

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет «Запорізька політехніка»

КОНСПЕКТ ЛЕКЦІЙ

**з дисципліни «Інформаційно аналітичне
забезпечення економічної безпеки» для
здобувачів вищої освіти за освітнім ступенем
«магістр» денної та заочної форм навчання
спеціальностей 072 «Фінанси, банківська
справа, страхування та фондовий ринок»**

2023

Конспект лекцій з дисципліни «Інформаційно аналітичне забезпечення економічної безпеки» для здобувачів вищої освіти за освітнім ступенем «магістр» денної та заочної форм навчання спеціальностей 072 «Фінанси, банківська справа, страхування та фондовий ринок» / Укл.І.Є.Андрющенко, – Запоріжжя: НУЗП, 2023.- 39 с.

Укладач: д.е.н., професор Андрющенко І.Є, к.е.н, доцент О. Ю. Литовченко

Рецензент: к.е.н.,доцент Фатюха Н.Г.

Відповідальний за випуск: к.е.н., доцент С.В. Шарова

Затверджено
на засіданні кафедри
“Фінанси, банківська справа
та страхування ”
Протокол № 1
від 18.08.2023р.

Рекомендовано
до видання НМК
факультету Економіки
та управління
Протокол № 43
Від 30.08.2023р.

ЗМІСТ

ВСТУП	4
Тема 1. Концептуально-методологічні засади інформаційно-аналітичної діяльності	5
Тема 2. Законодавча база, що регламентує діяльність із аналітичного забезпечення економічної безпеки підприємств, установ, організацій	8
Тема 3. Аналіз впливу зовнішнього та внутрішнього середовищ на стан економічної безпеки підприємства, установи, організації	10
Тема 4. Організаційні засади інформаційно-аналітичного забезпечення системи економічної безпеки підприємства, установи, організації. Стейкхолдерно-орієнтований підхід до системи формування інформаційно-аналітичного забезпечення	14
Тема 5. Організаційно-економічні засади діяльності підрозділу аналітичного забезпечення системи економічної безпеки підприємства	22
Тема 6. Техніка моніторингу та критерії оцінки результатів підрозділу аналітичного забезпечення економічної безпеки підприємства	26
Тема 7. Сучасні технології проведення аналітичної роботи в галузі економічної безпеки підприємства	29
Тема 8 Документування і документообіг в установі, організації, підприємстві та безпека комунікацій	33
СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ	37

ВСТУП

Стрімкий розвиток ринкових перетворень вимагає застосування спеціальних знань і навичок, пов'язаних з аналітичною діяльністю щодо оцінки факторів ризиків і загроз економічної діяльності підприємств.

Предметом дисципліни є інформаційно-аналітична діяльність в сфері забезпечення фінансово-економічної безпеки підприємств. Метою викладання дисципліни є підготовка компетентних фахівців-управлінців, здатних професійно організовувати роботу з інформаційно-аналітичного забезпечення безпеки підприємства, здійснювати управління та координування такою роботою, бути професіоналом у сфері конкурентної розвідки при організації та управлінні комплексним забезпеченням функціонування системи фінансово-економічної безпеки підприємств.

При вивченні дисципліни студенти повинні знати нормативно-правові документи, що регулюють аналітичну діяльність фахівців в сфері економічної безпеки; функції, загальні принципи побудови та організації комплексної системи захисту економічних інтересів підприємства; методи проведення аналітичних досліджень в даній галузі; організацію та технологію інформаційно-аналітичного забезпечення економічної безпеки; форми та методи діагностування небезпек, загроз і ризиків їх оцінки та мінімізації; порядок розроблення та ведення аналітичної документації з питань економічної безпеки підприємства. Студенти повинні вміти використовувати на практиці набуті навички та знання при оцінці рівня економічної безпеки; визначати критерії та індикатори оцінки ефективності діяльності суб'єктів системи економічної безпеки підприємства; проводити аналіз стану забезпечення інформаційної безпеки та захист комерційної таємниці підприємства; визначати умови проведення експертної оцінки отриманої інформації та рівень її достовірності; знати і вміти самостійно розроблювати заходи стратегічної орієнтації підприємства з урахуванням вимог до забезпечення економічної безпеки

ЗМІСТОВИЙ МОДУЛЬ 1 ОРГАНІЗАЦІЯ ТА УПРАВЛІННЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНИМ ЗАБЕЗПЕЧЕННЯМ БЕЗПЕКИ ПІДПРИЄМСТВА

Тема 1. Концептуально-методологічні засади інформаційно - аналітичної діяльності

Інформаційно-аналітичне забезпечення є однією з обов'язкових складових організації системи управління будь-якої функціональної системи, яка надає можливість зважено приймати управлінські рішення на різних щаблях управління.

Термін «забезпечення» означає дію, а також зберігання, виконання чого-небудь, служить гарантією того чи іншого процесу. Коли мова йде про будь-яке забезпечення, вказуючи на його конкретний якісний аспект (інформаційно-аналітичний), то мають на увазі насамперед сукупність засобів, умов і дій, які гарантують нормальне проходження процесів.

У правовій літературі визначення *інформаційно-аналітичного забезпечення* відображає систему взаємопов'язаних методів, заходів і засобів (науково-методичного, соціально-політичного, техніко-економічного й організаційно-правового характеру), які реалізують створення і функціонування технології процесу збирання, передачі, переробки, зберігання та видачі (відображення), а також використання інформації з метою здійснення ефективної діяльності в тій чи іншій сфері.

З огляду на визначну роль інформаційного обміну вагоме значення набуває інформаційно-аналітичне забезпечення системи безпеки суб'єкта господарювання. Інформаційно-аналітичне забезпечення охоплює процеси збирання, обробки, перетворення інформації, включаючи класифікаційні переліки всіх даних, методи їхнього кодування, зберігання для аналізу та передачі відповідним

органам управління. Інформація функціонує в різних формах – від потоків даних, що мають короткострокове значення, до даних довгострокових, накопичених за роки досліджень, які зберігаються в бібліотеках, архівах, у пам'яті комп'ютерів або фахівців.

Термін «інформація» вперше було розглянуто в розділі знань інформатика, а саме, в напрямі кібернетика. У роботах вчених наводиться різне тлумачення категорії інформація, наприклад: інформація – визначення змісту, отриманого з навколишнього світу; інформація – комунікація, зв'язок у процесі якого встановлюється невизначеність. Управліннями інформація розглядається як *чинник управління*.

Основною складовою інформації є *інформаційний ресурс*, який формується різними міністерствами, установами, фірмами тощо. У соціальному плані інформаційний ресурс є множиною даних різного спрямування. Програми, алгоритми, різні технічні і технологічні, неопубліковані і тому подібні фонди і системи інформації можна розглядати як інформаційний ресурс.

Другою важливою складовою інформаційно-аналітичного забезпечення є *аналітична діяльність*, яка сьогодні перетворилася на професійну діяльність, забезпечуючи вимоги практично всіх сфер громадського життя. Аналітика має глибоке історичне коріння, починаючи з Сократа, Стагірита, Аристотеля тощо. *Мета аналізу* – надати масивам неопрацьованих даних зрозумілого значення. У разі наявності як кількісних, так і якісних даних завдання полягає в тому, щоб відібрати, класифікувати, обробити і зрозуміти їхнє значення. Крім того, потрібно знайти таке тлумачення, яке відображає необроблені дані, і використати його точно для осмисленого подання подій.

