

ЗМІСТ

ВСТУП.....	3
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ КАДРОВОЇ БЕЗПЕКИ.....	4
1.1 Сутність та зміст кадрової безпеки підприємства в умовах цифровізації.....	4
1.2 Суб'єкти, об'єкти та методи кадрової безпеки.....	6
1.3 Зарубіжний та вітчизняний досвід впровадження ІТ-технологій у кадрову безпеку підприємства.....	9
РОЗДІЛ 2. АНАЛІЗ ТРЕНДІВ 2019 РОКУ В ДІДЖІТАЛІЗАЦІІ HR.....	13
2.1 Особливості цифрового покоління Z.....	13
2.2 Новітні тренди у розвитку соціально-трудових відносин.....	15
2.3 Діджиталізація в HR.....	17
РОЗДІЛ 3. ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ В УДОСКОНАЛЕННІ КАДРОВОЇ БЕЗПЕКИ.....	20
3.1 Додатки для рекрутерів та HR-ів.....	20
3.2 Google-форми як найдоступніший метод визначення рівня лояльності персоналу.....	22
3.3 Переваги використання ІТ-технологій у кадровій безпеці.....	26
ВИСНОВКИ.....	28
СПИСОК ЛІТЕРАТУРИ.....	30

ВСТУП

В умовах ринкової економіки одним з актуальних питань є управління підприємством з позиції економічної безпеки. Підприємства повинні протистояти різного роду загрозам і відновлюватися після їх настання. Успішне функціонування підприємства в умовах ринкової економіки передбачає забезпечення ефективної системи заходів економічної безпеки.

В останні роки підприємства відчують зростання загроз з боку власного персоналу, супроводжується погіршенням економічної безпеки підприємства внаслідок збільшення ризиків в управлінні персоналом. За оцінками фахівців, такі ризики можуть не тільки викликати підприємству фінансові втрати, але і привести до його повної втрати власниками або істотного зменшення ринкової вартості активів.

Розвиток і успішне функціонування підприємництва в ринковій економіці передбачає забезпечення ефективної системи кадрової безпеки. Така безпечність вважається домінуючою у відношенні інших елементів системи безпеки підприємства, оскільки пов'язана з персоналом, якість якого є першоосновою в будь-якій діяльності.

З використанням цифрових технологій повсякденне життя людини змінюється, а разом з тим змінюється структура національної економіки та соціально-економічні відносини, а також виникають нові вимоги до комунікацій, інформаційних систем і сервісів.

Цифровізація або діджиталізація – це впровадження цифрових технологій в усі сфери життя: від взаємодії між людьми до промислових виробництв, від предметів побуту до дитячих іграшок, одягу тощо. Це перехід біологічних та фізичних систем у кібербіологічні та кіберфізичні. Перехід діяльності з реального світу у світ віртуальний (онлайн) [1]. Цифрові системи та технології можна використовувати майже всюди, кадрова безпека не є виключенням.

РОЗДІЛ 1

ТЕОРЕТИЧНІ ОСНОВИ КАДРОВОЇ БЕЗПЕКИ

1.1 Сутність та зміст кадрової безпеки підприємства в умовах цифровізації

Кадрова безпека – це процес мінімізації або остаточне зведення до нуля будь-яких несприятливих впливів (як зовнішніх, так і внутрішніх) на економічну безпеку підприємства за рахунок ліквідації або зниження ризиків загроз, пов'язаних з персоналом, його інтелектуальним потенціалом і трудовими відносинами в цілому. Саме тому кадрова безпека повинна займати на підприємстві пріоритетне місце в забезпеченні безпеки в цілому (по відношенню до інших складових). Визначимо завдання безпеки по кадровій політиці:

1) виявлення, а також припинення будь-яких видів загроз, що виходять від співробітників – кримінальна діяльність, розголошення комерційної таємниці, незаконне співробітництво з конкурентами, нанесення шкоди бізнесу тощо;

2) оцінка обстановки в цілому в трудовому колективі, відносин між працівниками;

3) визначення рівня лояльності персоналу до підприємства, виявлення так званих «груп ризику», розробка та варіанти їх в життя заходів по нейтралізації негативно налаштованих співробітників;

4) збір та аналіз даних про претендентів для створення достовірного портрета претендента, надання інформації керівництву для прийняття правильного і об'єктивного рішень про прийом (відмову) на роботу;

5) надання консультаційних послуг, проведення навчальних курсів з підготовки персоналу, пов'язаних з питаннями забезпечення кадрової безпеки тощо.

Кадрова безпека – це можливість, а також всі допустимі заходи щодо забезпечення безпеки підприємства в економічному плані за допомогою мінімізації всіх існуючих і передбачуваних ризиків і загроз, пов'язаних, перш за все, з неблагонадійністю співробітників і неякісно виконаної роботи. Це також відноситься до інтелектуальному потенціалу компанії як усім, так і окремим робітникам, а також трудових відносин в цілому [2].

Незважаючи на те, що поняття «кадрова безпека» все частіше використовується в наукових дискусіях і все більше застосовується на практиці, до сих пір немає єдиного визначення цієї категорії. Так, А. Джобава визначає поняття кадрова безпека як сукупність заходів спрямованих на запобігання протиправних дій, або сприяння їм з боку персоналу підприємства [3].

З точки зору безпеки в розрізі трудових взаємовідносин присутній невеликий, але вагомий нюанс – кожен претендент на вакансію, кожен співробітник фірми повинен розглядатися як джерело потенційної загрози для кадрової безпеки.

У кожній компанії повинен бути, перш за все, розроблений і впроваджений дієвий комплекс заходів щодо забезпечення даного виду безпеки. Це заходи щодо запобігання та мінімізації загроз з боку власних працівників будь-якого рівня незалежно від відділу:

- підбір досвідчених і благонадійних працівників;

- контроль благонадійності і лояльності персоналу, відстеження змін в настрої трудового колективу;

- своєчасне виявлення, а також усунення причин та загроз;

- правильне і обґрунтоване відсіювання джерел зовнішніх і внутрішніх загроз з боку співробітників.

Тільки в синергії всіх заходів дані показники можуть дати позитивний ефект стосовно забезпечення кадрової безпеки. Це в якійсь мірі допоможе запобігти можливості розголошення в інтересах третіх осіб певної частини інформації підприємства [4].

Кадрові ресурси поповнюються значною кількістю представників нового покоління. Молоді працівники набувають все більше досвіду у використанні наявних технологічних інструментів, вимагаючи повної свободи вибору щодо того, як, де і коли вони працюють. З використанням цифрових технологій змінюються не тільки повсякденне життя людини, а й структура національної економіки та виробничі відносини. Сьогодні персонал підприємств виступає в як великий актив для реалізації нових ідей.

Цифровізація передбачає використання соціальних мереж і цифрових платформ, а також аналітики великих обсягів даних, хмарних сервісів, можливостей штучного інтелекту, доповненої реальності, спеціальних мобільних додатків. Це може привести до збільшення компетентнісних та професійних вимог працівників.

1.2 Суб'єкти, об'єкти та методи кадрової безпеки

Служба управління персоналом – основний суб'єкт кадрової безпеки підприємства. Служба безпеки так само виступає суб'єктом, як і СУП (служба управління персоналом), але у деяких компаніях, підприємствах, організаціях існує думка, що проблемами, які пов'язані із безпекою, повинна займатися в основному тільки служба безпеки.

