Додаток 4

**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ**

# **Дніпропетровський державний університет внутрішніх справ**

**КАФЕДРА ЕКОНОМІЧНОЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**

# **лекції НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

**Ідентифікація загроз безпеці підприємництва**

# 

Освітній ступінь магістр

(назва ступеня вищої освіти)

Спеціальність 262 «Правоохоронна діяльність»

Освітня програма освітньо-професійна підготовки магістра

Правоохоронна діяльність

Форма навчання денна / заочна

(денна/заочна)

у 2019 / 2020 навчальному році

Лекції обговорені та схвалені на засіданні

кафедри економічної та інформаційної безпеки

протокол від 27.08.2019  № 14

**Керівник кафедри**

**Едуард РИЖКОВ**

\_\_\_\_\_\_\_\_\_\_\_\_

(підпис)

**Дніпро – 2019**

Ідентифікація загроз безпеці підприємництва // Лекції для денної/заочної форм навчання. – Дніпро: Дніпропетровський державний університет внутрішніх справ, 2019. – 79 с.

**РОЗРОБНИК**:

Рибальченко Л.В., доцент кафедри економічної та інформаційної безпеки, кандидат економічних наук.

**Лекція №1**

**Тема 1. Основи безпеки підприємництва** (1 год)

План лекції

Вступ

1.Суть та зміст безпеки підприємництва, її мета і завдання.

2. Засоби і методи забезпечення безпеки підприємства

# **РЕКОМЕНДОВАНА ЛІТЕРАТУРА**

1. Економічна та майнова безпека бізнесу: навчальний посібник / Б.М. Андрушків, Л.Я. Малюта. –Тернопіль: ФОП Паляниця В.А., 2016. – 180 с.

2.Економічна безпека підприємства : навчальний посібник / [Небава М. І., Міронова Ю.В.] – Вінниця : ВНТУ, 2017. – 73 с

3. Раєвнева О. В. Управління розвитком підприємства: методологія, механізми, моделі: Монографія/ О. В. Раєвнева. - Харків: ІНЖЕК, 2016. - 496 с.

4.Моделювання економічної безпеки: держава, регіон, підприємство: Монографія/ В. М. Гаєць, М. О. Кизим, Т. С. Клебанова, О. І. Черняк. - Х. : ІНЖЕК, 2016. - 240 с.

5**.** Рибальченко Л.В., Сенько В.В. Зміст і переваги комплексного підходу до забезпечення економічної безпеки підприємства / Міжнародної наукової конференції «Динаміка розвитку сучасної науки» 15 листопада 2019 р., м.Чернігів. С-40-43.

**МЕТА ЛЕКЦІЇ**

Метою лекції є надання необхідних теоретичних знань здобувачам вищої освіти юридичного факультету, що навчаються на магістерському рівні вищої освіти, щодо основних понять безпеки підприємництва, засобів і методів забезпечення безпеки підприємства.

**ВСТУП**

Безпека підприємства передбачає стійкий розвиток (тобто збалансований і безупинний), що досягається за допомогою використання усіх видів ресурсів і підприємницьких можливостей, за якими гарантується найбільш ефективне їх використання для стабільного функціонування та динамічного науково-технічного й соціального розвитку, запобігання внутрішнім і зовнішнім негативним впливам (загрозам).

Найбільш поширеним є визначення безпеки підприємства як стану ефективного використання його ресурсів (ресурсів капіталу, персоналу, інформації і технології, техніки та устаткування, прав) і існуючих ринкових можливостей, що дозволяє запобігати внутрішнім і зовнішнім негативним впливам (загрозам) і забезпечити його тривале виживання і стійкий розвиток на ринку відповідно до обраної місії.

Об’єктами безпеки є держава, суспільство і суспільні об’єднання, регіони, підприємства і окремі громадяни.

Необхідність постійного дотримання безпеки зумовлюється об'єктивно наявним для кожного суб'єкта господарювання завданням забезпечення стабільності функціонування та досягнення головних цілей своєї діяльності. Рівень економічної безпеки фірми залежить від того, наскільки ефективно її керівництво і спеціалісти (менеджери) будуть спроможні уникнути можливих загроз і ліквідувати шкідливі наслідки окремих негативних складових зовнішнього і внутрішнього середовища.

**І. ПИТАННЯ**

Суть та зміст безпеки підприємництва, її мета і завдання

В умовах розвитку відносин, коли держава вже не несе відповідальності за результати фінансово-господарської діяльності підприємства, забезпечення безпеки стає однією з найбільш важливих і актуальних проблем його життєдіяльності.

Серед вітчизняних і зарубіжних учених немає єдиного визначення терміну „безпека”. Разом з тим, принципових розходжень у підходах до трактування змісту даної категорії не спостерігається. Серед різних тлумачень цих понять є наступні:

-     безпека підприємства – це становище найбільш ефективного використання ресурсів для запобігання загроз і забезпечення стабільного функціонування підприємства на теперішній час і в майбутньому;

-     безпека підприємства – це захищеність його діяльності від негативного впливу зовнішнього оточення, а також здатність своєчасно усунути різноманітні загрози або пристосуватися до існуючих умов, які не відбиваються негативно на його діяльності;

-     безпека підприємства це комплекс заходів, які сприяють підвищенню фінансової стійкості господарчих суб’єктів за умов ринкової економіки, які захищають їх комерційні інтереси від впливу негативних ринкових процесів;

-     безпека підприємства – це сукупність чинників, які забезпечують незалежність, стійкість, здатність до прогресу в умовах дестабілізуючих факторів;

-     безпека підприємства (господарюючого суб'єкта) – це захищеність його науково-технічного, технологічного, виробничого та кадрового потенціалу від прямих (активних) або непрямих (пасивних) загроз.

Джерелами негативних впливів на безпеку підприємства можуть бути:

1) свідомі чи несвідомі дії окремих посадових осіб і суб'єктів господарювання (органів державної влади, міжнародних організацій, підприємств-конкурентів);

2) збіг об'єктивних обставин (стан фінансової кон'юнктури на ринках даного підприємства, наукові відкриття та технологічні розробки, форс мажорні обставини тощо). Залежно від суб'єктної обумовленості негативні впливи на безпеку можуть мати об'єктивний і суб'єктивний характер. Об'єктивними вважаються такі негативні впливи, які виникають не з волі конкретного підприємства, або його окремих працівників. Суб'єктивні впливи мають місце внаслідок неефективної роботи підприємства в цілому або окремих його працівників (передовсім керівників і функціональних менеджерів).

Головна мета безпеки підприємства полягає в тому, щоб гарантувати його стабільне та максимально ефективне функціонування тепер, і високий потенціал розвитку в майбутньому.

До основних функціональних цілей безпеки належать:

-     забезпечення високої фінансової ефективності роботи, фінансової стійкості та незалежності підприємства;

-     забезпечення технологічної незалежності та досягнення високої конкурентоспроможності технічного потенціалу того чи іншого суб'єкта господарювання;

-     досягнення високої ефективності менеджменту, оптимальної та ефективної організаційної структури управління підприємством;

-     досягнення високого рівня кваліфікації персоналу та його інтелектуального потенціалу;

-     мінімізація руйнівного впливу результатів виробничо-господарської діяльності на стан навколишнього середовища;

-     якісна правова захищеність усіх аспектів діяльності підприємства;

-     забезпечення захисту інформаційного поля, комерційної таємниці і досягнення необхідного рівня інформаційного забезпечення роботи всіх підрозділів підприємства та відділів організації;

-     ефективна організація безпеки персоналу підприємства, його капіталу та майна, а також комерційних інтересів.

Головна та функціональні цілі зумовлюють формування необхідних структуроутворюючих елементів і загальної схеми організації безпеки підприємства.

Забезпечення безпеки передбачає виділення, аналіз і оцінку існуючих загроз з кожної функціональної складової та розроблення на їх основі системи протидіючих і застережних заходів.