Якщо раніше термін аналітика вживався як самостійний, то сьогодні в інформаційному суспільстві все частіше вживається термін *інформаційно-аналітична діяльність*. Від якості і повноти інформаційно-аналітичного забезпечення залежить ефективність рішення. Відбувається постійний

динамічний процес взаємозв'язку аналітичної діяльності із зовнішнім середовищем.

Сучасна структура аналітики, яка сьогодні являє собою розгалужену і складну систему знань, для застосування в аналітичній діяльності включає в себе такі складові, як *логіка, інформатика, евристика і методологія*. Ці основні складові аналітичної діяльності розвиваються за своїми законами, правилами і методами.

Практичні дії в аналітичному забезпеченні базуються на двох напрямках, а саме: на виборі *методу аналізу* і застосуванні *технологій і алгоритмів*. Методи аналізу включають певні правила, підходи, принципи, прийоми, які сформульовано людським досвідом і знаннями в чітку систему застосування. Одночасно можуть використовуватися декілька методів, але всі вони спрямовуються на генерування нового результату, нових знань про ту чи іншу проблему. Другим етапом практичних дій аналітиків є етап застосування *технологій* аналізу. Технології можуть бути різними залежно від завдання чи замовлення. Сьогодні таких технологій багато і вони характеризуються різноманітністю і неповторністю, але вони мають і загальні стадії: ·визначення об'єкта і предмета та проблеми аналізу; ·побудова моделі об'єкта і предмета аналізу; ·побудова гіпотез; ·вибір типу аналізу; вибір або розробка методів аналізу; доведення гіпотез; формування аналітичних висновків.

Є різні види аналітичної діяльності і застосовуються вони залежно від галузі знань і практики. Кожен із видів аналізу має свої параметри і характеристики, свої особливості і технологію. Як правило, вид аналізу залежить від характеру замовлення і вимог споживача до кінцевого продукту аналізу.

Тема 2. Законодавча база, що регламентує діяльність із аналітичного забезпечення економічної безпеки підприємств, установ, організацій

На сьогоднішньому етапі розуміння терміну «інформація» слід використовувати юридичні норми, які є в законах України і державних стандартах. Є багато видів інформації, які закріплені цими документами, наприклад: документована, науково-технічна, правова, статистична, таємна; соціологічна тощо.

У Законі України «Про інформацію» (2012 р. № 2657-12) у статті 1 надано законодавче визначення поняття «інформація». *Інформація* – це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Визначення категорії «інформаційний ресурс» надано в Законі України «Про наукову і науково-технічну діяльність» (2012 р. №1977-12): *інформаційний ресурс* – сукупність документів в інформаційних системах (бібліотеках, архівах, банках даних тощо).

У Законі України «Про друковані засоби масової інформації (пресу)» (1992 р. № 2782-XII) зазначено, що інформація може розглядатись як результат аналітико-синтетичної обробки даних (відомостей) суб'єктом щодо об'єкта. Таким чином, інформація має переважно порівняльний і прикладний характер. Вона складається тільки з нових відомостей, які оцінюються користувачем як корисні знання.

На сьогодні діяльність у сфері створення і використання інформаційних ресурсів в Україні регламентують ще понад 20 законодавчих і нормативних документів. Але і цього не вистачає в повній мірі для того, щоб здійснювати управління процесом створення і використання національних інформаційних ресурсів.

Аналіз існуючого законодавства показує, що інформація є фактично новим об'єктом цивільного права. Нині вона виступає як особливий об'єкт договірних відносин, що стосуються її збирання, збереження, пошуку, переробки, поширення, захисту і використання в усіх сферах людської діяльності. Зокрема, науково-технічна інформація може розглядатися як об'єкт інтелектуальної власності, тому що вона, як і інтелектуальна власність, є результатом творчої праці людини. Це виходить із співставлення Законів України «Про науково технічну інформацію» (2011р., № 3322-12) та «Про авторське право і суміжні права» (2012 р., № 3792-12). Інформаційні ресурси науково-технічної інформації є об'єктами права інтелектуальної власності і на них розповсюджуються норми Закону України «Про авторське право і суміжні права» (2012 р., № 3792-12). Таким чином, інформація і інформаційний ресурс відносяться до об'єктів інтелектуальної власності, тому є необхідність створення науково-методичної бази для розгляду інформаційного ресурсу, інформації з позиції товару і авторського права.

В Україні на рівні законодавства досі не визначено поняття *правовий режим інформації*, яке є основою для встановлення правил доступу інших держав до інформаційних ресурсів України. Чинне законодавство встановлює лише окремі фрагменти правового режиму інформації з обмеженим доступом (крім державної та банківської таємниці), а саме ця категорія, тобто інформація з обмеженим доступом, становить, за деякими оцінками, до 80 % інформаційного ресурсу України.

Для вирішення означених проблем необхідно прийняти низку законодавчих актів та державних рішень, в яких було б можливим визначити ключові вихідні системні поняття і терміни інформаційного права (інформаційний суверенітет України, національний інформаційний простір, правовий режим інформації, принципи міжнародного інформаційного

співробітництва та ін.), що є основою для подальшого вдосконалення інформаційного законодавства, прийняття законів з формуванням важливих правових ознак суверенної та незалежної держави.

Тема 3 Аналіз впливу зовнішнього та внутрішнього середовищ на стан економічної безпеки підприємства, установи, організації

Різноманіття господарських зв'язків, в які вступає підприємство в процесі своєї господарської діяльності, призводить до виникнення великої кількості факторів впливу на економічну безпеку його діяльності. Тому виявлення факторів ризику, небезпек і загроз – одне з найбільш важливих завдань забезпечення економічної безпеки.

Для обґрунтування чітких і ефективних шляхів зміцнення економічної безпеки підприємств дуже важливо виділити найбільш важливі сучасні небезпеки і загрози. Тому, при аналізі факторів економічної безпеки пріоритетне значення має ідентифікація деструктивних чинників (загроз).

В сучасній теорії безпеки виділяють декілька *ступенів деструктивних факторів*:

- ймовірність виникнення обстановки, здатної породити небезпеку (поява зони ризику);
- провокаційні дії або засіб тиску (виклик);
- реальна можливість заподіяти зло, завдати шкоди (небезпека);
- намір завдати шкоди або ненавмисний небезпечний збіг обставин (загроза).

Приймаючи господарські рішення, підприємство не завжди в змозі витримати жорстке випробування обставинами, в яких опиняється бізнес, а отже, повинно

заздалегідь враховувати джерела та фактори небезпек і загроз економічній безпеці.

Загроза – це можлива небезпека. Це найбільш конкретна і безпосередня форма економічної небезпеки або сукупність умов і факторів, що створюють небезпеку. Загрози економічній безпеці класифікуються за ознаками: за джерелом виникнення; за відношенням до людської діяльності; за систематичністю прояву; за ступенем керованості; за можливістю нейтралізації; за впливом на складові економічної безпеки підприємства за моментом виникнення; за об'єктивністю існування; за частотою виникнення; за ступенем очевидності; за впливом на об'єкт; за сферою виникнення; за вірогідністю реалізації; за тривалістю впливу на функціонування і розвиток підприємства; за характером прояву. Найбільшого поширення набуло виділення небезпек і загроз залежно від сфери їх виникнення – *зовнішні (екзогенні фактори) і внутрішні (ендогенні фактори)*.