Як зазначає Г. Назарова, служба управління персоналом є не менш важливим суб'єктом, а в деяких питаннях – і значнішим [5]. Оскільки підбором, оцінкою, розвитком співробітників служби безпеки займається саме СУП, вона безпосередньо має вплив на забезпечення та якість безпеки, у тому числі кадрової. Прямим обов'язком працівників служби управління персоналом є сприяння досягненню цілей підприємства за допомогою персоналу, тобто мінімізація негативних впливів з боку персоналу. До того ж, велика кількість методів і можливостей забезпечення кадрової безпеки знаходиться в руках саме співробітників служби персоналу.

Для ефективної роботи із забезпечення кадрової безпеки співробітники служби управління персоналом (при наявності відповідного допуску) повинні мати доступ до необхідної інформації, що стосується як діяльності компанії, так і співробітників компанії.

В області забезпечення безпеки підприємства служба управління персоналом здійснює тісну взаємодію зі службою безпеки. Їх функції в контексті кадрової безпеки по своїй суті подібні, але є й відмінності.

Головна відмінність полягає в спрямованості діяльності. Якщо служба безпеки забезпечує всебічну безпеку компанії (силову, інформаційну, технічну), то служба управління персоналом займається тільки кадровими питаннями, хоча і в широкому сенсі. Однак, діяльність служби управління персоналом більш спеціалізована з точки зору безпеки [6].

Негативні внутрішні ризики компанії і загрози, пов'язаних з діяльністю персоналу можна вважати об'єктом кадрової безпеки.

Вплив суб'єкта на об'єкт кадрової безпеки можливий тільки при циркуляції інформації між ними, що передбачає отримання, передачу, переробку і використання інформації самого різного роду: економічної, статистичної, фінансової тощо. Своєчасне надання інформації дозволяє правильно продіагностувати ситуацію і прийняти правильне рішення.

З іншого боку, вплив суб'єкта на об'єкт кадрової безпеки також передбачає збереження як конфіденційної інформації, так і комерційної таємниці. Іншими словами, суб'єкт кадрової безпеки повинен охороняти відповідну інформацію, добувати, аналізувати, перетворювати і передавати на певний рівень потрібні дані.

Визначення основних загроз кадровій безпеці підприємства розширює понятійно-категоріальний апарат щодо соціально-економічної безпеки підприємства, спрощує діагностику та аналіз механізму забезпечення безпеки та дає можливість обґрунтувати основні методи забезпечення кадрової безпеки підприємства [6].

Відповідно до існуючих видів загроз, можна визначити такі основні методи забезпечення кадрової безпеки підприємства: економічні, технологічні, організаційні, соціально-психологічні, адміністративні та дисциплінарні. Також до методів безпеки можна віднести процедурні та інтерактивні (рис. 1.1).

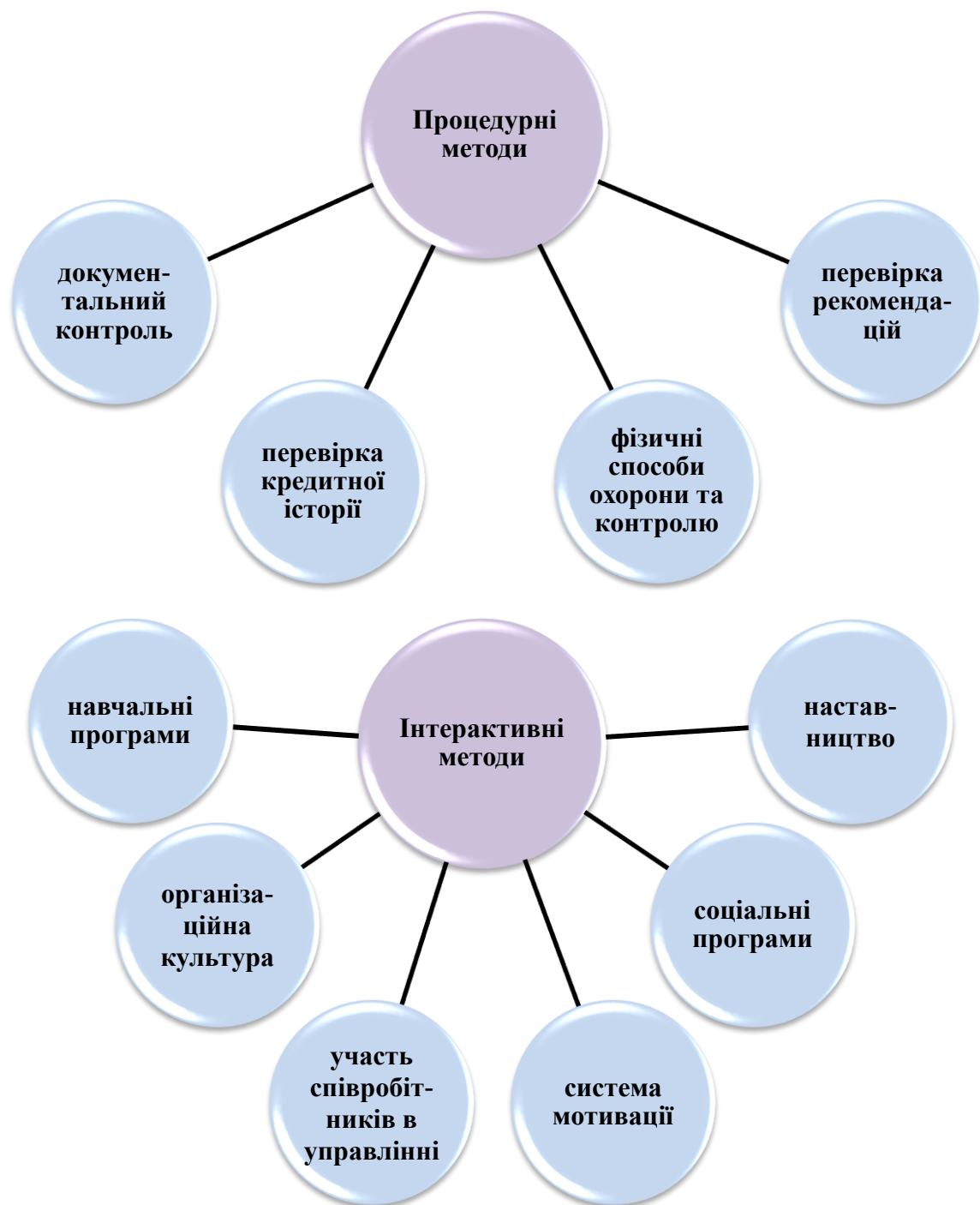


Рис. 1.1. Процедурні та інтерактивні методи безпеки

1.3 Зарубіжний та вітчизняний досвід впровадження ІТ-технологій у кадрову безпеку підприємства

В сучасній Україні економічні умови не стабільні, тому як наслідок ведення бізнесу стає агресивнішим. Усе спрямовано на перш за все на подавлення конкурентів. «Кадри вирішують все» – відомий вислів, завжди актуальний, особливо зараз в нашій країні.

Однією з головних цілей вітчизняних підприємств на сучасності етапі є забезпечення їх економічної безпеки. Досягнення цієї мети можливе не тільки через виявлення зовнішніх і внутрішніх загроз діяльності підприємства, а й через запобігання та мінімізації загроз та ризиків з боку власного персоналу.

У стратегії і тактиці роботи підприємств усе частіше звертають увагу на набір, звільнення, роботу і відносини з персоналом, а також різні професійно-кваліфікаційні групи працівників, які є невід'ємною частиною всієї виробничо-економічної діяльності та безпеки будь-якого підприємства.

