріальної мотивації позитивно впливає на:

- якість роботи кожного співробітника і відділу в цілому;
- рівень продуктивності праці в компанії;
- рентабельність компанії;
- розвиток і успіх компанії.

Відповідно, від вірно обраної і реалізованої програми нематеріальної мотивації залежить не тільки продуктивність однієї людини, але й усієї компанії загалом, що безпосередньо впливає і на рентабельність та стійкість бізнесу.

Для успішної реалізації програми нематеріальної мотивації необхідним є дотримання таких ключових принципів:

- формування здорової конкурентної робочої атмосфери, в якій водночас працівники почувають себе комфортно;

- створення механізмів для набуття і закріплення професійних знань, умінь і навичок у практичний спосіб, а також підтримання в персоналу бажання їх отримання;

- постійне й обґрунтоване підвищення кваліфікації працівників, створення умов для творчої самореалізації.

На думку фахівців, до основних видів нематеріальної мотивації відносяться:

1. Соціальна мотивація. Найпростішим прикладом такої мотивації є медична страховка, або періодичні безкоштовні курси з підвищення кваліфікації, навчальні курси. Також соціальної мотивацією може стати і відкритість, прозорість в питанні кар'єрного зростання, тобто якщо начальник конкретно і ясно пояснює за які заслуги, протягом якого періоду часу і інші деталі можливості зростання по кар'єрних сходах, тоді працівник виявляється, дійсно, готовий і мотивувати виконувати ці вимоги, тим самим підвищуючи продуктивність і якість роботи.

2. Психологічна мотивація. Цей вже більш тонка і обережна робота з працівниками, яка дає не менш відчутні плоди. Основа психологічної мотивації - це спілкування. Причому важливо розуміти, що це не просто спілкування на рівних, а спілкування, побудоване на взаємній повазі, на необхідної субординації між керівництвом і підлеглими. Важливо, щоб керівник розумів співробітників і враховував особисті потреби кожного з них, йшов на зустріч в деяких особистих питаннях, але при цьому, не забував про необхідної дисципліни і дистанції. Добре, якщо керівник виявиться здатним мотивувати особистим прикладом. Очевидний плюс такої роботи - ніяких матеріальних витрат, зате психологічно керівнику доведеться викладатися повністю.

3. Моральна мотивація. Важливо вміти відрізняти мотивацію психологічну від моральної. Так, працівники мають усвідомлювати й відчувати моральне задоволення від того, що їхня робота належним чином оцінена. Досягти цього можна при допомоги різних заохочень за досягнення тих чи інших успіхів. Причому, як заохочення можна використовувати як матеріальні блага, так і нематеріальні за умови чіткого розуміння персоналом підстав для заохочення.

Одним із прикладів моральної мотивації є публічне визнання заслуг працівника, зокрема вручення грамот, відзнак на офіційних зборах колективу.

4. Організаційна мотивація. Має на меті забезпечення комфортного перебування працівників на роботі шляхом належної організації робочого місця, місць відпочинку та харчування, спортивних залів та приміщень для роботи із психологом.

Незважаючи на додаткові витрати, заходи організаційної мотивації мають великий позитивний ефект, який проявляється в покращенні атмосфери робочого простору [13].

Це основні способи нематеріальної мотивації, існують також додаткові [9]:

- Постановка загальної мети, тобто формування розуміння місії компанії;

- Наставництво. Досить непоганий прийом для формування мотивації, його плюс в тому, що працює він в обидві сторони. І на новачка, над яким здійснюється наставництво, так як він відчуває підтримку; і на людину, який сам здійснює наставництво, так як це накладає на нього деяку відповідальність, людина відчуває себе більш значущим;

- Додаткова відповідальність і самостійність. якщо дозволити співробітнику вирішувати деякі питання особисто, без узгодження з начальством і наділяти НЕ об'ємної, але додаткової відповідальною роботою, то ефективність такого працівника зросте.

- Горизонтальне зростання. Добре зрозуміло, що таке кар'єрне зростання, це підвищення по кар'єрі від рядового співробітника до директора. Однак в компанії можна використовувати ротації, при цьому змінюючи значимість співробітника лише всередині групи, наприклад - менеджер, старший менеджер, старший групи. Таке підвищення передбачає невеликі привілеї - наприклад, можливість вибрати період відпустки протягом року, а не заздалегідь, або продовжений обідню перерву;

- Приватне. Це повсякденні заходи, на які не прийнято звертати належної уваги. Однак при мінімальних витратах часом така мотивація дає вельми позитивні результати. До таких заходів належать - потиск руки при зустрічі,

звернення на ім'я по батькові, вітання в формі «Доброго дня», «Доброго вечора», похвала після робочого дня, інтерес про самопочуття співробітника особисто.