Отже, безпека підприємництва являє собою універсальну категорію, що відбиває захищеність суб'єктів соціально-економічних відносин на всіх рівнях, починаючи з держави і закінчуючи кожним її громадянином. Зміст даного поняття містить у собі систему засобів, що забезпечують конкурентопотенційність і економічну стабільність підприємства а також сприяють підвищенню рівня добробуту робітників і тільки за здійснення в необхідному обсязі зазначених дій можна буде досягти належного рівня безпеки підприємства.

Система безпеки кожного підприємства цілком індивідуальна. Її повнота та дієвість залежать від існуючої в державі законодавчої бази, від обсягу матеріально-технічних та фінансових ресурсів, виділених керівниками підприємств, від розуміння кожним з працівників важливості забезпечення безпеки бізнесу, а також від досвіду роботи керівників служб безпеки підприємств.

Надійний захист безпеки підприємства можливий лише при комплексному та системному підході до її організації. Тому в економіці має місце таке поняття як система безпеки підприємства.

Система безпеки підприємства – це комплекс організаційно-управлінських, режимних, технічних, профілактичних і пропагандистських заходів, спрямованих на кількісну реалізацію захисту інтересів підприємства від зовнішніх та внутрішніх загроз.

Основними елементами системи безпеки підприємства є:

1) захист комерційної таємниці та конфіденційності інформації;

2) комп’ютерна безпека;

3) внутрішня безпека;

4) безпека будинків та споруд;

5) фізична безпека;

6) технічна безпека;

7) безпека зв’язку;

8) безпека господарсько-договірної діяльності;

9) безпека перевезень вантажів та осіб;

10) безпека рекламних, культурних, масових заходів, ділових зустрічей та переговорів;

11) протипожежна безпека;

12) екологічна безпека;

13) радіаційно-хімічна безпека;

14) конкурентна розвідка;

15) інформаційно-аналітична робота;

17) експертна перевірка механізму системи забезпечення.

***Алгоритм побудови системи безпеки підприємства***

Система безпеки підприємства може бути побудована на основі наступних принципів:

1) Пріоритет заходів попередження. Зміст цього принципу полягає у своєчасному виявленні тенденцій та передумов, що сприяють розвитку загроз.

2) Законність. Заходи безпеки підприємства розробляються на основі та в межах діючих правових актів.

3) Комплексне застосування сил та коштів. Для забезпечення безпеки використовуються всі наявні в розпорядженні підприємства ресурси та кошти.

4) Координація та взаємодія ззовні та всередині підприємства. Тобто протидія загрозам здійснюється завдяки об’єднанню зусиль усіх підрозділів та служб підприємств.

6) Компетентність. Працівники повинні вирішувати питання безпеки на професійному рівні.

7) Економічна доцільність. Вартість фінансових витрат на забезпечення безпеки підприємства не повинна перевищувати оптимального рівня, при якому губиться економічний зміст їх застосування.

8) Планова основа діяльності. Діяльність по забезпеченню безпеки повинна будуватися на основі комплексної програми забезпечення безпеки підприємства, підпрограм забезпечення безпеки по основним її видам та розроблених для їх виконання планів роботи підрозділів підприємства.

9) Системність. Цей принцип припускає врахування усіх факторів, здійснюючих вплив на безпеку підприємства.

Забезпеченням безпеки підприємства займаються дві групи суб’єктів. Суб’єкти безпеки підприємства. Друга група зовнішні органи та організації, які функціонують самостійно і не підкоряються керівництву підприємства, але при цьому їх діяльність здійснює істотний вплив на безпеку підприємства Суб’єктами цієї групи є:

1) Законодавчі органи;

2) Органи виконавчої влади;

3) Суди;

4) Правоохоронні органи;

5) Науково-освітні заклади.

Вони інколи (а іноді й ніколи) приєднуються до діяльності підприємства щодо забезпечення його економічної безпеки. Організаційною формою такого приєднання може стати комплексна програма безпеки підприємства, в якій необхідно передбачати форми і методи цієї роботи. Крім того, можна рекомендувати розробку планів структурних підрозділів та всього підприємства в цілому по організації взаємодії з вищевказаними органами та організаціями напівспеціалізовані суб’єкти, у яких частина функцій спрямована на забезпечення безпеки підприємства (маркетингова служба, юридичний підрозділ тощо) решта персоналу та підрозділи підприємства, які в межах своїх посадових інструкцій та положень про підрозділи зобов’язані вживати заходів з метою забезпечення безпеки підприємства.

**ІІ. ПИТАННЯ**

**Засоби і методи забезпечення безпеки підприємства**

Серед існуючих засобів забезпечення безпеки підприємства можна виокремити наступні:

1) Технічні засоби. До них відносяться охоронно-пожежні системи, відео-радіоапаратура, засоби виявлення вибухових приладів, бронежилети, огородження тощо.

2) Організаційні засоби. Створення спеціалізованих оргструктурних формувань, що забезпечують безпеку підприємства.

3) Інформаційні засоби. Передусім це друкована і відеопродукція з питань збереження конфіденційної інформації. Крім цього, важлива інформація для прийняття рішень з питань економічної безпеки зберігається на комп’ютерах.

4) Фінансові засоби. Без достатніх фінансових коштів не можливе функціонування системи безпеки підприємства, питання лиш в тому, щоб використати їх цілеспрямовано та з високою віддачею.

5) Правові засоби. Підприємство повинне у своїй діяльності керуватися не лише виданими вищестоящими органами влади законами та підзаконними актами, але й розробляти власні локальні правові акти з питань забезпечення безпеки підприємства.

6) Кадрові засоби. Підприємство повинне бути забезпечене кадрами, що займаються питаннями його безпеки.

7) Інтелектуальні засоби. Залучення до роботи кваліфікованих спеціалістів, наукових робітників, що дозволяє модернізувати систему безпеки підприємства

Одночасне впровадження усіх цих засобів неможливе. Воно проходить в кілька етапів:

I етап. Виділення фінансових ресурсів.

II етап. Формування кадрових і організаційних засобів.

III етап. Розробка системи правових засобів.

IV етап. Залучення технічних, інформаційних та інтелектуальних засобів.

Переведені з статичного в динамічний стан вищевказані засоби перетворюються в методи забезпечення безпеки підприємства. Відповідно можна виділити технічні, інформаційні, фінансові, правові, інтелектуальні методи. Наведемо стислий перелік цих методів

1. технічні — спостереження, контроль, ідентифікація;

2. інформаційні — складання характеристик на працівників, аналітичні матеріали конфіденційного характеру тощо;

3. фінансові — матеріальне стимулювання працівників, що мають досягнення в забезпеченні безпеки підприємства;

4. правові — судовий захист законних прав і інтересів, сприяння діям правоохоронних органів;

5. кадрові — підбір, навчання кадрів, що забезпечують безпеку підприємства;

6. інтелектуальні — патентування, ноу-хау тощо.

Під безпекою треба розуміти і такий стан соціально-технічної системи підприємства, котрий дає змогу уникнути зовнішніх загроз і протистояти внутрішнім чинникам дезорганізації за допомогою наявних ресурсів, підприємницьких здібностей менеджерів, а також структурної організації та зв'язків менеджменту. Зауважимо, що традиційно термін уживався в юридичній практиці для позначення системи прав зі збереження ресурсів і результатів їх продуктивного використання. Однак з економічного погляду таке трактування поняття, на нашу думку, не є вичерпним, а сам механізм збереження не входить до системи управління підприємством (що зумовлено історичним досвідом ведення бізнесу на постсоціалістичному просторі).

Головна мета управління безпекою підприємства — забезпечення найефективнішого функціонування, найпродуктивнішої роботи операційної системи та економічного використання ресурсів, забезпечення певного рівня трудового життя персоналу та якості господарських процесів підприємства, а також постійного стимулювати нарощування наявного потенціалу та його стабільного розвитку.