Основним джерелом надходження персоналу на підприємство є набір персоналу. Це досить важливий і трудомісткий процес. В Україні процес набору кадрів проводиться не тільки за участю як директора підприємства, працівника відділу кадрів, начальника відділу куди буде влаштовуватися майбутній працівник, а й за участю начальника служби безпеки підприємства.

При відборі персоналу найчастіше доводиться мати справу з оцінкою особистих якостей людини на відповідність вимогам посади. У минулі роки на перше місце, особливо при відборі керівників, висувалося оцінювання ідеологічної позиції людини. В даний час такого роду критерій втратив своє значення, але відношення претендента до економічних реформ, знання нових офіційних матеріалів та наявність елементів нового економічного мислення представляються важливими. Головною вимогою при відборі кадрів є професійна компетентність претендента [7].

В сучасній українській HR-практиці присутні одночасно і перспективні цифрові технології, що дозволяють компаніям швидко знаходити та інтегрувати в бізнес потрібних людей.

«Цифрова» дійсність диктує свої умови з розвитку та адаптації співробітників і потенційних кандидатів на посади і робочі місця до майбутніх змін, звичайно ж, не без існуючих проблем (рис. 1.2).

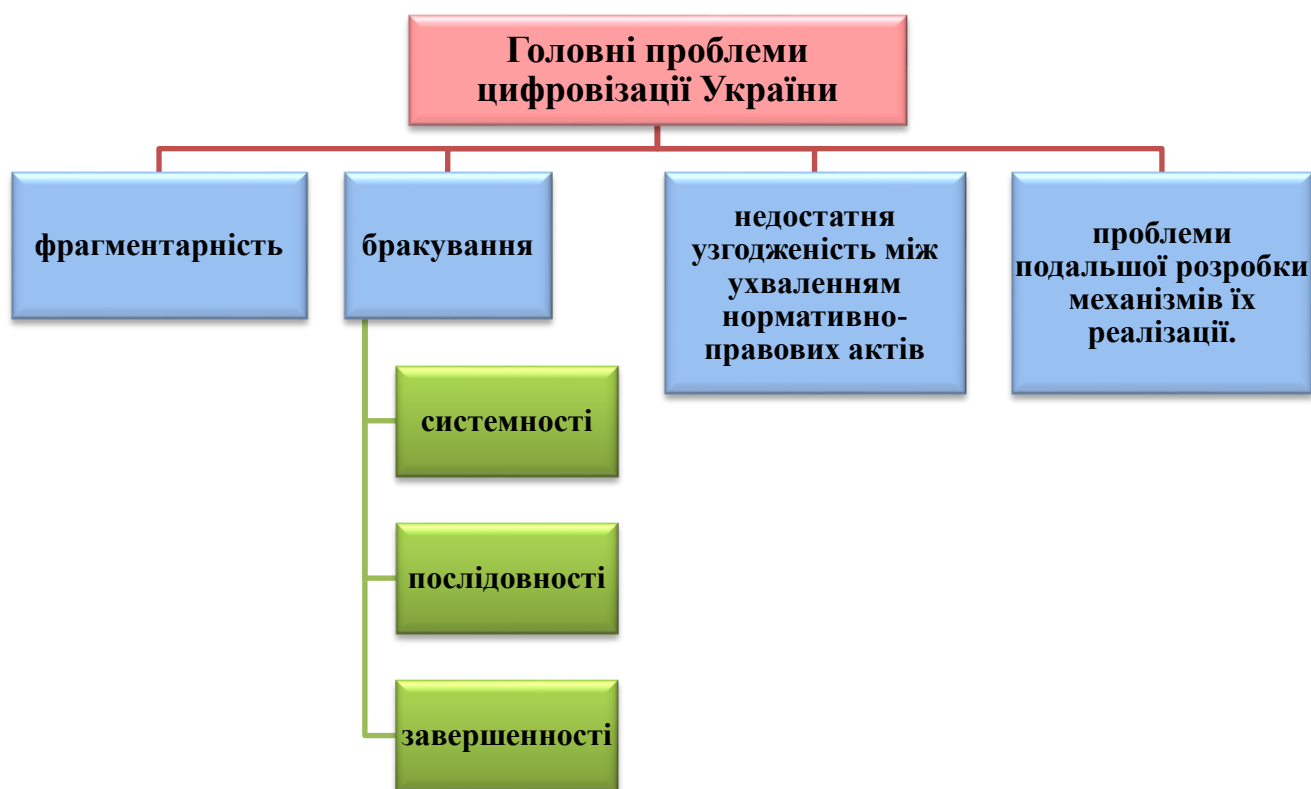


Рис. 1.2. Проблеми цифровізації України.

У зарубіжних організаціях функції з проведення оцінки кадрів розподіляються між лінійними керівниками і кадровими службами. Кадрові служби, виходячи з корпоративної політики, розробляють процедури їх практичного використання. Кадровики допомагають впроваджувати систему оцінок, розробляють програми навчання, проводять опитування, організовують збереження всієї інформації в банках даних. Фактична і оцінна інформація, яку збирають на багатьох фірмах по широкій програмі, являє собою реальну базу кадрового планування, розрахунку потреб в додатковому персоналі, прогнозування програм внутрішньо фірмового навчання, організації

конкурсного заміщення вакантних посад і, безумовно, оплати праці співробітників. У різних організаціях акцент робиться в залежності від кадрової політики на ті чи інші проблеми.

Вирішальна роль в оцінці персоналу належить безпосередньо начальнику, який добре знає своїх підлеглих, несе повну відповідальність за результати їх діяльності, застосовує заходи заохочень і покарань за їх навчання і розвиток.

У японських фірмах вважають, що менеджер повинен бути фахівцем, який може працювати на будь-якій ділянці, а не виконувати окремі функції, тому при підвищенні кваліфікації керівник відділу підрозділу вибирає для вивчення нову сферу діяльності, в якій він раніше не працював.

В Японії кожна фірма дуже вимогливо ставиться до підбору нових кадрів. Для країни з незначним рівнем безробіття (близько 1,5-2%) ця проблема більш актуальна безпосередньо для організацій, ніж для рівня державного управління. Але практика підбору персоналу в Японії заслуговує на особливу увагу. Таким чином, кожна фірма формує для себе фахівця, орієнтуючись на довгострокову співпрацю [8].

У рейтингу країн, в яких власники компаній частіш інших тримають службу безпеки, лідирують Філіппіни (72%), Мексика (71%) і Росія (63%). Недалеко пішли США, Вірменія і ПАР. Тут 60% компаній вважають за необхідне убезпечити себе від шахрайства власних співробітників за рахунок внутрішньої СБ. У Канаді, Аргентині, Нідерландах та Австралії - по 40% «обережних» компаній. Замикають список В'єтнам, Данія і Японія, де служби внутрішнього контролю є тільки у п'ятій частині компаній (рис. 1.3).

Аналізуючи наявні дані, можна зробити висновок про те, що на даному етапі не існує загальноприйнятої, «оптимальною» схеми для вітчизняних підприємств аналізу та вжиття заходів щодо кадрової безпеки [9].

