Summary.. In article the organization of system of strategic planning at the building enterprises of railway transportation in modern conditions is considered.

Keywords: strategic planning, market strategy, the general purposes of the enterprise, a problem and function of strategic planning.

Рецензент *д.е.н., професор УкрДАЗТ Дейнека О.Г.*
Експерт редакційної колегії *к.е.н., доцент УкрДАЗТ Токмакова І.В.*

УДК 65.012.8

ФОРМУВАННЯ СИСТЕМИ ПОКАЗНИКІВ ОЦІНКИ РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Журавель М.Ю., стажист-дослідник,
Полозова Т.В., к.е.н., доцент,
Стороженко О.В., к.т.н., доцент (ХНУРЕ)

Запропоновано діагностику рівня інформаційної безпеки підприємства проводити за трьома ключовими напрямками: оцінка програмно-технічної захищеності інформації; оцінка інформаційної надійності персоналу; оцінка інформації, що надається особам, що приймають рішення, інформаційною службою підприємства. Сформовано системи показників оцінки рівня інформаційної безпеки за кожним запропонованим напрямком.

Ключові слова: інформаційна безпека підприємства, напрямки діагностики інформаційної безпеки, система показників оцінки рівня інформаційної безпеки.

Постановка проблеми. Для забезпечення свого ефективного функціонування підприємство має підтримувати належний рівень інформаційної безпеки. Необхідною ж умовою підтримання належного рівня інформаційної безпеки підприємства є систематичне проведення діагностики її рівня.

Аналіз останніх досліджень і публікацій. Багато вчених як в Україні, так і в країнах ближнього і далекого зарубіжжя займаються питаннями, пов'язаними з забезпеченням належного рівня інформаційної безпеки підприємств. Вагомий внесок в розкриття цієї проблеми зробили Н. Реверчук [1], С. Ілляшенко [2], О. Кравчук [3], Д. Ковальов [4], Є. Олєйников [5], В. Пономарьов [6], Т. Клєбанова [7] та інші. Проте, на думку більшості фахівців, теоретико-методологічні засади діагностики рівня інформаційної безпеки підприємства ще не в достатній мірі є розробленими.

Автор наукової праці [1] пропонує використовувати такі показники інформаційної безпеки підприємства як продуктивність інформації, коефіцієнт інформаційної озброєності та коефіцієнт захищеності інформації. Такий перелік коефіцієнтів є досить обмеженим, оскільки рівень інформаційної безпеки не може бути об'єктивно оцінений за допомогою лише трьох запропонованих показників. Варто зазначити, що всі три показники відображають лише фінансовий аспект інформаційної безпеки, оскільки в якості вихідних даних для розрахунку зазначених показників виступають витрати на придбання інформаційних ресурсів.

Ілляшенко С.М. [2] рівень інформаційної безпеки визначає часткою неповної, неточної і суперечливої інформації, яка використовується в процесі прийняття управлінських рішень. Відтак, автор оцінює лише якість інформації, що надається особам, що приймають рішення. Перелік індикаторів потребує доповнення різноманітними показниками, що характеризують стан програмно-технічної захищеності інформації та інформаційної надійності персоналу.

Автори роботи [3] для оцінки рівня інформаційної безпеки пропонують розраховувати п'ять показників, що характеризують рівень інформаційно-аналітичного супроводження діяльності підприємства, захисту комерційної інформації та безпеки документообігу, рівень ділової репутації та іміджу продукції.

© Журавель М.Ю.,
Полозова Т.В.,
Стороженко О.В.