Усі перелічені методи нематеріальної мотивації використовують як окремо, так і комплексно. Побудова програми нематеріальної мотивації, яка поєднує реалізацію великої кількості різноманітних прийомів є найбільш оптимальним варіантом.

А якщо говорити в цілому, то нематеріальна мотивація в основному будується на умінні розуміти кожного співробітника, прислухатися до його побажань і поважати кожного працівника як людини. Для цього треба розуміти, що використовувати один вид нематеріальної мотивації в компанії не вийде. Залежно від віку, сімейного стану, захоплень, освіти і приналежності до тієї чи іншої соціальної групи потреби у співробітників різні.

Так, молоді працівники віддадуть перевагу можливості отримати кілька додаткових оплачуваних днів відпочинку або закінчувати роботу трохи раніше для виконання своїх батьківських обов’язків, а літні люди радше скористаються можливостями додаткового відпочинку в санаторії за рахунок компанії. Тому і виникає потреба у розробці і впровадженні системи нематеріальної мотивації.

Для успішної розробки та впровадження програми нематеріальної мотивації необхідно дотримуватися таких вимог [7]:

- програма має бути спрямована на найбільш значущі напрямки роботи компанії;

- охоплювати весь персонал, а не на «точково» заохочувати найбільш успішних працівників;

- має бути динамічною, регулярно оновлюватися і коригуватися відповідно до побажань і зауважень керівництва і трудового колективу;

- бути націленою на групи працівників зі схожими мотиваційними потребами, що забезпечує якість і цільовий характер мотиваційних заходів, а також полегшує їх контроль.

Обов’язковою вимогою є також офіційне й документальне оформлення всіх мотиваційних заходів. Так буде забезпечено прозорість і відкритість програми

нематеріальної мотивації, що слугуватиме додатковим прийомом нематеріального стимулювання для персоналу.

Таким чином, певні фінансові вкладення на впровадження програми нематеріального стимулювання персоналу цілком виправдовують себе в кінцевому рахунку є меншими, ніж прямі витрати на виплату премій.

Підсумовуючи, серед найбільш результативних кроків із формування нематеріальної мотивації та корпоративної лояльності персоналу варто виділити такі:

– визнання значущості працівника з боку колег і керівників, сприйняття керівництвом персоналу як людського капіталу, а не ресурсу. Важливо забезпечити, щоб працівник міг легко встановити свій особистий внесок в життя організації й переконатися, у праведливій його оцінці і винагороді;

– відкритість і зрозумілість цілей організації для персоналу, наявність достовірних відомостей про результати організаційної діяльності і стратегії. Колектив організації має знати, що він працює у стабільній і успішній організації, володіти інформацією про її сильні сторони, мати позитивне ставлення до своєї організації;

– створення сприятливого робочого середовища, в якому працівники можуть проявити себе у повній мірі для досягнення цілей організації та реалізації своїх власних потреб та інтересів, комфортно працювати і творити. У цьому контексті необхідно залучати персонал до вирішення організаційних проблем, завдяки чому працівники відчуватимуть свою цінність для організації.

3.3. Рекомендації практиків щодо використання методів мотивування персоналу у забезпеченні інформаційної безпеки

Незважаючи на значну кількість наукових публікацій і розробок з питань матеріальної і нематеріальної мотивації, на нашу думку, варто розглянути рекомендації практикуючих менеджерів з персоналу, які щодня стикаються з новими викликами і впроваджують інноваційні методи роботи з людьми.

Варто відзначити, що у більшості випадків методи і заходи мотивування персоналу є подібними для працівників із усіх сфер. Так, основні причини вмотивованості фахівців IT та інформаційної безпеки, за результатами дослідження Luxoft Personnel, фактично є стандартними: основним стимулом у роботі, крім матеріальної винагороди, є професійне зростання (62%); робота над дуже відповідальними і цікавими проектами (56%), а також гнучкий робочий графік (41%) і визнання колег (30%) [24].

Керівники провідних західних компаній вже давно зрозуміли, що методи адміністративного примусу і контролю є менш ефективними, ніж методи стимулювання і мотивування підлеглих. Цей принцип є особливо актуальним для сфери інформаційної безпеки, яка постійно потребує спеціалістів. А, отже, працівник з легкістю може змінити місце роботи на нове.

