УДК 331.108:651.3:004
https://doi.org/10.33296/2707-0654-18(36)-12

**КІР'ЯН ОЛЕНА**
кандидат економічних наук, доцент,
доцент кафедри економіки та менеджменту,
Українська інженерно-педагогічна академія,
м. Харків, Україна
ORCIDiD : https://orcid.org/0000-0002-1357-0497

**ТОРЯНИК ДЕНИС**
здобувач третього (освітньо-наукового)
рівня вищої освіти
кафедри економіки та менеджменту,
Українська інженерно-педагогічна академія
м. Харків, Україна
ORCIDiD : https://orcid.org/0000-0002-1146-2679

**ЯГНЕША НАТАЛІЯ**
здобувач другого (магістерського)
рівня вищої освіти
кафедри економіки та менеджменту,
Українська інженерно-педагогічна академія,
м. Харків, Україна

# КАДРОВА СКЛАДОВА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

**Анотація.** Метою статті є формування пропозицій щодо удосконалення змісту кадрової складової стратегії інформаційної безпеки підприємства, в першу чергу, за рахунок розвитку персоналу залежно від їх потенційної участі в забезпеченні системи інформаційної безпеки підприємства.

В статті розглянуто сучасні напрямки інформаційної безпеки підприємства, правове забезпечення цього процесу, адаптованого до умов сьогодення. Відмічено значущість освітніх процесів, які важливо враховувати для формування персоналу підприємства з тим, щоб робітники були адаптовані до протистояння ризикам.

Також в роботі наведено елементи кадрової стратегії, які підтримують стратегію інформаційної безпеки підприємства і, відповідно до змісту законодавчих актів України, є найбільш актуальними. Для них було визначено групи працівників підприємства, які потребують постійного спеціалізованого розвитку, виокремлено тематику цього спеціалізованого розвитку.

Наведені дані стосовно ключових компетенцій для майбутнього розвитку

персоналу і груп персоналу, до яких їх слід застосувати в першу чергу, було систематизовано в єдину табличну форму. Це дозволить спростити процес формування освітньої складової кадрової стратегії розвитку інформаційної безпеки.

Тематика статті дає базу для цілої низки подальших досліджень: розробки механізмів формування моделей визначення інформаційних ризиків та джерел їх ефективного попередження; удосконалення системи підбору та відбору персоналу з урахуванням потреб інформаційної безпеки; оптимізація механізму моніторингу глобального середовища на предмет розвитку інформаційних технологій, оновлення шахрайських схем та погроз інформаційній безпеці підприємства.

**Ключові слова:** інформаційна безпека, персонал підприємства, кадрова стратегія, захист інформації, класифікація документації, поводження з інформаційними каналами, служба безпеки підприємства, розвиток персоналу.

**Вступ.** Інформаційна безпека в умовах глобалізації економіки, активного використання інформаційних мереж, штучного інтелекту з розряду одного з чинників, що потребує від організації уваги та контролю, переходить поступово в чинник, який потребує постійної уваги та постійної негайної реакції на зміни в середовищі кожного працівника організації з додатковим поглибленим контролем не тільки служби безпеки організації та інформаційного підрозділу, а й кожного керівника на всіх без винятку рівнях управління. Швидкі зміни в середовищі демонструють певне відставання персоналу на посадах, не пов’язаних прямо з відповідальністю за безпеку, від постійно оновлюваних інформаційних ризиків. Додаткова потреба швидкого навчання всього персоналу новим програмам, можливостям мережі та в цілому інформаційного простору, користуванню новим інформаційним продуктом без достатнього усвідомлення потенційної появи додаткових можливостей для порушників постійно посилює загрози для інформаційної безпеки підприємства, зводячи нанівець якість підготовки персоналу в питаннях інформаційної безпеки.

Фахівцям відомо, що разом з інформаційним продуктом розвивають і шляхи його використання в якості шпигунського ресурсу як джерела впливу на суб’єкт ринку. При цьому відсутність постійного зв’язку фахівців в сфері інформаційної безпеки і всього колективу підприємства створюють «білі

плями» в розумінні колективом потенційно передбачуваних проблем і можливих шляхів їх попередження.

