DOI: https://doi.org/10.37634/efp.2025.3.3
УДК 338.24.021.8

*Олег Сергійович РЕМЕЗ*
*аспірант, Приватний вищий навчальний заклад "Європейський університет"*
*ORCID: https://orcid.org/0009-0009-0227-5669*
*e-mail: rem2025o@ukr.net*

# ХАРАКТЕРИСТИКА ПІДХОДІВ ДО ФОРМУВАННЯ СИСТЕМИ БЕЗПЕКИ НА ПІДПРИЄМСТВАХ

*Ефективний ринковий розвиток пов'язано із створенням оптимальної системи безпеки компанії, яка враховує основні ризики та загрози. Встановлення підходів до формування системи безпеки підприємств дасть змогу виокремити напрями, в площині яких може бути розроблено методологічну базу дослідження ефективності зазначеного процесу. В дослідженні виокремлено такі підходи до формування системи безпеки підприємств, зокрема: секторальний підхід; процесний підхід; факторний підхід; середовищний підхід; цільовий підхід; ситуаційний підхід. Зазначено, що склад та характеристики підходів до формування системи безпеки підприємств можуть трансформуватися залежно від розвитку наукових розвідок, впливу зовнішніх та внутрішніх чинників, появи нових викликів становлення зазначеного феномену.*

***Ключові слова:*** *формування системи безпеки підприємств, секторальний підхід, процесний підхід, факторний підхід, середовищний підхід, цільовий підхід, ситуаційний підхід, цифровізація*

## ВСТУП

Важливою ціллю суб'єктів підприємництва незалежно від їх видів діяльності та розмірів є виживання та забезпечення подальшого розвитку. На ріст можливостей реалізації вказаної цілі може впливати стан підприємства, який свідчить про життєздатність та гарантію її підтримання. Інакше кажучи, це безпека підприємства. Феномен системи безпеки може визначатися як у площині механізму протидії загрозам і викликам (коли система здатна до обмежень наслідків подій, які чинять негативну дію на її стан), так і в розрізі здатності забезпечити безперебійне функціонування суб'єкта підприємництва (здійснення наслідкової дії на розвиток). Слід зазначити, що дві наведені позиції з визначення системи безпеки маю причинно-наслідковий зв'язок. А саме завдяки протидії відповідних загрозам та негативним впливам (причини) підприємством забезпечується відповідний стан розвитку за основними сферами (наслідки).

Для скоординованого управління розвитком підприємств необхідно врахування потенційних та фактичних загроз. Відповідно до теоретичних засад стратегічного управління передбачено, що ключове джерело загроз – це середовище підприємства. До складу загроз відносяться подієві компоненти (тенденції) макросередовища (демографічні трансформації, нормативно-правові зміни, економічна політика тощо) галузеві особивості розвитку. Ефективний ринковий розвиток пов'язано зі створенням оптимальної системи безпеки компанії, яка враховує вказані загрози. Встановлення підходів до формування системи безпеки підприємств дасть змогу виокремити напрями, в площині яких може бути розроблено методологічну базу дослідження ефективності зазначеного процесу.

Особливості формування системи безпеки підприємств подано в роботах вітчизняних та зарубіжних науковців.

У дослідженнях І. Каліної та ін. [6], Т. Маккрейта [8], П. Кабави [3] висвітлено характеристики процесу формування системи безпеки підприємств з позицій секторального підходу. В роботі М. Квієчіньського [7] визначено зазначений процес у розрізі процесного підходу, в дослідженні Б. Турсунова [10] – у площині факторного підходу. Наукові розвідки А. Гарагулі та ін. [5], А. Рамського та А. Сольнько [9] присвячено вивченню розроблення системи безпеки крізь призму середовищного підходу. Дослідження С. Аль-Гамді та ін. [2] націлено на висвітлення зазначеного процесу в контексті цільового підходу.

**МЕТА** роботи – виокремлення та характеристика підходів стосовно формування системи безпеки підприємств. Для реалізації зазначеної цілі виділено низку *завдань*, серед яких: визначення підходів зазначеної категорії; характеристика та висвітлення особливостей підходів до формування системи безпеки підприємств.

## МЕТОДИ ДОСЛІДЖЕННЯ

Серед методів дослідження, що застосовано для реалізації зазначеної цілі, можна відмітити такі. Застосовано порівняльний метод, необхідний для спів ставлення позицій науковців з визначення формування системи безпеки підприємства. За допомогою фреймінгу здійснено встановлення ключових рамок стосовно характеристик підходів до досліджуваного напряму. Із застосуванням положень методу індукції здійснено збір матеріалів для формування комплексного розуміння змісту кожного підходу стосовно формування системи безпеки підприємства.