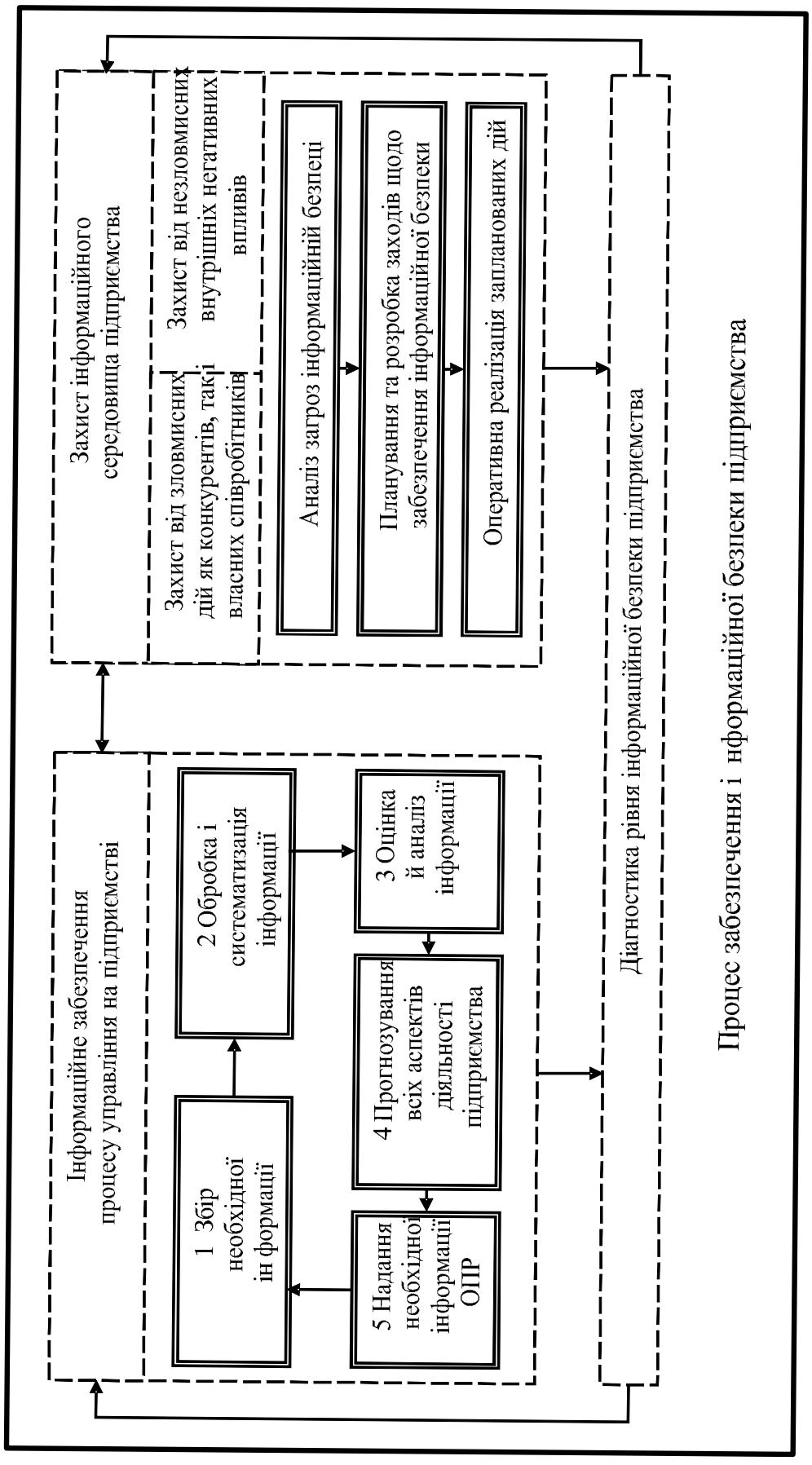

Рисунок 1 – Процес забезпечення інформаційної безпеки підприємства

Рисунок 2 – Напрямки діагностики рівня інформаційної безпеки підприємства

Одним з недоліків такого підходу є те, що автор більшість показників розраховує на основі експертного методу, що значно посилює вплив суб'єктивного фактору на кінцевий результат розрахунків. Також запропонована система індикаторів не враховує всіх аспектів інформаційної безпеки підприємства. Зокрема, як і методика, представлена в науковій праці [2], не включає показників, що характеризують інформаційну надійність персоналу та програмну захищеність інформації.