Вказані виклики вимагають від кожної організації закладати в стратегію не тільки елемент підтримки технічної та програмної безпеки інформаційного забезпечення, а й приділяти систематичну увагу кадровій складовій, особливо її предметному розвитку. Це доводить актуальність теми статті та її практичну вагомість для сучасного існування будь-якого суб'єкта господарювання в бізнес-просторі.

**Аналіз останніх досліджень і публікацій.** Різноманітним питанням кадрової стратегії та безпосередньо питанням розвитку персоналу приділяють увагу всі стейкхолдери та велика кількість сучасних науковців, в тому числі: Ансоф І., Армстронг М., Балабанова Л., Білодід А., Назарова Г., Сардак О., Терещенко І. та багато інших.

Питанням інформаційної безпеки, які стали вкрай нагальними в сучасному глобалізованому світі, приділяють увагу Березовська І.. Грицюк Ю., Довгань В., Новицький Г [7]., Сороківська О., Турчак А., Френч Х., Цимбалюк В. В тій чи іншій мірі всі вони відмічають можливі загрози, звертають увагу на шляхи їх подолання та загальне забезпечення системи інформаційної безпеки. Однак сьогодення є високодинамічним, що вимагає постійного оновлення механізму забезпечення інформаційної безпеки, в тому числі кадрового.

І якщо окремо зміст та механізм впровадження економічної стратегії безпеки підприємства, загальний зміст та процес формування кадрової стратегії розглядали та розглядають багато фахівців, то складова створення кадрового забезпечення, його розвитку як одного з ключових елементів кадрової складової стратегії інформаційної безпеки підприємства окремо поки не знайшла свого достатнього відображення в наукових публікаціях.

**Формулювання мети статті.** Метою статті є розробка пропозицій щодо удосконалення змісту кадрової складової в контексті формалізації елементів кадрової стратегії, які підтримують стратегію інформаційної безпеки

підприємства задля забезпечення постійно високого рівня інформаційної безпеки з акцентом на процес розвитку персоналу в залежності від виду, змісту та призначення інформаційних джерел, які використовує організація в повсякденній роботі, та з урахуванням прогнозу розвитку вказаних інформаційних джерел.

**Виклад основного матеріалу дослідження.** «Інформаційна безпека – стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому запобігається завдання шкоди через неповноту, несвоєчасність і недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій» [4, с. 3], тоді як «загрози інформаційній безпеці – наявні та потенційно можливі явища і чинники, які створюють небезпеку життєво важливим інтересам людини і громадянина,суспільства і держави в інформаційній сфері» [4, с. 3].

З розвитком інформаційних технологій питання інформаційної безпеки стає все більш актуальним не тільки для компаній, які безпосередньо зайняті в сфері комп’ютеризації різноманітних процесів і виготовленням гаджетів, але для кожної організації. Сьогодення передбачає впровадження в економічне життя країни та, відповідно, в життєдіяльність кожного підприємства значну кількість е-врядування у вигляді взаємодії з фіскальними органами, з територіальною та регіональною адміністрацією; он-лайн діяльності у вигляді більшості управлінських, маркетингових, інформаційно-комунікаційних процесів; он-лайн внутрішніх комунікацій у вигляді внутрішніх мереж для документообігу та зберігання інформації (документів та масивів баз даних); спілкування, управління, проектування та ін. Значна частина освітніх процесів для працівників підприємства також перемістилась в віртуальне середовище. Більшість інформації, документації, будь-яких даних середніх та крупних

компаній сучасні фахівці вважають за доцільне зберігати в хмарному сховищі. Відсоток робочих місць, функцій в діяльності підприємства, в яких би не було задіяно ті чи інші інформаційні технології, знайти все важче.