Система безпеки підприємства традиційно включає такі складові :

1) інтелектуальну і кадрову;

2) інформаційну;

3) техніко-технологічну;

4) фінансову;

5) політико-правову та екологічну:

6) силову.

Для аналітичної оцінки кожної з них слід визначити спектр можливих загроз (ризиків) та оцінити ймовірність і наслідки їх реалізації. За умов невизначеності існує, сказати б, суперечність між теоретично досконалим і практично можливим підходами. Теоретично досконалий підхід полягає в тому, щоб урахувати всі, можливі варіанти сценаріїв руху грошових потоків. Однак практично це здебільшого неможливо зробити, оскільки доведеться враховувати надто багато альтернатив.

Суть основного завдання полягає в процедурі проведення таких розрахунків, котрі навіть у разі їх неповної адекватності уможливлювали б отримання достатньо надійних результатів, на які можна спиратися за вибору господарської альтернативи. Крім цього, слід особливо наголосити, що механізм створення безпеки має базуватися на внутрішньо системних характеристиках підприємства, тобто сама соціально-економічна система має включати «вбудовані» механізми запобігання зовнішнім і внутрішнім загрозам.

Загалом усі ризики підприємницької діяльності можна класифікувати так:

1. За сферами виявлення:

1.1. Економічний — ризик, пов'язаний зі змінами економічних факторів у ході реалізації інвестиційного проекту.

1.2. Політичний — ризик виникнення різноманітних адміністративно-законодавчих обмежень інвестиційної діяльності, які пов'язані зі зміною інвестиційної політики держави.

1.3. Соціальний — ризик страйків, здійснення під тиском робітників незапланованих соціальних програм та інші аналогічні види ризиків.

1.4. Екологічний — ризик виникнення екологічних катастроф і різних стихійних лих (землетруси, лісові пожежі, повені тощо), котрі негативно впливають на інвестиційний проект,

1.5. Інші – ризик рекету, крадіжок майна, нечесності партнерів тощо.

2. За формами інвестування:

2.1. Ризики реального інвестування — ризики, пов'язані з помилковим вибором місцезнаходження об'єкта будівництва, порушення графіків поставок необхідних матеріалів, комплектувальних деталей за проектами, суттєвим зростанням цін на інвестиційні товари, неправильним підбором підрядчиків та з іншими факторами, що знижують ефективність інвестиційного проекту.

2.2. Ризики фінансового інвестування — цю групу ризиків пов'язано з непродуманим вибором фінансових інструментів для інвестування, фінансовими труднощами чи банкрутством окремих емітентів, непередбаченими змінами умов інвестування і т. п. Ризики інвестицій у фінансові інструменти мають таку структуру:

а) ризики втраченого зиску;

б) ризики зниження дохідності, а саме: відсоткові ризики; кредитні ризики; біржові ризики; селективні ризики; ризики втрати ліквідності; ризики банкрутства.

3. За джерелами:

3.1. Системний ризик — на цей вид ризику наражаються всі учасники інвестиційної діяльності і форм інвестування. Він значною мірою визначається зміною стадій економічного розвитку країни чи кон'юнктурних циклів розвитку інвестиційного ринку та іншими аналогічними факторами, на які інвестор не може вплинути, добираючи об'єкти інвестування.

3.2. Несистемний ризик — цей вид ризику притаманний конкретному об'єкту інвестування чи діяльності конкретною інвестора. Він може бути пов'язаний з некваліфікованим менеджментом проекту, посиленням конкуренції на певному сегменті інвестиційного ринку, нераціональною структурою інвестиційних ресурсів та іншими аналогічними факторами, негативним наслідкам, яких значною мірою можна запобігти за допомогою ефективного управління інвестиційним процесом.

Для інтегральної оцінки рівня безпеки можна рекомендувати методику, що базується на використанні традиційних показників, темпів їхньої зміни та ймовірності реалізації специфічних ризиків. Процедура проведення розрахунків складається з таких етапів:

1. Визначення нормативного рівня показників кожної складової безпеки (наприклад, фінансову складову можна охарактеризувати системою показників фінансової стійкості; інформаційну — показниками ефективності інвестицій в інформаційні технології, ефективності володіння інформацією, показниками новизни інформації тощо).

2. Визначення системи цільових показників, сформованої на по­передньому етапі, на поточний період, а також визначення темпів їхньої зміни (вибір того чи іншого показника здійснюється керівництвом підприємства на базі корпоративної стратегії розвитку).

3. Визначення системи ризиків, якими переобтяжено діяльність підприємства, їх перегрупування за складовими та оцінка ймовірності їх реалізації (формування спектра можливих загроз за кожною складовою).

4. Визначення порівняльних індексів за кожним показником у розрізі складових безпеки підприємства (під порівняльним індексом слід розуміти співвідношення фактичного значення кожного показника з його нормативним (середньогалузевим) значенням).

5. Визначення рівня безпеки для кожної складової.

Таким чином, найвлучнішим є визначення безпеки підприємства як стану ефективного використання його ресурсів (ресурсів капіталу, персоналу, інформації і технології, техніки та устаткування, прав) і існуючих ринкових можливостей, що дозволяє запобігати внутрішнім і зовнішнім негативним впливам (загрозам) і забезпечити його тривале виживання і стійкий розвиток на ринку відповідно до обраної місії.

**Тема 2.** **Загрози безпеці підприємництва** (1 год)

ПЛАН ЛЕКЦІЇ

Вступ

1. Характеристика зовнішніх та внутрішніх загроз.

*2.* Банківська та фінансова безпека.

3. Шахрайство.

# **РЕКОМЕНДОВАНА ЛІТЕРАТУРА**

1. Економічна та майнова безпека бізнесу: навчальний посібник / Б.М. Андрушків, Л.Я. Малюта. –Тернопіль: ФОП Паляниця В.А., 2016. – 180 с.

2.Економічна безпека підприємства : навчальний посібник / [Небава М. І., Міронова Ю.В.] – Вінниця : ВНТУ, 2017. – 73 с

3. Раєвнева О. В. Управління розвитком підприємства: методологія, механізми, моделі: Монографія/ О. В. Раєвнева. - Харків: ІНЖЕК, 2016. - 496 с.

4.Моделювання економічної безпеки: держава, регіон, підприємство: Монографія/ В. М. Гаєць, М. О. Кизим, Т. С. Клебанова, О. І. Черняк. - Х. : ІНЖЕК, 2016. - 240 с.

5. Рибальченко Л.В., Сенько В.В. Умови розвитку управління економічною безпекою підприємництва в Україні / Міжнародної науково-практичної конференції «Пріоритетні напрями досліджень в науковій та освітній діяльності» 5-6 грудня 2019 р., м.Львів. Львівський науковий форум, С-45-47

6. Рибальченко Л.В., Гребенюк А.М. Стандарти управління інформаційною безпекою / Кібербезпека в Україні: правові та організаційні питання: матеріали міжн. наук. практ. конф., м. Одеса, 22 листопада 2019 р. Одеса : ОДУВС, 2019. 108 с. ISBN 678-717-70204

**МЕТА ЛЕКЦІЇ**

Метою лекції є надання необхідних теоретичних знань здобувачам вищої освіти юридичного факультету, що навчаються на магістерському рівні вищої освіти, щодо основних понять зовнішніх та внутрішніх загроз, ризиковості банківської та фінансової безпеки, а також шахрайства на підприємстві.

**ВСТУП**

Трансформаційні перетворення в економіці України характеризуються не тільки формуванням нових виробничих можливостей, а й зміною відносин в інших сферах життя. Переходу до ринкових відносин стали притаманні різного роду кризи, у тому числі політичного, економічного, суспільного характеру. Кризи, як правило, супроводжуються різноманітними негативними явищами в економіці:

* поширенням недобросовісної конкуренції;
* зростанням злочинності;
* появою корупції;
* збільшенням частки кримінально-тіньового сектора економіки.

