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:

ТЕХНОЛОГІЇ УПРАВЛІННЯ ЛЮДСЬКИМИ РЕСУРСАМИ У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

СТУДЕНТ: Клюквін Сергій Сергійович _____
(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 Клюквіну Сергію Сергійовичу

Тема роботи: «ТЕХНОЛОГІЇ УПРАВЛІННЯ ЛЮДСЬКИМИ РЕСУРСАМИ У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА», затверджена наказом по університету № 230 від «13» жовтня 2020 р.

1. **Термін здачі** студентом оформленої роботи «___» _____ 2020 р.
2. **Об'єкт дослідження:** забезпечення інформаційної безпеки підприємства.
3. **Предмет дослідження:** технології управління людськими ресурсами у забезпеченні інформаційної безпеки підприємства.
4. **Мета дослідження** полягає у вивченні технологій управління людськими ресурсами у забезпеченні інформаційної безпеки підприємства.
5. **Перелік питань, які мають бути розроблені:**

5.1 Дослідити сутність і технології управління людськими ресурсами як складової забезпечення інформаційної безпеки підприємства.

5.2 Проаналізувати підходи до організації навчання персоналу у сфері інформаційної безпеки.

5.3 З'ясувати форми і методи здійснення контролю й оцінювання персоналу з інформаційної безпеки.

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

Науковий керівник _____ Т.М. Мужанова
підпис

Завдання прийнято до виконання _____ С.С. Клюквін
підпис

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

КАЛЕНДАРНИЙ ПЛАН
виконання дипломної роботи
студентом Клюквіним Сергієм Сергійовичем

Дата видачі завдання: «16» вересня 2020 р.

№ з/п	Етапи дипломної роботи	Термін виконання етапів	Примітка
1.	Визначення об'єкта, предмета, мети та завдань дослідження.	21.09.2020	
2.	Збір та аналіз літератури.	28.09.2020	
3.	Дослідження сутності і технологій управління людськими ресурсами як складової забезпечення інформаційної безпеки підприємства.	12.10.2020	
4.	Аналіз підходів до організації навчання персоналу у сфері інформаційної безпеки.	26.10.2020	
5.	З'ясування форм і методів здійснення контролю й оцінювання персоналу з інформаційної безпеки.	09.11.2020	
6.	Формулювання висновків за результатами проведеного дослідження.	23.11.2020	
7.	Оформлення роботи.	07.12.2020	
8.	Оформлення презентації.	14.12.2020	
9.	Отримання рецензії на роботу.	25.12.2020	
10.	Захист у ДЕК.	.01.2021	

Студент С.С. Клюквін
(підпис)

Науковий керівник Т.М. Мужанова
(підпис)

РЕФЕРАТ

Дипломна робота присвячена дослідженню технологій управління людськими ресурсами у забезпеченні інформаційної безпеки підприємства. Робота складається зі вступу, трьох розділів, що містять 10 рисунків, висновків та списку використаних джерел з 43 найменувань. Загальний обсяг роботи становить 82 аркуші, з яких 4 аркуші займає список використаних джерел.

Об'єктом дослідження є забезпечення інформаційної безпеки підприємства.

Метою роботи є вивчення технологій управління людськими ресурсами у забезпеченні інформаційної безпеки підприємства.

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

Як результат у роботі досліджено сутність і технології управління людськими ресурсами як складової забезпечення інформаційної безпеки підприємства; проаналізовано підходи до організації навчання персоналу у сфері інформаційної безпеки; з'ясовано форми і методи здійснення контролю й оцінювання персоналу з інформаційної безпеки.

Галузь застосування. Розроблені підходи можуть бути використані при впровадженні технологій управління людськими ресурсами з метою забезпечення інформаційної безпеки підприємства.

Ключові слова: УПРАВЛІННЯ ЛЮДСЬКИМИ РЕСУРСАМИ, ТЕХНОЛОГІЇ УПРАВЛІННЯ ЛЮДСЬКИМИ РЕСУРСАМИ, ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА, НАВЧАННЯ ПЕРСОНАЛУ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, КОНТРОЛЬ І ОЦІНЮВАННЯ ПЕРСОНАЛУ.

ЗМІСТ

ВСТУП

Актуальність теми. Статистика інцидентів інформаційної безпеки свідчить на користь негативного впливу «людського фактора» на стан захищеності інформаційного середовища підприємства. Сьогодні саме персонал найчастіше є джерелом порушень інформаційної безпеки, серед яких здійснення протиправних маніпуляцій з інформацією та засобами її обробки, розкриття конфіденційної інформації підприємства, надання неавторизованого доступу до корпоративних ІТКС злочинним суб'єктам тощо, які є наслідком непрофесійності, халатності або навмисних деструктивних намірів безвідповідальних або невдоволених працівників.

Тому кожне сучасне підприємство має приділяти велику увагу роботі з персоналом, який є основним корпоративним ресурсом, і використовувати для цього різноманітні технології управлінського впливу.

З огляду на зазначені чинники дослідження технологій управління людськими ресурсами у забезпеченні інформаційної безпеки підприємства є актуальним науковим завданням.

Мета і завдання дослідження. **Мета роботи** полягає у вивченні технологій управління людськими ресурсами у забезпеченні інформаційної безпеки підприємства.

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

1. Дослідити сутність і технології управління людськими ресурсами як складової забезпечення інформаційної безпеки підприємства.
2. Проаналізувати підходи до організації навчання персоналу у сфері інформаційної безпеки.
3. З'ясувати форми і методи здійснення контролю й оцінювання персоналу з інформаційної безпеки.

Об'єкт дослідження - забезпечення інформаційної безпеки підприємства.

Предмет дослідження - технології управління людськими ресурсами у забезпеченні інформаційної безпеки підприємства.

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

Наукова новизна одержаних результатів. Розроблені підходи можуть бути використані при впровадженні управлінських та інформаційних технологій управління людськими ресурсами у забезпеченні інформаційної безпеки підприємства.

Практичне значення одержаних результатів. Застосування напрацювань дасть змогу здійснити обґрунтований вибір методів і засобів управління людськими ресурсами для вирішення завдань інформаційної безпеки, допоможе підібрати ефективні програмні продукти для навчання й формування обізнаності працівників з питань інформаційної безпеки, а також надійні IT-рішення для контролю й оцінювання роботи персоналу в контексті забезпечення інформаційної безпеки.

Розділ 1.
УПРАВЛІННЯ ЛЮДСЬКИМИ РЕСУРСАМИ ЯК СКЛАДОВА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Сутність і основні технології управління людськими ресурсами

Як свідчить практика, у нинішніх умовах одним з найважливіших завдань і ключовою передумовою розвитку підприємства є робота з персоналом, який по праву вважається головною цінністю підприємства, основою його стабільного функціонування і рушійною силою позитивних та інноваційних змін у бізнесі.

Однак, таких результатів можна досягти тільки завдяки ефективному управлінню персоналу. У науковій літературі та на практиці сьогодні усе частіше зустрічається формулювання «управління людськими ресурсами», що по суті і відображає зміни у ставленні до працівників з огляду на визнання їх ролі у забезпеченні сталого розвитку підприємства чи організації. Поява назви «управління людськими ресурсами» є результатом дослідження людських відносин на початку XX століття, коли науковці і практики довели можливості підвищення вартості бізнесу за рахунок стратегічного управління робочою силою.

Управління людськими ресурсами (HRM – Human Resource Management) є цілеспрямованою та узгодженою діяльністю топ-менеджменту підприємства, керівників і фахівців підрозділів управління, яка складається з таки видів робіт як розробка концепції, стратегій кадрової політики, принципів і методів управління людськими ресурсами.

HRM - це системний, спланований організований вплив шляхом здійснення комплексу взаємопов'язаних організаційних, економічних і соціальних заходів з метою створення умов сталого розвитку і ефективного використання потенціалу робочої сили підприємства. Планування, формування, перерозподіл і раціональне використання людських ресурсів є його основним змістом [20].

Розглянемо основні положення теорії управління людськими ресурсами.

Так, управління людськими ресурсами розглядає персонал як важливий ресурс підприємства, впроваджує індивідуалістичний підхід (більша увагу кожному окремому працівникові з його особливими потребами); звертає більшу увагу на реалізацію стратегічного, а не тактичного підходу до вирішення проблем персоналу.

HRM, на відміну від управління персоналу, покладає відповідальність за роботу з персоналом не тільки на відділ кадрів, але й на лінійних менеджерів, які безпосередньо працюють з колективом.

Якщо завданням управління персоналом є досягнення економії видатків на працівників, то управління людськими ресурсами підприємства передбачає вкладення інвестицій в розвиток своїх кадрів [30].

Управління людськими ресурсами покликане максимізувати ефективність праці персоналу для досягнення стратегічних цілей роботодавця. Усі процеси і програми, пов’язані з людською діяльністю, є частиною HRM.

Сьогодні функції управління людськими ресурсами на рівні департаментів і підрозділів часто покладають на лінійних менеджерів. HRM охоплює низку заходів, в тому числі виплати працівникам за участь в проектах, навчання і розвиток, додаткову атестацію і переатестацію, нагороди від громадських організацій. HRM також регулює організаційні зміни і виробничі відносини, тобто підтримує баланс організаційного управління з вимогами відповідно до колективних договорів та інших угод. В управлінні людськими ресурсами велика увага приділяється розвитку нематеріальних активів та інтелектуального потенціалу підприємства, які не підлягають кадровому і бухгалтерському обліку.

Починаючи з досліджень проблем трансакційних витрат (заробітної плати і пільг), розробники теорії управління людськими ресурсами на основі врахування чинників глобалізації, інтеграції компаній і технологічних нововведень зосередилися на таких стратегічних ініціативах, як злиття і поглинання, управління талантами, планування наступності (передачі виробничих функцій наступнику посади), якості виробничих і трудових відносин тощо.

У рамках HRM розробляють системи компенсації, програми пільг та знижок, дозвілля та сімейного відпочинку, які працівники можуть отримати за

продуктивну та якісну робота. Значної уваги в управління людськими ресурсами приділяється питанням інформаційної взаємодії з працівниками, яка допомагає вирішувати низку важливих проблем, таких як дискримінація або домагання. Фахівці з HR вносять свій методологічний внесок у прийняття стратегічних рішень та формування конкурентоспроможності підприємства.

Таким чином, робота з персоналом стала сферою бізнесу, спрямованою на зростання продуктивності праці [5].

Принципи управління людськими ресурсами підприємств мають багаторівневий характер.

У наукових публікаціях виділяють такі принципи:

- загальнонаукові принципи управління людськими ресурсами: науковість, нормативність, плановість, системність, безперервність, оперативності, відповідальність, економічна обґрунтованість тощо та
- часткові принципи: відповідність функцій управління меті бізнесу; індивідуальний підхід, демократизму (врахування колективної думки працівників при прийнятті кадрових рішень, автономність), інформатизація роботи з персоналом, урахуванням психологічної сумісності при підборі персоналу в колективі.

Окрім того, принципи управління людськими ресурсами розділяють залежно від стадії життєвого циклу системи управління, визначаючи принципи побудови та принципи розвитку.

На думку фахівців, сучасне високотехнологічне підприємство має сповідувати в управлінні людськими ресурсами таких принципів: вище згадані принципи плановості, демократизму та системності, а також принципи єдиноначальності (чіткого розподілу повноважень та встановлення відповідальності), оптимальності (вибір рішення, найбільш прийнятного для конкретної ситуації), адаптивності (пристосування системи управління персоналом до змін середовища, вимог бізнесу та потреб працівників), соціальної доцільності (заходи з управління персоналом мають бути соціально виправдані з огляду на ризики, притаманні людські діяльності), соціального партнерства, тобто співпраці між роботодавцем та

працівниками, економічної зацікавленості (створення гнучкої системи мотивування персоналу), справедливого винагородження і визнання внеску працівника, відкритості та прозорості, що забезпечує розуміння дій керівництва з боку персоналу та їх підтримку, формування сприятливого мікроклімату в колективі, належне технічне забезпечення робочих місць [9,20].

Як зазначалося вище, управління людськими ресурсами є комплексною діяльністю з метою створення умов сталого розвитку і ефективного використання потенціалу робочої сили підприємства. Розглянемо основні функції HRM у сучасних умовах.

Функції є тими завданнями, які реалізуються як на великих, так і дрібних підприємствах та організаціях у процесі формування та координації їхніх трудових ресурсів.

Фахівці виділяють такі функції HRM:

- розробка і впровадження політики управління людськими ресурсами, забезпечення її виконання;
- створення рівних можливостей для всіх працівників і дотримання вимог законодавства і нормативів;
- визначення потреб у персоналі;
- визначення специфічних вимог до кожного робочого місця або посади на основі детального їх аналізу;
- вивчення й оцінка можливостей персоналу, які сприяють досягненню місії підприємства;
- набір персоналу відповідно до потреб підприємства;
- відбір і наймання працівників на вакансії;
- професійна орієнтація і навчання персоналу;
- розробка і впровадження програм розвитку персоналу;
- створення систем оцінювання роботи працівників;
- планування кар'єри працівників;

- робота з кращими працівниками, які забезпечують конкурентну перевагу підприємства та є носіями особистого або корпоративного бренду;
- розробка систем оплати праці;
- посередництво між роботодавцем і профспілками;
- розробка і впровадження програм із забезпечення здоров'я і безпеки персоналу;
- надання допомоги працівникам у вирішенні особистих проблем, що впливають на якість праці;
- створення систем комунікації для зв'язок між працівниками [3].

Також на макрорівні HRM відповідає за контроль організаційного керівництва і культури управління.

Відповідно до іншого підходу управління людськими ресурсами як цілісна система виконує функції:

- організаційну - планування потреб і джерел укомплектування персоналу;
- соціально-економічну - забезпечення комплексу умов і факторів, спрямованих на раціональний розподіл і використання трудового потенціалу;
- відтворювальну - забезпечення розвитку персоналу (професійного, кар'єрного та особистісного).

Загальна структура принципів та функцій управління людськими ресурсами показана на Рис.1.1.

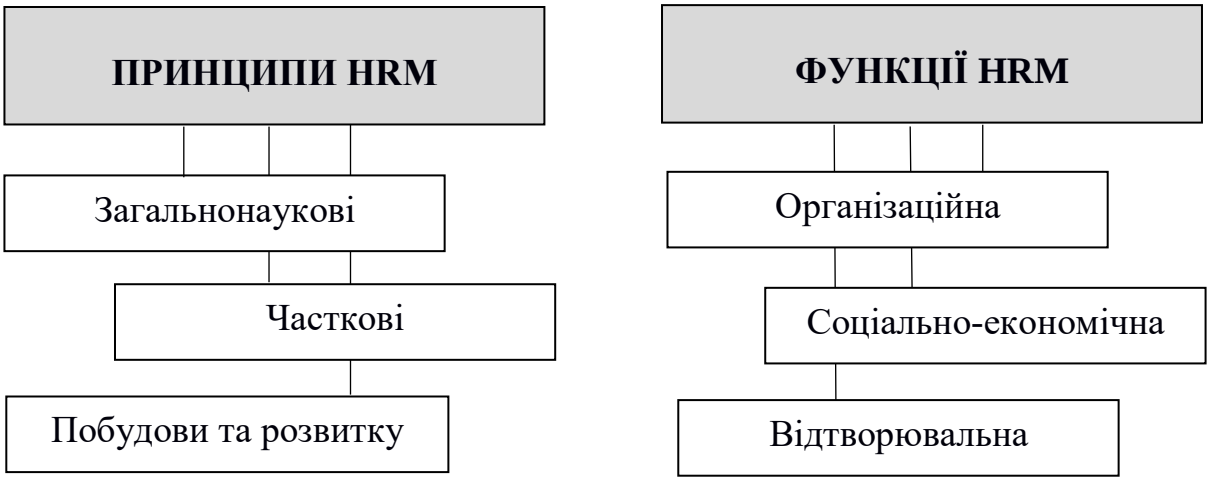

Рис.1.1. Принципи та функції управління людськими ресурсами.

Ще раз варто закцентувати увагу на супроводжуючій ролі HR-підрозділу, основним завданням якого є забезпечити підтримку лінійним менеджерам у роботі з персоналом. Таким чином, HR-підрозділ діє переважно як консультаційний орган, організує і координує процеси наймання і навчання, реалізує програми з розвитку персоналу, працює в якості посередника у зв'язках між менеджерами, працівниками й роботодавцем і координує програми безпеки [3].

Управління людськими ресурсами для вирішення своїх завдань використовує низку кадрових технологій. Раніше поняття «технологія» найчастіше трактували у суто виробничому або технічному контексті. Так, наприклад, під інформаційними технологіями розуміють сукупність методів і засобів, що використовуються для збору, зберігання, обробки і поширення інформації.

Однак, сьогодні поняття «технологія» широко застосовують для визначення набору способів, засобів і методів вибору й реалізації здійснення управлінського процесу у багатьох гуманітарних сферах. До компонентів технології, у тому числі технології у сфері управління людськими ресурсами, відносять:

- мету реалізації процесу;
- предмет, що підлягає технологічним змінам;
- способи і методи впливу;
- засоби технологічного впливу;
- впорядкованість і організацію, які протиставляють стихійним процесам [18].

Фахівці з питань управління персоналом умовно розділяють HRM-технології на три групи. До першої групи відносять HRM-технології, що забезпечують збирання й оцінювання всесторонньої достовірної і актуальної особистої інформації про особу, зокрема при підборі претендентів на посаду.

Другу групу становлять кадрові технології, які забезпечують відбір, формування резерву, кадрове планування і професійний розвиток працівників підприємства через збирання й аналіз кількісних та якісних характеристик складу персоналу.

До третьої групи належать кадрові технології, які дозволяють підвищити результативність праці кожного фахівця і забезпечити синергетичний ефект від

злагодженої роботи усього персоналу. Сюди можна віднести такі технології, як підбір персоналу, ротація, управління кар'єрою персоналу [29].

Вартим уваги є підхід до визначення структури HR-системи, представлений закордонними науковцями [13], відповідно до якого управління людськими ресурсами вибудовується зверху вниз, відштовхуючись від місії організації на трьох рівнях управління: загально-організаційному, груповому та рівні виконавців (Рис.1.2).

Рис.1.2. Рівні управління людськими ресурсами.