До переліку ключових питань, які зазвичай цікавили порушників та шахраїв, крім фінансової та інноваційної складової додалась і кадрова. Якщо десятиліття тому головною метою деструктивного впливу зовнішнього середовища було отримання даних про новітні розробки та технології або отримання доступу до фінансових рахунків організацій, то сьогодення додає активні намагання отримати особисті дані працівників з метою їх подальшого використання в тому числі в шахрайських фінансових схемах, або для передачі ворогу (оскільки країна знаходиться в стані війни вже більше 10 років, і персональні дані багатьох людей цікавлять ворога).

Це ставить «під удар» як інформаційні бази кадрової та фінансової служб підприємств, так і кожну інформаційну точку, яку створили та/або використовують робітники, яка прямо чи опосередковано має вихід в мережу; а також і кожного працівника підприємства як потенційне джерело інформації. При цьому більшість працівників не сприймають інформаційну загрозу як реальну та/або суттєву. Тож вони не надають належного значення інформаційній профілактиці при спілкуванні, збереженні інформації як в інтернет-просторі, так і на робочих місцях та поза територією підприємства (в соціумі).

Однак значущість, вагомість цього питання можна оцінити, спираючись на зміст «Стратегії інформаційної безпеки» [9] та «Стратегії кібербезпеки України» [10], на які, в свою чергу, спирається Закон України «Про національну безпеку України»[8]; та на впроваджений в 2021 році Нормативний документ системи технічного захисту інформації НД ТЗІ 3.6-004-21[5], де система безпеки інформації визначена як рівноправна, важлива складова загальної системи управління сучасною організацією і є обов’язковою для організацій державного сектора й наполегливо рекомендована для організацій

всіх форм власності. В цьому документі чітко і послідовно сформовано механізм якісного удосконалення організаційної системи безпеки інформації за участю всіх рівнів управління і всього колективу підприємства – від інституціонального рівня управління до окремого робітника.

Спираючись на ключові складові рекомендованих заходів щодо розробки і вдосконалення систем безпеки інформації [5, 9], сформуємо пропозиції щодо змісту та особливостей підтримуючих складових кадрової стратегії підприємств, які в першу чергу будуть відноситись до підготовки кадрів до роботи в нових реаліях.

Визначимо основні елементи, які повинні бути враховані, та шляхи їх забезпечення за допомогою розвитку (освіти) персоналу підприємства:

1. Наявність чітких та зрозумілих вимог щодо необхідного рівня безпеки, приватності, захисту інформації. Класифікація (з використанням стандартної Державної з доповненням внутрішньо організаційної). Так само – рекомендації для робітників по захисту приватної інформації самих робітників.

Цей елемент вимагає навчання кількох груп працівників підприємства різноплановим процесам. В першу чергу – здатність знайти, застосувати класифікацію інформації по відношенню до тієї, якою користується підприємство. Тобто, всі працівники, які виконують діловодні функції, повинні навчитися в рамках своїх повноважень ідентифікувати документацію, матеріали, дані, та фіксувати їх приналежність в прийнятій на підприємстві системі.

Для цього особу, яка відповідає за безпеку в організації, керівників інституціонального рівня слід навчити формувати та узгоджувати відповідну систему фіксації класифікації.

Так само їх слід навчити розробляти заходи убезпечення інформаційних джерел залежно від приналежності до того чи іншого рівня класифікації стандартів захисту інформації. Необхідним стає навчання цієї ж групи працівників щодо формування логічних, інформаційно ємних, але не великих за

обсягами інструкцій по реалізації розроблених заходів. На цьому кроці до навчання варто залучати й працівників кадрової служби та до цього не задіяних в навчанні керівників, які володіють розумінням якостей та особливостей персоналу підзвітних підрозділів (керівники) і в цілому на підприємстві (кадрова служба за результатами оцінки співробітників).

2. Політика інформаційної безпеки підприємства, яка потребує поглибленої оцінки, розробки (радикального реінжинірингу) змісту з регулярним його подальшим оновленням. Для її підтримки на відповідному потребам рівні з урахуванням динаміки змін потенційних загроз – увага до механізмів її всебічного забезпечення(техніко-технологічного, інформаційного, фінансового). Системність, безперервність, якість реалізації політики інформаційної безпеки на підприємстві.