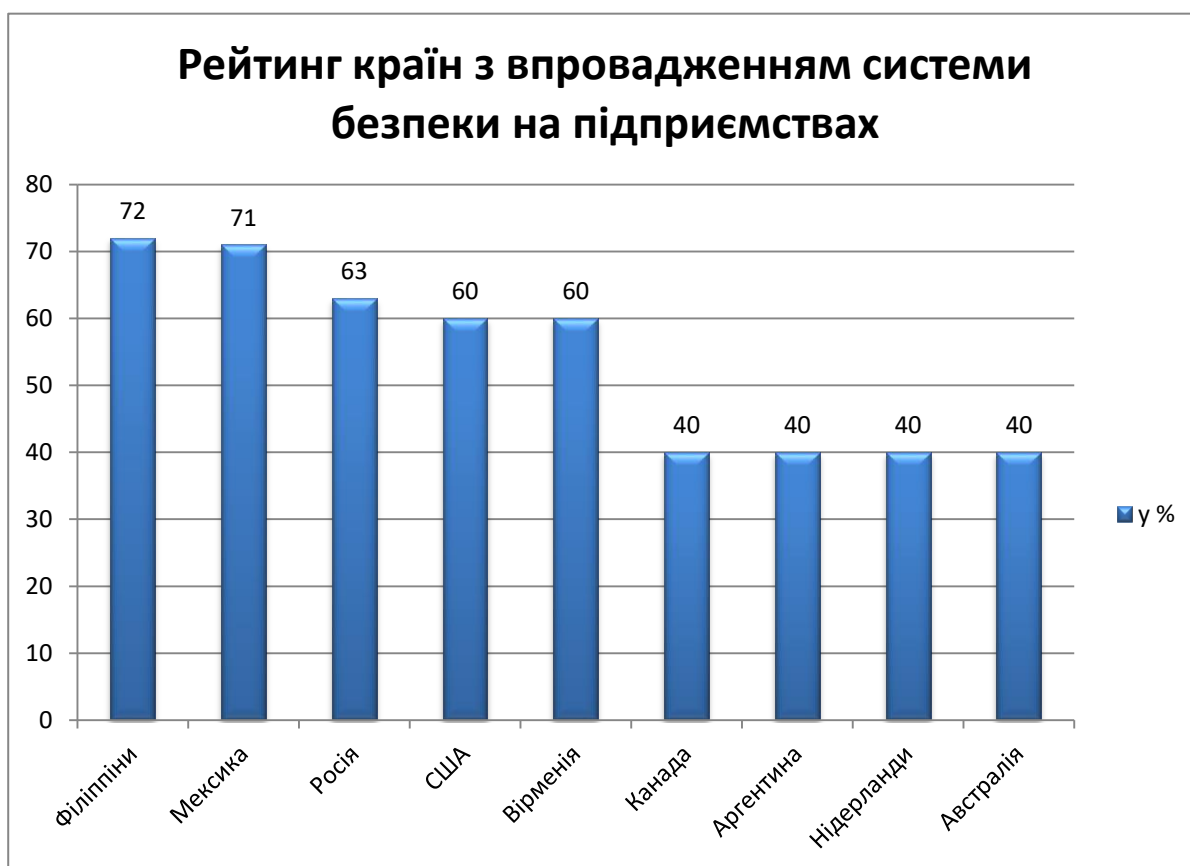


Рис. 1.3. Діаграма рейтингу країн світу

Сінгапур, Великобританія, Нова Зеландія, ОАЕ, Естонія, Японія, Ізраїль – країни-лідери з розвитку цифрової економіки та діджиталізації в цілому. Ці країни взяли курс на цифровий розвиток у сферах діяльності та новітніх технологіях. По всьому світу частка традиційної економіки зменшується, а цифрової – навпаки збільшується. Це надає країнам величезні переваги як для бізнесу, так і в цілому.

Проте Україна, ІТ-фахівці якої аутсорсінгом оцифровували все майже півсвіту, тільки зараз на державному рівні взяла курс на розвиток цифрової економіки [10].

РОЗДІЛ 2

АНАЛІЗ ТРЕНДІВ 2019 РОКУ В ДІДЖІТАЛІЗАЦІІ HR

2.1 Особливості цифрового покоління Z

Теорія поколінь тісно пов'язана з економічними циклами розвитку держав. Підйом, стабільність, спад, криза, потім знову підйом. Розвиваються технології, змінюється суспільство, зростають потреби, з'являються і вимирають нові професії, навіть цілі індустрії, але історичні витки залишаються незмінними. Кожен з цих періодів впливає на формування цінностей поколінь.

Представникам кожного з цих поколінь властиві свої особливості світогляду, цінності, погляди на життя, у кожного своя місія і доля. Зрозуміло, структура особистості формується під впливом різних факторів: сім'ї, соціуму, оточення, професії. Але все ж людей одного покоління об'єднують якісь фундаментальні особливості (рис.2.1). Цінності поколінь формуються під впливом найбільших, значущих подій в країні та світі, під впливом ЗМІ, прийнятої в суспільстві системи виховання.



Рис. 2.1. Особливості і динаміка формування поколінь.

Покоління Z – це діти, народжені в період між 1990-м і серединою 2000-х років. Це перше покоління, яке народилося в цифровому світі й вже не може уявити своє життя без мобільного Інтернету та інших гаджетів. Вони від народження живуть у світі без кордонів, правда, часто цей світ обмежений екраном монітора.

Важливим для покоління Z є:

- 1) робота в чесній фірмі де цінують працівників;
- 2) визнання і впевненість в тому, що їх праця приносить віддачу;
- 3) отримання розумного доходу;
- 4) пільги у вигляді турботи про здоров'я;
- 5) гнучке робоче середовище і робочій графік;
- 6) нові можливості.

Покоління Z звикло виражати свої думки за допомогою постів, твіттів чи поновлення статусу. Вони щодня діляться подробицями свого повсякденного життя на онлайн платформах. Саме тому очікування можливостей від покоління Z взаємодіяти зі своїми улюбленими брендами в магазинах, на своїх телефонах і, звичайно ж, в соціальних мережах мають сенс.

Для взаємодії з представниками покоління Z слід використовувати платформи, зображені на рисунку 2.2.

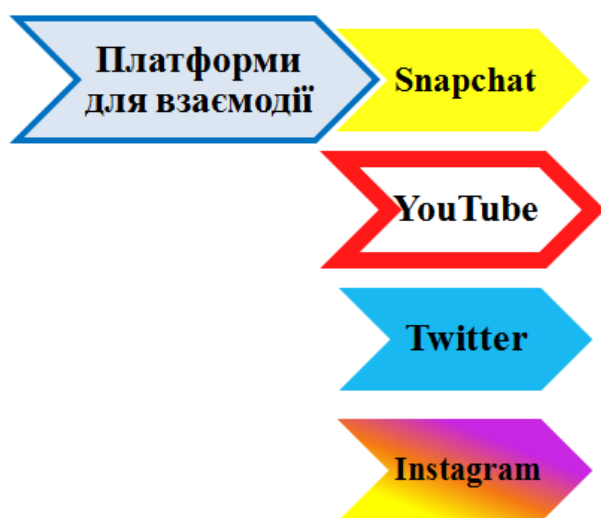


Рис.2.2. IT-платформи комунікаційної взаємодії.

Поширення позитивних фактів про компанію онлайн, демонстрація в усіх соціальних мережах відкритості й прозорості фірми та реальні історії про співробітників, сприймання своєї культури як бренду і встановлення контакту з цікавою групою за допомогою блогів, надання важливої інформації, оптимізація сайтів для мобільних пристроїв – це найголовніші складові стратегії компаній, де працює покоління Z.