Зовнішні фактори небезпек і загроз виникають за межами підприємства і не пов'язані безпосередньо з його виробничою діяльністю, але впливають як на сам процес виробництва, так і на результати діяльності. На зовнішні фактори підприємство не може впливати або цей вплив може бути незначним. *Внутрішні* фактори пов'язані з господарською діяльністю підприємства, його персоналом і безпосередньо залежать від форм, методів та організації роботи на підприємстві. Вони обумовлені тими процесами, які виникають в ході виробництва та реалізації продукції, і можуть вплинути на результати бізнесу.

Зовнішні фактори впливу на економічну безпеку підприємств можна згрупувати у декілька груп: політичні; макроекономічні; мезоекономічні; мікроекономічні; екологічні; науково-технічні та технологічні; юридичні (правові); соціально-культурні; інформаційні; природно-

техногенні; демографічні; криміналістичні фактори; морально-психологічні та ін.

Групи факторів загроз і небезпек, які мають *внутрішній* характер, і пов'язані з господарською діяльністю підприємства і роботою його персоналу: виробничого значення; пов'язані із зовнішнім середовищем підприємства; пов'язані з персоналом підприємства; пов'язані з інформаційними ресурсами; у сфері планування; пов'язані з конкурентною позицією; пов'язані зі збутовою, маркетинговою стратегією і політикою; екстенсивні фактори виробництва; у сфері фінансового менеджменту; у сфері виробничого менеджменту; юридичні (правові); форс-мажорні та ін.

З усіх можливих видів зовнішніх загроз (факторів) економічній безпеці, важливо виділити ті, що безпосередньо спрямовані на руйнування або ослаблення потенціалу підприємства.

Виділяють загальні та спеціальні заходи безпеки щодо боротьби із загрозами та небезпеками. Основною метою *загальних* заходів безпеки є запобігання виникненню можливих загроз та їх здійсненню, розроблення і дотримання так званих *нормативів безпеки* (системи правил та режимів безпеки), регламентація й мотивація поведінки працівників організації.

У розробленні й виконанні загальних заходів економічної безпеки бере участь управлінський персонал (керівники різних рівнів управління та структурних підрозділів, управлінці) й рядові працівники, для яких цей вид діяльності передбачений у посадових обов'язках або є складовою їх роботи, але не є їх основною діяльністю. Основною метою *спеціальних* заходів є припинення дії загрози на будь-якій стадії її реалізації конфіденційними методами та методами роботи в надзвичайних ситуаціях. Реалізацією

спеціальних заходів безпеки займаються працівники, для яких це є предметом діяльності і основною роботою.

Вибір засобів впливу на загрози і небезпеки має на меті мінімізувати можливий збиток у майбутньому. *Методи захисту від загроз і нейтралізації їх негативних наслідків* можна представити декілька напрямками: методи ухиляння від загроз; методи локалізації загроз; методи передачі ризиків від загроз; методи компенсації; методи диверсифікації; методи лімітування; встановлення максимального розміру споживчого кредиту, наданого одному покупцю; встановлення мінімального розміру оборотних активів у високоліквідній формі; встановлення граничного розміру використання позикових коштів в обороті; встановлення максимального розміру депозитного внеску, розміщуваного в одному комерційному банку та інші.

До основних завдань системи економічної безпеки підприємства щодо попередження й нейтралізації загроз і небезпек належать: вивчення партнерів, конкурентів, споживачів, майбутніх інвесторів та співробітників підприємства; отримання необхідної інформації для прийняття найбільш оптимальних управлінських рішень з питань стратегії і тактики економічної діяльності підприємства; збір, аналіз, оцінка даних і прогнозування розвитку подій; своєчасне виявлення з боку зовнішнього середовища можливих загроз підприємству та його співробітникам; недопущення проникнення підприємство структур економічної розвідки конкурентів, злочинців й окремих осіб з протиправними намірами; протидія технічному проникненню злочинних цілях; забезпечення збереження матеріальних цінностей і відомостей, що становлять комерційну таємницю підприємства; формування серед споживачів і ділових партнерів позитивної думки про підприємство; контроль за ефективністю функціонування системи безпеки, удосконалення її елементів тощо.

Тема 4. Організаційні засади інформаційно-аналітичного забезпечення системи економічної безпеки підприємства, установи, організації. Стейкхолдерно-орієнтований підхід до системи формування інформаційно-аналітичного забезпечення

Забезпечення економічної безпеки підприємства можливе лише за умови гармонізації інтересів із суб'єктами зовнішнього та внутрішнього середовищ, тому цей процес повинен носити безперервний організаційно оформлений характер. Для проведення інформаційно-аналітичної діяльності створюють *підрозділ аналітичного забезпечення* економічної безпеки підприємства. Основними нормативно *правовими документами* для забезпечення діяльності підрозділу аналітичного забезпечення економічної безпеки є: Конституція України; закони та постанови Верховної Ради України; укази Президента України; постанови та розпорядження Кабінету Міністрів України; інші нормативно-правові документи, що стосуються сфери економічної безпеки.

Аналітичний підрозділ з питань економічної безпеки виконує *наступні завдання*: забезпечує підготовку документів, необхідних для прийняття управлінських рішень щодо діяльності підприємств в умовах реальних потенційних загроз і небезпек; розроблює проекти наказів, положень, інструкції щодо організації діяльності аналітиків з питань економічної безпеки та інформаційно-аналітичного забезпечення функціонування системи економічної безпеки; визначає та оцінює стан і рівень економічної безпеки свого підприємства, партнерів і конкурентів; здійснює всі види інформаційного, аналітичного та обліково-аналітичного забезпечення функціонування системи економічної безпеки підприємства; розроблює аналітичні документи за якими здійснюється оцінка стану та надаються пропозиції щодо

діяльності підприємства в умовах загроз, небезпек, рекомендації щодо їх зниження.

Аналітик з питань економічної безпеки *повинен знати*: функції, загальні принципи побудови та організації діяльності комплексної системи забезпечення економічної безпеки підприємства; методи проведення аналітичних досліджень; технології, форми та методи діагностування небезпек, загроз і ризиків, критерії їх оцінювання на підприємстві; механізми інформаційно-аналітичного забезпечення управління системою економічної безпеки; порядок організації проведення контролю та оцінки рівня економічної безпеки.

Основними документами, які необхідні для проведення аналітичної роботи є: Баланс (форма №1); Звіт про рух грошових коштів (форма №2); - Звіт про фінансові результати (форма №3); Звіт про власний капітал (форма №4); Примітки до фінансових звітів, статистична звітність, дані бухгалтерського обліку, що стосуються аналізу економічних показників.

Організація аналітичної розробки показників економічної безпеки підприємства включає наступні роботи: розробку аналітичної номенклатури; розробку та вибір методики обчислення показників; визначення логічної послідовності обробки даних; розробка форм, таблиць і графіків руху аналітичної інформації; забезпечення комплексу робіт, що виконуються на етапі аналітичної обробки інформації, який полягає у перетворенні вихідної інформації в кінцеву шляхом логічних і обчислювальних операцій.

Під *аналітичною номенклатурою* розуміють складний перелік даних, передбачених в планах, нормах, нормативах, кошторисах, фактично врахованих і тих, що характеризують господарські явища і процеси. Аналітичні номенклатури формуються в різних показниках господарської діяльності:

натуральні і вартісні; фактичні, базові, нормативні за звітний період; фактичні і базові за фактичний період.