На думку авторів підходу, можливість впливати на персонал можна отримати через приналежність до організації, групи (формальної, як підрозділ, та неформальної, як група за інтересами) і через систему індивідуальних цінностей.

Для здійснення такого впливу використовують різні інструменти на кожному з рівнів управління: для рівня організації - політики в галузі управління людськими ресурсами; для рівня груп – процедури; для рівня окремо взятих виконавців - технічні завдання.

Кожен зі згаданих інструментів виконує свої завдання. Політики встановлюють загальні принципи прийняття рішень за напрямами управління людськими ресурсами, наприклад відбору й оцінки персоналу, навчання та

професійного розвитку, винагородження та пільг, контролю продуктивності та якості праці тощо.

Процедури вказують способи втілення політик в життя, окреслюють послідовність дій, яку необхідно дотримуватися всім учасникам процесу. Вони, по суті, є покроковими інструкціями з виконання певних дій. Наприклад, процедури проведення співбесіди при найманні працівника, здійснення інструктажу з користування пристроєм, преміювання чи звільнення працівника. У процедурах визначають підстави для прийняття рішення про проведення дій; встановлюються відповідальних осіб та правила проведення тощо.

Головною ціллю технічних завдань є надати відповідь на питання щодо конкретних дій виконавця для досягнення запланованого результату. Прикладами технічних завдань є посадові інструкції або вказівки для претендентів на посаду, які працевлаштовуються на нове місце роботи.

Загалом основним завданням системи управління людськими ресурсами є забезпечити зростання економічної ефективності організації шляхом формування бажаної трудової поведінки персоналу та забезпечення потрібної результативності праці [14].

1.2. Внутрішні порушники як об’єкти забезпечення інформаційної безпеки

Дослідження проблем інформаційної безпеки підприємства щораз свідчать про те, що «ахіллесовою п’ятою» системи захисту була і залишається людина, а саме працівник підприємства. Наприклад, результати дослідження компанії InfoWatch показали, що майже 78% інцидентів, які мали наслідком компрометацію інформації, були спровоковані навмисними або необережними діями персоналу. За I-III квартали 2020 року понад 47% випадків витоку інформації у світі сталися через внутрішніх порушників, водночас в Росії таких порушень було понад 79% [1], що недвозначно свідчить про відставання не тільки РФ, але й інших країн пострадянського простору у справі запобігання й протидії протиправним діям персоналу у сфері інформаційної безпеки.

Досліджуючи внутрішнього порушника, цікавим для вивчення є опис дій працівника, який відображає його практичні та теоретичні можливості, наявні у нього знання, час і місце порушення.

У більшості випадків метою порушника може бути: заволодіння необхідною цінною інформацією; модифікація даних та інформаційних процесів у власних інтересах (або інтересах третьої сторони); знищення інформаційних активів для нанесення матеріальних або репутаційних збитків організації.

Основними мотивами порушень інформаційної безпеки з боку працівників підприємства є: безвідповідальність, бажання самоствердження та наявність корисливого інтересу, тобто намірів отримати особисту вигоду.

Коротко розглянемо основні підходи до класифікації внутрішніх порушників, представлені відомими організаціями, які вважаються компетентними із зазначених питань.

Однією з найбільш деталізованих класифікацій внутрішніх порушників вважають екосистему внутрішніх порушників компанії InfoWatch (Рис. 1.3) [22,35].

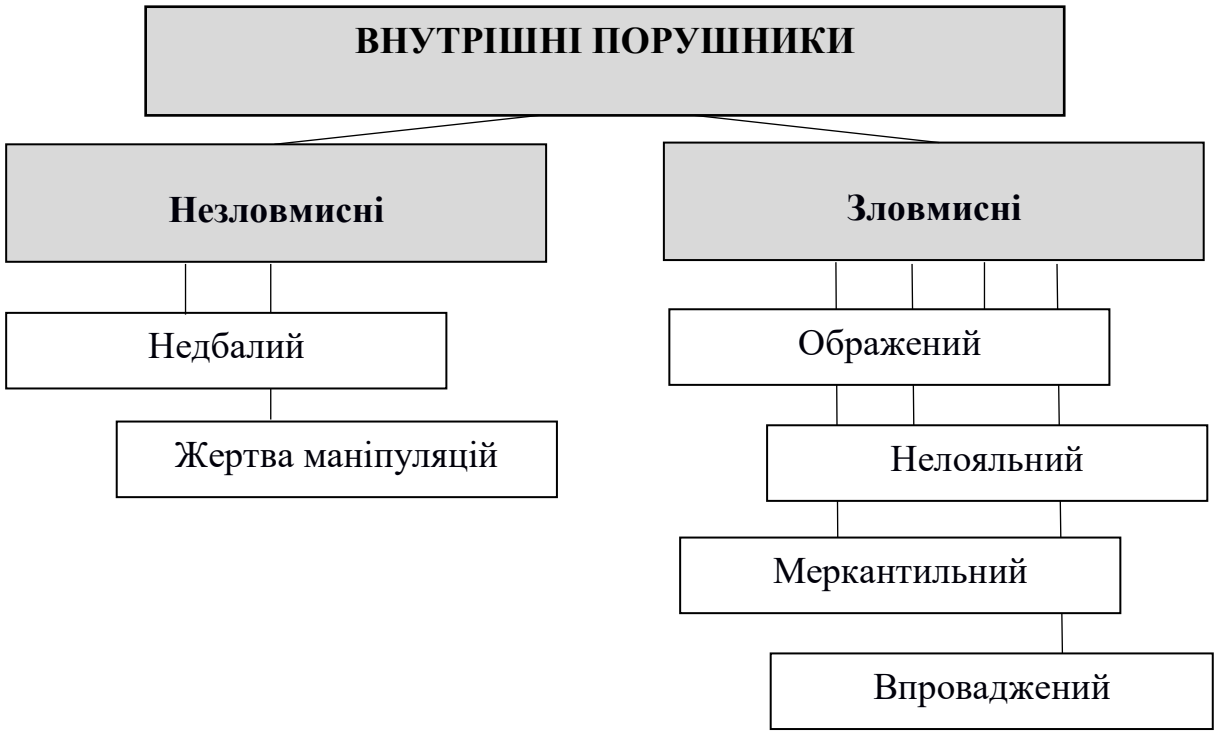

Рис.1.3. Екосистема внутрішніх порушників компанії InfoWatch.

Коротко охарактеризуємо кожну категорію. Перші дві категорії відносяться до незловмисних.

Працівник із категорії «недбалий інсайдер» є, як правило, рядовим фахівцем, який порушив вимоги про конфіденційність інформації через свою неуважність, не маючи злого умислу і не переслідуючи меркантильної мети. Однак, втрати від таких порушень можуть бути рівнозначними втратам внаслідок шпигунства.

«Інсайдер, яким маніпулюють» є жертвою використання методів «соціальної інженерії». Такий працівник під впливом обманних мотивів та інструкцій нехтує вимогами інформаційної безпеки заради «благих» цілей.

Наступні групи інсайдерів є зловмисниками, які діють усвідомлено і з власних переконань, розуміючи негативні наслідки своїх дій.

«Ображений інсайдер» або саботажник - це працівник, що розкриває конфіденційну інформацію, щоб помститися, нанести шкоду компанії загалом чи конкретній посадовій особі. Причиною може бути образа або просто відсутність моральних цінностей і бажання ефективно працювати на компанію.

Працівник типу «нелояльний інсайдер», як правило, збирається звільнитися або ж відкрити власний бізнес і паралельно прихопити конфіденційну інформацію, наприклад базу клієнтів. Особливістю таких внутрішніх порушників є те, що вони часто не приховують факт викрадення інформації, а навпаки відкрито заявляють про це, виторговуючи для себе більш вигідні умови звільнення.

Працівник, який «вирішив підзаробити», - це особа, яка завчасно налагодила контакт з потенційним покупцем інформації, яка буде викрадена. Мотиви таких інсайдерів можуть варіюватися від бажання заробити конкретну суму, якої не вистачає для реалізації своїх особистих планів, до вчинення порушення у результаті шантажу, коли в працівника фактично немає вибору. Як і вище загаданий «нелояльний інсайдер», «меркантильно налаштований» інсайдер часто застосовує імітація виробничої необхідності для досягнення своїх незаконних цілей.

«Засланий інсайдер» є працівником, який залучений до виконання завдань промислового шпигунства, тобто для вивідування комерційної таємниці, інноваційних технологій, стратегічних бізнес-планів, особистої інформації про

керівництво компанії для подальшого шантажування. Оскільки інсайдер-шпигун фінансується серйозно зацікавленими в успіху операції конкурентами, він є належним чином підготовлений і забезпечений відповідним технічним обладнанням для отримання і передачі конфіденційної інформації.

У нижченаведеній Таблиці 1.1. для кожного із згаданих видів інсайдерів проаналізовано види загроз та способи захисту.

Таблиця 1.1.

Види інсайдерів, загроз та способів захисту від них (за І.Шульгою)

Вид інсайдера	Характеристика загрози	Спосіб захисту
недбалий інсайдер	втрата інформації, її розголошення	централізація роботи пристроїв управління введенням / виведенням інформації
інсайдер, яким маніпулюють	ненавмисна передача конфіденційної інформації третім особам внаслідок «соціальної інженерії»	централізація роботи пристроїв управління введенням / виведенням інформації
скривджений інсайдер	поширення інформації у пресі або серед криміна-льних структур, її псування або пошкодження	підвищення ефективності роботи служби безпеки, HR-відділу та профспілок
нелояльний інсайдер	заволодіння інформацією з/або без зовнішнього розповсюдження, шантаж керівництва	
інсайдер, що вирішив підзаробити	передача інформації конкурентам, особам, що готують поглинання чи захоплення	підвищення ефективності роботи служби безпеки
впроваджений інсайдер		

У науковій літературі можна зустріти подібний підхід до класифікації внутрішніх порушників, відповідно до якого інсайдерів відносять до таких чотирьох груп:

1. персонал з підвищеною схильністю до конфліктів. Для цієї категорії працівників особливу небезпеку становлять ті конфлікти, які залишають неприємний осад, образу, відчуття незаслуженого покарання чи несправедливої підтримки іншого колеги з боку керівника, що в подальшому може їх підштовхнути до помсти та нанесення шкоди компанії або окремій людині.

2. працівники, які легко піддаються впливу, тобто мають підвищену схильність до навіювання та залежності від інших людей, що має наслідком зміну життєвих пріоритетів, принципів, неусвідомлені дії на користь третіх сторін.

3. кар'єристи – працівники, які не перебиратимуть способами і засобами для досягнення своїх цілей та захисту власних інтересів. Зазвичай, такі люди мають на меті зробити кар’єру та завоювати вищий соціальний статус.

4. незадоволені амбітні порушники - працівники із завищеною самооцінкою, які з різних причин не можуть реалізувати свої професійні чи особисті амбіції на роботі [21].

З огляду на те, що в нинішніх умовах масштабної інформатизації усіх процесів на підприємстві діяльність внутрішніх порушників тим чи іншим чином завжди пов’язана з засобами обробки й передачі інформації, розглянемо феномен інсайдера через призму використання інформаційно-телекомунікаційних систем [10].

У ролі внутрішніх порушників можуть виступати представники таких категорій персоналу:

- користувачі ІТКС;
- персонал, який обслуговує технічні засоби - інженери;
- працівники підрозділів програмного забезпечення - програмісти;
- персонал, який обслуговує будівлі, приміщення та системи забезпечення (прибиральники, електрики тощо);
- фахівці служби безпеки;
- керівництво.

У контексті використання ІТКС усіх порушників можна оцінювати за рівнем кваліфікації у сфері ІТ, можливостями здійснити порушення, за часом та місцем вчинення порушення.

За рівнем професійної підготовки з питань ІТКС інсайдер може бути працівником, який:

- є професійно недостатньо освіченим, але має певні навички роботи з технічними та програмними засобами;
- має середній рівень професійної підготовки, володіє навичками практичної роботи й обслуговування технічних засобів;
- є висококваліфікованим фахівцем у галузі програмування та ЕОМ, проектування й експлуатації ІТКС;
- володіє глибокими знаннями про засоби захисту інформації в ІТКС, в тому числі недоліки й переваги таких засобів.

За рівнем можливостей для вчинення протиправних дій інсайдер може застосовувати*:*

- тільки агентурні методи збирання інформації;
- технічні засоби перехоплення без зміни елементів системи;
- штатні засоби та вразливості системи захисту (використання дозволених засобів для заборонених дій), а також носії інформації, пронесені в зони безпеки;
- методи й засоби активного впливу (під'єднання додаткових технічних засобів, перехоплення даних у ході їх передавання, використання шкідливих закладок).

За часом дії внутрішній порушник може здійснювати несанкціоновані дії:

- під час роботи компонентів системи;
- у період неактивності системи (вихідні дні, планові переривання роботи, в тому числі на обслуговування й ремонт);
- в обох зазначених випадках.

Залежно від *зони доступу до ІТКС* інсайдер здійснювати порушення безпеки поза межами підприємства; з території, що охороняється, але без доступу до будівель і споруд; з приміщень, що охороняються, але без доступу до засобів обробки та передачі інформації; з робочих місць користувачів; із зон, де зберігаються конфіденційні дані (бази даних, архіви); із зон управління засобами захисту.

При аналізі дій внутрішнього порушника необхідно також враховувати *чинники, які мають вплив на його потенційну поведінку:* належним чином організована робота з підбору та розстановки, контролю діяльності персоналу ускладнює реалізацію несанкціонованих дій; приховування намірів інсайдера щодо запланованих несанкціонованих дії від інших працівників збільшує можливості порушень; на користь порушнику можуть зіграти випадкові помилки користувачів, адміністраторів, а також їхні хибні дії.

З іншого боку, важливим елементом оцінки внутрішнього порушника є *встановлення ймовірності реалізації загрози* (наявність вразливостей, недостатня організація заходів інформаційної безпеки), своєчасне виявлення та поширення інформації серед усіх зацікавлених сторін, збирання й аналіз усіх відомостей про порушення системи захисту ІТКС.

На основі аналізу всіх перелічених чинників автори підходу прийшли до висновку, що найбільшу загрозу інформаційній безпеці можуть становити фахівці служб ІТ та захисту інформації, насамперед ті, які мають ширші повноваження, наприклад, адміністратор [10]. Детальні дані представлені в таблиці 1.2.

Таблиця 1.2.

Модель внутрішнього порушника інформаційної безпеки

Категорія порушника	Мотив	Знання у сфері ІТ	Можливості для злому	Можливості за часом	Можливості за місцем	Сума загроз
Служба безпеки	1	1	1	4	3	14
Адміністратор ІТКС	1	4	1	4	4	17
Користувач	1	2	1	3	2	11
Інженер ІТКС	1	2	1	4	3	12
Електрик	1	1	1	1	1	8
Прибиральник	1	1	1	4	1	9

1.3. Напрями запобігання внутрішнім загрозам відповідно до міжнародного стандарту ISO 27002

Міжнародний стандарт ISO 27002 «Інформаційні технології. Методи забезпечення безпеки. Практичні правила управління інформаційною безпекою» дає досить детальні рекомендації для вибору, розробки, впровадження та управління заходами забезпечення інформаційної безпеки за різними напрямами, у тому числі і з забезпечення безпеки персоналу.

Відповідно до бачення розробників стандарту, робота, спрямована на запобігання загрозам з вини персоналу, поділена на три блоки:

I. до прийому на роботу,

II. у період зайнятості та

III. у разі припинення або зміни трудових відносин [40].

У рамках кожного із зазначених блоків розглянуто ті види роботи з персоналом, які, на думку фахівців ISO, є пріоритетними, але не вичерпними. Детальна схема представлена на Рис.1.4.

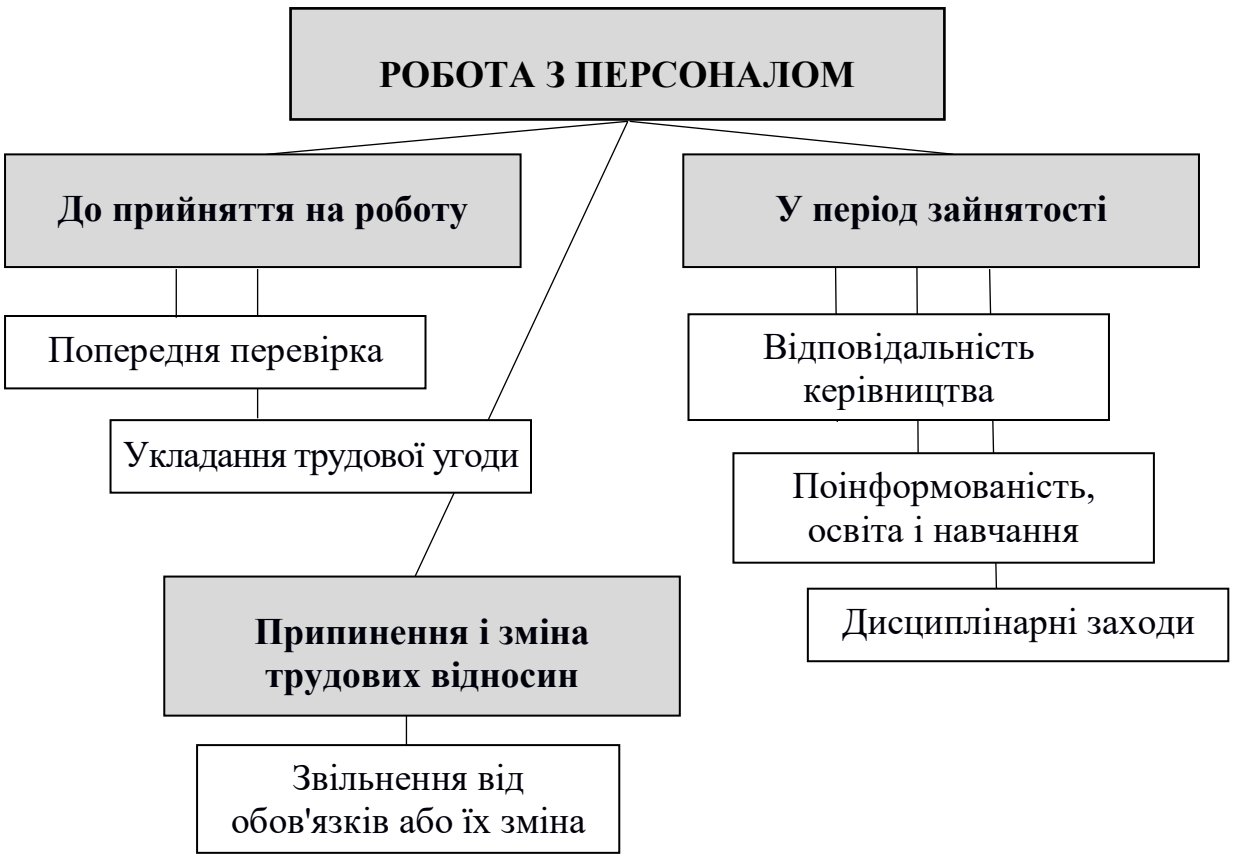

Рис.1.4. Напрями роботи з персоналом відповідно до стандарту ISO 27002.