2.2 Новітні тренди у розвитку соціально-трудова відносин та кадрової безпеки

Сучасні світові тенденції в сфері соціально-трудова відносин в першу чергу обумовлені глобалізацією національної економіки та зближенням трудових норм, прав і гарантій. До новітніх можна віднести тренди, зображені на рисунку 2.3.

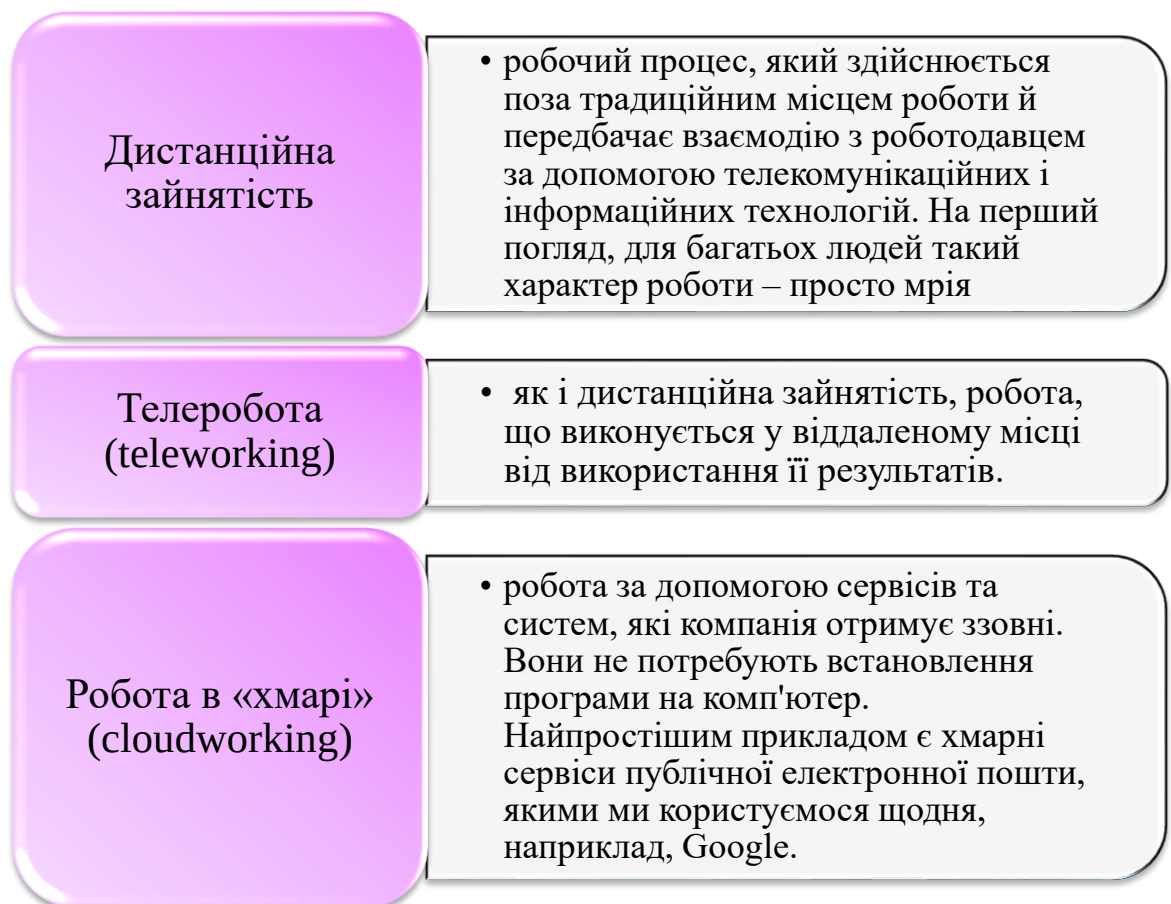


Рис. 2.3. Сучасні світові тенденції у сфері праці.



Рис.2.3. Сучасні світові тенденції у сфері праці (продовження).

2.3 Діджиталізація в HR

За останні роки цифровізація сфери HR стрімко почала зростати. Почали з'являтися тенденції в усіх напрямках управління персоналом на підприємствах, тож кадрова безпека не стала винятком.

За 2019 рік можна виділити такі тренди в діджиталізації HR:

1) Автоматичне заповнення профілів кандидатів на основі їх сторінок у професійних мережах (LinkedIn).



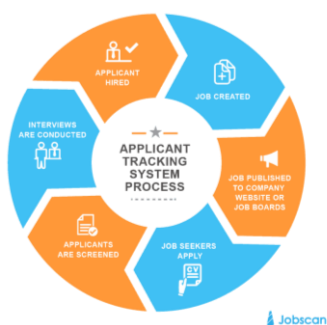
2) Анонімність у попередньому відборі (продукти Jobr, JobSnap, Switch, Inco.work, Djinni).



3) Використання соцмереж для підбору кандидатів (Facebook, Твіттер, Telegram).



4) Автоматизація підбору персоналу (цифрові системи ATS – Applicant Tracking System).



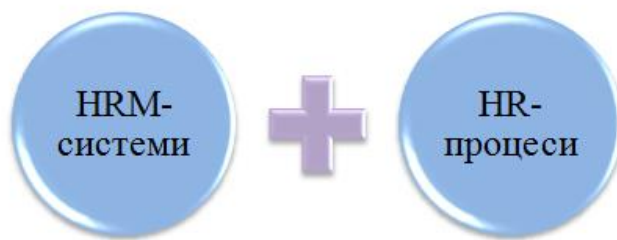
5) Автоматизація рекрутингових процесів – онбордінг, адаптація, навчання, розвиток, внутрішній документообіг компанії (ZohoPeople, Bamboo HR, Hurma System).



6) Прогнозування і HR – аналітика (штучний інтелект).

7) Моніторинг настрою співробітників (moodpolls– опитування настрою та вимірювання залученості персоналу – продукти eNPS і Gallup Q12, BambooHR, Hurma).

8) Поєднання процесів рекрутингу та HR.



9) Інтеграція з календарями, управління зустрічами (Google-Календар).



10) Корпоративне навчання.

11) Діджіталізація рекрутингу (відео конференції в Skype, GoogleHangouts або Zoom).



12) Сайти для перевірки навичок – Codility, TestDome, Tests4Geeks, Prometheus [11].






У сучасних умовах для українських підприємств все більшого значення набувають питання лояльності персоналу до організації. Пов'язано це в першу чергу з радикальною ломкою цінностей в сфері праці, зміною характеру відносин «роботодавець – найманий працівник». Великий інтерес до проблеми лояльності персоналу висловлюють керівники підприємств, він пов'язаний з усвідомленням того факту, що лояльні співробітники, поряд з грамотним менеджментом, правильної маркетинговою стратегією і якісним товаром або послугою є основою процвітання і безпеки компанії.

Лояльність персоналу – це, по-перше, рівень мотивації співробітника, при якому він проявляє відданість компанії, зацікавленість в її успіху і готовність якісно і ефективно виконувати свої посадові обов'язки. По-друге, це бажання бути корисним та потрібним. Лояльний співробітник завжди прагне бути чесним і щирим по відношенню до компанії, виконати свою роботу якнайкраще. Можна сказати, що лояльний співробітник – «безпечний» співробітник з точки зору кадрової безпеки та управління персоналом загалом.