Результати досліджень свідчать, що компанії з високо вмотивованим персоналом демонструють більш високі обсяги продуктивності й прибутковості, ніж їхні менш умотивовані конкуренти, наприклад колективи високо вмотивованих працівників ефективніше взаємодіють з клієнтами, показують вищу продуктивність і коефіцієнт утримання, а їх рентабельність є вищою на 21%.

Збільшення вкладень у мотивування персоналу на 10% може привести до підвищення прибутковості на 2,4 тис. дол. на одного співробітника в місяць. Компанії з мотивованим трудовим колективом випереджають своїх конкурентів з низьким рівнем мотивації на 202%. З іншого боку, дуже низька мотивація персоналу має наслідком зниження продуктивності, через що американські компанії втрачають 450-550 млрд. дол. щороку [35].

Розглянемо приклади використання методів стимулювання і мотивування працівників на основі рекомендацій практиків з управління персоналом [12,15,24,28,41].

У результаті опитування, проведеного серед працівників компаній Німеччини, Франції, Нідерландів, Італії та Іспанії встановлені такі чинники мотивації персоналу, які якраз і можна вважати основними принципами правильної політики мотивування персоналу:

1) керівництво компанії проявляє інтерес до благополуччя працівників;

2) компанія створює для працівників можливості для вдосконалення професійних навиків;

3) керівництво компанії подає приклад пропагування й дотримання корпоративних цінностей;

4) в компанії наявна свобода в прийнятті рішень, що має на меті досягнення кращих результатів;

5) компанія володіє хорошою репутацією як роботодавець, що приваблює нових працівників і дозволяє утримувати наявних;

6) компанія вирішує спектр завдань, які забезпечують постійну активність персоналу;

7) компанія заохочує командну роботу за участю працівників;

8) компанія підтримує високий рівень клієнтоорієнтованості, що приваблює працівників;

9) працівники задоволені загальною робочою атмосферою в компанії;

10) персонал влаштовує рівень їх особистої зарплати.

Говорячи про техніки мотивування персоналу, які пропонують фахівці з HR, варто зазначити, що вони є досить різноманітними, обираються відповідно до корпоративних цінностей, базуються на знанні людської психології і часто мають не тільки стимулюючий, але й маніпулятивний характер.

На думку практиків, нічого не мотивує краще, ніж *загальна мета або місія*. Це може бути ідея – сенс існування й діяльності компанії типу «Ми можемо випускати найкращий продукт у світі» або «Зробимо цей світ кращим» або «Підвищимо якість життя пенсіонерів удвічі». Головним є те, щоб працівники компанії вірили в ідею і віддаватися роботі по-максимуму. Такий принцип може бути застосований як у великих компаніях, так і малих фірмах і ПП.

Поряд із кар'єрним зростання (підвищення по вертикалі: менеджер - керівник відділу – директор) велике значення для мотивування персоналу відіграє «*зростання в ширину*»: менеджер - старший менеджер - старший групи, що дає працівнику додаткові привілеї в порівнянні з рештою колег. Прикладом такого

зростання може бути і розширення повноважень у колективі, здійснення функцій наставництва.

Надання працівнику *додаткової відповідальності* також має мотиваційний ефект, оскільки в більшості випадків починає діяти правило: чим більше відповідальності покладено на людину, тим краще вона працює. Так відбувається тому, що працівник, отримуючи можливості приймати рішення самостійно, відчуває себе важливим для компанії.

Незважаючи на те, що *наставництво* не можна назвати способом безпосередньої мотивації, воно є важливим чинником впливу на особистість працівника, оскільки наявність наставника сприймається ним як ознака піклування з боку компанії. Керівник або більш досвідчений колега формує у працівника відчуття міцного плеча поруч як у професійній, так і в особистій сферах.

Наставництво має позитивний мотиваційний ефект і в зворотному напрямку: працівник, якого призначили наставником, починає відчувати свою значимість через прояв довіри і надання владних повноважень.

Навчання працівників за кошти компанії є засобом, який дозволяє досягти подвійної мети: по-перше, підвищити професійний рівень працівника, а по-друге, показати турботу про нього як члена команди з боку компанії. Навчання може проводитися як на базі компанії, так і за її межами, наприклад у респектабельних тренінгових центрах. Максимум нематеріальної мотивації можна отримати, направивши працівника на навчання за його особистими інтересами. Завдяки навчанню персоналу покращується якість роботи і забезпечується високий ступінь умотивованості персоналу.