Розглянемо сутність рекомендацій детальніше.

І. До приймання на роботу основним завданням HRM є забезпечити працевлаштування таких фахівців, які, по перше, відповідають вимогам посадови, яку вони обійматимуть, і розуміють свої професійні обов'язки. З цією метою HR-менеджери спільно з профільними фахівцями з інформаційної безпеки проводять попередню перевірку претендентів на зайняття вакантних посад у сфері інформаційної безпеки.

Перевірка при прийомі на роботу, що здійснюється для всіх кандидатів, здійснюється в рамках законодавства, нормативних документів та етичних норм, а також вона має корелювати з бізнес-вимогами, категоріями інформації, до яких працівник у подальшому матиме доступ, і прогнозованими ризиками. Кандидатів заздалегідь інформують про етапи перевірки та час їх проведення.

У ході перевірки:

- встановлюється наявність у претендента задовільних характеристик з попереднього місця роботи або від колишнього керівника;
- резюме кандидата перевіряють на повноту і точність зазначених даних;
- підтверджується заявлена освіта і професійна кваліфікація шляхом звірки наданих документів про освіту або перевірки інформації у відповідних базах даних;
- крім незалежної перевірки особи за паспортом або іншим документом, що ідентифікує особу здійснюють за потреби перевірку кредитної історії або наявність кримінального минулого [40].

Також під час перевірки з’ясовують, чи рівень фахової підготовки кандидата відповідає вимогам посади і чи він вартий довіри з огляду на високий рівень відповідальності та доступ до критичних даних підприємства.

У разі, якщо фахівець вперше отримує доступ до конфіденційних даних підприємства або отримує доступ до інформації вищого рівня конфіденційності, наприклад, фінансової, або комерційної таємниці, проводять поглиблені перевірки.

Процедури проведення перевірок претендентів на зайняття вакантних посад визначають критерії та обмеження для перевірок, категорії посадовців, які мають право перевіряти потенційних працівників, послідовність і зміст їхніх дій, час і підстави для проведення перевірок. Перевірці підлягають також особи, які працевлаштовуються за контрактом.

Відомості про всіх кандидатів, які були допущені до участі в конкурсі, збираються, обробляються і зберігаються на підприємстві відповідно до чинного законодавства.

У випадку прийняття рішення про приймання на фахівця на роботу (в тому числі такого, якого залучають за контрактом) з ним укладають трудову угоду, в якій встановляється відповідальність працівника в частині інформаційної безпеки.

Трудові угоди зі штатними працівниками та тими, хто працює за контрактом, мають містити такі обов’язкові положення:

- працівник, який отримує доступ до конфіденційної інформації, підписує угоду про нерозголошення конфіденційної інформації до моменту отримання пристроїв обробки інформації у своє розпорядження;
- працівник несе юридичну відповідальність, а також володіє певними правами, що стосуються законодавства про захист авторських прав або захисту даних;
- обов'язки працівника щодо класифікації інформації та управління нею та іншими корпоративними активами, пов'язаними з інформацією, засобами обробки інформації та інформаційними послугами;
- обов'язки працівника щодо обробки інформації, отриманої від інших компаній або зовнішніх сторін;
- санкції, які настануть у випадку невиконання працівником вимоги інформаційної безпеки [40].

Кандидатів, схвалених для працевлаштування на посаді, заздалегідь інформують про їхні функції та обов'язки щодо інформаційної безпеки та отримують їхню письмову згоду. Важливим є гарантувати, що працівники погоджуються з положеннями та умовами праці, що стосуються інформаційної

безпеки відповідно до характеру і рівня доступу до корпоративних активів, пов'язаних з інформаційними системами і сервісами.

Обов'язки працівника (контрактника) щодо забезпечення конфіденційності, захисту даних, правил поведінки, належного використання обладнання підприємства, а також проходження вступної практики, можуть бути також закріплені у Кодексі поведінки.

II. У період зайнятості основним завданням роботи з персоналом є гарантувати, що працівники і фахівці, які працюють за контрактом, знають свої обов'язки з інформаційної безпеки та якісно їх виконують.

Керівництво підприємства відповідає за виконання усіма штатними працівниками та контрактниками вимог інформаційної безпеки відповідно до встановлених політик і процедур.

Керівники підприємства мають забезпечити, щоб працівники:

- були належним чином поінформовані про свої повноваження і відповідальність у сфері інформаційної безпеки до отримання доступу до конфіденційної інформації та засобів її оброки;
- були забезпечені керівними вказівками щодо способів дотримання ними вимог інформаційної безпеки, пов'язаних з виконанням їхніх повноважень;
- володіли високою мотивацією виконання політик інформаційної безпеки;
- погодилися з умовами зайнятості, в тому числі вимогами політики інформаційної безпеки та відповідними методами роботи;
- підтримували належний рівень навичок і кваліфікації і за потреби проходили навчання;
- знали про існування каналу для анонімного інформування про порушення інформаційної безпеки і користувалися ним у разі виявлення таких випадків [40].

Керівництво підприємства усіма засобами має демонструвати підтримку політик, процедур і засобів забезпечення інформаційної безпеки, а також показувати власний приклад відповідних дій.

Якщо персонал не буде обізнаним про вимоги інформаційної безпеки та відповідальність з їх порушення, це може завдати помітної шкоди підприємству

через нехтування правила безпекою або неправильну поведінку у критичних ситуаціях.

Поінформованість, освіта і навчання в сфері інформаційної безпеки є критично важливою для досягнення прийнятного рівня інформаційної безпеки підприємства. Увесь персонал підприємства має бути достатньо обізнаним і навченим, а також регулярно інформуватися про зміни в політиках і процедурах інформаційної безпеки, що стосуються виконання службових обов'язків конкретних працівників.

З цією метою на підприємстві розробляється програма з інформування з інформаційної безпеки, яка узгоджується з корпоративними політиками і процедурами інформаційної безпеки, а також враховує інформацію, яка підлягає захисту і заходи для її захисту.

У рамках програми проводять регулярні інформаційно-агітаційні заходи, випускають брошури та інформаційні листи, які обов’язково мають спрямовуватися на окремі цільові групи персоналу з урахуванням рівня їх відповідальності та обізнаності з питаннями інформаційної безпеки. Заходи програми можуть повторюватися і охоплювали новоприбулих працівників, регулярно оновлюватися у відповідності з політиками і процедурами інформаційної безпеки, а також враховувати уроки, винесені внаслідок інцидентів.

Для інформування персоналу можуть використовувати різні методи навчання, серед яких заняття в класах, самостійне ознайомлення, дистанційне та онлайн навчання тощо.

Працівників підприємства, задіяних у сфері інформаційної безпеки, та робота яких дотична до цієї сфери, інформують та навчають з таких питань:

- зобов’язання керівництва щодо інформаційної безпеки;
- правила й повноваження з інформаційної безпеки, обов’язкові до виконання;
- персональна відповідальність за дії або бездіяльність, а також спільна відповідальність щодо безпеки;

- основні процедури інформаційної безпеки, наприклад, звіти про порушення, і заходи забезпечення безпеки (використання безпечних паролів, контроль шкідливих програм тощо);
- контакти і ресурси для отримання додаткової інформації з питань інформаційної безпеки, включаючи додаткові матеріали для навчання та самостійної підготовки.

Програма інформування має забезпечити формування у персоналу здатності об'єктивно оцінити наслідки своїх неправомірних дій; стабільних звичок безпечної поведінки у сфері інформаційної безпеки на основі дотримання вимог політик безпеки та рекомендацій; навиків швидко і правильно реагувати в разі настання інциденту інформаційної безпеки та в критичних ситуаціях [32].

Навчання і підготовка в галузі інформаційної безпеки здійснюються регулярно на основі відповідної програми, яка включає використання різних форм навчання і підготовки. Первинне навчання та підготовка новоприбулих або новопризначених працівників проводяться до того, як вони приступлять до виконання обов'язків.

При формуванні програми важливо фокусувати увагу на тому, щоб працівники розуміли мету й завдання інформаційної безпеки та наслідки своїх потенційно небезпечних дій для підприємства. Успішність засвоєння працівниками представленого для навчання матеріалу перевіряють у кінці занять чи курсів шляхом анкетувань та відгуків.

Важливу роль у забезпеченні безпеки персоналу у контексті інформаційної безпеки відіграють *дисциплінарні заходи.* До відома персоналу насамперед має бути доведена інформація про заходи до тих працівників, які порушили вимоги інформаційної безпеки.

Дисциплінарні заходи, які застосовують тільки після попередньої перевірки і підтвердження фактів порушення інформаційної безпеки, мають гарантувати толерантність і справедливість до працівників, яких підозрюють у порушенні інформаційної безпеки; враховувати такі чинники як характер і серйозність порушення і його вплив на бізнес; одноразовість чи повторюваність подібних дій

з боку конкретної особи; наявність злого умислу; проходження порушником відповідної підготовки; відповідність дисциплінарного процесу вимогам законодавства та бізнес-контрактів.

Дисциплінарні заходи мають також і профілактичний ефект, запобігаючи подальшим порушенням вимог політик та процедур інформаційної безпеки з боку персоналу. Дисциплінарні заходи можуть бути мотивуючим фактором, якщо за зразкову поведінку з інформаційної безпеки передбачено використання заохочувальних засобів.

III. При припиненні або зміні трудових відносин з працівником підприємство має насамперед захистити власні інтереси від подальших можливих неправомірних дій з боку звільненої або переміщеної особи.

Для того, щоб зменшити вірогідність настання несприятливих для підприємства наслідків внаслідок звільнення чи зміни місця роботи штатного працівника чи контрактника необхідно, як зазначалося вище, перед працевлаштуванням визначити і довести до відома фахівця перелік його повноважень та міру відповідальності за порушення вимог інформаційної безпеки, звернувши його увагу, що вони залишаються в силі навіть після припинення або зміни трудових відносин.

Крім того, попередження про припинення трудових відносин має містити інформацію про існуючі вимоги з інформаційної безпеки та юридичні зобов'язання працівника, що зберігають свою силу протягом певного періоду після завершення трудових відносин з підприємством. Відповідальність і обов'язки, які залишаються в силі після завершення трудових відносин, зазначаються і в трудовій угоді або контракті.

Загальну відповідальність за процес припинення трудових відносин з працівником несе підрозділ з управління персоналом, який взаємодіє з лінійним керівником в частині виконання відповідних процедур з інформаційної безпеки. У випадку звільнення працівника чи зміни місця роботи в межах підприємства не лишнім є інформування решти персоналу, споживачів або підрядників про зміни в штатному складі та організаційній структурі підприємства.

Висновки до першого розділу

З огляду на те, що в нинішніх умовах ключовою передумовою розвитку підприємства і основним чинником забезпечення його інформаційної безпеки є відповідальний і надійний персонал, важливим завданням кожного підприємства є ефективне управління людськими ресурсами. Управління людськими ресурсами є комплексом взаємопов'язаних організаційних, економічних і соціальних заходів з метою створення умов сталого розвитку і ефективного використання потенціалу робочої сили підприємства.

Управління людськими ресурсами для вирішення своїх завдань використовує низку технологій, які розділяють на технології збирання й оцінювання особистої інформації про працівника; збирання й аналізу кількісних та якісних характеристик складу персоналу для здійснення відбору, формування резерву, кадрового планування; підвищення результативності праці персоналу, які використовують для підбору, ротації, управління кар'єрою працівників тощо.

Розглянуто різні категорії потенційних внутрішніх порушників (від фахівців служби безпеки підприємства до обслуговуючого персоналу) відповідно до таких критеріїв: рівень професійної підготовки з ІКТ, наявність можливостей для вчинення протиправних дій, час дії та зона доступу до ІТКС, чинники, що впливають на потенційну поведінку порушника, наявність вразливостей у системі захисту ІТКС, і зроблено висновок, що найбільшу загрозу інформаційній безпеці можуть становити фахівці служб ІТ та захисту інформації.

Вивчення положень міжнародного стандарту ISO 27002 «Інформаційні технології. Методи забезпечення безпеки. Практичні правила управління інформаційною безпекою» показало, що роботу з персоналом у сфері інформаційної безпеки умовно можна поділити на три блоки: до прийому на роботу (попередня перевірка, укладання трудової угоди та угоди про нерозголошення), у період зайнятості (розподіл відповідальності, забезпечення обізнаності й навчання персоналу, дисциплінарні заходи) та у разі припинення або зміни трудових відносин.

Розділ 2.
ОРГАНІЗАЦІЯ НАВЧАННЯ ПЕРСОНАЛУ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Форми і тематика навчання з питань інформаційної безпеки

Наука і практика інформаційної безпеки вже давно довели, що ключову роль у забезпеченні ефективного захисту інформаційних активів підприємства відіграє людина, з одного боку, це зовнішні порушники, які організовують і реалізують різноманітні атаки на корпоративні ІТКС, з іншого – інсайдери, які навмисно чи випадково порушують вимоги інформаційної безпеки.

Оскільки статистика інформаційної безпеки свідчить про велику кількість порушень з боку персоналу внаслідок незнання або недостатньої кваліфікації, тільки якісна підготовка працівників підприємства загалом і спеціалістів з інформаційної безпеки зокрема здатна сформувати достатній багаж знань і навичок поводження з конфіденційною інформацією, ІТКС і обчислювальною технікою, забезпечуючи дотримання регламентів та інструкцій щодо захисту інформації на кожному технологічному етапі її використання.

Якщо персонал підприємства знає правила роботи з відомостями обмеженого доступу та володіє необхідними для їх виконання навичками, реальним є забезпечення інформаційної безпеки на довгострокову перспективу. Відсутність освіти з питань безпеки персоналу може звести нанівець усі заходи технічного спрямування, нормативні та організаційні активності. Для того, щоб запобігти виникненню ризиків, пов'язаних із відсутністю або недостатністю необхідних фахових знань і навичок, необхідно впровадити комплексний підхід до навчання і тренувань персоналу з питань інформаційної безпеки.

Навчання з питань інформаційної безпеки традиційно розпочинають з офіційно оформленої процедури інформування новопризначеного фахівця про усі необхідні йому для роботи аспекти забезпечення захисту інформації, в тому числі положення політики безпеки, регламентів та процедур.

Надалі працівника ознайомлюють із детальними вимогами безпеки, правовою відповідальністю та бізнес-заходами, а також навчають безпечному використанню засобів обробки та передавання інформації.

Відповідно до ролі, повноважень та специфіки роботи працівника навичкам особи навчання має бути узгодженим і зорієнтованим на забезпечення результативного виконання професійних завдань. Працівник має знати про існування відомих загроз, каналів звітування щодо інцидентів інформаційної безпеки і контакти посадових осіб, з ким потрібно контактувати в умовах кризової ситуації для отримання подальших рекомендацій.

Навчання та практичну підготовку персоналу розглядають як засіб, що допомагає працівникам усвідомити проблеми, розуміти причини та наслідки інцидентів інформаційної безпеки і реагувати відповідно до встановлених процедур у рамках своїх посадових ролей. Загалом навчання й підвищення кваліфікації виконують запобіжну роль у забезпеченні інформаційної безпеки. Адже, у кінцевому рахунку завдяки системі своєчасного і актуального навчання забезпечується покращення поінформованості персоналу та підвищується рівень дотримання вимог інформаційної безпеки.

Здійснюючи регулярну та узгоджену освітню діяльність підприємство не тільки формує у співробітників розуміння основ інформаційної безпеки, розвиває їхні професійні навички й уміння, але також сприяє формуванню корпоративної культури інформаційної безпеки. Актуальність цього питання визнано на міжнародному рівні, зокрема у доктринах інформаційної безпеки країн НАТО серед першочергових завдань встановлено всебічне навчання персоналу основам забезпечення захисту інформації, безперервне підвищення кваліфікації працівників, проведення стажувань, тренінгів та інших заходів практичного спрямування [6]. Важливу роль у нинішніх умовах розвитку ІТКС відіграють інформаційні технології, використання яких дозволяє значно розширити підходи і методики навчання і контролю отриманих знань.

Основними принципами, яких варто дотримуватися при реалізації комплексу навчальних заходів з інформаційної безпеки на підприємстві, є:

1. вибудовувати поетапний процес навчання персоналу з моменту прийняття на роботу, залучати команду менеджерів, які відповідатимуть за реалізацію навчальних програм на кожному етапі.

2. безперервно і регулярно навчати працівників методам і вимогам інформаційної безпеки, прищеплювати культуру безпеки поводження з даними безпосередньо на кожному робочому місці, включати навчальні й ігрові моменти в повсякденну діяльність фахівців для пошуку і використання ефективних методів вирішення проблеми.

3. використовувати інноваційні рішення в галузі інформаційної безпеки, наводити актуальні й переконливих приклади із практики, робити акцент на здійсненні комплексного захисту інформації, який включає впровадження різноманітних дій та дозволяє отримати якісний результат і мінімізувати ризики інформаційним активам підприємства.

4. обирати оптимальний підхід чи методи вирішення проблем безпеки із демонстрацією багатьох можливих і аргументуванням, чому обраний є найбільш прийнятним варіантом. Працівник має дотримуватися правил безпеки на рівні інтуїції, практично автоматично застосовувати професійні навички і звички у відповідних ситуаціях.

5. пояснювати працівникам причину для посилених вимог безпеки, наводити вагомі докази і вдалі приклади. Наприклад, витік чи втрату облікових даних і документів користувача краще попередити, ніж мати такі негативні наслідки як відтік клієнтів, фінансові збитки чи репутаційні втрати. Розуміння причин обмежень інформаційної безпеки сприяє підвищенню відповідальності персоналу та зменшенню випадків недбалості в ситуаціях «високого ризику».