Щоб визначити рівень лояльності персоналу до підприємства, виявити так звані «групи ризику», розробити варіанти вжиття заходів стосовно нейтралізації негативно налаштованих співробітників, можна провести опитування або анкетування. В умовах діджиталізації це можна зробити значно простіше, використовуючи чат-боти, заповнення Google-форм, онлайн-анкетування. Однією з головних особливостей збору інформації таким шляхом є анонімність, тобто анонімне заповнення Google-форми дає можливість отримати більший відсоток правдивої інформації і вже на основі отриманої інформації аналізувати рівень лояльності персоналу на підприємстві.

РОЗДІЛ 3

ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ В УДОСКОНАЛЕННІ КАДРОВОЇ БЕЗПЕКИ

3.1 Додатки для рекрутерів та HR-ів

Додатки для рекрутерів і HR-ів сьогодні актуальні, як ніколи. Для поліпшення продуктивності і автоматизації HR-процесів створені сотні платформ.

Попередня оцінка знань, навичок, здібностей та інших кваліфікацій здобувачів допомагає вибрати самого відповідного кандидата. Тому HR-софт для тестування навичок користується великим попитом. Сайти, соціальні додатки, соціальні мережі – найкращі помічники як для попередньої оцінки кандидатів на певні посади, так і для перевірки вже існуючих співробітників.

Більше 66% керівників компаній вважають, що автоматизація HR-процесів може підвищити якість роботи відділу кадрів. HR-додатки для автоматизації – головна категорія програмного забезпечення для працівників у сучасній сфері управління персоналом [12].

За оцінками Jobscan, більшість найбільших корпорацій використовують Applicant Tracking Systems або ATS. Системи відстеження кандидатів є однією з найбільших категорій програмного забезпечення для рекрутерів та HR-ів. У 2018 році багато компаній міняли ATS, оскільки роботодавці продовжують шукати найбільш зручні варіанти (табл. 3.1).

Таблиця 3.1

Додатки для рекрутерів та HR-ів

Назва	Характеристика додатка
Bullhorn	Функціональна і проста у використанні система відстеження кандидатів, яка дозволяє управляти всіма процесами набору персоналу з одного інтерфейсу.

Продовження таблиці 3.1

Назва	Характеристика додатка
Breezy HR	Допомагає приймати більш обґрунтовані рішення про найм. Система пропонує звітність і аналітику, управління кандидатами, синхронізацію з e-mail і організацію планування.
Workable	ATS з вбудованим джерелом кандидатів. Це гнучке, глобальне, просте у використанні програмне забезпечення для HR. Підтримується на ПК і мобільних пристроях, а також має цілодобову підтримку по всьому світу.
Beamery	Програмне забезпечення для набору персоналу, орієнтоване на швидкозростаючі компанії. Підтримується на ПК і смартфонах.
Lever	Рекрутингова система, яка включає в себе такі сервіси: залучення кандидатів, оптимізація робочого часу, проведення співбесід, тестування кандидатів, аналіз продуктивності.

Сучасні компанії усвідомлюють, що їх найпотужніший актив і конкурентну перевагу – люди. З метою допомоги HR-менеджерам створені робочі програми та сервіси з управління персоналом:

VambooHR збирає і систематизує всю інформацію за час роботи співробітників, а потім допомагає використовувати її для досягнення загальних цілей.

Hurma дозволяє об'єднати всі HR-процеси рекрутингу в одній HRM/HRIS системі. Пошук кандидатів, тестові завдання та інтерв'ю, система планування зустрічей і всі події компанії в зручному інтерфейсі. На відміну від сервісів, представлених вище, функціональність системи більш оптимізована під завдання вітчизняного бізнесу, а ціна на порядок нижче. Hurma була створена для того, щоб у HR-менеджерів була можливість приділяти увагу більш важливим речам, а не рутинній роботі з паперами [13].

Також набирають популярності чат-боти в меседжері Telegram. Простий та зручний інтерфейс соціальної мережі дозволяє проводити як анонімні, так і

публічні опитування. Однією з переваг цієї соцмережі є доступ з різних пристроїв – як ПК, так і смартфони, планшети.

За 10 років чат-боти показали, що вони можуть успішно справлятися також із клієнтською підтримкою, економлячи компаніям час і гроші [14].

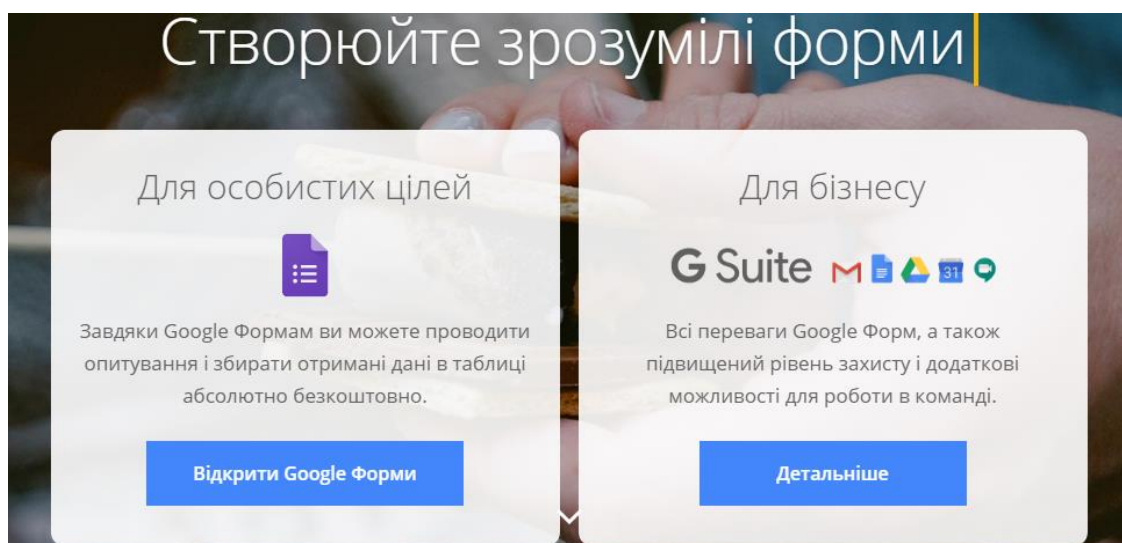
3.2 Google-форми як найдоступніший метод визначення рівня лояльності персоналу

Google Форми – це універсальний інструмент для створення форм і опитувань з рядом переваг:

- можливість створення різного виду питань, а також перемішування їх між собою;
- кожна анкета заповнена професійно під будь-якого клієнта;
- аналіз відповідей та автоматичні звіти;
- можливість відправити опитування поштою або опублікувати в соціальних мережах;
- для участі в опитуванні не потрібен акант Google.