Багато хто з практиків вважає, що дієвим методом нематеріальної мотивації є конкуренція, тобто *проведення конкурсів, змагань*. Сутність такого підходу у створенні умов, за яких працівники отримують можливість показати себе і перемогти суперника. І перемога може відігравати навіть не ключову роль. На думку автора, ідеальна тривалість конкурсу два тижні, приз має бути цікавий всім, а оптимальна мета конкурсу це досягнення кращих результатів у роботі.

Ймовірно, найкращим прикладом змагання мотиваційного спрямування є *конкурс на звання кращого працівника*. Ефективним є проведення конкурсів за різними номінаціями, оскільки таким чином розширюється коло осіб, які будуть відзначені.

У багатьох західних компаніях конкурси на звання кращого працівника запущені на постійній основі і переможця обирають щомісяця (наприклад, у МакДональдсі). Перемога у такому змаганні не тільки мотивує працівника через усвідомлення своєї значимості і цінності для компанії, але й шляхом надання різни привілеїв: можливість вибрати зручний графік роботи чи додаткові вихідні. Важливим є також публічне визнання заслуг працівника, що має подвійний мотиваційний результат.

Аналогічними прикладами є згадування кращих співробітників в корпоративній пресі, видання корпоративних буклетів, символіки з зображенням кращих працівників тощо. Цікавим є підхід до відзначення кращих працівників компанії WaltDisney, де прийнято присвячувати найціннішим співробітникам вікна кафе в парку Disneyland, де на склі пишуть їхні імена [12].

Як відомо, *умови роботи і зручність робочого простору* є дуже важливим чинником для більшості людей. Відповідно до наявних можливостей компанія просто зобов’язана створити такі умови, які будуть додатковою цінністю при влаштуванні на роботу, зокрема забезпечити проїзд, медичне страхування й оздоровлення, оплату стільникового зв'язку, харчування, умови для обіднього відпочинку. Великим плюсом буде зручний графік роботи, використання віддалених форм праці.

Не останніми чинниками формування мотивації працівників є створення сучасного й ергономічного робочого місця, підтримка комфортного температурного режиму й освітлення, раціональне планування робочих зон, а також наявність місця для відпочинку і проведення колективних заходів.

Так, практика свідчить, що одними із найбільш дієвих є методи, пов’язані з облаштуванням робочого простору, зокрема кухні для персоналу, автомата для

приготування кави (безкоштовно), кабінету для релаксу, кінозалу, тренажерного залу, душових кабін тощо.

Цікавим методом мотивування працівників є різні *доплати*, наприклад доплати за здоров'я. Багато організацій використовують премії за «нехворіння», проходження вакцинації (або самі оплачують та проводять вакцинацію), премії для тих, хто не палить, медичні страховки, знижки в тренажерні зали.

Одним із засобів, який часто використовують на практиці є *мотиваційна дошка* або дошка досягнень, коли в офісі розміщують дошку, де щодня відзначаєте результати кожного працівника за минулий день і в розрізі місяця. Таким чином підтримується постійне здорове конкурентне середовище в підрозділі чи цілому колективі. Для просунутих компаній фахівці рекомендують автоматизувати цей процес через виведення даних прямо на екран з CRM-системи (наприклад, Бітрікс24 або Мегаплан).

Не кожен серйозно сприйме ідею *перейменування посади* працівника на більш приємну і владну, наприклад, секретаря на господиню офісу, адміністратора на повелителя програм, менеджера з продажів на продавця щастя. Може здатися дивним, однак використання такого нестандартного методу має значний мотиваційний ефект, а також позитивно впливає на психологічну атмосферу в колективі.

Очевидно, що кожен любить отримувати *подарунки*, особливо приємно і часто неочікувано отримувати презенти на роботі. З огляду на це роль такого способу мотивації персоналу є немаловажною. Подарунки можна дарувати як на свята, так і без серйозного приводу. Маленькі приємні дрібнички роблять велику справу у налагодженні сприятливої атмосфери у колективі та позитивного ставлення до керівництва і, як наслідок, мотивують працівників працювати на благо компанії.

У цьому контексті варто згадати досвід компанії «Мастерфайб», яка у кінці щотижня оплачує роботу кожного працівника корпоративною «валютою» в однаковому розмірі, однак, «валюта» акумулюється на рахунку колеги, який працював найкраще; працівник, який за тиждень накопичив найбільшу кількість

«валюти», отримує золоту монету; зібравши п'ятдесят золотих, працівник отримує право відвідати Австралію за рахунок компанії. Заохочувальними призами є абонементи в басейн або тренажерний зал.