6. використовувати індивідуальний підхід до навчання різних категорій працівників, по перше, забезпечувати тісний зв’язок навчання з їх повноваженнями в системі інформаційної безпеки та ризиками, з якими вони стикаються у повсякденній фаховій діяльності; по друге, застосовувати нові методи і способи навчання, засновані на принципах креативності, у відповідності до професійних та особистісних характеристик працівників [26].

7. вивчати зразки передового досвіду, інноваційних технологій, ефективних методів організації праці в процесі навчання персоналу з інформаційної безпеки.

8. регулярно перевіряти рівень знань, зокрема положень політик і процедур, та їх застосування у практиці забезпечення інформаційної безпеки, використовувати також методи тестування для перевірки засвоєння необхідних знань.

9. створювати можливості регулярного навчання працівників незалежно від їх посади, місцезнаходження і без відриву від робочого процесу.

10. надавати навчальні та інформаційні матеріали користувачам у доступній і зрозумілій формі, забезпечуючи їх цільове спрямування.

Варто відзначити, що для всіх працівників підприємства, незалежно від сфери їх діяльності та займаної посади проводять заходи із загальних питань забезпечення інформаційної безпеки. Крім загальної програми забезпечення компетентності в питаннях безпеки, призначеної для кожного співробітника організації, необхідно спеціальне навчання персоналу, пов'язане із завданнями і обов'язками щодо забезпечення інформаційної безпеки.

Ступінь цього навчання залежить від рівня важливості інформаційної безпеки для організації і має змінюватися відповідно до вимог безпеки з урахуванням виконуваної роботи. Кожен новий проект зі спеціальними вимогами безпеки повинен супроводжуватися відповідною програмою навчання, розробленою до початку проекту і своєчасно виконуваною.

Теми курсів навчання інформаційної безпеки повинні відповідати функціям і посадовими обов'язкам працівників, які навчаються. Фахівці рекомендують включати в список такі теми:

- сутність поняття «безпека» та дотичних термінів;
- методи запобігання порушенням конфіденційності, цілісності та доступності інформації;
- потенційні загрози технологічного й антропогенного характеру;
- класифікація інформації (комерційна і професійні таємниці, персональні дані, конфіденційна, приватна інформація тощо);
- процес забезпечення інформаційної безпеки, етапи і зміст;

- підходи до аналізу ризиків;
- заходи, засоби захисту, прийоми їх застосування на практиці;
- ролі і обов'язки працівників;
- положення політики інформаційної безпеки, регламентів і стандартів, процедур, інструкцій, інших супроводжуючих документів.

Відповідно до вітчизняного законодавства підприємство може організувати й компенсувати у повному обсязі або частково своїм працівникам здобуття вищої або професійно-технічної освіти, післядипломне навчання (спеціалізацію, перепідготовку, підвищення кваліфікації), професійне навчання (первинну професійну підготовку, перепідготовку, підвищення кваліфікації або спеціалізацію, стажування [15].

На практиці найчастіше використовуються такі форми навчання як:

- заняття теоретичного характеру (лекції, семінари) та практичні заняття щодо дій персоналу в різних ситуаціях;
- тестування і оцінювання рівня підготовки персоналу;
- рольові ігри, ситуаційні завдання, пов’язані із вирішенням проблем захисту інформації;
- розв’язання інтелектуальних завдань з метою отримання навичок аналізу і прогнозування різних проблемних ситуацій у сфері інформаційної безпеки;
- застосування спеціалізованих програм навчання, в т.ч. дистанційної форми.

Також навчати персонал можна шляхом проведення вузькоспеціалізованих тренінгів, наставництва, участі у конференціях, форумах та інших заходах з обміну досвідом.

Крім навчання потрібно проводити перевірки отриманих знань в різних формах: тестування при навчанні, внутрішня перевірка на підприємстві, перевірка аудитором при тестуванні захисту, використання автоматизованих систем тестування, наприклад, Moodle.

Обов’язковим елементом програми навчання персоналу є проведення регулярних інструктажів, під час яких працівників інформують про зміни і доповнення у діючих нормативних і методичних документах, положення нових

наказів керівництва підприємства в галузі інформаційної безпеки; актуальні загрози інформації, канали витоку інформації, дії зловмисників, прийняті додаткові заходи щодо захисту інформації. Також у рамках інструктажів аналізуються випадки порушення персоналом правил захисту інформації [37].

До «нестандартних» методів відносять методи, які, зазвичай, не використовують для навчання, однак завдяки яким на рівні підсвідомості у працівника закарбовуються ключові положення і формується розуміння важливих вимог, наприклад: відеозаписи, анімаційні ролики, новини з проблем інформаційної безпеки, заставка екрану з нормами безпечної поведінки, офісне приладдя (ручки, календарі, щоденники тощо) [31].

Загальна схема форм і типової тематики навчання персоналу з інформаційної безпеки показано на Рис.2.1.

Рис.2.1. Форми і тематика навчання персоналу з інформаційної безпеки.

Для збільшення зацікавленості персоналу в навчанні та дотриманні вимог інформаційної треба правильно і цілеспрямовано мотивувати працівників, або

залучати їх безпосередньо в навчальний процес шляхом використання методів гейміфікації (занурення в тему і полегшення сприйняття інформації); проведення кібернавчань (створення атмосфери реальної кризової ситуації і спонукання працівника до здійснення конкретних дій) тощо [8].

Корисним при вивченні підходів до навчання персоналу з питань інформаційної безпеки є розгляд практичних зразків реалізації навчальних програм провідними компаніями у сфері ІТ та безпеки. Наприклад, компанія «Лабораторія Касперського» впроваджує освітні програми для своїх фахівців та персоналу інших організацій, які передбачають навчання спеціалістів на базовому, середньому й експертному рівнях і зорієнтовані на рядових працівників, лінійних керівників та топ-менеджмент підприємства відповідно. Також освітні курси з інформаційної безпеки «Лабораторії Касперського» варіюються в залежності від рівня професійної підготовки та повноважень аудиторії та пропонують різні форми навчання. Зазначений інноваційний підхід проілюстровано в Таблиці 2.1.

Таблиця 2.1.

Інноваційні освітні програми «Лабораторії Касперського»

Працівники	Рівень 1, базовий	
Онлайн-платформа	Основи ІБ *Базові знання в галузі ІТ*	Основи ІБ, практичний курс *Базові навички в галузі ІТ*
Лінійні керівники	Рівень 2, середній	
Ігровий формат	Цифрова криміналістика *Потрібні навички системного адміністрування*	Аналіз і зворотна розробка шкідливого ПЗ *Потрібні навички програмування*
Топ-менеджмент	Рівень 3, експертний	
Оцінка рівня обізнаності з ІБ	Цифрова криміналістика. Професійний рівень *Потрібні експертні навички системного адміністрування*	Аналіз і зворотна розробка шкідливого ПЗ *Потрібні навички програмування на мові Ассемблер*

Перевагами даної програми є диференціація цільових аудиторій навчання, використання різних методів навчання, в тому числі заняття онлайн, практичне спрямування курсів, які передбачають використання сучасних засобів, залучення до викладання і тренінгів фахівців високого класу, що дозволить вивчити передовий досвід виявлення та запобігання порушенням інформаційної безпеки за допомогою новітніх технологій [33].

2.2. Розробка програми навчання персоналу з інформаційної безпеки

Як відзначалося вище, навчально-просвітницька діяльність підприємства чи організації має впроваджуватися на основі та в рамках відповідної програми. Програма має на меті систематизацію й узгодження різних видів діяльності, спрямованих на навчання персоналу з інформаційної безпеки.

Розглянемо основні елементи такої типової програми (Рис. 2.2.).

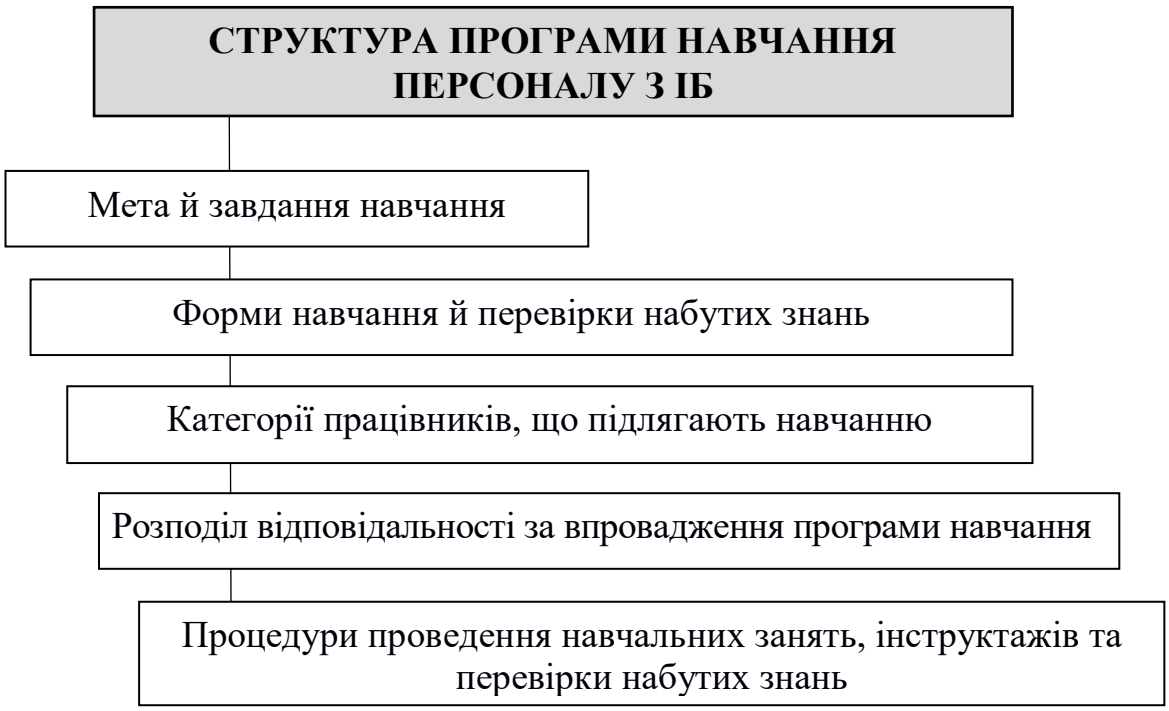

Рис. 2.2. Структура програми навчання персоналу з інформаційної безпеки.

Типова програма навчання персоналу з інформаційної безпеки має включати такі структурні *елементи*:

- мета й завдання навчання,
- основні види навчання,

• порядок взаємодії структурних підрозділів підприємства в ході навчальної діяльності,

• ролі й повноваження працівників, відповідальних за організацію [28].

Метою навчання персоналу є формування та підтримання належного рівня знань та навичок працівників у сфері інформаційної безпеки та забезпечення високого рівня їхньої безпечної поведінки в корпоративних інформаційно-телекомунікаційних системах.

Завданнями програми навчання з інформаційної безпеки є:

• виявлення потреби в навчанні;

• планування комплексу заходів відповідно до специфіки бізнес-процесів компанії та на основі кращого досвіду й апробованих методів організації навчання персоналу з інформаційної безпеки;

• встановлення бюджету на впровадження навчальних заходів;

• організація навчання і контроль його результативності;

• мотивування персоналу до вивчення й розуміння вимог безпеки і відповідального ставлення до їх дотримання;

• регулярна перевірка знань в сфері інформаційної безпеки та ступеню їх застосування на практиці.

Для забезпечення результативної професійної підготовки персоналу з інформаційної безпеки необхідно використовувати різні *форми навчання*, зокрема планові і позапланові.

Планові навчально-просвітницькі заходи проводять відповідно до плану, встановленого програмою, і включають:

для нового працівника

• вступний інструктаж – для новопризначеного фахівця після підписання контракту і перед вступом на посаду;

• первинний інструктаж на робочому місці;

• первинну перевірку знань, яка відбувається не раніше, ніж через три місяці після призначення на посаду.

для працюючого персоналу

повторне навчання - для працівників і керівників підрозділів, до роботи яких висувають додаткові (посилені) вимоги з інформаційної безпеки.

Позапланові навчально-просвітницькі заходи проводять у випадку виробничої необхідності, а також у відповідь на запит керівників структурних підрозділів компанії. Причинами можуть бути зміни у вимогах інформаційної безпеки, технологічних процесах або поява нових типів порушень інформаційної безпеки. Позапланові навчальні заходи також супроводжуються перевіркою рівня засвоєння знань персоналом [31].

Окремим напрямом освітньої діяльності компанії є *цільове навчання*, яке здійснюється при виконанні працівником нетипових, разових видів робіт, безпосередньо не пов'язаних з його функціональними обов'язками. *Спеціальне навчання* проводять при виконанні працівником робіт з додатковими (посиленими) вимогами у сфері інформаційної безпеки.

За формами проведення заходи навчання й перевірки знань поділяють на індивідуальні та корпоративні (групові), внутрішні і зовнішні. Індивідуальне навчання передбачає проведення особистих бесід і занять з працівником. Корпоративне (групове) навчання використовує методи організації освітньої чи практичної діяльності для групи або кількох фахівців підрозділу одночасно. Внутрішнє навчання проводять за рахунок внутрішніх фінансових, матеріальних та людських ресурсів компанії; зовнішнє - із залученням зовнішніх освітніх або тренінгових організацій.

Навчальні та інструктивні заходи з інформаційної безпеки проводяться в робочий час.

До персоналу, що охоплюється заходами навчання з інформаційної безпеки, відносять такі категорії працівників:

- керівники підрозділів і працівники, робота яких прямо або опосередковано пов’язана з забезпеченням інформаційної безпеки;
- практиканти та працівники, які тимчасово працевлаштовані або залучені на основі контрактів;

• працівники, які виконують роботи з додатковими (посиленими) вимогами з інформаційної безпеки [25].

Відповідальність за організацію навчання з інформаційної безпеки на рівні компанії покладають на голову правління або представника топ-менеджменту, відповідального за безпековий напрям, у структурних підрозділах компанії відповідальність за навчання персоналу покладається на їхніх керівників. Підрозділ інформаційної безпеки здійснює загальний нагляд за своєчасністю і дотриманням термінів проведення навчальних заходів.

Проведення первинного інструктажу для новопризначених фахівців здійснює працівник підрозділу інформаційної безпеки. Перевірка знань з інформаційної безпеки новопризначених працівників здійснюється не пізніше трьох місяців після призначення на посаду і не рідше разу на три роки.

Працівники та керівники підрозділів, які працюють у відповідності з посиленими (додатковими) вимогами з інформаційної безпеки, проходять навчання і перевірку наявних професійних знань і навичок за посадою раз на три роки. До цієї категорії відносять і фахівців підрозділу інформаційної безпеки.

Позапланове навчання з інформаційної безпеки проходять працівники і керівники компанії незалежно від часу проходження попереднього навчання за умови введення в дію нових нормативів, змін у технологічних процесах та обладнанні, виявленні у працівника браку знань та навичок за фахом, виникнення інцидентів інформаційної безпеки, більш, ніж річній перерві у виконанні особою професійних функцій.

Для проведення перевірки знань персоналу з питань інформаційної безпеки згідно з наказом керівника компанії створюється спеціальна комісія, до складу якої входять фахівці з інформаційної безпеки, представники підрозділів, працівники яких підлягають перевірці, та за потреби фахівці зовнішніх організацій.

Навчання персоналу з питань інформаційної безпеки проводиться за програмами, розробленими навчальними та тренінговими центрами, освітніми установами, що мають дозвіл на проведення навчання за конкретною спеціалізацією. Програми узгоджуються з керівництвом компанії-замовника.

Спеціальне навчання для працівників, які виконують функції згідно з додатковими (посиленими) вимогами з інформаційної безпеки, проводиться у порядку, за формою, з періодичністю і тривалістю, встановленими керівництвом компанії з огляду на спеціальність, види операцій, специфіку й умови праці персоналу.

Після завершення працівником курсу навчання зазначена комісія перевіряє ступінь засвоєння ним теоретичних знань і володіння практичними навичками за темою. Результати усіх перевірок результативності та якості навчання фіксуються документально. Право приступити до самостійної роботи надається працівникові після завершення навчання тільки за умови успішного проходження перевірки рівня знань і навичок [28].

Вступний інструктаж з інформаційної безпеки проводять для всіх осіб, які прийняті на роботу незалежно від освіти, стажу роботи за фахом або посади, тимчасово працевлаштованих і відряджених працівників, представників сторонніх організацій, які працюють у компанії. Фахівець підрозділу інформаційної безпеки знайомить новачка з нормами законодавчих та нормативних актів з інформаційної безпеки, правилами безпечної роботи в корпоративних ІТКС, його посадовими обов'язками з інформаційної безпеки.

Зміст і структура вступного інструктажу формуються відповідно до положень стандартів, нормативів, правил та інструкцій з інформаційної безпеки, а також з урахуванням специфіки корпоративних технологічних процесів.

Первинний інструктаж на робочому місці проводить фахівець підрозділу інформаційної безпеки, який найчастіше є керівником робіт, до початку виконання новопризначеним працівником своїх обов'язків за посадою з додатковими (посиленими) вимогами з інформаційної безпеки. У рамках первинного інструктажу на робочому місці індивідуально для кожного працівника на практиці показують безпечні прийоми і методи виконання його обов'язків. Можливим є проведення первинного інструктажу для групи працівників, які виконують типові операції в межах загального робочого місця [21].

Новопризначений працівник допускається до роботи після стажування, успішного проходження перевірки теоретичних знань і набутих навичок щодо належного і безпечного виконання робіт за фахом.

Результати первинного інструктажу фіксуються документально.

Повторний інструктаж проходять усі працівники компанії незалежно від кваліфікації, освіти, стажу, характеру роботи не рідше разу на три роки.