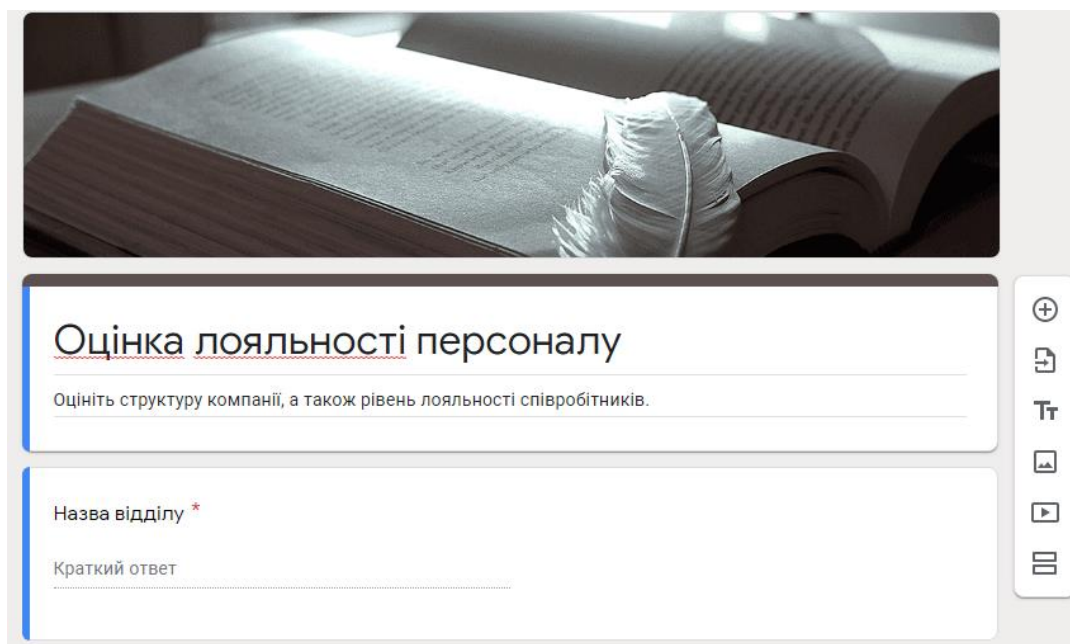
Доступність, простота у використанні, можливість доступу із різних гаджетів – найголовніша перевага даної платформи.

Створювати Google Форми можна як для особистих цілей, так і для бізнесу.



За допомогою Google Форм можна легко і швидко планувати заходи, складати опитування та анкети. Форму можна підключити до Електронної таблиці Google, і тоді відповіді респондентів будуть автоматично в ній зберігатися.

Для оцінки рівня лояльності персоналу як складової кадрової безпеки персоналу було складено анкету в Google Формі.



Запропоновано декілька питань, що виражають різноманітні почуття, які може відчувати співробітник по відношенню до своєї організації. Відповіддю на запитання є перелік варіантів, з яких треба обрати лише один:

1. Я готовий докласти зусиль, які навіть перевищують загальноприйняті очікування, щоб моя організація процвітала

- ☐ абсолютно не згоден;
- ☐ помірно не згоден;
- ☐ в чомусь не згоден;
- ☐ важко відповісти;
- ☒ згоден до певної міри;
- ☐ згоден в цілому;
- ☐ повністю згоден.

Таблиця 3.2

Питання GoogleФорми щодо оцінки лояльності персоналу

№	Питання
1.	Я готовий докласти зусиль, які навіть перевищують загальноприйняті очікування, щоб моя організація процвітала
2.	Я завжди кажу своїм друзям, що працюю в чудовій організації
3.	Я не відчуваю ніякої лояльності по відношенню до цієї організації
4.	Я погоджуся практично з будь-яким призначенням, аби залишитися працювати в цій організації
5.	Я вважаю, що мої особисті цінності і цінності, прийняті в моїй організації, дуже близькі
6.	Я з гордістю заявляю іншим, що є частиною цієї організації
7.	З таким же успіхом я працював би в будь-який інший організації, якби можна було виконувати аналогічну роботу
8.	Моя організація дійсно надихає мене працювати якомога краще
9.	Потрібні дуже незначні зміни в моїх особистих обставин, щоб я залишив роботу в цій організації
10.	Я дуже радий, що вибрав саме цю організацію, коли шукав роботу й розглядав інші пропозиції
11.	Не має сенсу надовго затримуватися в цій організації
12.	У багатьох випадках я не згоден з основними напрямками політики організації по відношенню до своїх співробітників
13.	Мені дійсно небайдужа доля організації
14.	Для мене це найкраща з організацій, де я міг би працювати
15.	Рішення почати працювати в цій організації було, безумовно, помилкою з мого боку

Для того, отримання результату треба підрахувати підсумкову суму. Для цього необхідно скласти числа, що відповідають вибраним співробітником відповіді під час заповнення Google Форми.

Таблиця 3.3

Критерії оцінювання

№	Кількість балів	Трактування
1.	0-30	Співробітник абсолютно не лояльний до організації.
2.	31-45	Співробітник регулярно виконує передбачені правила і вимоги, але лише з побоювання покарання або через очікування винагороди.
3.	46-60	В цілому лояльний співробітник, зовнішня поведінка відповідає нормам корпоративної культури.
4.	61-75	Лояльний до своєї організації співробітник, його влаштовує практично все, він готовий жертвувати деякими власними інтересами заради успіху організації.
5.	76-90	Лояльний і відданий співробітник, розділяє переконання організації та її цінності.
6.	91-105	Завищена оцінка співробітника – або через бажання сподобатися керівництву, або щоб уникнути покарання за невідповідність. Дана оцінка не використовується в загальному аналізі.

Оцінки на питання № 3, 7, 9, 11, 12, 15 необхідно перетворити в зворотні. Так, якщо відповідь співробітника співставлень з цифрою 1, потрібно змінити цифру на 7; 2 змінюється на 6; 3 – на 5; відповідь 4 НЕ змінюється.

Після здійснення даного перетворення підрахуємо підсумкову суму.

Залежно від кількості балів треба зробити висновок щодо лояльності персоналу в організації.

Посилання на Google Форму:

https://docs.google.com/forms/d/14kxNdJi94eabf_01Zfr7dwyqsDIAud3UgXjpx3TifkA/edit

3.3 Переваги використання ІТ-технологій у кадровій безпеці.

Цифрові системи та технології можна використовувати практично скрізь, варто лише назвати яку-небудь операцію, яку необхідно провести, наприклад, розповісти про компанію за допомогою презентацій на виступах, що сприяє більш яскравому відтворенню інформації, більш доступному і такому, що запам'ятовується. Потрібно влаштувати нараду – різні програми для відео та аудіо конференцій можуть допомогти в цьому і особливо корисними вони будуть, якщо члени наради знаходяться, наприклад, в різних містах. Провести тренінг – все залежить від особливостей тренінгу, проте, використовувати інформаційні технології в процесі тренування можуть допомогти в засвоєнні матеріалу, що викладається. Поширення інформації – корпоративна пошта також може в цьому допомогти. Часто використовують практику публічного вручення грамот, але чи є це настільки необхідним відривати всіх від роботи заради «папірця». Можна зробити публічну розсилку в якій описати, хто молодець і чому. Таким чином можна відмітити, що жорстких кордонів у використанні таких прогресивних систем і технологій практично нічим не обмежується [15].

У зв'язку з цим, впровадження нових технологій (виробничих, фінансових, управлінських, соціальних та будь-яких інших) може призвести до величезної кількості позитивних ефектів і наслідків для підприємства:

- 1) підвищення продуктивності праці;
- 2) підвищення конкурентоспроможності;
- 3) удосконалення процесу відбору та вивільнення персоналу;
- 4) удосконалення процесу адаптації персоналу на підприємстві;
- 5) мінімізація всіх існуючих і передбачуваних ризиків і загроз, пов'язаних, перш за все, з неблагонадійністю співробітників і неякісно виконаною роботою;
- 6) підвищення лояльності персоналу;
- 7) підвищення ефективності роботи персоналу;

- 8) удосконалення мотивації;
- 9) підвищення кадрової безпеки.

Без сумніву, діджиталізація та використання ІТ-технологій на підприємстві може допомогти вирішити такі задачі, як комунікація з клієнтами та реклама, удосконалення продукту та засобів його доставки, автоматизація внутрішніх бізнес-процесів, спрощення взаємодії з державними органами [16].