У практиці великих компаній зустрічаються випадки придбання особливо цінним працівникам квартири або автомобіля, оплати стажування, навчання або проходження курсів на отримання сертифікатів.

Спільне дозвілля - це коли колектив збирається всією командою і разом проводить вільний від роботи час – це важливий елемент діяльності з мотивування персоналу. Форми проведення вільного часу можуть бути різними: від загального корпоративу з нагоди річниці компанії чи професійного свята до інтерактивних ігор, спортивних змагань та інтелектуальних конкурсів, що мають на меті формування корпоративної єдності і зміцнення основ командної роботи. Такі заходи є дуже корисними для зміцнення мотивації, але, водночас, потребують серйозної підготовки для того, щоб поєднати інтереси різних професійних та вікових груп, окремих колективів, керівництва компанії та рядових фахівців.

Ще одним нестандартним, але дуже ефективним методом замотивувати працівника є *подяка мамі*. Мова йде саме про мам (батьки реагують більш стримано), які сприймають такі дії емоційно і з захватом, а потім підживлюють позитивні мотиваційні настрої своїх дітей. Відповідно у дітей, які є працівниками компанії, це викликає почуття вдячності і готовність віддано працювати на благо компанії, яка не тільки турбується про них, але й проявляє знаки уваги до їхніх батьків.

Окремий потужний блок мотиваційних технік становить сукупність методів, яку можна умовно назвати «*Особисте*» - те, що багато людей роблять щодня, навіть не усвідомлюючи. Мова йде про особисте й людське спілкування, надати якому мотиваційний ефект можна різними способами, зокрема звертатися по імені, похвалити після робочого дня, провести особисту бесіду про «життя», привітатися за руку, зателефонувати і дізнатися, як справи, працювати у відкритому кабінеті тощо.

У таких випадках потрібно чітко встановлювати грань робочих та особистих відносин, з одного боку - зменшуючи дистанцію між керівником і підлеглим, з іншого – зберігаючи субординацію.

Узагальнені методи мотивування персоналу на основі рекомендацій практиків у сфері управління персоналом представлено на Рис.3.3.

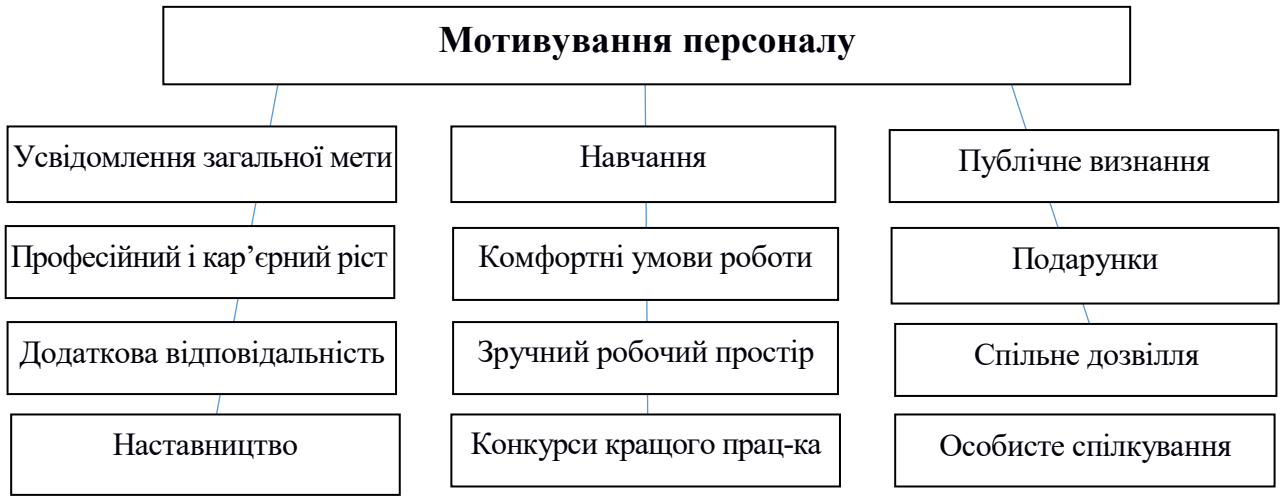

Рис.3.3. Методи мотивування персоналу (рекомендації HR-фахівців).

Загалом варто відзначити, що вся система мотивації персоналу базується насамперед на загальнолюдському гуманістичному підході: турботі і вдячності, уважності до життя й думки працівників, публічному визнанні заслуг, заохоченні ініціативи, створенні умов для професійного, кар'єрного й особистісного розвитку, підтриманні сприятливого морально-психологічного клімату й проведенні спільного дозвілля.