Позаплановий інструктаж проводять, якщо:

• введено в дію нові або відкориговано положення діючих нормативних документів з інформаційної безпеки;

• внесено зміни в технологічні процеси, здійснено заміну обладнання або програмного забезпечення, внаслідок чого виникла потреба в додаткових знаннях та навичках персоналу з інформаційної безпеки;

• працівника призначено або переведено на іншу посаду, і нові обов'язки вимагають додаткових знань і навичок з інформаційної безпеки;

• встановлено недостатній для виконання функціональних обов’язків рівень знань працівника;

• відбулися серйозні інциденти і зросла вірогідність реалізації загроз інформаційній безпеці, а також зафіксовані випадки порушення з боку персоналу вимог нормативних документів з інформаційної безпеки;

• працівник перервав роботу на посаді терміном понад півроку/рік;

• органи державного нагляду звернулися з відповідними вимогами.

Позаплановий інструктаж може бути проведено персонально або для групи фахівців однієї спеціальності. Обсяг і зміст інструктивних матеріалів визначають в кожному конкретному випадку з урахуванням причин його проведення.

Дані про результати первинного інструктажу фіксуються документально із зазначенням причин його проведення.

Цільовий інструктаж проводять перед початком виконання одноразових робіт, безпосередньо не пов'язаних з обов'язками працівника. Цільовий інструктаж проводять керівники підрозділів або безпосередньо керівник робіт, наприклад робіт із усунення наслідків інцидентів інформаційної безпеки [31].

По завершенню інструктажів на робочому місці в обов'язковому порядку здійснюють перевірку рівня засвоєних знань шляхом усного опитування, а набутих навичок щодо безпечних способів роботи через виконання практичних завдань. Працівник допускається до роботи тільки після успішного проходження зазначеної перевірки.

У випадках проведення усіх видів первинного інструктажу на робочому місці робиться запис у відповідному реєстраційному документі за підписом інструктора та особи, яку інструктували. У реєстраційному записі про позаплановий і цільовий інструктаж зазначаються причини їхнього проведення.

2.3. Огляд програмного забезпечення для навчання й інформування з питань інформаційної безпеки

Для задоволення потреб підприємства у забезпеченні високого рівня обізнаності та професійної підготовки персоналу з інформаційної безпеки сьогодні використовують велику кількість різноманітних програмних інструментів.

Сьогодні, коли традиційне навчання стає менш ефективним, а забезпечення інформаційної безпеки особи та підприємства стає критичним, розробники спеціалізованого ПЗ у даній сфері шукають рішення, які фокусуються на формуванні безпечної поведінки та зміні культури безпеки, надають всебічну і безперервну підтримку на глобальному рівні незалежно від локалізації компанії-замовника, і пропонують позитивний, надійний і легкий для сприйняття зміст.

Зараз продовжують зміщуватися акценти з понять короткої часової дії - «обізнаність» і «покарання», на поняття довготривалої перспективи: «поведінка» і «культура», що точно відображає зміну розуміння і ставлення до проблем недостатньої фахової підготовки персоналу в галузі інформаційної безпеки.

Ринок ПЗ з навчання і формування інформованості, який є надзвичайно динамічним, конкурентним і затребуваним, постійно представляє нових постачальників та нові пропозиції від уже досвідчених гравців. Сьогодні

розробники ПЗ у сфері навчання та формування обізнаності пропонують програмні інструменти, які:

- виховують культуру безпеки, замість того, щоб проводити бездоганну підготовку та тестування;
- надають цікаві, всеосяжні рішення. створюють позитивний вміст з інклюзивними, чіткими, і переконливими зображеннями;
- залучають користувачів до альтернативних типів вмісту, таких як гейміфікація, мікронавчання та віртуальна реальність;
- можуть розмовляти з усіма користувачами незалежно від місця проживання та мови спілкування - і для цього потрібні різні стилі для кожного регіону;
- мають центри підтримки у всіх регіонах, де вони проводять операції та локалізують вербальну, текстову та аудіо- та візуальну комунікацію.

На користь використання ПЗ для навчання та підвищення обізнаності персоналу та розгляду їх у числі пріоритетних засобів посилення інформаційної безпеки свідчать дослідження компанії Webroot у 2019 році. Так, дані Webroot підтверджують, що:

• проведення 1-5 кампаній з підвищення обізнаності з інформаційної безпеки протягом 1-2 місяців показало середній рівень переходів за посиланнями на симуляції фішингу - 37%;

• проведення 6-10 кампаній та тренінгів протягом 3-4 місяців знизили рівень переходів до 28%;

• проведення 11 та більше курсів упродовж 4-6 місяців знизило їхній рівень до 13% [43].

Основою для здійснення огляду й характеристики найбільш значущих постачальників програмного забезпечення для обізнаності та навчання з інформаційної безпеки (Security Awareness And Training, SA&T) стало дослідження компанії Forrester «Security Awareness And Training Solutions, Q1 2020» [42].

За результатами дослідження визначено 12 найкращих компаній розробників ПЗ у сфері SA&T, які були поділені на чотири групи: лідери, стійкі гравці, конкуренти і претенденти (Рис. 2.3.).

Рис.2.3. Ринкові позиції компаній-розробників ПЗ у сфері SA&T.

Для внесення постачальника до списку були використані такі критерії:

- глобальна присутність та база клієнтів (не менше, ніж на двох континентах);
- сегментація даних користувачів для збору показників програми;
- просування ідеї поширення культури безпеки та кращих практик на всю робочу силу;
- значний інтерес до виробника з боку клієнтів компанії Forrester.

Отже, відповідно до результатів дослідження компанії Forrester до п’ятірки найкращих виробників ПЗ з питань навчання та формування обізнаності у сфері інформаційної безпеки віднесено західні компанії KnowBe4, CybSafe, Infosec та Elevate Security (3 з 4-х створені у США). Коротко охарактеризуємо компанії-лідерів.

І. Платформа *KnowBe4 Mitnick Security Awareness Training* має величезну бібліотека контенту безпеки, містить багато видів навчальних занять, тисячу навчальних модулів від десяти різних виробників контенту, 3,5 тисячі фішинг-

шаблонів та засоби оцінювання рівня культури безпеки. Також платформа KnowBe4 дозволяє проводити «гігієнічні» заходи безпеки, що забезпечують комплексне, перспективне мислення персоналу, пропозиції, орієнтовані на споживача, включаючи прозорі ключові показники ефективності.

Фахівці компанії Forrester рекомендують продукт KnowBe4 для використання як такий, що забезпечує реалізацію комплексної програми підвищення обізнаності щодо інформаційної безпеки з урахуванням уподобань самих працівників.

II. Програмне рішення британської компанії *CybSafe*, яка є новачком на ринку SA&T, зосереджено на зміні поведінки персоналу у сфері інформаційної безпеки. Місія CybSafe - допомогти організаціям ефективніше справлятися з ризиками людського фактора шляхом надання підтримки та допомоги, а не просто навчати працівників. Концепція виробника полягає у тому, щоб зрозуміти поведінку працівника і втрутитися до моменту, коли особа здійснить потенційно небезпечні дії. Програма дає змогу зрозуміти рівень впевненості персоналу в безпеці та використання методів захисту, таких як використання більш надійних паролів.

За висновками аналітиків Forrester, ПЗ CybSafe дозволяє сформувати культуру безпеки у персоналу в сучасний і навіть революційний спосіб.

III. Всесвітньо відомий постачальник ПЗ *Infosec* пропонує для навчання та інформування з інформаційної безпеки платформу Infosec IQ, яка охоплює широкий спектр тем безпеки й отримує часті оновлення з новим вмістом. Типи контенту включають відео, мікронавчання та комп'ютерні модулі навчання, які тривають від 10 секунд до 10 хвилин. Керівники програм можуть визначати тривалість вправи й дату завершення навчання, автоматично призначати навчання та складати навчальну стратегію на календарний рік. Концепція Infosec надає найбільшої важливості й спрямована на поведінкові та культурні зміни. Компанія має величезну бібліотеку контенту, а для вибору необхідних тематик пропонує відштовхуватися від досвіду учнів і полегшує сприйняття змісту шляхом його візуалізації.

Програмне забезпечення Infosec IQ отримало позитивні відгуки клієнтів і рекомендоване компаніям, які прагнуть розширити функції формування обізнаності персоналу з питань інформаційної безпеки.

IV. Компанія *Elevate Security* представила на ринку SA&T новий навчальний підхід, який використовує розроблену в рамках поведінкових наук концепцію соціального доказу, щоб впливати на зміни поведінки працівників. Надаючи користувачам уявлення про обсяги та сутність інформаційних ризиків, платформа підштовхує їх до коригування своєї поведінки. Для цього ПЗ передає дані про поведінку працівника в галузі інформаційної безпеки з різних інструментів і вимірює зміни в його поведінці після навчання (наприклад, застосування менеджерів паролів або VPN-з'єднання).

На думку фахівців Forrester, продукт Elevate Security під назвою «Розум хакера» («Hacker's Mind») - це єдиний на ринку програмних продуктів SA&T діючий зразок використання гейміфікації, який використовує позитивну мову й інклюзивні образи.

V. Програмне забезпечення *Inspired eLearning* стилізує свій контент, використовує теорію навчання дорослих та психології, призначені для посилення сприйняття інформації. Дане рішення розглядає різноманітні дослідження в ході навчального процесу як чинник, що забезпечує засвоєння і утримання всієї наданої інформації учнем. Програма включає зразки кращих практик з інформаційної безпеки для вивчення на роботі й удома, адаптує свою графіку та мову для різних культур, прагнучи залучити глобальну аудиторію. Компанія Inspired eLearning планує розширити використання прийомів гейміфікації, які дадуть користувачам уявлення про мислення хакерів і покращать рівень їхньої культури безпеки.

Аналітики Forrester відзначили простоту використання платформи й управління курсами і рекомендували її як зручну у використанні платформу з інтерактивним підходом до навчання.

Відповідно до дослідження організації Forrester до категорії сильних гравців віднесено західні компанії-виробників Proofpoint, Mimecast і Webroot.

VI. Програмний продукт для цільового навчання *Proofpoint Security Awareness Training*, створений на основі досліджень загроз, з якими стикнулася сама компанія-розробник, і її технічного досвіду вирішення проблем інформаційної безпеки. Proofpoint використовує зібрану компанією інформацію про загрози як основу для моделювання фішингових атак, аналізу електронної пошти та розробки рішень реагування на інциденти. Розробник пропонує різноманітний навчальний контент на 38 мовах світу, надає клієнтам можливість замовляти свій власний зміст навчальних програм, спроможний забезпечити користувачам навчання з будь-якого підключеного пристрою.

Фахівці відзначили, що ПЗ Proofpoint найкраще підійде замовникам, які вже використовують е-пошту Proofpoint і шукають інтегрований та заснований на даних підхід до управління SA&T.

VII. Компанія Mimecast створила й розмістила на Amazon Web Services, платформу *Mimecast Awareness Training*, яка реалізує методологію ненав'язливого навчання, використовує принципи гумору та мікронавчання. АТ пропонує тренінги за семи категоріями змісту безпеки, які проводять два головні герої: «Людська помилка» і «Обґрунтоване судження», які вносять у навчальний процес елементи людськості і розваг. Платформа, яка навчає як фахівців з інформаційної безпеки, так і тих, хто безпосередньо не пов'язані з цією сферою, користувачів та членів їхніх родин, використовує короткі вірусні відео, тестування в реальному режимі й засоби оцінювання ризику.

Відгуки клієнтів свідчать про їх високу оцінку нестандартного підходу Mimecast до вивчення питань інформаційної безпеки. Таке рішення буде прийнятним для тих організацій, де цінують гумор і вважають доцільним використання елементів розваг у безпосередній трудовій діяльності персоналу.

VIII. Програмне рішення *Webroot's security awareness platform* є частиною комбінованого набору рішень щодо захисту даних та кібербезпеки. Webroot надає свої послуги у багатьох регіонах, включаючи США, країни Європи, Близького Сходу й Африки, Японію та Австралію. Зазначене SA&T ПЗ націлене переважно на постачальників ІТ-послуг і компаній малого та середнього бізнесу. Його

навчальний зміст відповідає принципам мікронавчання, охоплює відносно невелику кількість тем з акцентом на фішинг.

Програмний продукт Webroot, на думку експертів, є прийнятним для малих і середніх підприємств, яким потрібна проста у використанні платформа для вивчення засад протидії фішингу.

Третю низхідну категорію становлять компанії, яких умовно назвали конкурентами для своїх потужніших колег. До цієї категорії віднесені три виробника спеціалізованого ПЗ SA&T, один з яких і єдиний зі списку розглянутих аналітиками Forrester – російська компанія Kaspersky.

IX. Програмний продукт *Cofense PhishMe and LMS*, одного з найбільш відомих гравців на ринку фішингового моделювання - компанії Cofense, є вузькоспеціалізований інструментом, який зосереджений на формуванні в персоналу навичок запобігання й протидії Інтернет-шахрайству, дозволяє моделювати фішингові атаки, надає можливості користувачам інформувати спеціальні служби про випадки фішингу.

Висновок фахівців і клієнтів стверджує, що програмне забезпечення Cofense найкраще підходить для організацій, які хочуть запустити фішинг-моделювання, але не мають на меті формування корпоративної культури безпеки та безпечної поведінки персоналу.

X. Новітнє програмне забезпечення російської компанії Kaspersky у сфері SA&T є продуктом, яким виробник намагається заповнити прогалину в своїх технічних лінійках продуктів для вирішення проблем впливу людського фактору. Платформа Kaspersky Security Awareness - це повністю автоматизоване рішення, орієнтоване на малі та середні підприємства, яким не вистачає досвіду власне у забезпеченні інформаційної безпеки або навчанні з питань безпеки. Програмний продукт, який продається у понад 60 країнах світу, націлений на різні цільові аудиторії від топ-менеджменту до фахівців із захисту інформації нижчої ланки. Ключовою відмінністю платформи Касперського є автоматизовані індивідуальні навчальні траєкторії, у рамках яких конкретні особи проходять навчання за конкретним графіком.

Клієнти позитивно оцінили рівень технічної підтримки, обсяг контенту та автоматизовані комунікації в межах платформи. Експерти відзначили, що зазначене ПЗ варто розглянути невеликим фірмам, зацікавленим у масштабному контенті й автоматизованому SA&T рішенні.

XI. Американський виробник ПЗ MediaPRO надає традиційне рішення для підвищення обізнаності та навчання з використанням величезної бібліотеки, доступної через навчальну платформу TrainingCenter та набір стандартних навчальних пакетів. MediaPRO надає вміст у різноманітних формах, включаючи модулі електронного навчання, мікронавчання, відео та статті. Клієнти можуть розгорнути власний контент як у своїй системі управління навчанням (LMS), в системі MediaPRO або на інших веб-платформах.

На думку фахівців, організації з консервативним корпоративним середовищем, які прагнуть отримати традиційний досвід у сфері інформаційної безпеки, слід розглядати продукти MediaPRO.

До останньої категорії - претендентів на зайняття місця на ринку програмних рішень SA&T, експерти віднесли американську компанію PhishLabs.

XII. *PhishLabs* пропонує фішинг-орієнтований підхід до надання IT-послуг, коли за кожним клієнтом призначається відповідальна особа, яка курує послугу. Клієнти практично не контролюють свою програму, окрім як через відповідального менеджмера PhishLabs. Постачальник пропонує свої послуги у формі прямих продажів переважно для північно-американських фірм. PhishLabs забезпечує контент за допомогою принципів нано- та мікронавчання і планує подальше зміцнення своєї позиції на ринку як постачальника навчальних послуг, орієнтованих на безпеку електронної пошти.

Аналітики Forrester відзначили, що PhishLabs ідеально підходить для організацій, які хочуть, щоб постачальник організовував і супроводжував фішинг-орієнтовану програму навчання персоналу.

Висновки до другого розділу

З огляду на те, що значна кількість порушень інформаційної безпеки з боку персоналу стається внаслідок незнання або недостатньої кваліфікації, важливим напрямом забезпечення інформаційної безпеки є здійснення системної і якісної підготовки працівників підприємства.

Основними принципами навчальної діяльності з інформаційної безпеки на підприємстві є: поетапність, безперервність і регулярність навчального процесу з моменту прийняття працівника на роботу; індивідуальний підхід до навчання різних категорій працівників; здійснення перевірки рівня отриманих знань; використання інноваційних рішень, технологій та кращих практик тощо. Для досягнення поставлених цілей доцільно використовувати різні форми й методи навчання, обирати різнопланові тематики від загальнотеоретичних до вузькоспеціалізованих.

Дослідження показало, що навчальна діяльність підприємства у сфері інформаційної безпеки має впроваджуватися на основі та в рамках програми, яка встановлює мету й завдання навчальної діяльності, визначає основні види навчання й категорії працівників, що проходять підготовку, регулює порядок взаємодії структурних підрозділів підприємства в ході навчальної діяльності, розподіляє відповідальності за організацію навчання, встановлює процедури проведення навчальних занять, інструктажів та перевірки набутих знань.

Встановлено, що навчання персоналу з інформаційної безпеки сьогодні практично не можливе без використання спеціалізованого ПЗ. Динамічний ринок програмних продуктів з навчання і формування обізнаності постійно представляє нових постачальників і нові рішення, які забезпечують досягнення цілей інформаційної безпеки. Новітні програмні розробки фокусуються на формуванні безпечної поведінки та корпоративної культури безпеки, залучають користувачів до альтернативних типів вмісту (гейміфікація, мікронавчання та віртуальна реальність), пропонують позитивний, надійний і легкий для сприйняття зміст, надають замовнику всебічну і безперервну підтримку незалежно від його локалізації.

Розділ 3.
КОНТРОЛЬ І ОЦІНЮВАННЯ РОБОТИ ПЕРСОНАЛУ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1. Види і форми контролю діяльності персоналу

У сучасній теорії управління людськими ресурсами велике значення у формуванні лояльного, надійного та відповідального працівника відводять заходам стимулювання та мотивації, які мають спонукати працівників до належного виконання своїх обов’язків та дотримання встановлених правил поведінки.

Водночас, безсумнівно важливою є роль засобів контролю персоналу. Під контролем у науці розуміють комплекс заходів зі встановлених для персоналу (в тому числі керівників різного рівня) режимів, регламентів, обмежень, технологічних процесів, оцінювальних, контрольних та інших процедур і операцій безпеки, який спрямований на запобіганню випадкам нанесення шкоди організації [22].

Контрольні заходи спрямовані на:

- забезпечення продуктивності та стабільності управлінського процесу;
- запобігання небажаної або небезпечної поведінки працівників, неадекватної реакції на кризові ситуації;
- збирання інформації для внесення коректив у плани та стратегію розвитку підприємства чи організації.