Проаналізувавши існуючі погляди щодо оцінки рівня інформаційної безпеки підприємства, можна зробити висновок, що на сьогоднішній день немає єдиної методики для оцінки рівня інформаційної безпеки підприємства. Системи показників, які пропонують науковці, є недосконалими, оскільки не враховують всіх аспектів інформаційної безпеки підприємства.

Виділення невирішених частин загальної проблеми. Недостатня розробленість теоретико-методологічної бази діагностики інформаційної безпеки підприємства обумовлює необхідність вдосконалення існуючого методологічного інструментарію її оцінки.

Формування цілей статті. Виходячи з цього метою статті є виділення ключових напрямків діагностики інформаційної безпеки підприємства та формування системи показників оцінки її рівня.

Виклад основного матеріалу. Інформаційна безпека відображає захищеність інформаційного середовища та ефективність інформаційного забезпечення процесу управління на підприємстві.

Процес забезпечення інформаційної безпеки підприємства можна представити як взаємодію трьох підсистем:

– підсистема інформаційного забезпечення процесу управління на підприємстві;
– підсистема захисту інформаційного середовища підприємства;
– підсистема діагностики рівня інформаційної безпеки.

Структурно-логічна схема процесу забезпечення інформаційної безпеки представлена на рисунку 1.

Ключовими задачами підсистеми інформаційного забезпечення процесу управління на підприємстві є:

– збір необхідної інформації;
– обробка і систематизація інформації;
– оцінка й аналіз інформації;
– прогнозування всіх аспектів діяльності підприємства;
– надання необхідної інформації особам, що приймають рішення.

Безперервне виконання всіх цих задач необхідне для ефективного функціонування зазначеної підсистеми.

Захист інформаційного середовища підприємства включає захист від зловмисних дій як конкурентів, так і власних співробітників, а також захист від незловмисних внутрішніх негативних впливів.

Для забезпечення захисту інформаційного середовища підприємства необхідне систематичне виконання наступних етапів:

– аналіз загроз інформаційній безпеці;
– планування та розробка заходів щодо забезпечення інформаційної безпеки;
– оперативна реалізація запланованих дій.

Діагностику рівня інформаційної безпеки підприємства пропонується проводити за трьома ключовими напрямками (рис. 2):

1. Оцінка програмно-технічної захищеності інформації.
2. Оцінка інформаційної надійності персоналу.
3. Оцінка інформації, що надається особам, що приймають рішення, інформаційною службою підприємства.

Актуальність виділення запропонованих напрямків витікає з ключових задач щодо забезпечення інформаційної безпеки підприємства, а саме [8]:

Таблиця 1

Система показників оцінки рівня інформаційної безпеки

№ п/п	Індикатор інформаційної безпеки	Розрахункова формула	Умовні позначення	Можливе порогове значення
1	2	3	4	5
Оцінка програмно-технічної захищеності інформації				
1	Коефіцієнт технічного захисту інформації ($К_{т.з.}$)	$К_{т.з.} = ІА_{нв}$	$ІА_{нв}$ – кількість не відвернутих інформаційних атак, од.;	зменшення
2	Коефіцієнт програмної захищеності інформації ($К_{п.з.}$)	$К_{п.з.} = \frac{Ч_{б.ф.}}{Ч_{н.ф.}}$	$Ч_{б.ф.}$ – час безперебійного функціонування корпоративної інформаційної системи, год.; $Ч_{н.ф.}$ – нормативний час функціонування корпоративної інформаційної системи, год.	1, зростання
3	Коефіцієнт фінансового захисту інформації ($К_{ф.з.}$) [1]	$К_{ф.з.} = \frac{В_{з.ін.}}{В_{пр.ін.}}$	$В_{з.ін.}$ – витрати на захист інформаційних ресурсів, грн.; $В_{пр.ін.}$ – витрати на придбання інформаційних ресурсів, грн.	0,15, зростання
4	Коефіцієнт фінансування інформаційних служб підприємства ($К_{фін}$)	$К_{фін} = \frac{В_{фін}}{В_{з}}$	$В_{фін}$ – витрати на фінансування інформаційних служб підприємства, грн.; $В_{з}$ – загальні витрати підприємства, грн.	0,05-0,15, зростання
Оцінка інформаційної надійності персоналу				
5	Коефіцієнт правової захищеності інформації ($К_{пр.з}$)	$К_{пр.з} = \frac{І}{І_{юр.з.}}$	$І$ – обсяг інформації, розголошення якої може спричинити негативні наслідки для підприємства, %; $І_{юр.з.}$ – загальний обсяг юридично захищеної інформації, %	1, зменшення
6	Коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку підприємства ($К_{д.р.}$)	$К_{д.р.} = \frac{ЧП_1}{ЧП_з}$	$ЧП_1$ – чисельність працівників, маючих доступ до комерційної таємниці, що працюють на підприємстві більше одного року, ос.; $ЧП_з$ – загальна чисельність працівників, що мають доступ до комерційної таємниці, ос.	1, зростання