За таких обставин суб'єкти підприємницької діяльності все частіше стають об'єктами різного роду загроз. Тому об'єктивно сформувалась необхідність впровадження заходів захисту бізнесу, спрямованих на створення протидії таким загрозам.

Під поняттям "загроза" розуміють реальну можливість дії навмисного чи ненавмисного характеру, яка порушує режим функціонування підприємства (фірми), завдає матеріальну або моральну шкоду, виводить зі стану стійкої рівноваги.

**І. ПИТАННЯ**

**Характеристика зовнішніх та внутрішніх загроз**

Загрози за своїм походженням поділяють на ті, що надходять ззовні (екзогенні), і ті, що виникають усередині підприємства (ендогенні).

Окрім того, ці загрози відносно людської діяльності поділяють на: об'єктивні та суб'єктивні.

**Об'єктивні** — загрози, які зумовлюються стихійними природними явищами (землетрус, повінь, буревій тощо).

**Суб'єктивні** пов'язані з діяльністю людини. Окрім того, за спрямуванням і характером впливу їх можна поділити на економічні, фізичні та інтелектуальні.

**Економічні загрози** можуть реалізуватись у формі корупції, шахрайства, недобросовісної конкуренції, використання банками неефективних технологій банківського виробництва.

**Фізичні загрози** реалізуються у формі крадіжок, пограбувань, поломок, виведення з ладу обладнання.

**Інтелектуальні загрози** проявляються у розголошенні або неправомірному використанні банківської інформації, дискредитації банку на ринку банківських послуг, а також у формі різного роду соціально-психологічних конфліктів довкола банківських установ або в них самих.

Оскільки економіка є однією із найважливіших сторін життєдіяльності людини, то проблеми економічної безпеки стають актуальними не тільки для підприємств чи окремих осіб, але й для суспільства загалом. У науковій літературі економічна безпека визначається як стан захищеності життєво важливих інтересів особи, суб'єкта підприємницької діяльності, країни, їх можливість без втручання ззовні вибирати шляхи і форми економічного розвитку та здійснювати їх реалізацію.

**Отже, економічна безпека** — це універсальне поняття, що акцентує увагу на необхідності захисту суб'єктів підприємницької діяльності на всіх рівнях — від держави до кожного громадянина. Тому збільшення кількості підприємств із високим рівнем економічної безпеки, її стійкістю від можливих загроз сприятиме зміцненню економічної безпеки України.

Безпека підприємницької діяльності тісно пов'язана з ризиками, які є невід'ємною складовою ринкової форми господарювання.

**Ризик** — це можливість відхилення результатів конкретних рішень та дій від запланованих. Вони можуть бути пов'язані як з додатковими прибутками, так і з додатковими витратами.

Отже, ризик є видом небезпеки, на яку необхідно реагувати. Чинниками небезпек економічної діяльності підприємств можуть бути:

* 1. Матеріальні та нематеріальні активи.
* 2. Фінанси.
* 3. Інформація.
* 4. Персонал.

Вищезазначений перелік сфер дії загроз дає можливість виділити певні види безпеки:

* 1. **Матеріально-технологічну безпеку (МТБ**) — це захист від можливих втрат унаслідок розкрадання нерухомості, обладнання, продукції, винаходів, програм та ін., а також захист від можливих втрат унаслідок аварій, катастроф через використання фізично застарілого устаткування, низьку кваліфікацію і безвідповідальність працівників.
* 2. **Фінансову безпеку (ФБ**) — це захист від можливих фінансових втрат і попередження банкрутства підприємства. Вона є провідною і вирішальною, оскільки за ринкових умов господарювання є "двигуном" будь-якої економічної системи.
* 3. **Інформаційну безпеку (ІБ)** — це захист конфіденційної інформації, попередження її витоку, захист програмних продуктів.
* 4. **Кадрову безпеку (КБ)**, яка полягає у попередженні і зменшенні небезпеки негативного впливу на економічну безпеку через дії недостатньо кваліфікованих працівників, неефективне управління підприємством, а також у захисті фізичної особи (життя і здоров'я) від кримінальних посягань.

Особливо уважно до своєї безпеки ставляться американці, у США функціонують знати різноманітні курси, де можна пройти спеціальну підготовку. Наприклад, охочі можуть звернутися в Інсбезпеки підприємництва тощо.

На практиці всі ці види безпеки здійснює служба безпеки (охорони), яка організовує пропускний режим, охорону будівель, споруд, приміщень, обладнання. Захищає інформацію від несанкціонованого доступу, забезпечує режим конфіденційності документів і матеріалів.

Отже, безпека підприємництва спрямована на усунення чи зменшення ризику економічних збитків.

Особливе місце в структурі підприємницької діяльності посідає банківська діяльність, яка дедалі частіше підпадає під вплив кримінальних структур.

Із впровадженням ринкових відносин банківська система стає центральною ланкою у сфері фінансово-господарських відносин. Умовно її можна назвати кровоносними судинами, що забезпечують функціонування всього господарського комплексу країни. Однак, крім законних товарно-фінансових потоків, через цілу низку чинників і обставин упродовж останніх років відбувається стрімкий процес криміналізації банківської системи. Вона стає центральним вузлом у технологічному ланцюзі з "відмивання" капіталів, здобутих злочинним шляхом, а також основним виконавцем випуску у безготівковий платіжний обіг фіктивно утворених коштів. Різке загострення криміногенної ситуації у банківській системі України викликане дією багатьох обставин, які можна поділити на дві групи.

**Перша група обставин** функціонує на загальносуспільному рівні і вбирає в себе недоліки, упущення та прорахунки у соціальній та економічній політиці, організацію управління господарським комплексом.

**Друга група обставин** зумовлена специфічними особливостями діяльності банківської системи України і, передусім, негативними наслідками розпаду єдиної державної банківської системи, недосконалістю чинної нормативно-правової бази з питань функціонування банківських структур у нових економічних умовах. Серед обставин, які сприяють скоєнню корисливих злочинів у сфері банківської діяльності, можна виділити:

* — соціально-економічні (порушення господарських зв'язків між глибоко інтегрованими підприємствами, розбалансування фінансової системи, криза платежів тощо);
* — організаційно-управлінські (відсутність спеціалістів у галузі розробки методології, організації банківської діяльності в нових економічних умовах, невизначеність чіткої концепції структурної побудови системи контролю, взаємовідносин комерційних банків з НБУ, правоохоронними та іншими контролюючими органами);
* — нормативно-правові (недосконалість чинного законодавства і відомчих нормативно-правових актів з питань регулювання сфери банківської діяльності).

Питання безпеки бізнесу в країнах з розвинутою ринковою економікою вважається знати одним із основних, а на заходи безпеки в комерційних структурах витрачається від 10 % до 15% прибутку.

**ІІ. ПИТАННЯ**

**Банківська та фінансова безпека**

Проблеми безпеки підприємницької діяльності загалом і, зокрема, банківської безпеки потрапили у сфер; зацікавлення представників української науки відносно недавно. Чинником виникнення та постійного посилення уваги до цих проблем є трансформаційна криз української економіки, що охопила всі сфери і стала суттєвою перешкодою на шляху до забезпечення сталого розвитку економіки та суспільства.

Крім того, чинником постійного посилення уваги д цієї проблеми є те, що керівники підприємницьких структур не вивчали в навчальних закладах питання банківської безпеки, що є суттєвим недоліком у їх комерційній діяльності. В умовах сучасного економічного розвитку України — це один з необхідних видів знань майбутнього підприємця.