Також контроль позитивно впливає на трудову поведінку працівників, як тих, кого перевіряють, так і тих, хто спостерігає або залучений до цього процесу. Зокрема контроль сприяє зростанню почуття відповідальності персоналу за свою працю, формує підстави для оцінювання працівників і, як наслідок, заохочення, просування по службі, тобто мотивування до успішної і якісної праці. У випадку негативних результатів контролю обов'язковим має бути покарання, пониження в посаді або навіть звільнення.

Заходи контролю використовують для виявлення резервів для підвищення продуктивності праці, пошуку потенційних кандидатів на вищі або керівні посади, заохочення раціоналізаторської ініціативи працівників, подолання або запобігання службовим конфліктам у колективі.

Для зменшення негативних ефектів (створення видимості якісної роботи, надмірних емоційних переживань тощо) система корпоративного контролю має збільшувати відсоток методів внутрішнього контролю або самоконтролю у порівнянні з зовнішніми контролюючими заходами. Головне завдання перших полягає в тому, щоб вчасно виявити проблему й знайти шляхи її вирішення, а не встановити винуватця і покарати його. У цих умовах виконавці готові брати активну участь у формулюванні цілей своєї діяльності й самостійно контролювати їхню реалізацію.

Для підвищення результативності заходів контролю необхідно забезпечити його максимальну прозорість і наочність, що реалізується через розробку системи стандартів і рекомендацій щодо виконання заходів контролю та обов'язковим їх оприлюдненням.

Система контролю діяльності персоналу включає заходи внутрішнього (корпоративного) і зовнішнього (незалежного) контролю.

Внутрішній контроль має на меті підвищення ефективності управлінської діяльності організації та продуктивності роботи персоналу, своєчасне реагування на конфліктні ситуації або збалансування інтересів різних трудових груп. У рамках заходів внутрішнього контролю комплексно досліджують виконання планів, управлінських рішень, дотримання стандартів, рекомендацій та встановлених організаційних вимог.

Зовнішній контроль спрямований на перевірку дотримання вимог законодавства і нормативних документів, соціально-економічних засад бізнес-діяльності. Заходи зовнішнього контролю здійснюють керівники або працівники, наділені спеціальними контролюючими повноваженнями, а також представники відповідних державних органів або недержавних суб'єктів (незалежних, громадських організацій).

Контроль діяльності персоналу може здійснюватися через:

1) управління діями (поведінкою);

2) управління через взаємний контроль;

3) управління за результатами [24].

Управління діями, по суті, є спостереженням за трудовою діяльністю працівників і використовується, щоб виявити причинно-наслідковий зв'язок у процесах, що підлягають контролю. У ході здійснення контролю мають впроваджуватися коригувальні заходи з метою отримання запланованого результати на виході, тобто усунути чи виправити небажані дії персоналу.

Контроль у контексті управління діями персоналу використовує такі інструменти, як розробка нормативних документів щодо робочих процедур та процесів, формування робочих планів для окремих працівників, встановлення адміністративних і поведінкових обмежень. Такий підхід буде ефективним на підприємства, де не передбачено складних або слабо детермінованих виробничих функцій.

У рамках управління на основі взаємного контролю застосовують механізми особистісного контролю, які забезпечують якісне виконання працівниками своїх робочих повноважень, базуючись на їхньому природньому бажанні контролювати власні дії. За таких умов працівники мають володіти необхідними знаннями, кваліфікацією й професійним досвідом, а також відповідними засобами праці, що в сукупності дозволяє виконувати роботу якісно.

Завдяки таким заходам контролю здійснюється ефективний пошук фахівців, здатних виконувати певні функції, відбір і розподіл персоналу, планування виробничих робіт, встановлення порядку виконання окремих завдань, визначення очікуваних результатів.

Також управління через взаємний контроль ґрунтується на використанні сукупності цінностей і соціальних норм, під впливом яких реалізується трудова діяльність людей. Таким чином у кожного працівника формується почуття солідарності з іншими членами колективу, а залучення до процесу досягнення спільної мети має наслідком підвищення результативності роботи персоналу.

Здійснення управлінського контролю на основі особистісних і культурних цінностей пов'язане з найменшими витратами фінансових і матеріальних ресурсів, водночас додаткових зусиль потребує узгодження особистих цінностей працівників і корпоративних норм.

Управління за результатами трудової діяльності ґрунтується на збиранні й обробці інформації про результати виконаної працівником роботи. Перевагою цього типу управління є те, що керівники підприємства чи організації не вдаються в деталі методики контролю, яку використовують для досягнення бажаних результатів, а отримують інформацію про досягнуті результати зі звітів менеджерів нижчого рівня управління (центрів відповідальності). Ефективність управління за результатами можна оцінити як у грошовому вимірі (витрати, доходи), так і через кількісно-якісні показники надання послуг, дотримання процедур, вирішення критичних ситуацій тощо.

Для здійснення контролю результатів професійної діяльності персоналу потрібно описати умови, за яких максимізується ймовірність бажаної трудової поведінки; визначити цільові показники професійної діяльності; розробити порядок оцінювання результатів роботи та систему мотиваційних заходів за кращу результативність праці.

Впровадження заходів контролю на підставі оцінки досягнутих результатів потребує чіткого встановлення планових завдань, виражених у числові формі; розробити систему неупереджених, точних і зрозумілих для працівників заходів стимулювання за виконання планових завдань [12].

У нинішніх умовах динамічних змін бізнесового й інформаційного середовища організації контроль персоналу починає виконувати не наглядову, а регуляторну роль, тобто керівництво впливає на працівників не через засоби примусу й покарання, а таким чином, щоб вони якісно виконували роботу, усвідомлюючи і розділяючи необхідність досягнення цілей організації. Зазначений підхід дозволяє працівникам не діяти відповідно до жорстко встановленого стандарту, а самим знаходити оптимальні рішення для досягнення запланованих результатів.

Заходи контролю поділяють на такі види:

- регулярні, які проводять за встановленим заздалегідь графіком;
- оперативні, які проводяться за гнучким графіком або спонтанно без попереднього повідомлення тих, кого перевіряють. Причинами таких заходів можуть бути виникнення надзвичайної ситуації, розголошення конфіденційної інформації, поява підозр щодо вчинення неправомірних дій працівниками).

Відповідно до іншої класифікації за критерієм поінформованості про перевірки підрозділів-об’єктів контролю контрольні заходи можуть бути:

- гласними – заходи, проведені відповідно до інструкції, із здійсненням обліку всієї необхідної документації та дій тощо;
- негласними – заходи, які проводяться таємно, без відомо від тих, кого перевіряють, залученими працівниками служби безпеки або зовнішніх організацій [12].

Форми контролю результативності трудової діяльності персоналу такі:

- вхідний контроль – перевірка потенційних претендентів на зайняття вакантної посади щодо відповідності пропонованій посаді, перевірка кримінального минулого, фінансових порушень, психологічної стійкості тощо);
- атестація персоналу – перевірка професійної підготовки і встановлення відповідності займаній посаді. Умови проведення атестації персоналу визначаються законодавством, а процедури встановлюються на рівні організації. За результатами атестації приймаються управлінські кадрові рішення про відповідність займаній посаді, підвищення або пониження у посаді, звільнення працівника, що власне і є основним завданням атестації.
- контроль і оцінювання персоналу – з боку безпосереднього керівника у процесі повсякденної професійної діяльності працівника з метою встановлення відповідності трудової поведінки завданням та методам роботи організації, виявлення сильних сторін та недоліків працівника та визначення результативності його роботи. Таке оцінювання також може бути підставою для професійного розвитку й підвищення по службі [23].

Узагальнена схема видів та форм контролю діяльності персоналу за Г. Дорошенко [24] представлена на Рис.3.1.

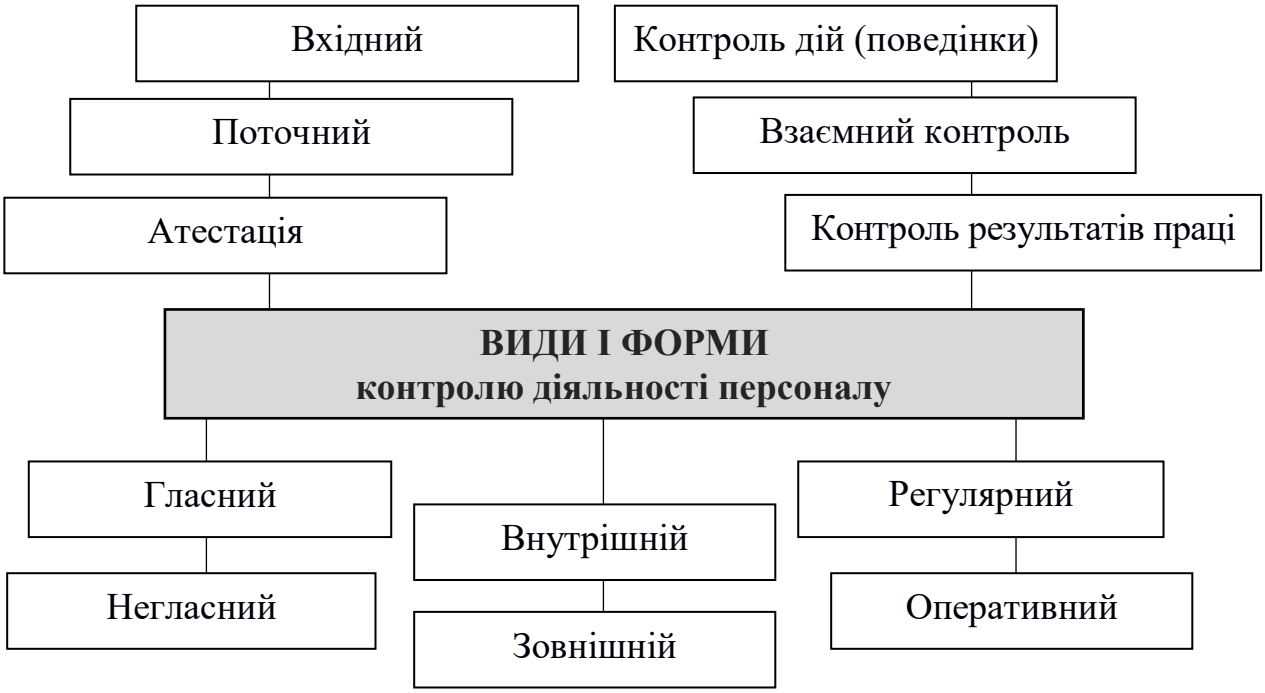

Рис.3.1. Види і форми контролю діяльності персоналу.

Оцінюючи різні види і форми контролю персоналу, варто відзначити, що більшість із них успішно використовують у сфері інформаційної безпеки. Так у ході поточного контролю та атестації фахівців із захисту інформації та інших дотичних сфер є можливість перевірити рівень дотримання інформаційної безпеки підприємства. У частині дотримання вимог захисту інформації розглядаються такі характеристики персоналу, як знання положень політики інформаційної безпеки, стандартів, процедур та інструкцій щодо захисту інформації, вміння застосовувати норми цих документів на практиці, вміння діяти відповідно до вимог у критичних ситуаціях, працювати з конфіденційними документами, дотримуватися обмежень безпеки.

Також у процесі контролю роботи працівників з інформаційної безпеки використовують нетрадиційні методи, такі як: контроль здатності працювати в команді, оцінювання здібностей до оволодіння новими вміннями і практичними навичками, психологічної вразливості та схильності до протиправних дій.

Керівники структурних підрозділів та служби безпеки можуть звітувати про стан дотримання вимог захисту інформації та виконанні вимог безпеки

працівниками своїх підрозділів у сукупності. Формою контролю є також регулярні перевірки виконання працівниками вимог до роботи з конфіденційною інформацією, документами і базами даних, а також наявність та умови зберігання закріплених за ними документів, носіїв інформації.

У випадку встановлення фактів невиконання персоналом вимог та обмежень інформаційної безпеки (як правило, за результатами службового розслідування) винні особи підлягають застосуванню покарання: оголошення догани, пониження в посаді, позбавлення премії, відсторонення від роботи з конфіденційною інформацією, звільнення, а у випадку особливо тяжких порушень – кримінальній відповідальності [36].

Оцінюючи підходи до здійснення контролю діяльності персоналу, фахівці особливо наголошують на необхідності позитивного зворотного зв'язку з працівниками: керівник має відзначати позитивні зрушення у роботі, повідомляти про зростання кількісних показників праці, оголошувати кадрові рішення про підвищення кращих фахівців на посаді, тим самим мотивуючи працівників працювати ще краще.

Отже, налагодження якісної системи контролю є не тільки запорукою зростання продуктивності праці, але й інструментом виявлення неблагонадійних претендентів на роботу ще на етапі відбору і нейтралізації загроз інформаційній безпеці підприємства з боку діючого персоналу.

3.2. Критерії і методи оцінювання персоналу з інформаційної безпеки

Оцінювання персоналу має двоєдину природу: по перше, це процес визначення ефективності виконання працівниками підприємства своїх обов’язків за посадою і реалізації корпоративних цілей; по друге, процес встановлення відповідності професійних та особистих характеристик персоналу (здібностей, умінь, мотивів, рис характеру) вимогам посади або робочого місця [23,38].

Оцінювання персоналу є сукупністю показників для встановлення, чи відповідає працівник займаній посади, наскільки ефективно він/вона виконує свої

професійні обов'язки, які аспекти своєї трудової діяльності йому/їй потрібно «підтягнути», щоб відповідати вимогам посади і підприємства.

Оцінювання персоналу виконує такі *функції*:

Адміністративну – є основою для прийняття адміністративних (кадрових) рішень про прийняття на роботу, підвищення/зниження на посаді, звільнення, переміщення, преміювання/покарання тощо;

Інформаційну – інформує працівників про їх професійні переваги і недоліки, даючи можливість покращити рівень своєї компетентності;

Стимулюючу – оцінювання відіграє роль мотиваційного чинника: визнання високого рівня результативності праці або заслуг перед підприємством спонукає працівника покращувати свої професійні компетенції і нарощувати продуктивність [2].

Оцінювання персоналу виконує ще низку *завдань* у системі менеджменту персоналу та управління підприємством загалом, зокрема:

• допомагає визначити рівень професійних знань, навичок і компетенцій для подальшого прийняття кадрових рішень;

• сприяє усвідомленню потреби у кадрових перестановках та визначенню напрямів дій HR-менеджерів;

• завдяки аналізу даних оцінювання персоналу вдосконалює систему мотивації і ключові показників результативності персоналу (KPI - key performance indicators);

• сприяє впорядкованості управлінських процесів на підприємстві;

• допомагає керівництву володіти актуальною та об'єктивною інформацією про ефективність використання людських ресурсів підприємства.

Також результати оцінювання персоналу в багатьох випадках є основою для прийняття стратегічних рішень, наприклад для:

• розробки системи кадрового планування й зокрема матриці кар'єрного просування персоналу;

• створення комплексу показників і засобів оцінювання персоналу, які базуються на об’єктивній інформації про рівень знань і навичок працівників підприємства;

• коригування корпоративної програми навчання, плану проведення і змісту навчальних і тренінгових курсів тощо;

• формування кадрового резерву на основі актуальних відомостей про працівників, які в перспективі можуть бути підвищені на керівні посади, виявлення потенційних формальних і неформальних лідерів;

• аналізу ефективності робочих процесів, системи мотивації, бізнес-логіки підприємства [19].

Види оцінювання персоналу.

Оцінювання персоналу сучасного підприємства проводять:

• відповідно до плану - планове оцінювання, яке відбувається згідно з нормами законодавства, як правило, раз на кілька років;

• у випадку реорганізації, коли виникає кризова ситуація, підприємство потребує зміни бізнес-тактики, виводить на ринок новий продукт або освоює новий сегмент ринку тощо;

• одиничне оцінювання – коли не вистачає об’єктивної інформації для прийняття управлінського рішення щодо призначення працівника на нову керівну посаду чи звільнення;

• для оцінювання претендентів на зайняття вакантних посад, яке є основою для прийняття рішення про прийом на роботу.

Способи оцінювання персоналу

Незважаючи на наявність багатьох підходів і критеріїв оцінювання професійної роботи фахівців, їх можна умовно звести до трьох основних груп.

Перша з них – це збирання й обробка даних в ручному режимі, яке передбачає зазвичай індивідуальну або групову співбесіду з працівниками. Перевагою такого методу є можливість здійснення прискіпливої оцінки особистих і професійних якостей, здібностей і навичок працівників, водночас для

проведення безпосередніх зустрічей потрібно багато ресурсів, крім того є ймовірність похибок в оцінці та впливу суб’єктивного фактору.

Автоматичне оцінювання працівників здійснюється через тестування, найчастіше за допомогою комп'ютерних програм. Цей метод є швидким і ефективним, комп’ютерна програма є цілком об’єктивною в аналізі даних і може проводити тестування великої кількості осіб. Добре підходить для оцінювання посадових осіб з формалізованими повноваженнями. Однак, незважаючи на всі плюси, такий метод складно оцінює індивідуальні особливості.

Комбінований метод поєднує використання тестування для перевірки компетенцій працівників і методів безпосереднього спілкування для оцінювання індивідуальних особливостей працівників.

Критерії оцінювання персоналу

На думку фахівців [19], оцінювання персоналу доцільно здійснювати за такими критеріями: професійні знання і навички, особистісні характеристики, ключові показники результатів діяльності (KPI), рівень лояльності, здібності до навчання і розвитку, специфічні вимоги. Схема показана на Рис. 3.2.

Рис. 3.2. Критерії оцінювання персоналу.

Оцінюючи *професійні знання і навички*, варто розділити їх на дві частини: знання і навички, які потрібні фахівцю для повсякденної роботи, та ті, які також важливі, але використовуються особою час від часу. Як відзначалося вище, професійні знання і навички краще й ефективніше перевіряти за допомогою автоматизованих методів, зокрема тестування. Рекомендовано для розробки

таблиці результатів використовувати метод коефіцієнтів, відповідно до якого для оцінки знань кожній відповіді надається свій рівень важливості для роботи.