## РЕЗУЛЬТАТИ

Проведемо розгляд основних наукових підходів до оцінюваної проблематики, які є на нинішній стадії вивчення зазначеного питання. Виокремлення вказаних підходів здійснено нами на підставі аналізу та класифікації положень наукових розвідок в цій сфері.

По-перше, можемо відмітити підхід до створення системи безпеки суб'єктів підприємництва, визначений у площині орієнтиру на протидії загрозам, пов'язаним зі змінами секторального середовища (секторальний підхід). Виникнення секторальних загроз обумовлене рішеннями, які ухвалені з боку конкурентів, кооператорів та клієнтів. Рівень дії таких рішень пов'язано з потенціалом розвитку компаній.

В контексті орієнтиру на секторальний підхід мо-

 

жемо відмітити позиції І. Каліної та ін. [6]. Авторами наведено дослідження практики корпорацій Польщі стосовно створення системи безпеки з огляду на галузеві та традиційні ризики. В рамках комплексного аналізу дослідники сформулювали склад найбільш суттєвих ризиків для основних секторів польської економіки. Зазначено, що до складу таких секторів можна віднести харчову промисловість, інші сектори промисловості, сільське господарство. Окрім вказаного, автори відмічають, що у розробленні системи безпеки компаній визначених секторів потрібно звертати увагу на параметр розміру підприємств. А саме вказано, що великі компанії більш чутливі до негативних впливів зовнішніх і внутрішніх ризиків, заснованих на шахрайських схемах. Цей факт обумовлено тим, що зазначені компанії через свої масштаби і ресурси підпадають у поле уваги більшої чисельності зацікавлених осіб, які можуть завдяки шахрайству порушити корпоративні права та інтереси.

Положення секторального підходу до досліджуваного процесу подано в роботі Т. Маккрейта [8]. За твердженням автора, стратегія системи безпеки компаній повинна розроблятись в розрізі орієнтиру на її здатність забезпечити організаційну стійкість під дією основних ризиків, які діють на галузевому рівні. Дослідник вказує, що компанія може розраховувати на отримання вагомих переваг у стратегічному плануванні у разі визначення і постійного оновлення даних стосовно галузевих ризиків у площині основних вимірів (місцевого, територіального, національного, регіонального, міжнародного, глобального). Такий захід дасть змогу забезпечити більш ефективний розвиток як компаній, так і галузей економіки, економіки загалом тощо. Автором висунуто типологію організаційної стійкості, що характерно для компаній у площині різних умов функціонування. Також дослідником відзначено, що типи організаційної стійкості можуть трансформуватись під дією змін у галузі. Важливо відмітити, що автором ідентифіковано феномен організаційної стійкості та феномен системи безпеки. Т. Маккрейтом зазначено потребу збільшення наукових розвідок у площині збору наборів великих баз даних стосовно секторальних ризиків (зокрема для найбільш вразливих до ризиків секторів).

У площині акценту на визначенні формування системи безпеки підприємств з позицій секторального підходу можна відмітити роботу П. Кабави [3]. Дослідник вказує, що створення системи безпеки стосовно секторальних загроз має бути тісно інтегрованим із процесами розроблення, реалізації та моніторингу впровадження загальної стратегії розвитку компанії. Автор пропонує формувати політику управління системою безпеки згідно з поведінковими стратегіями. У площині орієнтиру на поведінкові стратегії дослідником висунуто класифікацію стратегій управління системою безпеки компаній. А саме виділено стратегію розвитку, стратегію управління, стратегію зростання та стратегію стабілізації. Можемо відмітити, що хоча зазначена класифікація є доцільною та слушною, на наш погляд, вона стосується не категорії поведінкових стратегій, а стратегій розвитку. Зазначена категорія визначається стратегіями згідно зі стадіями життєвого циклу підприємств (стадія стабілізації, стадія росту та стадія скорочення). Водночас дослідник визначає їх як поведінкові стратегії.

П. Кабава відмічає, що підставою такої категоризації постають наведені нижче складники стратегії, зокрема: технології, продукти, партнери, ринок. Складники (продукти, партнери та ринок) напряму співвідносяться із секторальними загрозами, Складник технології може розглядатись, за твердженням автора, як макросистемний фактор, хоча з огляду на те, що на нинішньому етапі відбувається зростання впливу технологічного чинника на розвиток секторів економіки, її враховано також у складі секторальних загроз.