В процесі аналізу показників економічної безпеки формуються і використовуються такі види номенклатури: *первинна або вихідна* – джерела фактичних, облікових і планових даних; *проміжні*, які не являють собою результати порівняння даних і відносні числа; *заклучні або підсумкові* – аналітичні характеристики, що даються у висновках і пропозиціях по результатах аналітичних досліджень.

Комплексність, глибина і ефективність аналізу в галузі економічної безпеки залежить від обсягу та якості інформації, що використовується. Носії інформації поділяють на *машинні* та *безмашинні*.

За якісною та компетентною роботою необхідна певна кількісно- обмежена інформація. Нестача інформації не дає змоги одержати повне уявлення про стан досліджуваного об'єкта, доводиться інтуїтивно доповнювати її можливими варіантами. Надмірна кількість інформації заважає швидкості обробки і осмислення, вимагає додаткових витрат часу і праці. Вихід з даного положення – комп'ютеризація, автоматизована система управління, впровадження автоматизації робочих місць.

В процесі проведення аналізу використовують такі *носії інформації*: - фактичні або нормативні дані; дані бухгалтерії або оперативного обліку - бухгалтерська або статистична звітність; позаоблікові дані – дані спеціальних обстежень, акти ревізій, технічні та технологічні документи матеріально-виробничих нарад; розрахункові аналітичні таблиці; пояснювальні записки до річного звіту, різні довідки і закінчення.

Для забезпечення раціонального руху потоку інформації в аналітичному процесі, необхідно дотримуватись таких *принципів*: виявлення інформаційних потреб і визначення способів найбільш ефективного задоволення цих

потреб; об'єктивне відображення господарських фактів, єдність інформації різних джерел; усунення дублювання інформації; передбачити можливість всесторонньої комп'ютерної обробки аналітичної інформації.

Відібрані для використання джерела інформації підлягають інформативній (технічній) та суттєвій (логічній) перевіркам: правильність оформлення документів, звітів з точки зору наявності та заповнення реквізитів таблиць, підписів; перевірка арифметичних сум, підсумків; відповідність цифр, перенесених з інших документів і попередніх років; погодженість цифр у різних формах; погодженість взаємозалежних величин. При суттєвій перевірці встановлюють: доброякість матеріалів; їх відповідність об'єктивній дійсності; можливість використання для аналізу.

Стейкхолдери – це фізичні та юридичні особи, зацікавлені у фінансових та інших результатах діяльності підприємства і здатних здійснювати на неї вплив. Вони мають «частку» (stake) впливу на підприємство. Всі зацікавлені сторони характеризуються фінансовими інтересами та очікують отримання вигоди від функціонування. Під фінансовим інтересом розуміють очікувану економічну вигоду від реалізації стратегії, що виражена у фінансовій формі (грошовій, часовій, ризиковій).

Існують різноманітні класифікації загроз з точки зору впливу на діяльність підприємства та стейкхолдерів, які знаходяться у тісній взаємодії з підприємством. Приміром, загрози розділяють за об'єктами посягань в розрізі самого підприємства та його стейкхолдерів (внутрішніх і зовнішніх).

Вплив стейкхолдерів на економічну безпеку може мати як позитивний, так і негативний характер, може бути прямим або непрямим, сильним або слабким. Чим більше у стейкхолдерів інструментів, завдяки яким вони впливають на діяльність та економічну безпеку підприємства, тим

важливішими вони є для кожного окремого підприємства, потребуючи ретельного вивчення їх впливу.

Загрози з боку внутрішніх стейкхолдерів (персонал, власники) – виникають в процесі звичайної діяльності підприємства, а загрози зовнішнього характеру пов'язані з репутацією підприємства (їх генерують покупці, замовники, постачальники, конкуренти, державні органи, ЗМІ, фінансові установи).

Класифікація стейкхолдерів відносно їх впливу на підприємство, в таблиці 1, дозволяє систематизувати загрози економічній безпеці підприємства та визначити перелік показників для оцінювання ступеня та спрямованості (негативної або позитивної) їх впливу. Кожне підприємство визначає пріоритетними 2–3 групи стейкхолдерів, як правило, конкурентів, покупців (замовників) та персонал.

Класифікація загроз та показників оцінки рівня економічної безпеки підприємства за групами стейкхолдерів

Таблиця 1

Стейкхолдери	Загрози	Показники
1	2	3
Персонал	Низький професіоналізм, розкрадання матеріальних цінностей, розголошення комерційної таємниці, відсутність стабільної середньої ланки менеджерів, невідповідність кваліфікації займаній посаді, неефективна організація системи управління персоналом, неефективна система мотивації, неналагоджена система відбору персоналу, несприятливий клімат у колективі	Продуктивність праці, показник укомплектованості кадрами, коефіцієнт постійності кадрів, рівень трудової дисципліни, чисельність кваліфікованих кадрів, плинність кадрів, освітній рівень персоналу, рівень соціальної захищеності

Власники	Прозорість ведення бізнесу, непрофесійний підхід до набору персоналу, превалювання власних інтересів над корпоративними, розголошення комерційної таємниці, прийняття необґрунтованих рішень	Фінансові показники (ліквідності, фінансової стійкості, рентабельності, ділової активності), показник захищеності інформації
Покупці	Низька платоспроможність покупців, зміна вподобань населення, незадоволеність якістю продукції, навмисна шкода підприємству	Маркетингові дослідження щодо якості, ціни та асортименту продукції (опитування), індекс лояльності споживачів, показник ринкової віддачі активів, частка підприємства на ринку, показник інноваційних витрат, ритмічність збуту; конкурентоспроможність виробів
Постачальники	Відсутність довгострокових контрактів з постачальниками, підвищення цін, банкрутство постачальника, недотримання строків поставки, поставка неякісної продукції, змова з конкурентами	Показники ділової активності та ліквідності, кількість та терміни контрактів з постачальниками, основні фінансові показники постачальника
Державні органи	Недосконалість чинного законодавства, правова незахищеність підприємств, несприятлива податкова політика	Показники ліквідності, фінансової стійкості, рентабельності підприємства

Конкуренти	Наявність на ринку товарів-конкурентів, поява нових конкурентів, ефективна політика конкурента щодо лояльності покупців, промислове та економічне шпигунство, фальсифікація та підробка продукції конкурентами, переманювання кваліфікованого персоналу, інформаційна війна, грінмейл, використання державних органів з метою впливу на підприємство	Маркетингові дослідження (експертне оцінювання), вивчення економічного стану підприємства-конкурента, конкурентоспроможність виробів, частка підприємства на ринку, рівень інноваційних витрат, ефективність рекламних заходів
Фінансові організації	Підвищення відсотків за кредитами, зміна кредитної політики фінансових установ, зміна валютного курсу	Показники ліквідності, фінансової стійкості, рентабельності підприємства

Аналіз впливу *персоналу* на економічну безпеку підприємства полягає в попередженні ризиків та загроз з боку співробітників підприємства, які можуть вплинути на його безпечне функціонування. Саме від кваліфікованого та вмотивованого персоналу, в першу чергу, залежить успішна діяльність підприємства. Однією з основних загроз безпеці підприємства є розголошення комерційної таємниці та конфіденційної інформації, якою володіють керівники та менеджери підприємства.

Щодо *суб'єктів зовнішнього середовища*, то найвпливовішою відносно економічної безпеки підприємства групою стейкхолдерів є покупці (замовники). Саме завдяки лояльності покупців, сприятливого відношення споживачів до підприємства та продукції досягаються показники успішності та стабільності підприємства.