Наприклад, для фахівця з управління інформаційною безпекою пріоритетний рівень матимуть знання міжнародних стандартів ISO 27000, структури корпоративної політики та процедур, технологій захисту інформаційних активів, підходів до організації заходів інформаційної безпеки та їх контролю тощо. Другий рівень пріоритетності можуть становити знання і навички технічного профілю, зокрема розуміння основних засад функціонування інформаційних систем і мереж, засобів захисту інформації, навички адміністрування інформаційних систем та впровадження різних технологій перевірки ефективності системи інформаційної безпеки тощо.

Важливою і обов'язковою складовою оцінювання персоналу, і особливо з інформаційної безпеки, є вивчення *особистих рис працівника*. Фахівці рекомендують розділити процес оцінювання на дві частини:

- під час першої дослідити особисті якості, які важливі для роботи за фахом конкретного працівника (для кожної професії і посади вони будуть відрізнятися),
- в ході другої – встановити, чи загалом працівник відповідає сучасній концепції сталого розвитку особистості (гнучкість, особистий та професійний розвиток, самоосвіта, відповідальність, робота в команді тощо).

Для прикладу, менеджер з інформаційної безпеки має володіти такими особистими якостями та здібностями як стійкі організаційні та комунікативні навички, сильні аналітичні здібності, схильність до лідерства, здатність працювати в команді, стратегічне мислення тощо.

Оцінюючи працівників у таким спосіб, важливо не просто збирати інформацію, але пам'ятати, що за результатами оцінювання особистісних характеристик кожного працівника має бути зроблений висновок щодо її відповідності посаді, можливості бути потенційним лідером тощо.

Оцінювання *ключових показників результативності* працівника має здійснюватися на постійній основі і без відволікання від професійної діяльності. Метою такого оцінювання є встановлення, чи фахівець справляється зі своїми

повноваженнями. Оцінку ключових показників результативності часто проводять в комплексі: спочатку аналізують дані про роботу відділу, потім розглядають показники кожного окремого працівника. Завдяки такому оцінюванню можна зробити висновки стратегічного характеру, які стосуються усього підприємства, зокрема щодо причин невиконання запланованих показників і дій для підвищення ефективності бізнес-процесів.

Завдання оцінки *лояльності* персоналу полягає у встановленні рівня вмотивованості кожного працівника працювати у своїй компанії. Загалом лояльність персоналу включає прихильність, здійснення свідомих дій в інтересах компанії, прийняття корпоративних принципів та цілей, зацікавленість у результатах діяльності підприємства [27].

Оцінку рівня лояльності проводять шляхом індивідуальних бесід, тестування, кількісними методами. Досить поширеним є поєднання різних підходів. Для збору інформації про задоволеність працівників роботою у своїй компанії доцільно використати метод спостереження, наприклад, за поведінкою працівників на робочих місцях, під час корпоративних заходів, в період кризових ситуацій. Бажано робити це в природньому для всіх вигляді, не відволікаючи від повсякденних справ, не привертаючи уваги і не озвучуючи причин присутності спостерігачів.

Компанії, націлені на подальший розвиток, оцінюють не тільки актуальні знання й навички своїх працівників, але і їх *здібності до навчання і розвитку,* оскільки підприємству вигідніше розвивати своїх працівників на перспективу, ніж потім залучати їх ззовні чи переманювати у конкурентів.

Для цього можна використати два підходи: діагностичний і прогностичний. Діагностичний підхід визначає актуальні досягнення працівника в тій чи іншій сфері і розглядає їх як результат здібностей до навчання. Для цього використовуються методи оцінювання результатів діяльності й тестування.

У рамках прогностичного підходу перевіряють, наскільки добре і швидко працівник засвоює невеликий обсяг матеріалу чи вирішує незначне інтелектуальне завдання, і на цій основі роблять висновок щодо його здібностей

до навчання. Для цього застосовують інші методи - моделювання ситуацій та інтерв'ю. Саме метод інтерв'ю фахівці радять застосовувати для оцінювання здібності кадрів до навчання як найбільш інформативного й економного [16].

Потреба в виявленні *специфічних характеристик* виникає при оцінюванні керівників, фахівців рідкісних професій або професіоналів найвищого класу. Тут головну роль відіграють методи ручного оцінювання, наприклад, співбесіди та інтерв'ю. Наприклад, для фахівця з інформаційної безпеки важливим є наявність таких рис як небалакучість, уважність, критичне мислення, які найлегше виявити у процесі міжособистісного спілкування.

Методи оцінки

У науці та практиці представлено багато методів оцінювання персоналу [2,11,34], які умовно поділяють на кількісні і якісні. Деякі з них є універсальними і застосовуються практично в усіх компаніях, деякі – специфічні і потребують особливих умов проведення і значної підготовки. Вибір методів залежить від цілей оцінювання, наявність ресурсів та особливостей бізнесу.

Кількісні методи вважають найбільш об'єктивними, оскільки їхні результати представлені у цифрах. До кількісних методів відносять:

Метод заданої бальної оцінки. За кожен результат у фаховій діяльності працівник отримує певну кількість балів у відповідності до встановленої заздалегідь бальної шкали. Оцінювання відбувається, як правило, за підсумками конкретного періоду роботи, наприклад місяця або року.

Метод вільної бальної оцінки полягає у виставленні оцінки у балах по факту досягнення результатів праці або якості професійних характеристик працівника. Сума балів або середній бал становить загальну оцінку працівника.

Рейтинговий метод. На основі оцінювання працівників за бальною системою формується список персоналу у відповідності до кількості набраних балів за результатами професійної діяльності від найбільших до найменших.

Метод графічного профілю представляє оцінки у балах за кожне виконане працівником завдання або рівень його ділових якостей у вигляді графіку.

До *якісних методів*, які передбачають збирання й аналіз описової інформації, яку часто важко порахувати і виразити у вигляді цифр, відносять:

Матричний метод, який здійснює порівняння якостей конкретної особи з ідеальною моделлю працівника для визначеної посади або робочого місця.

Метод довільних характеристик – відповідно до якого збираються відомості про найбільш вагомі професійні досягнення і найсерйозніші порушення в роботі окремого працівника і на основі їх співставлення роблять висновки про його професійну придатність.

Оцінка виконання завдань - найпростіший метод, коли оцінюється робота співробітника в цілому.

Метод «360 градусів» дозволяє оцінити працівника за допомогою його оточення і передбачає оцінювання його професійної діяльності та особистих якостей керівником, колегами, підлеглими, клієнтами, а також його ним самим.

Групова дискусія може проходити у вигляді співбесіди працівника з керівником та профільними фахівцями щодо результатів його праці, або обговорення діяльності працівника групою експертів і, за потреби керівника, без його участі. За результатами таких зустрічей з різними фахівцями обираються найбільш кваліфіковані спеціалісти.

Найбільш ефективними методами оцінювання персоналу вважають *комбіновані методи*, які поєднують описові і кількісні елементи. До них відносять метод суми оцінок, коли кожна характеристика працівника оцінюється за певною шкалою, а потім вираховується середній показник, який порівнюють з еталоном для певної посади; метод групування, коли весь персонал поділяють на кілька груп від найкращих до найгірших.

Для оцінювання компетенцій персоналу використовують такі методи як:

Центр оцінювання (Assessment Centre) - сучасний метод оцінки персоналу, що дозволяє отримати комплексну і достовірну інформацію про професійний рівень, ділові й особисті риси персоналу і зробити висновок про відповідність кадрового складу підприємства його місії, політиці і структурі. Центр оцінювання використовує для роботи з персоналом ділові ігри, кейси, групові дискусії,

індивідуальні інтерв'ю і тести. За результатами заходів проводиться загальна оцінка працівників й отримання зворотного зв'язку.

Тестування є досить поширеним методом оцінювання персоналу і включає як професійні, так і психологічні тести.

Метод експертних оцінок персоналу полягає в залученні до оцінки персоналу експертів, які вивчають і аналізують працівника відповідно до встановленого завдання і з урахуванням власного професійного досвіду оцінюють його компетентність.

Ділові гри, які передбачають оцінювання працівника у процесі імітації ділової активності, дозволяють змоделювати поведінку особи за певних робочих обставин та оцінити її.

Найбільш відомим методом оцінювання результативності праці персоналу є метод ключових показників результативності (KPI). Цей підхід базується на оцінюванні праці за реальними здобутками й використовує засоби об'єктивного вимірювання. Так, для конкретного працівника встановлюється перелік завдань для виконання, кожному з яких присвоюється свій коефіцієнт важливості. В кінці оціночного періоду розраховується загальна оцінка роботи фахівця.

Підсумовуючи варто наголосити, що для здійснення системної та якісної оцінки персоналу необхідно дотримуватися принципів комплексності, об'єктивності, прозорості, достовірності й простоти розуміння, а також використовувати різноманітні, в тому числі новітні методи оцінювання, обирати їх відповідно до ситуації та потреби [19].

3.3. Типи програмних продуктів для здійснення контролю й оцінювання персоналу

Сьогодні на ринку програмних рішень з оцінювання персоналу представлено багато різноманітних розробок. Серед них великі програмні комплекси для автоматизації більшості бізнес-процесів, в тому числі HR-менеджменту. Однією з найбільш відомих таких платформ є Бітрікс24, яка поряд з чотирма іншими

інструментами для організації бізнес-діяльності включає потужний HR-блок, в тому числі бази даних працівників та їх профілі, управління заробітною платою та компенсаціями, управління набором персоналу та його продуктивністю, часом та відвідуваністю тощо.

Окрему категорію становлять програмні продукти власне для процесів управління персоналом як, наприклад, американська BambooHR (https://www.bamboohr.com/). Це хмарне програмне рішення для управління персоналом для малого та середнього бізнесу, яке пропонує невеликим та зростаючим компаніям інформаційну систему людських ресурсів (HRIS), яка включає систему відстеження кандидатів на зайняття вакантних посад, відстеження часу, обробку заробітної плати, адміністрування виплат, інструменти залучення працівників, автоматичні нагадування й аналіз даних робочої сили для управління всіма аспекти життєвого циклу працівника.

Як свідчить аналіз ринку пострадянського простору, такі HRM-систем крім облікового та розрахункового блоків включають, як правило, HR-блок, який забезпечує виконання завдань з управління: кадровим бюджетом, «профілями компетенцій» працівників, плануванням персоналу, даними кандидатів на зайняття вакантних посад, кваліфікаційними вимогами та системою атестації, навчанням і перепідготовкою, мотивацією персоналу, ефективністю та оцінюванням персоналу, моделюванням та оптимізацією штатів, інформаційною взаємодією працівників [17].

Також на ринку представлені розробки, які забезпечують автоматизацію набору процесів у межах виділеного напряму «Контроль і оцінювання персоналу» з:

а) набору персоналу й оцінки кандидатів (і працюючих фахівців);

б) оцінювання професійних та особистих якостей працівників;

в) оцінювання результативності роботи й атестація персоналу;

г) навчання й підвищення кваліфікації персоналу;

д) моніторингу діяльності працівників.

Наявні також і більш вузькоспеціалізовані програмні продукти з управління персоналом як наприклад, моніторинг діяльності працівника в мережі Інтернет,

відстеження часу на виконання окремих завдань тощо. Водночас завдання для спеціалізованих галузей, наприклад, для сфери інформаційної безпеки, вирішуються в рамках наявних розробок шляхом створення вузько тематичних навчальних курсів і систем тестування, налаштування додаткових функцій та інструментів.

Розглянемо окремі зразки програмних продуктів за напрямом «Контроль і оцінювання персоналу» відповідно до представлених на Рис.3.3. категорій.

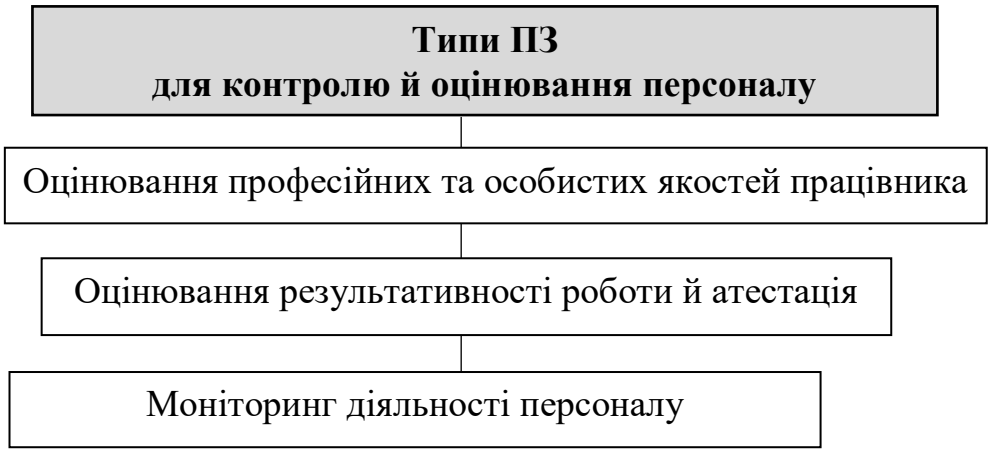

Рис. 3.3. Типи ПЗ для контролю й оцінювання персоналу.

Оцінювання професійних та особистих якостей

На сьогодні існує достатня кількість компаній-виробників ПЗ, що спеціалізуються на діагностиці різноманітних якостей і характеристик особистості шляхом проведення тестування. Значна частина з них надають такі послуги у рамках блоку з рекрутингу. Слід зазначити, що такі тестування здійснюються як щодо претендентів на конкретну посаду, так і щодо осіб, які вже працюють.

Серед багатьох таких поставників ПЗ варто виділити компанію Midot (https://midot.com/), яка пропонує програмне рішення для оцінювання ризиків деструктивної поведінки та зловживань персоналу на платформі Podium. Програма Midot System здійснює оцінювання працівника за трьома напрямами: благонадійність (надійність і ризики деструктивної поведінки); безпека (вимірювання потенційного ризику залучення кандидатів і персоналу в нещасні випадки на виробництві); стабільність (прогноз дострокового звільнення серед кандидатів). В основі рішень Midot System лежить алгоритм оцінювання етичних і

моральних цінностей особи, який є основою для прогнозування його професійної поведінки.

Заслуговує на увагу і система управління персоналом Extended DISC (www.extendeddisc.org), яка допомагає визначити індивідуальні особливості працівника для виконання певного виду робіт. Програма Extended DISC описує характер природної реакції або стиль поведінки особи в різних ситуаціях. Використання даного ПЗ дозволяє вирішувати такі кадрові питання: швидко і точно підібрати працівника на конкретну посаду; мотивувати персонал з урахуванням їхніх індивідуальних особливостей; встановити категорію персоналу і напрями навчання з найбільшою користю для компанії; створити злагоджену команду виконавців; сформувати сприятливий психологічний клімат у колективі.

Одним із найуспішніших англомовних стартапів останніх років у сфері оцінювання персоналу є система Greenhouse (https://www.greenhouse.io/), яка зараз є популярним хмарним рішенням у США. Система допомагає проводити інтерв'ювання кандидата на вакантну посаду, а також оцінювати його компетентність, виставити рейтинг по кожній з компетенцій і навичок, пропонує функції розширеної аналітики і звітності з питань наймання персоналу.

Російськомовна платформа для онлайн-тестування працівників і кандидатів Proaction.pro надає такі можливості для полегшення процесу наймання й оцінювання кандидатів: має готові профілі понад 20 керівних і лінійних посад (також можна створити додаткові самостійно) та інструменти для оцінювання найбільш поширених корпоративних компетенцій (методики, тести, мотиваційні кейси та засоби для визначення інтелектуальних здібностей), оцінює кандидатів на основі інформації з соцмереж.

Комплексний підхід до оцінювання професійних та особистих характеристик працівників га основі інноваційних психометричних рішень представила компанія Talent-Q (https://talent-q.ru/about/history/). У рамках програми можна проводити тестування загальних і професійних здібностей працівника, користуватися готовими вправами для центрів оцінювання й інструктивними матеріалами щодо розвитку компетенцій, оцінювати потенціал особи до навчання і розвитку, розробити і

використовувати особистісні опитувальники. Також замовник може скористатися сервісом оцінювання методом 360 градусів°, яке допомагає оцінити ефективність кожного окремого працівника, виявити його переваги та недоліки і розробити схему подальшого розвитку.

Варто згадати платформу Simformer Business Simulation (https://simformer.com/ru/), яка крім навчання, що поєднує онлайн-курси з реалістичною бізнес-симуляцією, надає матеріал для онлайн-оцінювання навичок, знань і компетенцій менеджерів. Така оцінка є об’єктивною, тому що формується за фактичними результатами роботи менеджерів в реалістичному бізнес-тренажері.

Занурення учасників в бізнес-симуляцію дозволяє провести масштабне онлайн-оцінювання багатьох учасників незалежно від часу і місця перебування; приховати мету програми від оцінюваних працівників, даючи їм можливість максимально проявити себе; отримати об'єктивні оцінки кожного учасника, сформувати загальний рейтинг усіх працівників. Для забезпечення об’єктивності оцінки програма передбачає не тільки автоматизоване оцінювання (у бізнес-симуляції), але й залучення експертів для надання обґрунтованого висновку за підсумками бізнес-гри.

Цікавим є онлайн-сервіс з підбору кандидатів на вакансії, що використовує алгоритми штучного інтелекту – GoRecruit (https://coba.tools/gorecruit). Програма аналізує профілі претендентів у соцмережах за понад 70 критеріями, формує рейтинги і співставляє результати аналізу з вимогами вакантної посади. При порівнянні система враховує ділові й особистісні риси кандидата, а також дані, знайдені в Інтернеті, які претенденти можуть приховати при працевлаштуванні. Роботодавцю залишається тільки обрати кращого з наявних кандидата.

Оцінювання результативності праці

Британська компанія Thomas (https://www.thomas.co/) пропонує програмні рішення з управління персоналом, які вирішують крім інших завдання оцінювання персоналу відповідно до посади, діагностики членів діючої команди і визначення потенціалу кожного працівника, визначення потреб працівників у навчанні та професійному розвитку, відстеження процесу розвитку та проведення

атестації персоналу, оцінювання мотивації та корпоративної лояльності, глибоке вивчення професійних та особистих характеристик працівника з метою розробки плану розвитку кар'єри. Також оцінюванню підлягають стиль поведінки, здатність до навчання, лідерські якості, особисті здібності, емоційний інтелект, особистість на робочому місці.