Автором подано порядок протидії секторальним загрозам у площині орієнтиру на застосування визначених стратегій системи безпеки підприємств [3]:

– стратегію розвитку пов'язано з розширенням сфери діяльності підприємства. Практично її застосування засноване на виході підприємств на інші сегменти та / або сектори ринкового середовища. Факт розвитку пов'язано з переходом з однієї стадії життєвого циклу до іншої, що супроводжується періодичними внутрішніми кризами, конфліктами, напруженнями. Автором справедливо зазначено, що орієнтир на стратегію розвитку передбачає інших підходів до системи безпеки, аніж орієнтир на зростання або стабілізацію;

– *Стратегію управління* системою безпеки, на думку автора, повинно бути націлено на подолання бар'єрів для передавання отриманих раніше знань із вказаного процесу. Можемо зазначити, що орієнтир на таку стратегію можливий за умови виникнення ризиків традиційного типу.

– *Стратегію росту* націлено на інтенсифікацію діяльності, що здійснюється в розрізі продуктів, які випускаються, просуваються і реалізуються компанією фактично. Застосування зазначеної стратегії пов'язане з планомірним збільшенням виробничого потенціалу підприємства, що демонструється у рості ринкових позицій. Як зазначає автор, ріст може бути пов'язано з поглинанням інших підприємств, самостійним відкриттям нових структурних підрозділів (органічним ростом). Стратегію росту орієнтовано на розвиток поточної ділової активності компаній. Водночас у разі стратегії росту на відміну від стратегії стабілізації здійснюється розширення ринкового охоплення компанії. Діяльність із застосуванням зазначеної стратегії супроводжується ростом загроз, що пов'язано з виходом на нові ринки збуту і що здійснюються з боку конкурентів компанії.

– *Стратегію стабілізації* стосовно секторальних загроз пов'язано зі здійсненням захисту позицій підприємства в ринковому середовищі. Орієнтир на зазначену стратегію передбачає підтримання вже здійснюваних заходів, дій стосовно продукції, ринків, на яких функціонує досліджуване підприємством разом із підприємствами-партнерами. В рамках орієнтиру на вказану стратегію передбачено коригування наявної стратегії розвитку з урахуванням акценту на підтримані заданого раніше рівня. За твердженням П. Кабави, практично застосування цієї стратегії пов'язане зі швидким реагуванням на збої (зокрема внесення коригувань у ланцюг постачання, якщо його порушено) та відповіддю на негативні наслідки, спричинені випадковими або природними подіями (проведення ремонту, технічного обслуговування). Дослідник зауважує, що таке реагування потрібно визначити на рівні стратегії.

Автором справедливо зазначено, що положення стратегій управління безпекою повинні включати систему встановлення впливів виникнення нових інформаційно-комунікаційних технологій на здійснення організації основної діяльності підприємств. Можемо підтримати дослідника, що досліджуваний процес повинен супроводжуватися функцією системи раннього реагування.

Слід відмітити, що підхід П. Кабави [3] вирізняється певною дискусійністю в розрізі питання стратегій створення систем безпеки компаній. Хоча бачення автора акценту на побудові вказаного процесу в площині орієнтиру на концепцію життєвого циклу в розрізі галузевого середовища є слушним через наявність великої кількості загроз, які виникають в тій або іншій галузі економіки.

По-друге, необхідно відмітити підхід, заснований на визначенні системи безпеки компаній у площині врахування основних процесів діяльності (процесний підхід). Підтримання ефективності та високої якості системи безпеки пов'язане із врахуванням безпеки на рівні основних процесів управління підприємствами. Формування системи безпеки можливе у разі орієнтиру на основні процеси, і їх визначення потрібне для подальшої побудови методологічного забезпечення оцінки ефективності в цій сфері.

У площині орієнтиру на вказаний підхід слід відзначити роботу М. Квієчіньського [7]. Автором розроблено модель побудови системи безпеки компаній, в рамках якої виділено ключові процеси. Зокрема, виділено формування фрагментарних та основних процесних векторів безпеки. М. Квієчіньський відмічає, що компоненти формування системи безпеки компаній у площині процесних векторів можуть складатися з:

1) фрагментарних процесних векторів, які складаються з: профілактики порушень системи безпеки; підсистеми управління складника оперативної безпеки; компонентів управління логістикою безпеки (безпечне транспортування, зберігання тощо); компонентів управління подоланням наслідків загроз, що фактично виникли;

2) основних процесних векторів, які подано: вхідним вектором (фактичні ресурси); процесами управління безпекою ресурсів; вихідним вектором (встановлення граничних параметрів системи безпеки підприємства).