Продовження табл. 1

1	2	3	4	5
7	Коефіцієнт надійності персоналу, що забезпечує інформаційну безпеку підприємства ($К_{н.п.}$)	$К_{н.п.} = \frac{ЧП_{з.зв.} - ЧП_{вит}}{ЧП_{з.зв.}}$	$ЧП_{вит}$ – чисельність працівників, звільнених за причиною витоку інформації, ос.; $ЧП_{з.зв.}$ – загальна чисельність звільнених працівників, ос.	1, зростання
8	Коефіцієнт підготовленості персоналу до розпізнавання погроз ($К_{п.п.}$)	$К_{п.п.} = \frac{ЧП_{з} - ЧП_{п}}{ЧП_{з}}$	$ЧП_{п}$ – чисельність працівників, ненавмисні дії яких призвели до витоку інформації завдяки низькому рівню підготовки персоналу до розпізнавання загроз безпеці, ос.; $ЧП_{з}$ – загальна чисельність працівників, що мають доступ до закритої інформації, ос.	1, зростання
Оцінка інформації, що надається особам, що приймають рішення (ОПР), інформаційною службою підприємства				
9	Коефіцієнт повноти інформації ($К_{п.ін.}$) [2]	$К_{п.ін.} = \frac{I_{н.}}{I_{необ.}}$	$I_{н.}$ – обсяг інформації, що є в розпорядженні ОПР, %; $I_{необ.}$ – обсяг інформації, необхідної для ухвалення обґрунтованого рішення, %	1, зменшення
10	Коефіцієнт точності інформації ($К_{т.ін.}$) [2]	$К_{т.ін.} = \frac{I_{р}}{I_{н}}$	$I_{р}$ – обсяг релевантної інформації, %; $I_{н}$ – загальний обсяг наявної в розпорядженні ОПР інформації, %	1, зростання
11	Коефіцієнт суперечливості інформації ($К_{с.ін.}$) [2]	$К_{с.ін.} = \frac{I_{ухв.}}{I_{з}}$	$I_{ухв.}$ – кількість незалежних свідчень на користь ухвалення рішення, %; $I_{з.}$ – загальна кількість незалежних свідчень у сумарному обсязі релевантної інформації, %	1, зростання
12	Коефіцієнт своєчасності надання інформації ($К_{с.н.ін.}$)	$К_{с.н.ін.} = \frac{I_{с.н.}}{I_{необ.}}$	$I_{с.н.}$ – обсяг своєчасно наданої ОПР інформації, %; $I_{необ.}$ – обсяг інформації, необхідної для ухвалення обґрунтованого рішення, %	1, зростання
13	Коефіцієнт надійності інформації ($К_{н.ін.}$)	$К_{н.ін.} = \frac{I_{н.д.}}{I_{з.н.}}$	$I_{н.д.}$ – обсяг інформації, наданої ОПР з надійних джерел, %; $I_{з.н.}$ – загальний обсяг наданої ОПР інформації, %	1, зростання

а) забезпечення програмно-технічного захисту від несанкціонованого доступу до закритої інформації;

б) забезпечення захисту від промислового шпигунства;

в) забезпечення безпеки підтримки зв'язків з контрагентами;

г) організація збору, оцінки, обробки, систематизації та аналізу інформації, необхідної для забезпечення ефективного процесу управління підприємством.