Висновки до третього розділу

Як свідчить практика, заходи матеріального стимулювання й мотивування персоналу показують високу результативність у запобіганні та протидії порушенням інформаційної безпеки і є основною передумовою створення й підтримки лояльного кадрового потенціалу організації.

Вивчення європейського досвіду показало, що основними причинами високої лояльності персоналу є чинники матеріального стимулювання, серед яких справедлива оплата праці відповідно до освіти, кваліфікації, якості роботи

працівника, здійснення доплат і надбавок за високу якість, ширшу відповідальність чи суміщення професій; виплата дивідендів, участь у прибутках і доходах; оплата харчування, медичного страхування; гнучкий графік або можливість дистанційної роботи.

Крім матеріального стимулювання обов'язковим елементом забезпечення ефективної роботи персоналу та формування його лояльності організації є нематеріальна мотивація. До заходів нематеріальної мотивації персоналу відносять залучення підлеглих до обговорення поточних питань і прийняття стратегічних рішень, справедливе оцінювання досягнутих результатів і відповідне нематеріальне заохочення, створення можливостей для кар'єрного просування і підвищення рівня професійної компетентності, розширення зони відповідальності, заохочення ініціативи і творчого підходу до праці.

Узагальнення рекомендацій фахівців-практиків у сфері управління персоналом та інформаційної безпеки засвідчило, що чинниками підвищення мотивації працівників з боку організації є такі: сприяння їхньому професійному і кар'єрному розвитку, надання додаткової відповідальності і більшої самостійності, наставництво, створення комфортних умов праці та сприятливої морально-психологічної атмосфери, забезпечення конкурентності у роботі, публічне визнання і заохочення, спільне дозвілля й особисте спілкування керівництва з колективом.

ВИСНОВКИ

Встановлено, що забезпечення інформаційної безпеки організації - це цілеспрямована діяльність її органів і посадових осіб з використанням дозволених методів і засобів по досягненню стану захищеності інформаційного середовища організації та забезпечення його нормального функціонування і динамічного розвитку. Важливим напрямом забезпечення інформаційної безпеки організації є створення середовища, в якому користувачі та персонал дотримуються вимог інформаційної безпеки.

Відзначено, що значний вплив на стан інформаційної безпеки мають внутрішні джерела загроз, тобто у більшості випадків персонал організації, який здійснює різноманітні протиправні дії щодо інформації та інформаційних систем організації внаслідок своєї некомпетентності, халатності або злого умислу.

На основі аналізу джерел загроз встановлено, що заходи мотивування персоналу, а в підсумку - формування й утримання високого рівня організаційної лояльності персоналу, є одними із найважливіших у нинішніх умовах сприяють зниження ймовірності шкідливого інсайду.

Аналіз наукової літератури показав, що лояльність персоналу розглядають як джерело організаційної безпеки або поведінку на благо компанії, в якій працівники дотримуються правил і норм; чинниками формування лояльності є попередній досвід роботи, особистісні характеристики співробітника і позитивне сприйняття організації. Вивчення феномену лояльності персоналу засвідчило існування різних наукових підходів до її оцінювання.

Для оцінювання лояльності персоналу з інформаційної безпеки використано модель оцінки лояльності (надійності) персоналу, згідно з якою підсумкова оцінка лояльності працівника є сумою оцінок рівня підготовки персоналу з інформаційної безпеки, рівня організаційної лояльності працівника та підозрілої активності персоналу, спрямованої проти організації.

З’ясовано, що заходи матеріального стимулювання й мотивування персоналу показують високу результативність у запобіганні та протидії порушенням

інформаційної безпеки і є основною передумовою створення й підтримки лояльного кадрового потенціалу організації.

Вивчення наукових джерел показало, що основними причинами високої лояльності персоналу є як чинники матеріального стимулювання, серед яких справедлива оплата праці, доплати і надбавки; виплата дивідендів, участь у прибутках і доходах; оплата харчування, медичного страхування; гнучкий графік або дистанційної роботи, так і заходи нематеріальної мотивації: участь в управлінні організацією, справедливе оцінювання досягнутих результатів, кар'єрний та професійний розвиток, заохочення ініціативи і творчого підходу до праці.