Загрози конкурентів на безпеку підприємства завжди обумовлені тим, наскільки сумлінні (несумлінні) методи конкурентної боротьби обирає підприємство-конкурент. Найбільший негативний характер несуть загрози, пов'язані з несумлінними методами конкурентної боротьби.

При визначенні інтегрального показника безпеки у взаємодії з його стейкхолдерами необхідно чітко визначити систему показників та їх граничні значення. Що стосується внутрішніх стейкхолдерів, то *основними показниками з боку персоналу* можуть бути: показник плинності кадрів, продуктивність праці, показник трудової дисципліни, показник мотивації зарплати, показник соціальної захищеності та інші. З боку власників підприємства розглядаються показники, пов'язані з фінансовою, інформаційною та політико-правовою складовими безпеки.

До показників, які характеризують *вплив стейкхолдерів зовнішнього середовища*, можна віднести: державні органи – величина податкових відрахувань, вартість державних замовлень; покупці (замовники) – показник ринкової віддачі активів, конкурентоспроможність виробів, темпи приросту ринкової частини, проміжок часу між поставками, вчасність виконання поставок, кількість пошкодженої продукції під час поставок, імовірність нестачі; фінансові організації – величина банківських відсотків, ступінь довіри з боку фінансових організацій до підприємства та основні фінансові показники підприємства та ін. Розрахунок інтегрального показника повинен базуватися на значущості кожної групи стейкхолдерів у загальному їх впливі на ефективність функціонування та економічну безпеку підприємства, яка визначається шляхом експертного опитування обраних респондентів.

ЗМІСТОВИЙ МОДУЛЬ 2 ТЕХНОЛОГІЇ ДІЯЛЬНОСТІ ФАХІВЦІВ ІЗ ПИТАНЬ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Тема 5. Організаційно-економічні засади діяльності підрозділу аналітичного забезпечення системи економічної безпеки підприємства

Механізм формування системи аналітичного забезпечення економічної безпеки підприємства – це набір аналітичних та економічних засобів, а також система організації їх використання і контролю, за допомогою яких досягається можливість стабільного та безпечного функціонування підприємства.

Завдання системи аналітичного забезпечення економічної безпеки підприємства: раціоналізація аналітичних процесів, що відбуваються на підприємстві; скорочення циклів їх функціонування, за рахунок зменшення часу на виконання окремих робіт; підвищення якості аналітичної інформації з питань економічної безпеки; забезпечення ефективного використання аналітичної інформації в управлінні підприємством; раціональна організація праці аналітиків, зайнятих збором, обробкою та видачею аналітичної інформації, яка використовується в системі економічної безпеки підприємства; забезпечення ефективності обліку та аналізу документів, їх вдосконалення в умовах реальних і потенційних загроз і небезпек функціонування системи економічної безпеки.

Організація аналітичного процесу з питань економічної безпеки повинна бути такою, щоб забезпечити виконання наступних *вимог*: мінімізація шляхів збору і обробки інформації, яка використовується в системі економічної безпеки підприємства; мінімізація кількості операцій та документації, пов'язаних із системою економічної безпеки;

підвищення ефективності праці аналітиків з питань економічної безпеки підприємства.

В діяльності підприємств склалося декілька напрямків організації аналітичної роботи з питань економічної безпеки: *децентралізована* форма організації аналітичної роботи – аналіз показників діяльності підприємства проводиться всіма структурними підрозділами за напрямками їх роботи; *централізована форма* – аналіз проводиться спеціальними аналітичними відділами, бюро та лабораторіями економічного аналізу (за місяць, квартал, півріччя або інший період в цілому по підприємству і в тому числі за окремими підрозділами за всією системою показників діяльності підприємства); *змішана форма* – аналіз проводиться окремими структурними підрозділами, а також спеціальними відділами.

Під *об'єктом* організації розуміють явище або процес, на який направлена організаторська діяльність. Об'єктами організації аналізу з питань економічної безпеки є: аналітичний процес; праця виконавців: забезпеченість аналізу (організаційна, інформаційна, технічна).

Оцінювання поточного рівня забезпечення економічної безпеки підприємства здійснюється за такими *напрямами*: аналіз фінансової звітності підприємства (дослідження ліквідності, рентабельності, структури прибутку та витрат тощо); аналіз конкурентоспроможності підприємства; аналіз асортименту продукції підприємства; аналіз кваліфікації та потенціалу персоналу, системи управління підприємством; аналіз теперішньої та прогнозованої вартості капіталу; аналіз поставок і клієнтури підприємства; аналіз кредитної політики суб'єкта господарювання; аналіз динаміки цінних паперів підприємства тощо.

Оцінювання рівня економічної безпеки підприємства повинно базуватися на таких *принципах*: відповідність параметрів оцінювання змісту процесів у системі економічної безпеки підприємства; комплексність, тобто врахування всіх

чинників, що впливають на загрози економічній безпеці підприємства; виділення головних елементів наявних або потенційних небезпек і загроз; періодичність оцінювання рівня економічної безпеки підприємства; можливість застосування необхідних запобіжних, попереджувальних, профілактичних та корегуючих заходів щодо виявлених або потенційних загроз.

Алгоритм проведення аналітичного дослідження економічної безпеки такий: визначення структури негативних впливів за кожною функціональною складовою економічної безпеки підприємства, відокремлення об'єктивних і суб'єктивних негативних впливів; формування системи заходів, що були вжиті підприємством до моменту проведення оцінки рівня його економічної безпеки для усунення негативних факторів; оцінка ефективності вжитих заходів із точки зору ефективності нейтралізації окремих факторів за кожною із функціональних складових; визначення недостатньої ефективності заходів, запроваджених із метою усунення негативних факторів та запобігання можливим негативним впливам; визначення відповідальних за неефективність реалізації запланованих заходів із підвищення рівня безпеки; визначення переліку очікуваних негативних впливів, до якого мають бути зараховані всі можливі негативні фактор, що не були усунуті, вплив яких може поширюватись в майбутньому; розробка рекомендацій щодо усунення негативних впливів та запобігання можливим; оцінювання вартості кожного із запропонованих заходів щодо усунення негативних впливів та визначення виконавців, відповідальних за проведення заходів.

У процесі аналітичного дослідження використовують *карту функціонального аналізу економічної безпеки підприємства*. При заповненні такої карти негативні фактори, що разом впливають на декілька функціональних складових економічної безпеки, повинні окремо

враховуватися по всіх складових, що змінились. При цьому збитки і ефекти слід також розділяти на відповідні складові, а вартість заходів у разі їх повторення в різних складових повинна враховуватися в бюджеті тільки один раз. Створення карти функціонального аналізу економічної безпеки підприємства дозволяє вирішувати одночасно сукупність найважливіших проблем забезпечення його економічної безпеки.

Оцінюючи значення фінансових збитків від очікуваних, реалізованих та відвернутих негативних впливів, можна отримати достовірне уявлення про масштаби потенційного, відверненого і зазнаного підприємством збитку від сукупності негативних впливів на його економічну безпеку. Також через аналіз питомої ваги функціональних збитків у загальному сукупному збитку можна досить точно оцінити значущість функціональних складових економічної безпеки підприємства.

Принцип розрахунку питомої ваги функціональних складових економічної безпеки підприємства на основі аналізу збитків дозволяє визначити однорідний параметр дослідження складно вимірюваних іншими засобами функціональних складових економічної безпеки, і тому цей метод є ефективним при розв'язанні проблеми оцінки функціональних складових економічної безпеки підприємства.