За такого підходу для оцінки програмно-технічної захищеності інформації пропонується використовувати показник фінансового захисту інформації, який наводить Реверчук Н.Й. [1], а також показники технічного захисту інформації, програмної захищеності інформації та коефіцієнт фінансування інформаційних служб підприємства.

Для оцінки інформаційної надійності персоналу пропонується розраховувати коефіцієнт правової захищеності інформації, коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку підприємства, коефіцієнт надійності персоналу, що забезпечує інформаційну безпеку підприємства та коефіцієнт підготовленості персоналу до розпізнавання погроз.

Оцінку інформації, що надається особам, що приймають рішення, інформаційною службою підприємства пропонується проводити за допомогою трьох показників, що наводить Ілляшенко С.М. [2] (коефіцієнт повноти інформації, коефіцієнт точності інформації та коефіцієнт суперечливості інформації), які варто доповнити коефіцієнтом своєчасності надання інформації та коефіцієнтом надійності інформації. Система показників оцінки рівня інформаційної безпеки підприємства за кожним з запропонованих напрямків з розрахунковими формулами та пороговими значеннями наведена в таблиці 1.

Варто зазначити, що для отримання інформації, необхідної для розрахунку наведених показників, обов'язковою умовою є наявність системи моніторингу діяльності інформаційної служби підприємства.

Висновки. Запропоновані напрямки діагностики рівня інформаційної безпеки підприємства ґрунтуються на врахуванні ключових аспектів інформаційної безпеки.

Отже, використання розробленої за кожним напрямком системи показників в процесі діагностики рівня інформаційної безпеки підприємства дозволить підвищити об'єктивність її результатів.

Перспективним напрямком досліджень у цій сфері може бути розробка алгоритму комплексної діагностики рівня інформаційної безпеки підприємства з детальним описом кожного етапу.

СПИСОК ЛІТЕРАТУРИ

1. Реверчук, Н.Й. Управління економічною безпекою підприємницьких структур [Текст]: монографія / Н.Й. Реверчук. – Львів: ЛБІ НБУ, 2004. – 195 с.

2. Ілляшенко, С.М. Економічний ризик [Текст]: навч. посіб. 2-ге вид., доп., перероб. / С.М. Ілляшенко – К.: Центр навчальної літератури, 2004. – 220с.

3. Кравчук, О.Я. Діагностика рівня та критерії оцінки корпоративної безпеки суб'єктів господарювання [Текст] / О.Я. Кравчук, П.Я. Кравчук // Економічні науки. Серія «Економіка та менеджмент»: збірник наукових праць. Луцький державний технічний університет. – Випуск 1. Редкол.: відп. ред. д.е.н., проф. Герасимчук З.В. – Луцьк, 2004. – С.85-109.

4. Ковалев, Д. Экономическая безопасность предприятия [Текст] / Д. Ковалев, Т. Сухорукова // Экономика Украины. – 1998. – № 10. – С. 48-51.

5. Экономическая и национальная безопасность [Текст] / Под ред. Е.А. Олейникова. – М.: Издательствово «Экзамен», 2004. – 768 с.

6. Козаченко, А.В. Экономическая безопасность предприятия: сущность и механизм обеспечения: монография [Текст] / А.В. Козаченко, В.П. Пономарев, А.Н. Ляшенко. – К.: Либра, 2003. – 280 с.

7. Клєбанова, Т.С. Моделі оцінки, аналізу та прогнозування економічної безпеки підприємства [Текст] / Т.С. Клєбанова, Є.А. Сергієнко // Бізнес Інформ. – 2006. – № 8. – С. 65-72.