Навчання персоналу підприємства для забезпечення цього елементу варто організовувати командне: кожен підрозділ підприємства повинен навчитися здійснювати моніторинг своєї частини інноваційних розробок, необхідних для врахування в механізмах забезпечення системи безпеки підприємства, які стають доступними на ринку, є проектами на майбутнє. Так інформаційний відділ повинен вивчати нові програмні продукти, динаміку їх розвитку, доцільність застосування на підприємстві та потенційну вартість придбання з джерелом їх отримання. Системні адміністратори та відділ технологічного супроводу повинні вивчити новітню техніко-технологічну складову інформаційних систем, сумісність їх елементів та потенційні загрози технічного змісту використання кожної новинки. Служба безпеки змушена постійно досліджувати розвиток небезпек, спричиняємих людським чинником зовнішнього середовища та розвиток інструментів, які ті використовують. І всі вони повинні навчитися систематизації досліджуваних даних.

Сформована та постійно оновлювана система даних, отримана від попередньо описаних процесів, стає підґрунтям для розробки політики інформаційної безпеки підприємства. Тож виникає потреба навчати керівника

служби безпеки здійснювати прогнозування ризиків (на основі отримуємих даних), створювати моделі відповідних процесів.

Керівників підприємства інституціонального рівня необхідно навчити приймати рішення швидко, раціонально, з об'єктивним підходом до оцінки отриманої інформації та представлених прогнозних моделей та з урахуванням наявних і можливих для отримання ресурсів.

3. Моніторинг поточного рівня дотримання безпеки інформації, поведінки персоналу залежно від умов, змісту та рівня впровадження політики інформаційної безпеки на підприємстві. Моніторинг змін в деструктивній увазі зовнішнього середовища до підприємства, змін рівнів можливих ризиків з урахуванням специфіки його діяльності.

Більшість керівників та персоналу підприємств помилково вважають, що весь цей процес є виключним обов'язком служби безпеки підприємства. Однак виконати цей процес жодна служба безпеки не в змозі. Тому виникає нагальна потреба навчити кожного керівника підрозділу, служби здійснювати постійний моніторинг дотримання безпекової поведінки підзвітного персоналу. Цей процес може бути одноразовим в ключових питаннях з постійною подальшою підтримкою рівня обізнаності щодо новітніх змін в безпеці та ризиках для неї.

Працівники служби безпеки, в тому числі керівник підрозділу, повинні постійно підвищувати кваліфікацію щодо можливих методів виявлення деструктивної уваги зовнішнього середовища та виокремлення тих її елементів, що становлять потенційну загрозу інформаційній безпеці підприємства.

4. Планування відповідних заходів оптимізації системи безпеки інформації. На підприємстві цей процес повинен базуватися на результатах моніторингу (п.3), сформованих системах даних (п.2), стратегії самого підприємства та елементах реалізованої кадрової стратегії щодо розвитку персоналу (п.1).

Для забезпечення цього елементу є потреба періодично оновлювати та розвивати навички керівника служби безпеки та керівників підприємства

інституціонального рівня формувати стратегію розвитку підприємства з урахуванням оновлених чинників впливу, оновленої інформаційної бази.

5. Розробка та регулярне оновлення кадрової стратегії. З метою ефективного забезпечення політики інформаційної безпеки підприємства важливо, спираючись на п.п. 1-4 та результати оцінки наявного персоналу підприємства кадровою службою щодо особистісних якостей повинна формуватися кадрова стратегія, яка буде містити складові оптимального розвитку персоналу в питаннях посилення інформаційної безпеки підприємства та оновлені вимоги й процедуру впорядкування змісту кадрового складу підприємства. Крім того, кадрова стратегія повинна містити механізм впровадження оновленої корпоративної культури як підґрунтя створення розуміння значущості змісту та дотримання правил інформаційної безпеки в будь-якому середовищі кожним членом трудового колективу. Так само стратегія підприємства повинна мати елемент розвитку власників підприємства з тих самих питань дотримання інформаційної безпеки та значущості її змісту та застосування (слід врахувати, що розвиток власників з ініціативи менеджменту підприємства, а не самих власників, які не є працівниками підприємства – явище унікальне).