Waytobi (https://waytobi.com/ua/) - інструмент для створення, відстеження, складання звітів, аналізу і візуалізації ключових показників результативності (KPI) працівника, підрозділу чи компанії. Основними функціями Waytobi є: збирання інформації про результати діяльності, її подальша обробка й візуалізація.

Сервіс дозволяє створити свої або вибрати готові шаблонні KPI, складені згідно з галузевими стандартами; впровадити складні формульні і «плаваючі» KPI; розподіляти призначені для користувача ролі і привілеї за чотирма рівнями доступу; формувати звіти в режимі реального часу й використовувати вбудовану аналітику. За допомогою програми керівник може встановити мету і розподілити завдання між працівниками, а також контролювати їх виконання.

Commito (https://commito.ru/) - сервіс розрахунку KPI і зарплат персоналу в інтеграції з amoCRM і Бітрікс24, який дозволяє контролювати ефективність роботи, розвивати персонал і платити за результат. Система розраховує понад 30 показників оцінювання результативності персоналу, зберігає історію оцінювання працівників, встановлює цілі на місяць, квартал чи рік, робить прогнози результативності, розробляє плани розвитку персоналу, відстежує динаміку розвитку компетенцій та досягнень, має функції самообслуговування працівників та зворотного зв’язку.

Відомою на ринку є система оцінювання кандидатів та працівників Squadrille (https://squadrille.com/). Програма здійснює оцінювання за компетенціями вже розробленими інструментами, сформованими в залежності від завдання, професійних навичок в різних сферах, зокрема і в сфері IT.

Компанія також надає можливості розробки спеціального програмного рішення «під ключ» (розробки карт компетенцій, автоматизованих оціночних

процедур, кейсів та опитувальників з набору компетенцій, гейміфікованих оціночних онлайн-інструментів) і готова здійснювати повне аутсорсингове оцінювання персоналу компанії-замовника. Таке рішення підійде для проведення атестації персоналу, планування навчання та оцінювання його ефективності, прогнозування й відстеження саморозвитку працівників, вирішення завдань стратегічного розвитку компанії.

Говорячи про вузько спеціалізовані сервіси, які забезпечують окремі аспекти оцінювання діяльності персоналу, варто згадати програму Todoist, яка є популярним інструментом з управління завданнями і роботою зі списками справ. Програма має простий інтерфейс, інтегрована з багатьма іншими онлайн-сервісами (Dropbox, Google Disk, Gmail, Google Календар), підтримує роботу в команді, передбачає можливість встановлення для кожного завдання термінів завершення, повторних дат, підпунктів, присвоєння пріоритетів, налаштування нагадувань, додавання вкладених файлів тощо. Todoist забезпечує автосинхронізацію завдань і списків з усіма пристроями, а також збереження списку справ у хмарі, на ресурсі Todoist.com.

Для встановлення витрати часу на виконання робочих завдань можна обрати програму TMETRIC, яка обраховує обсяг часу, який кожен працівник витрачає на виконання завдань, відстежує роботу на різних пристроях, дозволяє додавати клієнтів і ставку за годину, а потім виставляти рахунки. Сервіс є корисним інструментом для точного планування робочого часу.

Моніторинг діяльності персоналу

В умовах пандемії та дистанційної роботи зріс попит на програмні продукти, які відстежують діяльність працівників на робочому місці. Ці інструменти пропонують функції моніторингу веб-сайтів та додатків, а також знімки монітора, натискання клавіш та відстеження файлів тощо. Програми також збирають зазначені дані і передають їх для звітування та представлення на інформаційних панелях. Така статистика може стати основою для обґрунтованих висновків щодо продуктивності праці колективу чи підрозділу, а також допомогти виявити проблеми та прогалини у бізнес-процесах. Водночас, важливо розуміти, що

використання таких можливостей має на меті підвищення продуктивності праці, а не тотальний контроль діяльності персоналу.

На ринку представлені також і платформи, які пропонують комплексні послуги моніторингу, автоматизації та збирають майже вичерпні дані. Серед них - відомі продукти InterGuard, Staffcop Enterprise, Teramind та Veriato Cerebral, які є максимально наближені до інвазивних систем внутрішнього спостереження і у залежності від мети дозволяють встановити обсяг даних та вектори моніторингу щодо кожного працівника.

Зазначені продукти надають високоякісні основні сервіси відстеження часу, а також виконують функції мобільного відстеження GPS для працівників на місцях, надання приміток та фотографій, знімків монітора або базовий моніторинг використовуваних програм та відвідуваних URL-адрес. Інструменти цього рівня забезпечують фактично повномасштабну звітність і аналіз усіх зібраних даних про працівників [41].

Для здійснення контролю за діями персоналу у робочий час використовують програму CrocoTime (https://crocotime.com/ru/), яка фіксує все, що робить працівник за комп'ютером протягом робочого дня, зокрема користування сайтами і програмами; здійснення дзвінків із встановленням їх кількості й абонентів (інтеграція з IP-телефонією). CrocoTime розраховує коефіцієнти продуктивності для кожного фахівця і показує, які ресурси забирають найбільше часу. Програма допомагає встановити завантаженість персоналу і відповідним чином її оптимізувати, внаслідок чого зросте ефективність бізнес-процесів. Даний продукт є корисним для контролю за роботою персоналу, який працює віддалено.

Висновки до третього розділу

Встановлено важливу роль засобів контролю персоналу, який вирішує завдання забезпечення продуктивності та стабільності управлінського процесу; запобігання небажаній поведінці працівників; збирання інформації для внесення коректив у плани та стратегію розвитку підприємства. Система контролю

діяльності персоналу включає заходи внутрішнього і зовнішнього контролю, вхідного, поточного контролю та атестації. Контроль діяльності персоналу може здійснюватися через управління діями; управління за результатами і через взаємний контроль.

З'ясовано, що оцінювання персоналу має на меті визначення ефективності виконання працівниками своїх посадових обов'язків і реалізації корпоративних цілей; встановлення відповідності професійних та особистих характеристик персоналу вимогам посади або робочого місця. Також результати оцінювання персоналу можуть бути основою для прийняття стратегічних загально-організаційних та кадрових рішень.

Оцінювання персоналу з інформаційної безпеки здійснюють за такими критеріями: професійні знання і навички, особистісні характеристики, ключові показники результатів діяльності (KPI), рівень лояльності, здібності до навчання і розвитку, специфічні вимоги (відповідно до вузької спеціалізації).

Огляд ринку програмного забезпечення для контролю й оцінювання персоналу підтвердив наявність багатьох рішень, починаючи з великих програмних комплексів для автоматизації бізнес-процесів з потужними HRM-блоками, продуктів для управління життєвим циклом працівника і закінчуючи розробками, які забезпечують автоматизацію процесів контролю й оцінювання персоналу і вузькоспеціалізованих програм, наприклад, для моніторингу діяльності працівника в мережі Інтернет. Завдання з управління людськими ресурсами у сфері інформаційної безпеки вирішуються в рамках наявних розробок через встановлення додаткових функцій та інструментів.

У дослідженні розглянуто зразки програмних продуктів з оцінювання професійних та особистих якостей, оцінювання результативності праці й моніторингу діяльності персоналу.

ВИСНОВКИ

У результаті дослідження встановлено, що управління людськими ресурсами є комплексом взаємопов'язаних організаційних, економічних і соціальних заходів з метою створення умов сталого розвитку і ефективного використання потенціалу робочої сили підприємства. Управління людськими ресурсами для вирішення своїх завдань використовує низку технологій, зокрема технології збирання й оцінювання особистої інформації про працівника, даних про кількісні та якісні характеристики складу персоналу, рівень результативності його праці.

На основі аналізу різних категорій потенційних внутрішніх порушників (від фахівців служби безпеки підприємства до обслуговуючого персоналу) зроблено висновок, що найбільшу загрозу інформаційній безпеці можуть становити фахівці служб IT та захисту інформації. Розглянуто рекомендації міжнародного стандарту ISO 27002, відповідно до якого роботу з персоналом у сфері інформаційної безпеки умовно можна поділити на три блоки: до прийому на роботу (попередня перевірка, укладання трудової угоди та угоди про нерозголошення), у період зайнятості (розподіл відповідальності, забезпечення обізнаності й навчання персоналу, дисциплінарні заходи) та у разі припинення або зміни трудових відносин.

З огляду на те, що значна кількість порушень інформаційної безпеки з боку персоналу стається внаслідок незнання або недостатньої кваліфікації, важливим напрямом забезпечення інформаційної безпеки є здійснення системної і якісної навчальної підготовки працівників підприємства. Навчання персоналу має базуватися на дотриманні таких принципів: поетапність, безперервність і регулярність навчального процесу з моменту прийняття працівника на роботу; індивідуальний підхід до навчання різних категорій працівників; здійснення перевірки рівня отриманих знань; використання інноваційних рішень, технологій та кращих практик тощо.

Для досягнення поставлених цілей навчальна діяльність підприємства у сфері інформаційної безпеки має впроваджуватися в рамках відповідної програми,

використовувати різні форми й методи навчання, зосереджуватися на різнопланових темах відповідно до профілю персоналу.

Огляд ринку програмних продуктів з навчання і формування обізнаності показав наявність багатьох рішень, які забезпечують досягнення цілей інформаційної безпеки. Новітні програмні розробки фокусуються на формуванні безпечної поведінки та корпоративної культури безпеки, залучають користувачів до альтернативних типів вмісту (гейміфікація, мікронавчання та віртуальна реальність), пропонують позитивний, надійний і легкий для сприйняття зміст, надають замовнику всебічну і безперервну підтримку незалежно від його локалізації.

Встановлено важливу роль засобів контролю персоналу, який вирішує завдання забезпечення продуктивності та стабільності управлінського процесу; запобігання небажаній поведінці працівників; збирання інформації для внесення корективів у плани та стратегію розвитку підприємства.

З'ясовано, що оцінювання персоналу має на меті визначення ефективності виконання працівниками своїх посадових обов'язків і реалізації корпоративних цілей; встановлення відповідності професійних та особистих характеристик персоналу вимогам посади або робочого місця. Також результати оцінювання персоналу можуть бути основою для прийняття стратегічних загально-організаційних та кадрових рішень. Оцінювання персоналу з інформаційної безпеки здійснюють за такими критеріями: професійні знання і навички, особистісні характеристики, ключові показники результатів діяльності (KPI), рівень лояльності, здібності до навчання і розвитку, специфічні вимоги.

У результаті вивчення ринку програмного забезпечення для контролю й оцінювання персоналу виявлено велику кількість IT-рішень для виконання зазначених завдань як у межах великих програмних комплексів, так і окремих вузькоспеціалізованих програм контролю й оцінювання персоналу. Встановлено, що завдання з контролю й оцінювання персоналу у сфері інформаційної безпеки вирішуються в рамках наявних розробок через використання спеціальних інструментів і встановлення додаткових функцій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аналитика отрасли информационной безопасности. URL: https://www.infowatch.ru/analytics/reports (дата звернення: 23.12.2020)

2. Андреева И. Оценка персонала. URL: https://hrliga.com/index.php?module =profession&op=view&id=1831(дата звернення: 23.12.2020)

3. Байєрс Л.Л., Ру Л.В. Управління людськими ресурсами. URL: http://www.management.com.ua/ (дата звернення: 23.12.2020)

4. Башинська І.О. Глава 3.7 Основні порушники та загрози інформаційної безпеки промислових підприємств (с. 262-267) у міжнародній колективній монографії Problems of social and economic development of business: Collective monograph. – Publishing house «BREEZE», Montreal, Canada, 2014. 408 p.

5. Бутко Е. Управление человеческими ресурсами. Образовательные ресурсы и технологии. 2016. №5(17). С.3-9.

6. Вилкова А.В., Литвишков В.М., Швырев Б.А. Проблемы непрерывного обучения персонала информационной безопасности. Мир науки, культуры, образования. 2019. № 4 (77). С.29-31.

7. Вострецова Е.В. Основы информационной безопасности: учебное пособие для студентов вузов. Екатеринбург : Изд-во Урал. ун-та, 2019. 204 с.

8. Гатиятуллин Т.Р., Сухова А.Р. К вопросу обучения основам информационной безопасности сотрудников предприятия. Международный научный журнал «Символ науки». 2015. №12. С.128-130.

9. Герасименко Г.В. Принципи управління людськими ресурсами високотехнологічного підприємства як методологічний інструмент забезпечення ефективності. URL: https://ir.kneu.edu.ua/handle/2010/19452 (дата звернення: 23.12.2020)

10. Гребенніков В. Комплексні системи захисту інформації. Проектування, впровадження, супровід: Збірник лекцій, 2013. 161 с. URL: https://dspace.uzhnu.edu.ua/jspui/handle/lib/10070 (дата звернення: 23.12.2020)

11. Дідур К. М. Сучасні методи оцінки персоналу. Ефективна економіка. 2011. №11. URL: http://www.economy.nayka.com.ua/?op=1&z=776 (дата звернення: 23.12.2020)

12. Живко З. Б. Сучасні методи забезпечення надійності персоналу: навчальний посібник у схемах і таблицях. Львів: ЛьвДУВС, 2019. 128 с.

13. Зайцева Т.В. Модель управления человеческими ресурсами организации. Вестник МГУ. Серия 21. Управление (государство и общество) №2. 2007. С.1-22. URL: https://cyberleninka.ru/article/n/model-upravleniya-chelovecheskimi-resursami-organizatsii (дата звернення: 23.12.2020)

14. Зайцева Т.В. Стратегия управления человеческими ресурсами организации. Вестник МГУ. Серия 21. Управление (государство и общество) 2010. №1. С.3-16.

15. Закон України «Про професійний розвиток працівників». URL: https://zakon2.rada.gov.ua/laws/show/4312-17 (дата звернення: 23.12.2020)

16. Зімовін О. Як визначити здібність співробітників до навчання. Оплата праці. 2016. № 6/1. URL: https://i.factor.ua/ukr/journals/ot/2016/march/issue-6/1/article-16586.html (дата звернення: 23.12.2020)

17. Илюшникова Е.К., Илюшников К.К. Инструменты автоматизации процесса управления персоналом в коммерческой организации. Креативная экономика. 2019. Том 13. № 7. С.1443-1456.

18. Інформаційні технології та моделювання бізнес-процесів : Навч. посіб. / О. М. Томашевський, Г. Г. Цегелик, М. Б. Вітер, В. І. Дубук. К. : ЦУЛ, 2012. 296 с.

19. Кузьмин Д. Оценка персонала от А до Я. URL: https://uprav.ru/blog/otsenka-personala-ot-a-do-ya/ (дата звернення: 23.12.2020)

20. Лазоренко Л. Особливості сучасного управління людськими ресурсами. URL: http://personal.in.ua/article.php?ida=635 (дата звернення: 23.12.2020)

21. Лонцих Н.П., Кунаков Е.П. Методы работы с персоналом в рамках системы защиты информации. Сб. статей Всероссийской научной конференции. Иркутск: Изд-во Иркутского нац. исслед. техн. университета, 2017. С.44-50.

22. Маркова Т.И., Захарова К.В. Классификация инсайдеров. URL: https://cyberleninka.ru/article/n/klassifikatsiya-insayderov (дата звернення: 23.12.2020)

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

24. Менеджмент: навч.посібник /за заг. ред. Г.О. Дорошенко. Харків, "ВСВ-Принт", 2015. 300 с.

25. 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.

26. Основные принципы обеспечения информационной безопасности. URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/osnovnye-aspekty-informatsionnoj-bezopasnosti/osnovnye-printsipy-obespecheniya-informatsionnoj-bezopasnosti/ (дата звернення: 23.12.2020)

27. Оценка лояльности персонала. URL: https://dominyak.com/ (дата звернення: 23.12.2020)

28. Положение об обучении и проверке знаний по вопросам информационной безопасности. URL: http://securitypolicy.ru/ (дата звернення: 23.12.2020)

29. Пучкова С. І. Управління кадровою безпекою підприємства через сучасні кадрові технології. Науковий вісник. Одеський нац. екон. університет. Всеукраїнська асоціація молодих науковців. Науки: економіка, політологія, історія. 2013. № 26 (205). С. 43–54.

30. Разница между управлением персоналом и управлением человеческими ресурсами. URL: https://thedifference.ru/otlichie-upravleniya-personalom-ot-upravleniya-chelovecheskimi-resursami/ (дата звернення: 23.12.2020)

31. Романенко Е.А., Тимофеев Д.С. Методы обучения персонала по вопросам информационной безопасности. URL: http://ir.nmu.org.ua/bitstream/handle/ 123456789 /1667/14.pdf (дата звернення: 23.12.2020)

32. Свідомий працівник – безпечна організація, ч.3. URL: https://ua.ikmj.com/ conscious-worker-is-a-safe-organization-part-3/ (дата звернення: 23.12.2020)

33. Сервисы Kaspersky Security Intelligence. Тренинги по кибербезопасности. URL: https://media.kasperskycontenthub.com/wp-content/uploads/sites/67/2017/03/17205153/Leaflet_KSIS_training_RUS_WEB.pdf (дата звернення: 23.12.2020)

34. Системы и инструменты оценки персонала. URL: https://www.e-xecutive.ru/ (дата звернення: 23.12.2020)

35. Скиба В., Курбатов В. Руководство по защите от внутренних угроз информационной безопасности. М.,Спб.: Издательство Питер, 2008. 320 с.

36. 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: 23.12.2020)

37. Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации. М.: ИНФРА-М, 2010. 304 с.

38. Чевганова В. Я. Система оцінювання персоналу підприємства. Ефективна економіка. 2014. № 4. URL: http://www.economy.nayka.com.ua/?op=1&z=2906 (дата звернення: 23.12.2020)

39. ISO/IEC 27001:2005(E) Information technology - Security techniques - Information security management systems – Requirements, 2005. 34 p.

40. ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls, 2013. 80 p.

41. Employee Monitoring Software Reviews. URL: https://www.pcmag.com/categories/employee-monitoring (дата звернення: 23.12.2020)

42. The Forrester Wave™: Security Awareness And Training Solutions, Q1 2020. URL: http://i.crn.com/ (дата звернення: 23.12.2020)

43. Webroot® Security Awareness Training. URL: https://manufacturerstores.techdata.com/docs/default-source/carbonite/webroot_security_awareness_training_smb.pdf?sfvrsn=2 (дата звернення: 23.12.2020)