У впровадженні та в подальшому використанні ІТ-технологій не тільки в кадровій безпеці, а й в цілому, існують також недоліки та ризики діджиталізації. Серед них можна виділити основні:

1. Надмірні витрати, адже дійсно, не в кожній ситуації діджиталізація може забезпечити реальне підвищення прибутку компанії і покращення результативності від ведення господарської діяльності.

2. Складності у впровадженні. Наявність вже налагодженого, працюючого бізнес-процесу може стати великою перешкодою при переведенні його в цифрове поле, що може загрожувати появою помилок, неточностей і в цілому порушенням звичного ходу речей.

3. Витік інформації. Це одна з найголовніших проблем безпеки підприємства, у тому числі кадрової. Будь-які цифрові технології при впровадженні можуть значно збільшувати ризики витоку інформації, особливо в сфері зберігання персональних даних і роботи з конфіденційною інформацією. Забезпечення належного рівня безпеки, в свою чергу, може значно збільшити вартість діджиталізації.

Кадрова безпека підприємства напряму залежить від лояльності персоналу, тому її рівень та якість ніяк не можна ігнорувати. Знову ж таки, використання ІТ-технологій для оцінки лояльності персоналу значно може допомогти фахівцям, наприклад, запропонована вище Google Форма – простий, швидкий та зовсім невитратний спосіб моніторингу лояльності співробітників.

ВИСНОВКИ

У висновку хотілося б ще раз відзначити той факт, що кадрова безпека дійсно є важливою складовою у формулі перемоги в сучасній конкурентній боротьбі.

У зв'язку з цим у розвитку кадрової безпеки в рідкісних випадках застосовується фінансові впливання з визначенням бюджету на заходи. Оскільки всі дії можна втілити при наявності затвердженої стратегії розвитку компанії з прописаною кадрової стратегії, для їх втілення вистачить внутрішніх людських та інформаційних ресурсів.

Таким чином, кадрова безпека будь-якого підприємства будується за кількома напрямками: суворе дотримання прописаних заходів під час прийому нового персоналу, програма адаптації, створення сприятливого середовища для лояльності співробітників до компанії.

Говорячи про діджиталізацію та цифровізацію, неможливо не звертати увагу на особливості поколінь, їх фундаментальні цінності та особливості. Всесвіт в смартфоні – це покоління Z, яке народилося в цифровому світі й вже не може уявити своє життя без мобільного Інтернету та інших гаджетів.

Нові бізнес і HR-стратегії, в основу яких закладені Digital-технології, підвищують ефективність управлінських рішень: автоматизований рекрутинг, перехід на віртуальні робочі місця, індивідуалізація – створення для кожного співробітника середовища для самореалізації та розвитку, HR-аналітика та управління ефективністю. Однак, які б пріоритети в підходах і технологіях не використовувалися, ключове значення має саме людський потенціал компанії – люди, здатні їх генерувати і ними керувати.

Спеціально розроблені програми, мобільні додатки, платформи, чат-боти – без цього сучасний «цифровий» HR, рекрутер або хедхантер просто не зможе існувати. Використання перерахованих засобів взаємодії співробітників між собою та з компанією в цілому значно спрощує роботу шляхом підвищення швидкості та якості. Нові можливості, які відкриваються перед HR-ом під час

використання спеціальних програм, сприяють підвищенню його продуктивності, адже робота стає цікавішою, більш сучасною і менш «паперовою».

Незважаючи на всі видимі переваги впровадження ІТ-технологій не можна забувати про те, що однією з найбільш значущих загроз, супутніх цифровізації в майбутньому, буде відтік персоналу нижчої і середньої кваліфікації і бракування вузькоспеціалізованих працівників, які мають відповідні компетенції.

Благонадійність і прихильність співробітників – запорука стійкості, економічної успішності та кадрової безпеки підприємства. Економічні втрати організації через відсутність лояльності її персоналу можуть представляти різний характер, найбільш «страшними» є економічні злочини в процесі професійної діяльності. Тому регулярна оцінка лояльності персоналу та вчасне виявлення проблем – один з головних пунктів правильної та добре працюючої кадрової безпеки на підприємстві.

В сучасних умовах зростання питомої ваги службової та комерційної таємниці в бізнесі веде і до збільшення значення мотивації організаційної поведінки й кадрової безпеки в організації. Лояльність персоналу в таких умовах стає в один ряд з основними аспектами забезпечення економічної безпеки за важливістю і необхідності її стимулювання, а в сучасному світі зробити це без допомоги діджиталізації майже неможливо.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Україна 2030Е – країна з розвинутою цифровою економікою [Електронний ресурс] – Режим доступу : <https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html>
2. Digital Security: How to Protect your Personal Information & Privacy Online [Electronic resource]. – URL : https://help.opensrs.com/hc/en-us/articles/208063247-Digital-Security-How-to-Protect-your-Personal-Information-Privacy-Online?mobile_site=true
3. Маркова Н. С. Розвиток персоналу : навч. посіб. / Н.С. Маркова. – Х. : Вид. ХНЕУ, 2012. – 256 с.
4. The State of Digital HR 2019 [Electronic resource]. – URL : <https://www.analyticsinhr.com/blog/the-state-of-digital-hr-2019/>
5. Назарова Г. Передумови створення системи кадрової безпеки підприємства / Г. Назарова // Регіональні аспекти розвитку продуктивних сил України. – 2010. – Вип.15. – С. 34–37.
6. Ястремська О. М. Оцінювання результатів діяльності управлінського персоналу : теоретичні та практичні аспекти : монографія / О. М. Ястремська. – Х. : ХНЕУ, 2012. – 194 с.
7. Балабанова Л. В. Управління персоналом : підруч. / Л. В. Балабанова, О. В. Сардак. – К.: Центр учбової літератури. – 2011. – 468 с.
8. Михайлова Л. І. Управління персоналом : навч. посіб. / Л. І. Михайлова. – Київ: Центр учбової літератури. – 2007. – 248 с.
9. Єгорова О.С. Управління кадровою безпекою підприємства/ О. С. Єгорова // Портал магістрів. – 2010.
10. Діджиталізація – це лише початок. [Електронний ресурс] – Режим доступу : <https://day.kyiv.ua/uk/article/ekonomika/didzhytalizaciya-ce-lyshe-pochatok>
11. 30+ додатків для рекрутерів та HR-ів [Електронний ресурс] – Режим доступу : <https://hurma.work/blog/30-dodatktiv-dlya-rekruteriv-ta-hr-iv/>

12. Василик А. В. Використання соціальних мереж у сучасному рекрутингу України / А. В. Василик, О. В. Іщенко // Економічний простір. – 2018. – № 131. – С. 53–63.

13. HURMA – усі процеси рекрутингу та HR у одній системі[Електронний ресурс] –Режим доступу :<https://hurma.work/>

14. Как чат-боты помогают HR-специалистам [Електронний ресурс] – Режим доступу: <https://chatbotconf.com.ua/ru/article/kak-chat-boti-pomogayut-hr-spetsialistam-66378>.

15. Кешелава А. В. Введение в «Цифровую» экономику/ А.В. Кешелава, В.Г. Буданов, В.Ю. Румянцев и др.; под общ. ред. А.В. Кешелава; гл. «цифр.» конс. И.А. Зимненко. – ВНИИГеосистем, 2017. – 28 с. (На пороге «цифрового будущего». Книга первая).

16. Personnel and People Security [Electronic resource]. – URL : <https://www.cpni.gov.uk/personnel-and-people-security>