Слід зазначити, що позиції М. Квієчіньського [7] мають ознаки комплексності, враховують основні процеси побудови системи безпеки підприємств. Потрібно відмітити, що акцент на процесний складник – це ключовий напрям розроблення системи безпеки компаній різних галузей. Але структура таких процесів може вирізнятися, що обумовлює ефективність та стан формування системи безпеки підприємств різних галузей.

По-третє, заслуговує на увагу факторний підхід до побудови системи безпеки компаній, заснований на потребі врахування основних факторів впливу на стан їх розвитку. Вказаний підхід застосовується як у розробленні локальних підсистем безпеки компаній, так і у формування загальної системи безпеки компанії.

У розрізі орієнтиру на зміни цього підходу слід розглянути дослідження Б. Турсунова [10]. Зокрема, дослідник розробив на апробацію методичне забезпечення аналізу ефективності такої компоненти системи безпеки, як фінансова підсистема компаній текстильної галузі Узбекистану. Автор виходить з позицій, що фінансову підсистему системи безпеки підприємств зазначеного сектору може бути сформовано із застосуванням таких складників:

– Нефінансові параметри розвитку за основними сферами управління, які виникнуть під дією основних факторів впливу (кадрова сфера, технологічна сфера, технічна сфера, виробнича сфера, збутова сфера). Автором здійснено прогнозування на рівні 25 малих компаній текстильної галузі Узбекистану орієнтуючись на фактичні тренди, які показано у попередні періоди (2019, 2020 рр.). Дослідник довів, що основні нефінансові параметри розвитку, хоча і не відносяться до фінансової сфери управління, чинять вагомий вплив на її становлення. Можемо відмітити, що такі дослідники, як І. Новойтенко та Ю. Шишута [1], Л. Докієнко та ін. [4], Дж. Зімон та ін. [11] висувають перелік оціночних прогнозних нефінансових параметрів розвитку, аналогічний до переліку, поданого Б. Турсуновим.

– Прогнозні відхилення розвитку подій в рамках підприємств галузі від традиційних параметрів фінансової безпеки, які характерні для всіх суб'єктів галузі. Можливе виділення відхилень для підприємств галузі у площині орієнтиру на їх масштаби (малі, середні, великі підприємства).

Як справедливо зазначає автор, орієнтир на вказані складники дає змогу в рамках прогнозування визначити обсяги відносного та абсолютного рівня фінансової незахищеності компаній у площині визначених факторів, і це забезпечує інформаційну базу для ухвалення управлінських рішень з подолання загроз. Визначення впливів на рівні двох складників дасть змогу встановити такий стан фінансової підсистеми системи безпеки компанії, який буде мати стійкість до вказаних викликів.

По-четверте, необхідно відзначити середовищний підхід, що орієнтовано на розроблення системи безпеки компаній з урахуванням впливу умов внутрішнього та зовнішнього середовища. Орієнтир на зазначений підхід здійснюється на різних рівнях управління, зокрема, місцевому, територіальному, регіональному, міжнародному, глобальному рівнях. Варто зазначити, що в умовах цифрової економіки актуальним є врахування цифрової компоненти середовищного підходу.

Згідно з орієнтиром на цифровий середовищний підхід слід відзначити положення роботи А. Гарагулі та ін. [5]. За твердженням авторів, у розрізі орієнтиру на цифрову економіку слід зробити адаптацію системи економічної безпеки до нового типу ризиків, які формуються в рамках впливу цифрового переходу. А. Гарагуля та ін. виділяють склад основних етапів регулювання ризиків, які постають основою системи економічної безпеки підприємств, що задіяні на рівні процесів цифрової трансформації. Орієнтир на цифрові ризики є обов'язковим для всіх типів компаній та секторів економіки, що обумовлено тим, що цифровий перехід та цифровізація увійшли до основних сфер життєдіяльності. В дослідженні А. Гарагулі та ін. [5] визначено основні етапи розроблення системи економічної безпеки, засновані на регулюванні ризиків цифрового середовища, зокрема: етап моніторингу та оцінювання нового типу ризиків, пов'язаних із процесами цифрового переходу; етап зниження рівня дії ризиків (застосування дій, які відповідають стратегічним цільовим орієнтирам цифрової трансформації компанії); етап

оцінювання економічної безпеки підприємства. Дослідники вказують, що для здійснення кожного з етапів розроблення системи економічної безпеки компаній необхідне визначення критеріїв, граничних норм показників.