Оцінка ефективності діяльності структурних підрозділів на основі співвідношення бюджетів, з одного боку – на проведення заходів для запобігання негативних впливів і з другого – даних по збитках, що були попереджені, але все ж таки реалізувалися, дає об'єктивну і підкріплену фінансовими розрахунками картину ефективності діяльності усіх структурних підрозділів підприємства як в розрізі забезпечення функціональних складових економічної безпеки підприємства, так і всієї роботи підрозділу в цілому.

Тема 6. Техніка моніторингу та критерії оцінки результатів підрозділу аналітичного забезпечення економічної безпеки підприємства

Під *моніторингом* оцінювання рівня економічної безпеки підприємства розуміють механізм постійного спостереження за основними показниками поточної діяльності в умовах постійних змін кон'юнктури ринку. Побудова системи моніторингу економічної діяльності підприємства повинна ґрунтуватися на використанні таких принципів: *принцип вибору для спостереження найбільш важливих показників* економічної діяльності підприємства, які відображають пріоритетні напрями діяльності підприємства і, відповідно, системи контролю; *принцип розроблення системи інтегральних показників*, які відображають фактичні результати економічної діяльності у розрізі різних її аспектів; *принцип встановлення періодичності формування звітної бази даних*, що визначається необхідністю оперативного реагування, тобто своєчасністю здійснення внутрішнього контролю за окремими аспектами економічної діяльності; *принцип встановлення критичних розмірів відхилень фактичних результатів економічної діяльності від заданих*, який припускає, що на кожному підприємстві, з урахуванням специфіки його діяльності, має встановлюватися величина допустимих відхилень. Розмір цих відхилень повинен зменшуватися із збільшенням величини часового періоду спостереження (наприклад, для декади величина відхилення може становити приблизно 20 %, для місяця – приблизно 15 %, для кварталу – приблизно 10 %). У випадку виявлення відхилень фактичних результатів економічної діяльності від наперед заданих даних можна використовувати три стратегії поведінки: «бездіяльність» – ця форма реагування використовується у випадку, коли величина відхилень є значно нижча за допустиме критичне відхилення; «усунення відхилень» – для забезпечення

виконання нормативних або планових показників діяльності підприємства доцільне розроблення і впровадження відповідних управлінських рішень; «зміна системи нормативних або планових показників» – така система дій допустима в тих випадках, коли виконання встановлених нормативних і планових показників є нереальним і вимагає перегляду відповідних критичних значень; *принцип виявлення резервів*, який використовують для нормалізації фінансової діяльності та підвищення її ефективності, пов'язаний із застосуванням стратегії «усунення відхилення». У цьому випадку аналіз резервів проводиться з врахуванням окремих аспектів фінансової діяльності підприємства.

Система організації механізму моніторингу безпеки економічної діяльності підприємства може використовуватися як у процесі поточної діяльності підприємства, так і для диверсифікації та зміни його стратегічних цілей розвитку.

В процесі моніторингу для окремого підприємства, залежно від масштабу виробництва, визначається рівень та чинники економічної безпеки. У той же час у межах різних видів підприємств можуть існувати однакові чинники, які визначені станом економіки держави загалом (стан споживчого попиту, стан фінансово-кредитного сектора тощо). Проте вплив цих спільних чинників на кожен вид підприємства відрізнятиметься. Аналогічна ситуація характерна для різних підприємств залежно від їхньої галузевої приналежності.

Процес оцінювання стану і рівня економічної безпеки підприємства включає такі *кроки*: вибір критерію ефективності економічної безпеки, який характеризує ступінь наближення підприємства до безпечного стану; побудова множини показників (індикаторів) економічної безпеки; визначення порогових значень показників (індикаторів); моніторинг вибраних показників і зіставлення їх фактичних значень із пороговими; визначення інтегрального рівня економічної безпеки підприємства за обраними показниками.

Критичному рівню безпеки відповідає найнижчий стан, при якому найвищою є ймовірність припинення діяльності підприємства. У підприємства на стадії банкрутства суттєво знижується потреба у забезпеченні високого рівня прибутковості праці, витратомісткості. Тому про критично низький рівень економічної безпеки свідчатимуть передусім індикатори в межах таких функціональних складових, як силова та фінансова (наявність злочинних посягань, рейдерство, неправомірні та незаконні дії з боку органів державного управління і контролю, інших ринкових суб'єктів, збитковість діяльності, незадовільні показники фінансової стійкості, ліквідності та платоспроможності).

Передкритичним є такий стан економічної безпеки, при якому господарська діяльність суб'єкта господарювання неспроможна забезпечити належні обсяги доходу та є збитковою. На цьому рівні найважливішимискладовими економічної безпеки виступають фінансова та інформаційна, нездатність забезпечення належного рівня яких може призвести до зниження безпеки, а отже й до ліквідації підприємства. Індикаторами на цьому рівні забезпечення економічної безпеки, які свідчать про негативні тенденції у господарській діяльності первинної ланки економіки, виступають коефіцієнт автономії та маневрування, а також рентабельність доходу.

При *задовільному* рівні економічної безпеки підприємство здатне вести прибуткову діяльність, проте йому бракує висококваліфікованого персоналу, високою є плінність кадрів та низькою – ефективність їх праці. На цьому рівні підприємство неспроможне забезпечити споживачів товарами високої якості, що, у свою чергу, впливає на його імідж та господарський стан. Основні індикатори: коефіцієнт відношення продуктивності праці до середньої заробітної плати, рентабельність діяльності підприємства, фондоозброєність та плінність кадрів.

Найвищому (прийнятному) рівню безпеки відповідає такий стан функціонування підприємства, при якому проводиться достатньо ефективна господарська діяльність із невисокою ймовірністю настання зовнішніх та внутрішніх загроз. За такого стану безпеки підприємством сформована надійна система її забезпечення, що дозволяє управляти всіма її функціональними складовими, своєчасно виявляти та знешкоджувати загрози.

Тема 7 Сучасні технології проведення аналітичної роботи в галузі економічної безпеки підприємства

Аналіз діяльності підприємств у галузі економічної безпеки безпеки та показує технологію його проведення. Централізованими в цій технології є: збір; обробка; передача; видача інформації. На сучасному етапі існують 4 способи обробки і переробки інформації: ручний; механізований; автоматизований; автоматичний.

При *ручному* способі інформація оброблюється працівником апарату управління. При *механічному* способі інформація оброблюється при допомозі технічних засобів. При *автоматизованому* способі основу складають ЕОМ, які виконують найбільш трудомісткі роботи по обробці потоків інформації. При *автоматичному* способі, який носить чисто машинний характер, збір, обробка і видача інформації проводиться за допомогою програмних пристроїв.

Технологія проведення аналітичного процесу з питань економічної безпеки передбачає виконання таких *робіт*: складання плану проведення аналітичної роботи з питань економічної безпеки, в якому вказується перелік питань, що підлягають аналізу, строки і відповідальні за виконання або проведення робіт; перевірка достовірності інформації; вибір методики аналізу тих чи інших показників,

які використовують в галузі економічної безпеки підприємств; обробка аналітичної інформації та підрахунок резервів росту ефективності виробництва; складання аналітичних записок, формування висновків, в яких наводяться пропозиції для усунення виявлених недоліків.

На практиці використовують різні методи оцінювання рівня економічної безпеки підприємства.