Процес розвитку власників – не працівників підприємства повинен включати узагальнюючий матеріал щодо сучасного стану речей в системі інформаційної безпеки, зведені дані щодо можливих загроз та шляхів попередження й нейтралізації їх негативних наслідків.

Керівників всіх рівнів варто навчати формувати зміст та механізми впровадження корпоративної культури підприємства у відповідності з його ключовими потребами, працівників – довірі керівному складу та доцільності розробленої ними стратегії.

Ще одним ключовим елементом розвитку всього трудового колективу повинно стати формування командного духу, що дозволить адекватно сприймати гнучкі зміни процесів забезпечення інформаційної безпеки та

посилити взаємоконтролюючий процес співробітників на предмет дотримання ними правил і принципів інформаційної безпеки підприємства.

В цілому стратегія інформаційної безпеки підприємства, звісно, містить крім кадрової багато інших складових. але саме персонал забезпечує її розробку, підтримку та реалізацію.

Визначимо ключові компетенції, які важливо напрацювати працівниками підприємстві для більш ефективного формування механізмів розробки та реалізації інформаційної безпеки на підприємстві. Вони мають відмінності залежно від функціональних обов'язків та рівня відповідальності певного працівника (табл. 1) і які повинні бути сформовані в процесі розвитку персоналу підприємства в першу чергу.

Таблиця 1

Розвиток ключових компетенцій персоналу
з підтримки інформаційної безпеки підприємства

| Компетенція | Категорія, рівень, підрозділ | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | Керівники | | | | Працівники підрозділу | | | Працівники з діловодними функціями | Всі працівники |
| | Інституціональний рівень | Управлінський рівень | Технічний рівень | Служби безпеки | Служби безпеки | Інформаційного відділу | Відділу маркетингу | | |
| Розробка стратегії (відповідно до рівня) | + | + | + | + | | | | | |
| Класифікація документів та матеріалів відповідно до умов безпеки | + | | | | + | | | + | |
| Ідентифікація документів та матеріалів відповідно до класифікації рівня безпеки | + | + | + | + | | | | + | + |
| Формування методичних матеріалів, інструкцій | + | + | + | | | | | + | |
| Моніторинг зовнішнього середовища на предмет ризиків інформаційній безпеці | | | | + | + | + | | | |

Продовження табл. 1

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Збір, обробка та систематизація даних | | | | | + | + | + | + | |
| Створення інформаційних моделей | | | | + | + | + | + | | |
| Контроль за дотриманням правил інформаційної безпеки | + | + | + | + | | | | | |
| Дотримання правил інформаційної безпеки | + | + | + | + | | | | + | + |

Кадрова стратегія повинна, на наш погляд, передбачати регулярний перегляд посадових інструкцій, положень про підрозділи, принципів корпоративної культури, інструкцій поведінки працівників та підтримуючих даний процес методик (рекомендацій) поводження з тими чи іншими матеріалами, обладнанням, технологіями.

**Висновки та перспективи подальших досліджень**. В роботі було приділено увагу напрямкам розвитку персоналу підприємства, які повинні забезпечити реалізацію етапів сучасної стратегії інформаційної безпеки висококваліфікованими кадрами з наявними компетенціями, необхідними в умовах гнучкого середовища, глобалізації економіки та різкого збільшення загроз і ризиків інформаційній безпеці підприємства.

Відмічаючи посилення законодавчого процесу вдосконалення правової складової підтримки інформаційної безпеки та організації дієвого захисту інформації, варто відмітити певне відставання від глобальних складових питання прикладної частини, а саме змістовних елементів розвитку персоналу, його навчання поводженню в умовах агресивного інформаційного середовища.