Потрібною передумовою ефективного захисту сфери банківської діяльності від злочинних посягань є виявлення і вивчення обставин та умов, які передують здійсненню злочинів. Тільки комплексний та багатофункціональний підхід до аналізу банківської діяльності як внутрішнього (менеджмент банків, робота з клієнтом, аналіз ризиків тощо), так і зовнішнього (політика Національного банку України, дії національного та міжнародного криміналітету тощо) характеру може допомогти виявити і розробити цілеспрямовані заходи щодо запобігання криміналізації фінансово-кредитної системи. Банківська безпека є одним з основних елементів банківського менеджменту. Від ефективності організації банківської безпеки залежать практично всі напрями банківської діяльності.

Проблеми аналізу банківської безпеки, а також безпеки сучасного бізнесу розглядаються у навчальних посібниках (М. І. Зубок "Безпека банківської діяльності" та В. М. Заплатинський "Основи кримінологічної безпеки сучасного бізнесу").

У перелічених працях зроблено спробу сформулювати основні поняття банківської безпеки, розглянути умови, в яких здійснюється організація банківського бізнесу. Зокрема, до таких умов М. І. Зубок відносить:

* — внутрішньополітичні;
* — правові;
* — економічні;
* — соціальні.

У визначенні кримінологічних загроз автор В. М. Заплатинський виділяє діяльність організованої злочинності (злочинних угруповань), характерними ознаками якої є:

* — ієрархічна організаційна побудова;
* — корумпованість;
* — масштабність злочинної діяльності, включаючи вихід за кордон і зв'язок з міжнародною мафією;
* — згуртованість на конкретній злочинній основі;
* — відпрацьована система захисту від правоохоронних органів.

В аспекті теоретичної розробки питань банківської та фінансової безпеки як одних із найважливіших складових економічної безпеки варто звернути увагу на ґрунтовну монографію О. І. Барановського, що становить значний інтерес як для науковців, так і для аналітиків, викладачів та студентів ВНЗ, що займаються питаннями економічної безпеки, а також для фахівців фінансових та банківських установ. Наголошуючи, що на сьогодні практично не існує усталеного визначення категорії "фінансова безпека", автор звертає увагу на її всеосяжність, вплив на різні галузі економіки країни та наводить власне розгорнуте тлумачення. У монографії наведено структурну класифікацію видів фінансової безпеки, загроз, а також відповідних індикаторів.

Доцільно зазначити, що, аналізуючи банківську безпеку, необхідно звернути увагу на вирішення питання співвідношення термінів "безпека — загрози — ризик", визначити сферу їх використання стосовно банківської діяльності. Термінологічно вони різні, але в аспекті понять — переплетені. У широкому значенні вони можуть бути і тотожні, тобто синонімами, і взаємозамінні.

Безперечно, згадані наукові роботи не дають вичерпного та остаточного аналізу проблем банківської безпеки. Деякі положення потребують коригування і доповнень, можуть і мають бути предметом наукових дискусій. Проте вони, безперечно, мають науково-теоретичну і практичну цінність у дослідженні розуміння питань економічної і, зокрема, банківської безпеки.

Виходячи із аналізу вищезазначених наукових праць, можна сказати, що:

* 1. Під банківською безпекою розуміють організацію заходів із запобігання можливим загрозам діяльності банку. Розмір цих загроз, тобто наслідки реалізації, часто наперед математично визначити неможливо.
* 2. Банківський ризик — це вірогідна загроза фінансових втрат у банківських операціях. Величина ризику (його розмір) повинна бути кількісно визначена (інакше Його не розглядають). Тобто має бути розрахований розмір ризику.

Як бачимо з наведених визначень, основна мета банківської безпеки — виключити будь-які втрати банку (матеріальні, фінансові, кадрові, інформаційні та ін.), що мають економічні наслідки.

**ІІІ. ПИТАННЯ**

**Шахрайство**

Ні для кого не секрет, що шахрайство на підприємстві будь-якої форми власності є типовим явищем не лише в Україні, а й в усьому світі. Головна відмінність полягає в тому, що іноземні компанії та юристи виробили дієві механізми протидії цьому факту. До вказаних механізмів можна зарахувати комплаєнс-процедури, аудит, внутрішнє розслідування тощо. На жаль, компанії, які працюють лише на території України та спрямовані лише на українського споживача, майже не використовують відточені до ідеалу "західні" механізми протидії внутрішньому шахрайству. Керівників цих підприємств лякають можливі деструктивні явища, які можуть виникнути в колективі внаслідок внутрішнього розслідування, а також ціна за проведення таких розслідувань, яку пропонують на ринку послуг. Та й інколи дуже важко пояснити потенційному клієнту, що в перспективі витрачені ресурси на проведене внутрішнє розслідування – це значно менше шкоди, ніж постійні втрати через недобросовісних працівників.

Відповідно до світової статистики внаслідок економічних злочинів і шахрайства щорічно втрачається 6,3 трлн доларів США. У середньому через шахрайство компанія втрачає від 5 % свого прибутку.

*В Україні 61,5 % компаній зазнавали шахрайства. 20 % компаній оцінили свої збитки від шахрайства в сумі від $100 тис. до $5 млн на рік. Україна посідає 5 місце в рейтингу країн світу за рівнем корпоративного шахрайства.*

Шахрайство розглядають як цілісне явище, що формується складною взаємодією обставин економічного, психологічного й соціального порядку. Шахрайство можна розділити на ***кілька видів***, узявши за основу розподіл суб'єкта, від якого походить цей факт:

1) розтрата чи розкрадання з боку найманого працівника;

2) шахрайство з боку керівників або менеджерів;

3) афери з інвестиціями;

4) шахрайство з боку постачальників;

5) шахрайство з боку замовника або клієнта.

Попри таку видову різноманітність, найчастіше підприємство зазнає збитків через недобросовісні дії з боку працівників цієї ж компанії.

Шахрайство на підприємстві є доволі небезпечним явищем, що несе за собою багато ***несприятливих наслідків***. Передусім це шкода діловій репутації/бренду та втрата прибутку. Крім того, якщо інформація про ненадійність системи безпеки компанії пошириться серед широких мас (а інколи достатньо й бізнес-партнерів), компанії може бути відмовлено в доступі до публічних закупівель; ініційовано міжнародне розслідування – у разі співпраці з іноземними підприємствами; до компанії можуть бути застосовані заходи кримінально-правового характеру. І, звісно, за наявності факту шахрайства компанія, безумовно, зазнає збитків матеріального характеру.

Для запобігання зазначеним наслідкам міжнародний досвід спрямовує нас до використання такого засобу, як **Internal corporate investigation**. Внутрішні розслідування є важливим інструментом захисту компаній, який допомагає уникнути негативних дій із боку держави або акціонерів, співробітників чи клієнтів. Компанії та їхнє керівництво схильні до ризику бути втягнутими в судові процеси, кримінальні розслідування, постраждати від скарг незадоволених співробітників тощо. Тож захист компанії, її посадових осіб і директорів часто потребує внутрішнього розслідування, щоб особи, які ухвалюють рішення, були повністю проінформовані про реальний стан справ, наслідки дій проти компанії та директорів безпосередньо, а також про те, як зменшити збитки для компанії та її керівництва.

**Лекція №2**

**Тема 3. Соціально-економічна безпека підприємства: сутність і передумови формування** (1 год)

ПЛАН ЛЕКЦІЇ

Вступ

1. Поняття, предмет, зміст та суб'єкти соціально-економічної безпеки.

*2.* Принципи соціально-економічної безпеки

# **РЕКОМЕНДОВАНА ЛІТЕРАТУРА**

1. Економічна та майнова безпека бізнесу: навчальний посібник / Б.М. Андрушків, Л.Я. Малюта. –Тернопіль: ФОП Паляниця В.А., 2016. – 180 с.

2.Економічна безпека підприємства : навчальний посібник / [Небава М. І., Міронова Ю.В.] – Вінниця : ВНТУ, 2017. – 73 с

3. Раєвнева О. В. Управління розвитком підприємства: методологія, механізми, моделі: Монографія/ О. В. Раєвнева. - Харків: ІНЖЕК, 2016. - 496 с.