Методи експертного оцінювання використовують для опису кількісних і якісних характеристик досліджуваних процесів, зокрема для побудови логічних правил вибору рішень, які формують експерти на основі власних уявлень та знань про будь-яку галузь проблем; розроблення бального оцінювання рівня економічної безпеки на основі аналізу результатів розпізнавання фактичних індикаторів економічної безпеки за допомогою послідовних правил вибору, отриманих після навчання на запропонованих навчальних наборах індикаторів економічної безпеки.

Метод аналізу й обробки сценаріїв (сценарний підхід) передбачає багатоваріантний ситуаційний розгляд системи фінансової безпеки підприємства. *Сценарій* – це динамічна модель майбутнього, яка описує хід подій із передбаченням ймовірності їх реалізації. Сценарій відрізняється від прогнозу тим, що завдання прогнозу – передбачити специфічну ситуацію та бути прийнятим або відхиленим із урахуванням переваг і недоліків.

Для моделювання економічної безпеки підприємства використовують *методи оптимізації*, які полягають у виборі найкращого варіанта рішення із багатьох можливих (допустимих). Застосування методів оптимізації до управління економічною безпекою підприємства дає змогу вибрати такий режим його функціонування, який забезпечить досягнення екстремального значення цільової функції системи економічної безпеки (наприклад, величини прибутку (доходу) підприємства).

Теоретико-ігрові методи використовують для аналізу багатосторонніх конфліктних ситуацій, тобто ситуацій, коли інтереси учасників конфлікту є протилежними або не збігаються. Умовами застосування теоретико-ігрових методів є невизначеність та неповнота інформації. До них відносять теорію статистичних рішень, теорію ігор. Методи ігрового моделювання застосовують для розв'язання задач встановлення позиції підприємства на ринку, наприклад для визначення частки ринку, яку займає підприємство, за обмеженої множини допустимих стратегій поведінки.

Для дослідження стану та поведінки таких багатовимірних об'єктів доцільно застосовувати добре розвинутий апарат *економетрії*, наприклад методи кореляційно-регресійного аналізу. Економетричне дослідження системи економічної безпеки підприємства дозволяє досліджувати залежності між окремими чинниками цієї системи, а також аналізувати характеристики швидкості та інтенсивності динаміки стану економічної безпеки суб'єкта господарювання.

Після оцінювання рівня економічної безпеки підприємства *виникає проблема прогнозування її розвитку*. Під прогнозом розуміють науково обґрунтоване судження стосовно можливих станів об'єкта в майбутньому, альтернативні напрями і терміни їх здійснення. Під час прогнозування необхідно враховувати динаміку внутрішнього й зовнішнього середовищ. Методи прогнозування: *експертний метод*, базований на мобілізації професійного досвіду та інтуїції висококваліфікованих експертів для одержання прогнозів, що не мають кількісних характеристик; *екстраполяція*, яка полягає у дослідженні ретроспективних даних про розвиток об'єкта та перенесення закономірностей цього розвитку на майбутнє; *нейронні мережі* - обчислювальні структури, що моделюють прості біологічні процеси, які асоціюються з процесами людського мозку, їх можна також

використовувати для дослідження задач, розв'язування яких здійснюють за допомогою лінійних методів алгоритмів, а також статистичних методів аналізу (кореляційно-регресійний, кластерний, дискримінантний аналіз, аналіз часових рядів тощо); *математична теорія нечітких множин і нечітка логіка* використовують для моделювання економічних систем в умовах істотної невизначеності та інтерпретації класичних ймовірнісних й експертних оцінок рівня економічної безпеки підприємства; *моделі оцінювання схильності підприємства до банкрутства* – найбільше застосовуються економіко-математичні методи прогнозування банкрутства підприємства, зокрема *дискримінантний аналіз банкрутства*. (на основі Z-критерію Альтмана, модель Р. Ліса, метод рейтингового числа, прогнозна модель Таффлера, модель Спрінгейта тощо).

Аналіз і прогнозування рівня економічної безпеки підприємства можна також здійснювати за допомогою *трендових моделей*. Для цього застосовують два підходи: прогноз рівня економічної безпеки підприємства розраховано за допомогою моделі на основі розроблених прогнозів окремих показників, які визначають рівень його економічної безпеки; прогноз рівня економічної безпеки підприємства розроблено за допомогою побудованої трендової моделі інтегрального показника рівня економічної безпеки.

Аналіз рівня економічної безпеки підприємства можна також здійснювати на основі *економетричних симульативних моделей*, тобто систем кореляційно-регресійних рівнянь, які описують залежність між змінними. Симульативні моделі дають змогу врахувати структуру взаємозв'язків між ендогенними та екзогенними змінними, забезпечують системний підхід до дослідження фінансової безпеки підприємства.

Тема 8 Документування і документообіг в установі, організації, підприємстві та безпека комунікацій

Документообіг – це рух документів на підприємстві (в організації) з моменту їхнього створення або одержання до: завершення виконання; відправлення адресатові; передачі в архів.

Документообіг і організація управлінського процесу тісно пов'язані між собою і взаємозалежні. Від чіткості й оперативності руху, опрацювання документів та їх передавання на виконання залежить швидкість отримання інформації, необхідної для прийняття управлінського рішення. Недостатньо продуманий документообіг спричинює в установі зволікання з виконанням: на передавання документів з однієї інстанції до іншої витрачається в кілька разів більше часу, ніж на роботу з ними.

За умови чіткого розподілу функціональних обов'язків між керівником, його заступниками, структурними підрозділами і співробітниками значна частина документів відразу надходить до заступників керівника або до структурних підрозділів та безпосередніх виконавців, тобто шлях документів є значно коротшим. Так само від узвичаєного в установі порядку розподілу обов'язків і делегування повноважень співробітникам апарату залежить рух документів під час їх погодження та підписання. Рационалізація документообігу установи сприяє підвищенню ефективності роботи управлінського апарату, разом з тим форми і методи організації управлінської діяльності зумовлюють чіткість та оперативність документообігу. Оптимізації документообігу можна досягти шляхом скорочення кількості інстанцій, через які проходять документи, зменшення кількості і прискорення операцій з опрацювання документів, скорочення обсягу документообігу за рахунок застосування бездокументних зв'язків (телефон,

факс, електронна пошта, особисті переговори). Раціональна організація документообігу передбачає: прямоточний рух документів (документи мають проходити найкоротшим шляхом, без повторних переміщень); скорочення інстанцій, до яких мають потрапляти документи (наприклад, під час погодження); одноразовість операцій з опрацювання документів, уникнення паралелізму і дублювання у роботі з ними (це досягається централізацією, зосередженням однотипних операцій в одному місці); раціональне розташування в установі структурних підрозділів і робочих місць. Виконання зазначених вимог можливе лише за умови ретельно продуманої технології опрацювання документів, послідовності виконуваних операцій. Мають бути розроблені схеми документообігу, маршрутні й технологічні карти на службову документацію. Комплекс операцій, виконуваних з документами, можна представити у вигляді оперограми. *Оперограма* – організаційний документ, що регламентує процес опрацювання вхідних або вихідних документів, складений за допомогою таблиці, рядки якої відведено для позначення операцій з обліку, реєстрації, погодження тощо, а колонки (графи) – для зазначення відповідальних виконавців. Графічний спосіб дає можливість встановити логічні зв'язки між різними етапами роботи з певними видами документів в установі, простежити послідовність такої роботи та її зміст.