Важливим є акцент на виокремленні певний компетенцій, які слід терміново впровадити в освітні процеси як здобувачів освіти, так і працівників кожного підприємства для впорядкування поведінки колективу в процесі розробки та реалізації стратегії економічної безпеки.

**Використана література:**

1. Захаров О.І. Інформаційне забезпечення управління системою економічної безпеки підприємства. Електронний ресурс. URL: https://library.krok.edu.ua/media/library/category/statti/zakharov_0010.pdf.
2. Інформаційна безпека компанії та працівників – кожен має свою роль. Електронний ресурс. 26.02.2022. URL: https://eba.com.ua/informatsijna-bezpeka-kompaniyi-ta-pratsivnykiv-kozhen-maye-svoyu-rol/.
3. Качан О.І. Інформаційна безпека підприємства в умовах глобалізації. Розвиток малого та середнього бізнесу в умовах глобалізації світової економіки: матеріали Всеукраїнського економічного форуму з міжнародною участю (в онлайн форматі) (м. Житомир, 27 квітня 2017 р.). Житомир, 2017. С.234–237. URL: https://conf.ztu.edu.ua/wp-content/uploads/2017/09/234.pdf/.
4. Концепція інформаційної безпеки України (Проект). 14 с. https://www.osce.org/files/f/documents/0/2/175056.pdf.
5. НД ТЗІ 3.6-004-21 Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці. Київ : Адміністрація Держспецзв'язку, 2021. 23 с.
6. Нехай В.А., Нехай В.В. (2017) Інформаційна безпека як складова економічної безпеки підприємства. *Науковий вісник Міжнародного гуманітарного університету. Серія: Економіка і менеджмент. Збірник наукових праць.* Випуск 24. Частина 2. Одеса. С.137-140. URL: http://www.vestnik-econom.mgu.od.ua/journal/2017/24-2-2017/30.pdf.
7. Новицький В.Я. (2022) Стратегічні засади забезпечення інформаційної безпеки в сучасних умовах. *Інформація і право*. № 1 (40), С. 111-118. https://doi.org/10.37750/2616-6798.2022.1(40).254349.
8. Про національну безпеку України. Закон України від 21.06.2018 № 2469-VIII зі змінами. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text
9. Стратегія інформаційної безпеки. Затверджено Указом президента України від 28.12.2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text.
10. Стратегія кібербезпеки України. Затверджено Указом президента України від 26.08.2021 р. №447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n12.
11. Федорова Ю., Єльникова Г. (2021) Інноваційні інформаційні технології в підготовці та управлінні персоналом. *Адаптивне управління: теорія і практика. Серія Економіка*, № 11(22). https://doi.org/10.33296/2707-0654-11(22)-11.