А. Рамський та А. Сольнько [9] визначили структуру системи фінансової безпеки підприємства, сформульовану в площині орієнтиру на середовищний підхід. Дослідниками запропоновано враховувати внутрішній та зовнішній середовищний вплив на рівень фінансової підсистеми системи безпеки компаній. Авторами здійснено визначення механізм розроблення фінансової підсистеми системи безпеки компаній, який складається:

– зі стадії діагностики фінансової підсистеми компанії та дії на неї внутрішнього та зовнішнього середовища;

– зі стадії розроблення системи економічної безпеки, до реалізації якої може бути залучено всі зацікавлені сторони. На цій стадії потрібно враховувати результати попереднього етапу розроблення. В межах зазначеної стадії встановлюється методична база розроблення системи економічної безпеки і забезпечується його реалізація за основними рівнями відповідальності.

Вважаємо дискусійністю заміни дослідниками терміну «фінансова підсистема» («фінансова безпека») на «економічна безпека», оскільки загальну ціль дослідження спрямовано на фінансову безпеку. Подані результати показують, що інформація про дії середовища є основою для визначення прогнозу системи безпеки компанії.

По-п'яте, потрібно виокремити цільовий підхід, пов'язаний із розробленням системи безпеки компаній у площині врахування основних цілей, передбачених стратегією розвитку. Орієнтир на цілі розвитку компанії має бути встановлено в рамках ключових складників системи безпеки компанії. Врахування цільової ознаки, на наш погляд, є обов'язковою умовою розроблення системи безпеки компаній. Акцент на цільовому складнику у формуванні системи безпеки підприємств визначено в роботі С. Аль-Гамді та ін. [2], а також інших дослідженнях.

По-шосте, потрібно відмітити можливість орієнтиру на ситуаційний підхід у формуванні системи безпеки підприємств, заснований на застосування сукупності важелів, заходів реагування на середовищні впливи і внутрішній розвиток [авторська пропозиція]. Застосування зазначеного підходу напряму пов'язане як із цифровим середовищним, так і середовищним підлодом до формування системи безпеки підприємства. Потрібно зазначити, що вказаний підхід засновано на антикризовому менеджменті та ситуаційному моделюванні в межах акценту на стадії життєвого циклу компаній. Застосування зазначеного підходу особливо актуальне для окремих галузей економіки, які зазнають суттєвого негативного впливу під час воєнних дій в Україні, коли потрібне ситуаційне реагування для недопущення прояву ризиків та загроз.

## ВИСНОВКИ

Отже, можемо зазначити, що склад та характеристики підходів до формування системи безпеки підприємств можуть трансформуватися залежно від розвитку наукових розвідок, впливу зовнішніх та внутрішніх чинників, появи нових викликів становлення зазначеного феномену. Особлива увага в цьому разі стосується модифікації та адаптації ситуаційного підходу до врахування особливостей всіх інших підходів розроблення системи безпеки підприємств. Вказане сприятиме більшій адаптивності в умовах невизначеності розвитку підприємств різних галузей стосовно прогнозування параметрів системи безпеки. Така невизначеність виникає під дією появи загроз, які раніше не були характерними для суспільства, економіки в тих проявах та характеристиках. Серед вказаних загроз сучасного періоду можна відмітити ті, які виникли з огляду на пандемію COVID-19, повномасштабну війну росії проти України тощо. Врахування всіх можливих підходів до формування системи безпеки підприємств в контексті ситуаційного підходу зробить цей процес більш гнучким та сприятиме росту стійкості компаній під дією загроз та викликів.

***References***

1. Novoitenko I.V., Shyshuta Yu.M. Levers of influence on the economic stability of oil and fat enterprises in Ukraine. *Investments: practice and experience.* 2017. № 15. pp. 53–56. (in Ukrainian).

2. Al-Ghamdi S., Than W.K., Vlahu-Gjorgievska E. Information security governance challenges and critical success factors: Systematic review. *Computers & Security*. 2020. Vol. 99. URL: https://doi.org/10.1016/j.cose.2020.102030.