4.Моделювання економічної безпеки: держава, регіон, підприємство: Монографія/ В. М. Гаєць, М. О. Кизим, Т. С. Клебанова, О. І. Черняк. - Х. : ІНЖЕК, 2016. - 240 с.

5. Рибальченко Л.В., Сауліна А.І. ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА /«Використання сучасних інформаційних технологій в діяльності національної поліції України» : матеріали Всеукраїнського науково-практичного семінару (28 листопада 2019 р., м. Дніпро). – Дніпро: Дніпропетровський державний університет внутрішніх справ, 2019. – С.113-115

6. Rybalchenko L.V., [Ryzhkov E.](http://er.dduvs.in.ua/browse?type=author&value=Ryzhkov%2C+E.)V. Ensuring enterprise economic security /Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs. - 2019. - Special Issue № 1 (102). – P. 268-271

**МЕТА ЛЕКЦІЇ**

Метою лекції є надання необхідних теоретичних знань здобувачам вищої освіти юридичного факультету, що навчаються на магістерському рівні вищої освіти, щодо основних понять і принципів соціально-економічної безпеки підприємства.

**ВСТУП**

Потреба в безпеці притаманна будь-якій системі, у тому числі й підприємству. Безпека є однією з найважливіших умов функціонування підприємства. Серед численних досліджень безпеки найпоширенішим сьогодні є дослідження економічної безпеки підприємства. У сучасних умовах відбувається трансформація економічної безпеки підприємства в соціально-економічну. Така трансформація зумовлена посиленням впливу людського чинника в зовнішньому та внутрішньому середовищі підприємства.

Проявом такого впливу в зовнішньому середовищі підприємства є формування його соціальної відповідальності, а у внутрішньому – створення соціального партнерства.

Всі визначення такого поняття як «безпека», «соціально-економічна безпека», пряме чи опосередковано включають наступні моменти:

• наявність загроз (внутрішніх і зовнішніх);

• збалансованість інтересів (інтереси об’єктів захисту мають носити збалансований характер).

**І. ПИТАННЯ**

Поняття, предмет, зміст та суб'єкти соціально-економічної безпеки

Соціально-економічна безпека− це універсальна категорія, що відбиває захищеність суб’єктів соціально-економічних відносин на всіх рівнях, починаючи з держави і закінчуючи кожним його громадянином.

Соціально-економічна безпека підприємства− це системна захищеність діяльності від негативних впливів внутрішнього і зовнішнього середовища, а також здатність швидко ліквідувати різні варіанти погроз чи пристосуватися до існуючих умов, що не позначаються негативно на його діяльності.

Зміст даного поняття містить у собі систему заходів, що забезпечують конкурентоспроможність і економічну стабільність підприємства, а також сприяють підвищенню рівню соціального добробуту працівників.

Соціально-економічна безпека підприємства− це стан найбільш ефективного використання корпоративних ресурсів для запобігання погроз і забезпечення стабільного функціонування підприємства в даний час і в майбутньому.

Безпека підприємства характеризується сукупністю якісних і кількісних показників, найважливішим з яких є рівень соціально-економічної безпеки. Рівень соціально-економічної безпеки підприємства− це оцінка стану використання корпоративних ресурсів за критеріями рівня соціально-економічної безпеки підприємства.

Головною метою досягнення високого рівня соціально-економічної безпеки, є роботи з забезпечення максимальної безпеки основних функціональних складових діяльності підприємства.

Функціональні складові соціально-економічної безпеки підприємства − це сукупність основних напрямків його безпеки, що істотно відрізняються один від одного за своїм змістом.

Загальна схема процесу організації соціально-економічної безпеки включає такі дії (заходи), що здійснюються послідовно або одночасно:

а) формування необхідних корпоративних ресурсів (капіталу, персоналу, прав інформації, технології та устаткування);

б) стратегічне прогнозування та планування соціально-економічної безпеки за функціональними складовими;

в) стратегічне планування фінансово-господарської діяльності підприємства;

г) тактичне планування соціально-економічної безпеки за функціональними складовими;

г) тактичне планування фінансово-господарської діяльності підприємства;

д) оперативне управління фінансово-господарською діяльністю підприємства;

е) здійснення функціонального аналізу рівня соціально-економічної безпеки;

є) загальна оцінка досягнутою рівня соціально-економічної безпеки. Тільки за здійснення в необхідному обсязі зазначених дій (заходів) можна буде досягти належного рівня соціально-економічної безпеки підприємства.

Структура функціональних складових соціально-економічної безпеки підприємства:

а) фінансова складова;

б) інтелектуальна і кадрова складова;

в) техніко-технологічна складова;

г) політико-правова складова;

д) екологічна складова;

є) інформаційна складова;

ж) силова складова.

Кожна з перерахованих функціональних складових соціально-економічної безпеки підприємства характеризується власним змістом, набором функціональних критеріїв і способами забезпечення. Для забезпечення своєї соціально-економічної безпеки підприємство використовує сукупність своїх корпоративних ресурсів.

Корпоративні ресурси− фактори бізнесу, які використовуються власниками, керівництвом і менеджерами для виконання стратегічних цілей підприємства (організації).

Виділяють наступні корпоративні ресурси:

1) Ресурс капіталу. Акціонерний капітал підприємства в сполученні з позиковими фінансовими ресурсами є кровоносною системою підприємства і дозволяє здобувати і підтримувати інші корпоративні ресурси, що споконвічно відсутні у творців даного підприємства.

2) Ресурс персоналу. Керівництво, менеджери, штат інженерно-технічного персоналу, виробничих робітників та службовців з їхніми знаннями, досвідом і навичками є основною провідною ланкою, що з’єднує воєдино усі фактори бізнесу та забезпечує проведення в життя місії, а також досягнення цілей.

3) Ресурс інформації і технології. Інформація, що стосується всіх сторін діяльності підприємства, є найбільш дорогим з ресурсів підприємства.

Саме інформація про зміну політичної, соціальної, економічної й екологічної ситуації, зміни ринків підприємства, науково-технічна і технологічна інформація, конкретні “ноу-хау”, що стосуються яких-небудь аспектів даного бізнесу, нові підходи в методах організації і керування бізнесом дозволяють підприємству адекватно реагувати на будь-які зміни зовнішнього середовища бізнесу, ефективно планувати і здійснювати свою господарську діяльність.

4) Ресурс техніки й устаткування. На основі наявних фінансових, інформаційно-технологічних, інноваційних і кадрових можливостей підприємство покупає технологічне й інше устаткування для виробництва конкурентоспроможної продукції.

5) Ресурс прав. З розвитком цивілізації, зменшенням природних ресурсів і підвищенням цінності для бізнесу матеріальних і нематеріальних активів різко зросла роль ресурсу прав. Цей ресурс містить у собі права на використання патентів, ліцензій і квот на використання природних ресурсів, а також експортні квоти, права на користування землею. Використання цього ресурсу дозволяє підприємству прилучитися до передових технологічних розробок, не проводячи власних дорогих наукових досліджень, а також одержати доступ до не загальнодоступних можливостей розвитку бізнесу. Основною причиною необхідності забезпечення соціально-економічної безпеки підприємства є задача, що стоїть перед кожним підприємством, досягнення стабільності свого функціонування і створення перспектив зростання для виконання стратегічних цілей бізнесу.

Рівень соціально-економічної безпеки підприємства базується на тому, наскільки ефективно службам даного підприємства вдається попереджатизагрози й усувати збитки від негативних впливів на різні аспекти соціально-економічної безпеки. Джерелами таких негативних впливів можуть бути усвідомлені чи неусвідомлені дії людей, організацій, у тому числі органів державної влади, міжнародних чи організацій підприємств-конкурентів, а також збігу об’єктивних обставин, наприклад: стан фінансової кон’юнктури на ринках, як даного підприємства так і на міжнародних ринках, наукові відкриття і технологічні розробки, форс-мажорні обставини і т. ін.