Безупинний процес формування та обробки економічної інформації, необхідність її швидкого пошуку та збереження вимагають використання інформаційних систем (далі – ІС), що потребують захисту від випадкового або навмисного втручання в нормальний процес її функціонування, від спроб розкрадання (несанкціонованого отримання) інформації, модифікації або фізичного руйнування її компонентів, тобто здатність протидіяти різним впливів на ІС. Під загрозою безпеки інформації розуміються події або дії, які можуть призвести до спотворення, несанкціонованого

використання або навіть до руйнування інформаційних ресурсів керованої системи, а також програмних і апаратних засобів.

Створення систем інформаційної безпеки в ІС і ІТ ґрунтується на оптимальному поєднанні взаємозалежних організаційних, програмних, апаратних, фізичних і інших властивостей, підтверджених практикою створення вітчизняних і закордонних систем захисту й застосовуваних на всіх етапах технологічного циклу обробки інформації. Принципи захисту комунікацій достатньо багаточисельні. Основні з них наступні.

Принцип безперервного розвитку системи – є одним із основних для систем інформаційної безпеки (далі – СІБ). Це безперервний процес, що полягає в обґрунтуванні й реалізації найбільш раціональних методів, способів і шляхів удосконалювання СІБ, безперервному контролю, виявленні її вузьких і слабких місць, потенційних каналів витоку інформації й нових способів несанкціонованого доступу.

Поділ і мінімізація повноважень з доступу до оброблюваної інформації й процедур обробки, тобто надання як користувачам, так і самим працівникам

Повнота контролю й реєстрації спроб несанкціонованого доступу, тобто необхідність точного встановлення ідентичності кожного користувача й протоколювання його дій для проведення можливого розслідування, а також неможливість здійснення будь-якої операції обробки інформації в ІТ без її попередньої реєстрації.

Забезпечення надійності системи захисту, тобто неможливість зниження рівня надійності при виникненні в системі збоїв, відмов, навмисних дій зломщика або ненавмисних помилок користувачів і обслуговуючого персоналу.

Забезпечення контролю за функціонуванням системи захисту, тобто створення засобів і методів контролю працездатності механізмів захисту.

Забезпечення будь-яких засобів боротьби зі шкідливими програмами. Забезпечення економічної доцільності використання системи захисту,

що виражається в перевищенні можливого збитку ІС і ІТ від реалізації загроз над вартістю розробки й експлуатації систем інформаційної безпеки.

У результаті вирішення проблем безпеки інформації мають бути наступні основні *ознаки*: наявність інформації різного ступеня конфіденційності; забезпечення криптографічного захисту інформації різного ступеня конфіденційності при передачі даних; ієрархічність повноважень суб'єктів доступу до програм до компонентів ІС і ІТ (до файлів-серверів, каналів зв'язку й т. п.); обов'язковим керуванням потоками інформації як у локальних мережах, так і при передачі каналами зв'язку на далекі відстані; наявність механізму реєстрації й обліку спроб несанкціонованого доступу, подій в ІС і документів, виведених на друк; обов'язковість забезпечення цілісності ПЗ й інформації в ІТ; обов'язковість обліку магнітних носіїв; наявність фізичної охорони засобів обчислювальної техніки й магнітних носіїв; наявність спеціальної служби ІБ системи.

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

Основна

1. Ареф'єва О. В. Планування економічної безпеки підприємств / О. В. Ареф'єва, Т. Б. Кузенко. – Київ : Видавництво Європейського ун-ту, 2004. – 169 с.
2. Барановський О. І. Фінансова безпека в Україні (методологія оцінки та механізми забезпечення) / О. І. Барановський; Київ. нац. торг.-екон. ун-т. – Київ. : 2004. – 759 с.
3. Берлач А. І. Безпека бізнесу : навч. посібник / А. І. Берлач. – Київ: Університет «Україна», 2007. – 280 с.
4. Бланк И. А. Управление финансовой безопасностью предприятия/ И. А. Бланк. – Київ : Ника-Центр, Эльга, 2004. – 784 с.
5. Інформаційна та кібербезпека / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа. – Київ: ДУТ, 2015. – 288 с.
6. Кузнецов О. О. Захист інформації та економічна безпека підприємства : монографія / О. О. Кузнецов, С. П. Євсеев, С. В. Кавун. – Харків : ХНЕУ, 2008. – 360 с.
7. Моделювання економічної безпеки : держава, регіон, підприємство : монографія. / Геєць В. М., Кизим М. О., Клебанова Т. С., Черняк О. І. та ін. ; За ред. Гейця В. М. – Харків : ВД «ІНЖЕК», 2006. – 240 с.
8. Економічна безпека : навч. посібник / З. С. Варналій, П. В. Мельник, Л. Л. Тарангул та ін. ; за ред. д-ра екон. наук, проф. З. С. Варналія. – Київ : Знання, 2009. – 647 с.
9. Куркин Н. В. Управление экономической безопасностью развития предприятия / Н. В. Куркин. – Днепропетровск : Изд. АРТ-ПРЕСС, 2006. – 452 с.
10. Фінансова безпека підприємства: навчальний посібник / Т. Б. Кузенко, О. В. Грачов, Л. С. Мартюшева та ін. – Харків : Вид. ХНЕУ, 2010. – 300 с.

Додаткова

1. Андрощук Г. А. Экономическая безопасность предприятия : защита коммерческой тайны : монография / Г. А. Андрощук, П. П. Крайнев; ред. А. Д. Святоцкий. – Київ : ВД «Ін Юре», 2000. – 400 с.

2. Артемов В. Ю. Основи менеджменту для інформаційних аналітиків : курс лекцій / В. Ю. Артемов. – Київ : КНТ, 2007. – 272 с.

3. Богушов В. О. Безпека у сфері економічних відносин / В. О. Богушов. – Суми : УАБС НБУ, 2007. – 60 с.

4. Камлик М. І. Економічна безпека підприємницької діяльності. Економіко-правовий аспект : навчальний посібник / М. І. Камлик. – Київ : Атіка, 2005. – 432 с.

5. Кузнецов О. О. Захист інформації та економічна безпека підприємства: монографія / О. О. Кузнецов, С. П. Євсєєв, С. В. Кавун. – Харків : Вид. ХНЕУ, 2008. – 360 с.

6. Соснин А. С. Менеджмент безопасности предпринимательства : учеб. пособие / А. С. Соснин, П. Я. Прыгунов. – Київ : Изд-во Европ. ун-та, 2002. – 559 с.

Інформаційні ресурси

1. ЛигаБизнесИнформ. – [Електронний ресурс] – Режим доступу : www.liga.net.

2. Офіційний сайт Верховної Ради України. [Електронний ресурс] – Режим доступу : <http://rada.gov.ua>.

3. Офіційний сайт Державної служби статистики. [Електронний ресурс] – Режим доступу : www.ukrstat.gov.ua.

4. Офіційний сайт Інституту проблем законодавства ім. Ярослава Мудрого. [Електронний ресурс] – Режим доступу : <http://www.legality.kiev.ua>.

5. Офіційний сайт Кабінету Міністрів України

«Урядовий портал України». [Електронний ресурс] – Режим доступу: <http://www.kmu.gov.ua>.

6. Цифровий репозиторій ХНУМГ ім. О. М. Бекетова [Електронний ресурс] – Режим доступу: <http://eprints.kname.edu.ua>

7. Сервер Верховної Ради України. [Електронний ресурс]– Режим доступу : [www.zakon](http://www.zakon.gov.ua).