3. Cabała P. Strategie zarządzania bezpieczeństwem przedsiębiorstwa w warunkach zagrożeń sektorowych. *Prace naukowe Uniwersytetu Ekonomicznego we Wrocławiu.* 2016. Nr. 420. S. 36-45. URL: https://doi.org/10.15611/pn.2016.420.03

4. Dokiienko L., Hrynyuk N., Nakonechna O., Mykhailyk O. System for evaluation of financial security of operational activity of oil-and-fat industry enterprises. *Agricultural and Resource Economics: International Scientific E-Journal.* 2021. Vol. 7(4). pp. 138–159. URL: https://doi.org/10.51599/are.2021.07.04.08

5. Harahulia A., Suslov V., Horovoy O. Management of Economic Security of Enterprises in the context of Digital Transformation. *Baltic Journal of Economic Studies.* 2023. Vol. 9(5). pp. 87-93. URL: https://doi.org/10.30525/2256-0742/2023-9-5-87-93

6. Kalina I., Khurdei V., Shevchuk V., Vlasiuk T., Leonidov I. Introduction of a Corporate Security Risk Management System: The Experience of Poland. *Journal of Risk and Financial Management*. 2022. Vol. 15(8). URL: https://doi.org/10.3390/jrfm15080335

7. Kwieciński M. Zarządzanie bezpieczeństwem działalności przedsiębiorstwa – zarys problematyki. *Prace Naukowo-Dydaktyczne Państwowej Wyższej Szkoły Zawodowej im. Stanisława Pigonia w Krośnie*. 2016. Nr. 70. S. 149-170.

8. McCreight T. Building resilience: The role of enterprise security risk management in developing a resilient organisation. *Journal of Business Continuity & Emergency Planning.* 2024. Vol. 17. Issue 4. URL: https://doi.org/10.69554/FWWL3167

9. Ramskyi A., Solonko A. Mechanism of formation of Financial Security of an Enterprise. *European scientific journal of Economic and Financial innovation*. № 1. pp. 14-20. URL: http://doi.org/10.32750/2018-0102

10. Tursunov B.O. Financial Security of Textile Enterprises During the Pandemic: In Case of Uzbekistan. *Asian Journal of Technology & Management Research*. 2023. Spec. Issue 3. pp. 51-56.

11. Zimon G., Tarighi H., Salehi M., Sadowski A. Assessment of Financial Security of SMEs Operating in the Renewable Energy Industry during COVID-19 Pandemic. *Energies.* 2022. Vol. 15(24). URL: https://doi.org/10.3390/en15249627

***Oleh REMEZ***
*postgraduate student, Private higher educational institution "European University"*
*ORCID: https://orcid.org/0009-0009-0227-5669*
*e-mail: rem2025o@ukr.net*

## CHARACTERISTICS OF APPROACHES TO THE FORMATION OF SECURITY SYSTEMS AT ENTERPRISES

***Introduction.*** *Effective market development is associated with the creation of an optimal company security system that takes into account the main risks and threats. Establishing approaches to the formation of an enterprise security system will allow us to identify areas in which a methodological basis for studying the effectiveness of the specified process can be developed.*

***The purpose of the paper*** *is to identify and characterize approaches to the formation of an enterprise security system.*

***Results.*** *The paper identifies the following approaches to the formation of an enterprise security system, in particular: an approach to creating a security system for business entities, defined in terms of a reference point for countering threats associated with changes in the sectoral environment (sectoral approach); an approach based on defining a company security system in terms of taking into account the main processes of activity (process approach); a factor approach to building a company security system, based on the need to take into account the main factors influencing the state of their development; an environmental approach, which is focused on developing a company security system taking into account the influence of internal and external environmental conditions; a target approach related to developing a company security system in terms of taking into account the main goals provided for by the development strategy; a situational approach to the formation of a company security system, based on the use of a set of levers, measures to respond to environmental influences and internal development.*

***Conclusion.*** *It is noted that the composition and characteristics of approaches to the formation of an enterprise security system can be transformed depending on the development of scientific research, the influence of external and internal factors, the emergence of new challenges to the formation of the specified phenomenon. Special attention in this case is paid to the modification and adaptation of the situational approach to take into account the features of all other approaches to the development of an enterprise security system.*

***Keywords:*** *formation of an enterprise security system, sectoral approach, process approach, factor approach, environmental approach, target approach, situational approach, digitalization*