У залежності від суб’єктивної обумовленості негативних впливів на соціально-економічну безпеку підприємства може застосовуватися наступна градація цих негативних впливів. Об’єктивні негативні впливи− це такі негативні впливи, що виникають без участі і мимо волі підприємства чи його службовців.

Суб’єктивні негативні впливи − це негативні впливи, що виникли як наслідок неефективної роботи підприємства в цілому чи його працівників. Основні функціональні цілі соціально-економічної безпеки підприємства:

* забезпечення високої фінансової ефективності роботи підприємства, його фінансовій стійкості і незалежності;
* забезпечення технологічної незалежності підприємства і досягнення високої конкурентоспроможності його технологічного потенціалу;
* висока ефективність менеджменту підприємства, оптимальність і ефективність його організаційної структури;
* високий рівень кваліфікації персоналу підприємства і його інтелектуального потенціалу, ефективність корпоративних науководослідницьких та дослідно-конструкторських робіт;
* високий рівень екологічності роботи підприємства, мінімізація руйнівного впливу результатів виробничої діяльності на стан навколишнього середовища;
* якісна правова захищеність всіх аспектів діяльності підприємства;
* забезпечення захисту інформаційного середовища підприємства, комерційної таємниці і досягнення високого рівня інформаційного забезпечення роботи всіх його служб;
* забезпечення безпеки персоналу підприємства, його капіталу, майна і комерційних інтересів.

**ІІ. ПИТАННЯ**

**Принципи соціально-економічної безпеки**

До числа основних завдань соціально-економічної безпеки (СЕБП) підприємства належать:

§ захист законних прав і інтересів підприємства і його співробітників;

§ збір, аналіз, оцінка даних і прогнозування розвитку обстановки; вивчення партнерів, клієнтів, конкурентів, кандидатів на роботу в компанії;

§ своєчасне виявлення можливих устремлінь до підприємства і його співробітників з боку джерел зовнішніх погроз безпеки;

§ недопущення проникнення на підприємство структур економічної розвідки конкурентів, організованої злочинності й окремих осіб із протиправними намірами;

§ протидія технічному проникненню в злочинних цілях;

§ виявлення, попередження й припинення можливої протиправної й іншої негативної діяльності співробітників підприємства на шкоду його безпеки;

§ захист співробітників підприємства від насильницьких зазіхань; забезпечення схоронності матеріальних цінностей і відомостей, що становлять комерційну таємницю підприємства;

§ пошук необхідної інформації для вироблення оптимальних управлінських рішень із питань стратегії й тактики економічної діяльності; § фізична й технічна охорона будинків, споруджень, території й транспортних засобів;

§ формування серед населення й ділових партнерів сприятливої думки про підприємство, що сприяє реалізації планів економічної діяльності й статутних цілей;

§ відшкодування матеріального й морального збитку, завданого в результаті неправомірних дій організацій і окремих осіб;

§ контроль за ефективністю функціонування системи безпеки, удосконалювання її елементів.

Побудова ССЕБ підприємства повинна здійснюватися на основі дотримання принципів: · законності; · прав і свобод громадян; · централізованого управління; · компетентності; · конфіденційності; · розумної достатності, відповідності зовнішнім і внутрішнім погрозам безпеки; · комплексного використання сил і коштів; · самостійності й відповідальності за забезпечення безпеки; · передової матеріально-технічної оснащеності; · корпоративної етики; · координації й взаємодії з органами влади й управління.

До основних елементів ССЕБ підприємства належать:

1) захист комерційної таємниці й конфіденційної інформації;

2) комп’ютерна безпека;

3) внутрішня безпека;

4) безпека будинків і споруд;

5) фізична безпека;

6) технічна безпека;

7) безпека зв’язку;

8) безпека господарсько-договірної діяльності;

9) безпека перевезень вантажів і осіб;

10) безпека рекламних, культурних, масових заходів, ділових зустрічей і переговорів;

11) протипожежна безпека;

12) екологічна безпека;

13) радіаційно-хімічна безпека;

14) конкурентна розвідка;

15) інформаційно-аналітична робота;

16) пропагандистське забезпечення, соціально-психологічна, профілактична робота серед персоналу і його навчання з питань безпеки;

17) експертна перевірка механізму системи безпеки.

Основний зміст системи соціально-економічної безпеки підприємства полягає в тому, що вона повинна носити попереджальний характер, а основними критеріями оцінки її надійності й ефективності є:

- забезпечення стабільної роботи підприємства, схоронності й збільшення фінансів і матеріальних цінностей;

- попередження кризових ситуацій, у тому числі різних надзвичайних подій, пов’язаних з діяльністю «зовнішніх» і/або «внутрішніх» недоброзичливців. Особливістю й складністю побудови системи економічної безпеки підприємства є той факт, що її дієвість повністю залежить від людського фактору – рівня кваліфікації персоналу.

*Критерій та індикатори соціально-економічної безпеки*

У процесі здійснення підприємством своєї фінансово-господарської діяльності з’являється інформація для аналізу стану його соціально-економічної безпеки. На основі цієї інформації здійснюється оцінка функціональних і сукупних критеріїв економічної безпеки цього підприємства, їхніх відхилень від планових значень, аналізуються причини виникнення цих відхилень.

Після цього виробляються рекомендації з коректування набору корпоративних ресурсів, систем стратегічного і поточного планування фінансовогосподарської діяльності машинобудівного підприємства, а також системи оперативного керування його діяльністю. Аналіз рівня соціально-економічної безпеки підприємства проводиться на основі оцінки ефективності заходів для запобігання збитків і розрахунку функціональних і сукупного критерію економічної безпеки.

Безпека сучасного промислового підприємства включає:

– безпеку, пов’язану з типом підприємства;

– безпеку, пов’язану з життєдіяльністю підприємства;

– безпеку за складовими частинами сфер його діяльності.

**Тема 4. Організаційні та техніко-технологічні основи безпеки підприємства** (1 год)

ПЛАН ЛЕКЦІЇ

Вступ

1. Організація служби безпеки на підприємстві.

*2.* Техніко-технологічна безпека.

# **РЕКОМЕНДОВАНА ЛІТЕРАТУРА**

1. Економічна та майнова безпека бізнесу: навчальний посібник / Б.М. Андрушків, Л.Я. Малюта. –Тернопіль: ФОП Паляниця В.А., 2016. – 180 с.

2.Економічна безпека підприємства : навчальний посібник / [Небава М. І., Міронова Ю.В.] – Вінниця : ВНТУ, 2017. – 73 с

3. Раєвнева О. В. Управління розвитком підприємства: методологія, механізми, моделі: Монографія/ О. В. Раєвнева. - Харків: ІНЖЕК, 2016. - 496 с.

4.Моделювання економічної безпеки: держава, регіон, підприємство: Монографія/ В. М. Гаєць, М. О. Кизим, Т. С. Клебанова, О. І. Черняк. - Х. : ІНЖЕК, 2016. - 240 с.

**МЕТА ЛЕКЦІЇ**

Метою лекції є надання необхідних теоретичних знань здобувачам вищої освіти юридичного факультету, що навчаються на магістерському рівні вищої освіти, щодо основних понять організації служби безпеки на підприємстві.

**ВСТУП**

Завдання гарантування безпеки підприємства є одним із основних, пріоритетних завдань, що стоять перед усіма структурними ланками і всіма працівниками підприємства, так само як і завдання збільшення прибутку, підвищення власного добробуту. Ефективний захист економічних інтересів фірми може бути забезпечений лише у разі об'єднання зусиль її персоналу: адміністрації, інженерно-технічних працівників, службовців, робітників.