## References

1. Zakharov O.I. Informatsiine zabezpechennia upravlinnia systemoiu ekonomichnoi bezpekypid pryiemstva. Elektronnyi resurs. URL: https://library.krok.edu.ua/media/library/category/statti/zakharov_0010.pdf.
2. Informatsiina bezpeka kompanii ta pratsivnykiv – kozhen maie svoiu rol. Elektronnyi resurs. 26.02.2022. URL: https://eba.com.ua/informatsijna-bezpeka-kompaniyi-ta-pratsivnykiv-kozhen-maye-svoyu-rol/.
3. Kachan O.I. Informatsiina bezpeka pidpryiemstva v umovakh hlobalizatsii. Rozvytok maloho ta serednoho biznesu v umovakh hlobalizatsii svitovoi ekonomiky: materialy Vseukrainskoho ekonomichnoho forumu z mizhnarodnoiu uchastiu (v onlain formati) (m. Zhytomyr, 27 kvitnia 2017r.). Zhytomyr, 2017. S.234–237. URL: https://conf.ztu.edu.ua/wp-content/uploads/2017/09/234.pdf.
4. Kontseptsiia informatsiinoi bezpeky Ukrainy (Proekt). 14 s. https://www.osce.org/files/f/documents/0/2/175056.pdf.
5. ND TZI 3.6-004-21 Poriadok vprovadzhennia systemy bezpeky informatsii v derzhavnykh orhanakh, na pidpryiemstvakh, orhanizatsiiakh, v informatsiino-komunikatsiinykh systemakh yakykh obrobliaietsia informatsiia, vymoha shchodo zakhystu yakoiv stanovlena zakonom ta ne stanovyt derzhavnoi taiemnytsi. Kyiv : Administratsiia Derzhspetszviazku, 2021. 23 s.
6. Nekhai V.A., Nekhai V.V. (2017) Informatsiina bezpeka yak skladova ekonomichnoi bezpeky pidpryiemstva. Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu. Seriia: Ekonomika i menedzhment. Zbirnyk naukovykh prats. Vypusk 24. Chastyna 2. Odesa. S.137-140. URL: http://www.vestnik-econom.mgu.od.ua/journal/2017/24-2-2017/30.pdf.
7. Novytskyi V. Ia. (2022) Stratehichni zasady zabezpechennia informatsiinoi bezpeky v suchasnykh umovakh. Informatsiia i pravo. № 1 (40), S. 111-118. https://doi.org/10.37750/2616-6798.2022.1(40).254349.
8. Pro natsionalnu bezpeku Ukrainy. Zakon Ukrainy vid 21.06.2018 № 2469-VIII zi zminamy. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.
9. Stratehiia informatsiinoi bezpeky. Zatverdzheno Ukazom prezydenta Ukrainy vid 28.12.2021 r. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text.
10. Stratehiia kiberbezpeky Ukrainy. Zatverdzheno Ukazom prezydenta Ukrainy vid 26.08.2021 r. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n12.
11. Fedorova Yu., Yelnykova H. (2021) Innovatsiini informatsiini tekhnolohii v pidhotovtsi ta upravlinni personalom. Adaptyvne upravlinnia: teoriia i praktyka. Seriia Ekonomika, № 11 (22). https://doi.org/10.33296/2707-0654-11(22)-11.

**Olena Iv. Kirian**
Ph.D in Economics, Associate Professor,
Associate Professor of Economics and Management Department,
Ukrainian Engineering Pedagogics Academy, Kharkiv, Ukraine

**Denys Ol. Torianyk**
Post Graduate Student of Economics and Management Department,
Ukrainian Engineering Pedagogics Academy, Kharkiv, Ukraine

**Natalia Myk.Yagnesha**
Master's Student of Economics and Management Department,
Ukrainian Engineering Pedagogics Academy, Kharkiv, Ukraine

# Personnel component of the company's information security

**Abstract.** The purpose of the article is to formulate proposals for improving the content of the personnel component of the company's information security strategy, primarily due to the development of personnel, depending on their potential participation in ensuring the company's information security system.

The article examines modern directions of attention to the information security of the enterprise, the legal support of this concept and the process adapted to today's conditions. The importance of educational processes, which are important to apply for the company's personnel so that workers are adapted to confronting risks, is noted.

The work also provides elements of the HR strategy that support the company's information security strategy and, in accordance with the content of the legislative acts of Ukraine, are the most relevant. For them, groups of employees of the enterprise that need constant specialized development were determined, and the subject of this specialized development was singled out.

The given data on key competencies for the future development of personnel and groups of personnel to which they should be applied in the first place were systematized in a single tabular form. This will simplify the process of forming the educational component of the personnel strategy for the development of information security.

The topic of the article provides a basis for a number of further studies: development of mechanisms for forming models for determining information risks and sources of their effective prevention; improvement of the personnel recruitment and selection system taking into account information security needs; optimization of the monitoring mechanism of the global environment for the development of information technologies, updating fraudulent schemes and threats to the information security of the enterprise.

**Key words**: information security, enterprise personnel, personnel strategy, information protection, documentation classification, handling of information channels, enterprise security service, personnel development.