Узагальнення рекомендацій фахівців-практиків у сфері управління персоналом та інформаційної безпеки засвідчило, що система мотивації персоналу має базуватися насамперед на загальнолюдському гуманістичному підході: турботі і вдячності, уважності до життя й думки працівників, публічному визнанні заслуг, заохоченні ініціативи, створенні умов для професійного, кар'єрного й особистісного розвитку, підтриманні сприятливого морально-психологічного клімату й проведенні спільного дозвілля.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Анкета-опросник «Шкала организационной лояльности» https://hr-portal.ru/files/anketa-oprosnik_shkala_organizacionnoy_loyalnosti.pdf (дата звернення: 19.12.2020).

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

3. Баранская С.С. Методика измерения лояльности Психологические исследования. 2011. № 1(15) URL: http://psystudy.ru/index.php/num/2011n1-15/436-baranskaya15.html (дата звернення: 19.12.2020).

4. Бедненко А. Термометр лояльности URL: https://www.ippnou.ru/article.php?idarticle=008890 (дата звернення: 19.12.2020).

5. Богданович В.Ю., Романченко І.С., Свида І.Ю. Теоретичні основи забезпечення національної безпеки України в умовах позаблоковості: монографія. Львів.: АСВ. 2011. 414 с.

6. Бойдало М.К. Метод и модель оценки надежности персонала в обеспечении информационной безопасности организации. Диссертация на соискание ученой степени к.тех.н., Санкт-Петербург, С.-П. НИУ ИТ, механики и оптики, 2015. 136 с.

7. Бондаревська К.В., Товмашенко Т.О. Стимулювання персоналу: зарубіжний досвід та вітчизняні реалії . Молодий вчений. 2015. № 3(18). С. 26-31.

8. Бутиліна О. В. Лояльність персоналу організації: підходи до визначення. «SOCIOПРОСТІР: міждисциплінарний електронний збірник наукових праць з соціології та соціальної роботи». 2017. № 6. С.21-24.

9. Васюта В.Б. Адаптація європейських моделей мотивації працівників на підприємствах України, URL: http://reposit.nupp.edu.ua/xmlui/bitstream/handle/PoltNTU/2410/Vasuta_Tezy.pdf?sequence=1&isAllowed=y (дата звернення: 19.12.2020).

10. Германов И.А., Плотникова Е.Б. Измерение организационной лояльности персонала (опыт апробации методики Мейер-Аллен). Вестник Пермского универ-та. Философия. Психология. Социология. 2011. Выпуск 3 (7). С.106-111.

11. Грюнхольд Л., Мартенсен А. Лояльность работника - лояльность клиента - прибыльность компании. URL: https://www.cfin.ru/press/pmix/2001-6/11.shtml (дата звернення: 19.12.2020).

12. Денисёнок А. Нематериальная мотивация. URL: https://hrliga.com/index.php?module=profession&op=view&id=1551 (дата звернення: 19.12.2020).

13. Дмитриева Т.А. Особенности использования методов нематериальной мотивации персонала в организации. Вопросы науки и образования. 2018. № 23 (35). С. 46-48.

14. Доминяк В.И. Психологическая диагностика лояльности персонала Научно-технические ведомости СПбГПУ. Гуманитарные и общественные науки. Вопросы психологии. 2010. №2. С.122-126.

15. Жестков Н. Нематериальная мотивация персонала: 15 рабочих способов. URL: https://in-scale.ru/blog/nematerialnaya-motivaciya-personala (дата звернення: 19.12.2020).

16. Жук А. О. Шило Л.А. Іноземний досвід застосування ефективних систем оплати праці та мотивації працівників. International Electronic Scientific Journal "Science Online". URL: http://nauka-online.com/ (дата звернення: 19.12.2020).

17. Захаров А. Н. Зарубежный опыт мотивации и оплаты труда. URL: https://cyberleninka.ru/article/n/zarubezhnyy-opyt-motivatsii-i-oplaty-truda/viewer (дата звернення: 19.12.2020).

18. Зімовін О. Що означає «лояльність персоналу». Оплата труда. 2016. № 14/1. С.4-6.

19. Иванова Н.Е. Лояльность персонала как феномен Научный вестник ЮИМ. Экономическая политика и хозяйственная практика. 2019. №2. С. 23-28.

20. Информационная безопасность: Учебное пособие. Ясенев В.Н., Дорожкин А.В., Сочков А.Л., Ясенев О.В. Под общей редакцией проф. Ясенева В.Н. Нижний Новгород: Нижегородский госуниверситет им. Н.И. Лобачевского, 2017. 198 с.

21. 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.

22. Климчук А.О. Особливості використання зарубіжних моделей мотивації та стимулювання персоналу на промислових підприємствах. Вісник Хмельницького нац. ун-ту. Економічні науки. 2016. № 4. т. 1. С. 57- 60.