8. Полозова, Т.В. Організаційне забезпечення складових економічної безпеки підприємства [Текст] / Т.В. Полозова, М.Ю. Журавель // Економіка: проблеми теорії та практики: збірник наукових праць. – Випуск 257: В 7 т. – Т. ІІІ. – Дніпропетровськ: ДНУ, 2009. – С. 613-619.

Аннотация. Предложено диагностику уровня информационной безопасности предприятия проводить по трем ключевым направлениям: оценка программно-технической защищенности информации; оценка информационной надежности персонала; оценка информации, предоставляемой лицам, принимающим решения, информационной службой предприятия. Сформирована система показателей оценки уровня информационной безопасности по каждому предложенному направлению.

Ключевые слова: информационная безопасность предприятия, направления диагностики информационной безопасности, система показателей оценки уровня информационной безопасности.

Summary.. Diagnostic the level of information security of the enterprise proposed to carry out in three main directions: evaluation of program-technical protection of information; evaluation of informational reliability of personnel; evaluation of information provided to decision makers. The system of indicators to assessment the level of information security for each proposed direction was formed.

Keywords: information security of the enterprise, the directions of diagnostic of information security, system of indicators the level of information security.

Рецензент *д.е.н., професор ХНУРЕ Костін Ю.Д.*
Експерт редакційної колегії *к.е.н., доцент УкрДАЗТ Полякова О.М.*

УДК 658.013

АДАПТИВНЕ УПРАВЛІННЯ ПІДПРИЄМСТВОМ В КОНКУРЕНТНОМУ СЕРЕДОВИЩІ

Калініченко Л. Л., к.е.н, доцент (УкрДАЗТ)

Розглянуто теоретичні аспекти адаптивного управління підприємством в конкурентному середовищі

Ключові слова: адаптивне управління, конкурентне середовище, підприємство

Постановка проблеми та її зв'язки з науковими чи практичними завданнями. Нестабільність середовища господарювання є характерною умовою розвитку підприємства в ринковій економіці. Характерними умовами сучасної діяльності підприємства є невизначеність ринку, термінів і умов поставок, поведінки власників, конкурентів, органів державної влади. Підприємство існує та розвивається в активному зовнішньому середовищі, пристосовується до його змін. Складність і нестабільність ринкового оточення вимагають від підприємства постійного вдосконалювання форм і методів господарювання.

Зовнішнє середовище обмежується в залежності від цілей підприємства та поділяється на економічну, суспільну й екологічну системи. Кожна з цих систем є сукупністю факторів прямого та непрямого впливу. Фактори прямого впливу безпосередньо та негайно впливають на діяльність підприємства і відчувають на собі аналогічний вплив з його боку (постачальники, споживачі, конкуренти, посередники, групи інтересів, державне регулювання економіки). Фактори непрямого впливу можуть не надавати прямого негайного впливу на підприємство, але з часом позначаються на його діяльності (макроекономічні, соціально-культурні, політичні, природні, науково-технічні, демографічні фактори).

Для виживання і збереження конкурентоспроможності промислових підприємств в сучасних швидкоплинних умовах функціонування потрібне постійне коректування їх господарської діяльності з врахуванням змін навколишнього середовища. Управління змінами на вітчизняних підприємствах має бути більшою мірою орієнтоване не на вирішення існуючих проблем, а на використання наявних можливостей і сильних сторін підприємства. Інакше кажучи, управління організаційними змінами має здійснюватися на засадах адаптивного підходу, який передбачає використання в якості бази організаційних змін існуючого потенціалу підприємства та виявлення його резервів.

Аналіз останніх досліджень та виділення невирішених частин загальної проблеми. Проблеми розвитку адаптації механізму функціонування підприємств висвітлені такими дослідниками як Алексєєв С.Ю., Буднік М. М., Кравченко С. А., Степанова Ю.Л., Туріца Н.А. [1-

© Калініченко Л.Л.