23. Козаченко А. Зарубежный опыт мотивации труда. URL: https://hrliga.com/index.php?module=profession&op=view&id=1731 (дата звернення: 19.12.2020).

24. Креатив в мотивации: как переманить IT-специалистов. URL: https://security-corp.org/programming/19894-kreativ-v-motivacii-kak-peremanit-it-specialistov.html (дата звернення: 19.12.2020).

25. Лапина Н., Копейкин Г. Психологические аспекты информационной безопасности организации. URL: https://www.beltim.by/wiki/articles/psikhologicheskie-aspekty-informatsionnoy-bezopasnosti-organ/ (дата звернення: 19.12.2020).

26. Лояльность (за В. Доміняком). URL: https://dominyak.com/loyalty.html (дата звернення: 19.12.2020).

27. Нагірна О. О. Фактори лояльності персоналу комерційних організацій, Соціально-психологічні проблеми політики, бізнесу, управління. Наукові студії із соціальної та політичної психології. С.243-251.

28. Нестандартные методы мотивации персонала URL: https://searchinform.ru/kontrol-sotrudnikov/motivatsiya-personala/nestandartnye-metody-motivatsii-personala/ (дата звернення: 19.12.2020).

29. Нехай В.А., Нехай В.В. Інформаційна безпека як складова економічної безпеки підприємств. Науковий вісник Міжнародного гуманітарного університету. 2017. №1. С.137-140. URL: http://www.vestnik-econom.mgu.od.ua/journal/2017/24-2-2017/30.pdf (дата звернення: 19.12.2020).

30. Обеспечение информационной безопасности бизнеса / В. В. Андрианов, С. Л. Зефиров, В. Б. Голованов и др. 2-е, перераб. и доп. М. : ЦИПСиР, 2011. 373 с.

31. Ожиганова М. І., Хорошко В. О., Яремчук Ю. Є., Карпінець В. В. Управління персоналом : навч. посіб. Вінниця : ВНТУ, 2014. 187 с.

32. Сардак О.В. Формування лояльності в системі управління персонал-маркетингом підприємств. Науковий вісник НЛТУ України. 2012. Вип. 22.8. С.387-392.

33. Северина С.В. Інформаційна безпека та методи захисту інформації. Вісник Запорізького національного університету. 2016. № 1 (29). С.155-161.

34. 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: 19.12.2020).

35. Статистические данные о мотивации сотрудников на начало 2020 года. URL: https://www.wrike.com/ru/blog/statisticheskie-dannye-o-motivatsii-sotrudnikov-na-nachalo-2020-goda/ (дата звернення: 19.12.2020).

36. Харский К. В. Благонадежность и лояльность персонала. Изд-во: СПб: Питер, 2003. 496 с.

37. Челнокова Н.Ю. Лояльность сотрудников как способ повышения эффективности управления персоналом организации. Международный научный журнал «Инновационная наука». 2015. №11. С. 277-281.

38. BS ISO/IEC 27005:2008. Information technology - Security techniques - Information security risk management. 55p.

39. Data Breach Investigations Report – 2020. Learn to protect your organization from cyberthreats. URL: https://enterprise.verizon.com/resources/reports/dbir/ (дата звернення: 19.12.2020).

40. Employee Negligence Remains the Biggest Threat in Data Breaches. URL: https://businessinsights.bitdefender.com/employee-negligence-remains-the-biggest-threat-in-data-breaches (дата звернення: 19.12.2020).

41. HR-менеджмент. URL: https://www.e-xecutive.ru/career/hr-management (дата звернення: 19.12.2020).

42. Kipp S. P. Espionage and the Insider. SANS Institute Reading Room, 2001. URL: http://www.sans.org/reading_room/whitepapers/basics/espionage-insider_426 (дата звернення: 19.12.2020).

43. SANS 2019 SOC Survey – Common and Best Practices for Security Operations Centers. URL: https://www.cyberbit.com/resource/sans-2019-soc-survey-common-and-best-practices-for-security-operations-centers/ (дата звернення: 19.12.2020).

44. The Best Employee Monitoring Software for 2020 URL: https://www.pcmag.com/picks/the-best-employee-monitoring-software?test_uuid=001OQhoHLBxsrrrMgWU3gQF&test_variant=a (дата звернення: 19.12.2020).

45. 15 Alarming Cyber Security Facts and Stats 2020. URL: https://www.cybintsolutions.com/cyber-security-facts-stats/ (дата звернення: 19.12.2020).