Служба безпеки (СБ) фірми - це самостійний структурний підрозділ. Вона вирішує завдання безпосереднього забезпечення захисту життєво важливих інтересів фірми в умовах комерційного і підприємницького ризику, конкурентної боротьби. На всіх великих і середніх підприємствах (в організаціях) звичайно створюються автономні служби безпеки, а безпеку функціонування невеликих фірм можуть гарантувати територіальні (районні або міські) служби за договорами найму одного чи кількох охоронців. Такі служби охорони зазвичай створюються при місцевих органах внутрішніх справ або при державній службі безпеки.

**І. ПИТАННЯ**

**Організація служби безпеки на підприємстві**

Служба безпеки (СБ) підприємства створюється наказом директора з метою захисту економічних інтересів підприємства і забезпечення максимальної безпеки його діяльності як суб’єкта ринкових відносин. СБ є самостійним підрозділом і підпорядковується безпосередньо керівнику підприємства. Керівництво службою здійснює начальник СБ, що призначається і звільняється від займаної посади керівником підприємства. Структура і штати СБ за поданням її начальника затверджуються керівником підприємства. Діяльність СБ фінансується за рахунок включення її витрат у собівартість робіт, виконуваних підприємством. СБ у своїй діяльності керується законами України, указами Президента, постановами Кабінету Міністрів, відомчими наказами і вказівками, Статутом підприємства, наказами і вказівками керівника підприємства і внутрішнім Положенням про СБ.

*Загальні функції, що покладаються на службу безпеки підприємства*

Функції служби безпеки, які виконуються співробітниками СБ:

· організація й забезпечення пропускного і внутріоб’єктного режиму в будинках і приміщеннях, несення їхньої охорони, контроль за дотриманням установленого режиму співробітниками і відвідувачами;

· проведення заходів щодо правового й організаційного регулювання відносин щодо захисту підприємницької таємниці й економічної безпеки;

· участь у розробці основних нормативних документів (інструкцій, положень), що встановлюють порядок і принципи захисту підприємницької таємниці;

· участь у розробці посадових інструкцій, обов’язків керівників підрозділів, фахівців, усіх категорій працівників;

· забезпечення збереження документів, що містять інформацію, що є комерційною таємницею, припинення їхнього розкрадання або передачі зведень зацікавленим особам іншими способами;

· організація проведення службових розслідувань по фактах розголошення зведень, що складають підприємницьку таємницю, втрат документів і інших порушень безпеки фірми, а також і інші функції, що повинні бути встановлені в положенні про службу безпеки, затвердженому керівником підприємства.

До складу механізму захисту підприємницької таємниці й загальної безпеки підприємства входять наступні підсистеми:

* + правове забезпечення таємниці; правознавство організаційного захисту;
* здійснення інженернотехнічного захисту;
* мотивація в першу чергу тих співробітників, від поводження яких залежить витік зведень, що складають підприємницьку таємницю;
* посилення різних форм відповідальності за розголошення інформації, що наносять економічні збитки підприємству тощо.

Організація інженерно-технічного захисту – це сукупність спеціальних інженерно-технічних засобів, застосування яких забезпечує безпека фірми, її майна, ресурсів, а також зведень про діяльність підприємства. Завданням служби безпеки щодо гарантування режиму і охорони є організація і здійснення заходів щодо гарантування безпеки діяльності й захисту інформації всіма можливими за певних умов способами і засобами.

*Основними завданнями організації режиму і охорони є*:

· запобігання проникненню в службові приміщення, в зони, що охороняються, і на територію об’єкта сторонніх осіб;

· забезпечення порядку внесення (винесення), ввезення (вивезення) матеріальних цінностей і входу (виходу) працівників і клієнтів.

Для забезпечення надійної охорони матеріальних цінностей, конфіденційних документів та інформації, що містить відомості комерційного характеру, а також для своєчасного запобігання спробам несанкціонованого доступу до них встановлюють певний режим діяльності, дотримання якого є обов’язковим для всіх працівників, відвідувачів і клієнтів.

*Об’єкти, які підлягають захисту від потенційних загроз і протиправних дій на підприємстві*

У нормативних документах, які визначають організацію діяльності служб безпеки підприємств, виокремлюються конкретні об’єкти, які підлягають захисту від потенційних загроз і протиправних дій.

До них належать:

− персонал (керівники; персонал, який володіє інформацією, що становить комерційну таємницю підприємства);

− матеріальні цінності та фінансові кошти (приміщення, споруди, устаткування, транспорт; валюта, коштовні речі, фінансові документи);

− інформаційні ресурси з обмеженим доступом;

− засоби та системи комп’ютеризації діяльності підприємства;

− технічні засоби та системи охорони й захисту матеріальних та інформаційних ресурсів.

Для захисту від потенційних загроз і протиправних дій служба безпеки організує контрольно-пропускний режим на підприємстві. Контрольно-пропускний режим − це комплекс організаційноправових обмежень і правил пропуску через контрольно-пропускні пункти в окремі будівлі (приміщення) працівників об’єкта, відвідувачів, транспорту і матеріальних засобів. Це один із ключових моментів в організації системи безпеки на підприємстві. Отже, контрольно-пропускним режимом є комплекс організаційних заходів (адміністративно-обмежувальних), інженерно-технічних рішень і дій служби безпеки.

Основними цілями створення контрольно-пропускного режиму є:

· захист законних інтересів підприємства, підтримка порядку внутрішнього управління;

· захист власності підприємства, її раціональне й ефективне використання;

· зростання прибутків підприємства;

· внутрішня і зовнішня стабільність підприємства;

· захист комерційних таємниць і прав на інтелектуальну власність.

Контрольно-пропускний режим як частина системи безпеки дає змогу вирішити такі завдання:

· забезпечення санкціонованого проходження працівників і відвідувачів, ввезення (вивезення) продукції і матеріальних цінностей, ритмічної роботи підприємства;

· запобігання безконтрольному проникненню сторонніх осіб і транспортних засобів на території, що охороняються, і в окремі будівлі (приміщення);

· своєчасне виявлення загроз інтересам підприємства, а також потенційно небезпечних умов, що сприяють виникненню матеріального і морального збитку підприємства;

· створення надійних гарантій підтримки організаційної стабільності зовнішніх і внутрішніх зв’язків підприємства, відпрацювання механізму оперативного реагування на загрози й негативні тенденції;

· припинення посягань на законні інтереси підприємства, використання юридичних, економічних, організаційних, соціально-психологічних, технічних та інших засобів для виявлення і послаблення джерел загроз безпеці підприємства.

**ІІ.ПИТАННЯ**

**Техніко-технологічна безпека**

Техніко-технологічна безпека – це складова соціально-економічної безпеки, пріоритетним завданням для якої є захист від негативних чинників з метою створення та найбільш ефективного використання технічної бази та технологічних процесів для забезпечення високого рівня конкурентоспроможності підприємства.

До техніко-технологічної безпеки підприємства належить створення й використання технічної бази, устаткування та основних засобів виробництва і таких технологій та бізнес-процесів, які посилюють конкурентоздатність підприємства.

Ця складова є захистом від можливих витрат унаслідок використання застарілої техніки і технології виробництва продукції, неефективної організації виробничого процесу. Вона повинна відображати ступінь відповідності технологій, які застосовуються на підприємстві, сучасним світовим аналогам щодо оптимізації витрат ресурсів.

До основних негативних впливів техніко-технологічною безпеки відносяться дії, спрямовані на підрив технологічного потенціалу підприємства, порушення технологічної дисципліни, моральне старіння технологій, які використовуються.

Техніко-технологічна безпека характеризується такими ознаками:

− якістю і відповідністю технологічного процесу виробництва та основного капіталу потребам ринку;

− захищеністю техніко-технологічної сфери підприємства від негативного впливу зовнішніх і внутрішніх загроз;

− здатністю техніко-технологічної сфери підприємства забезпечувати його високу конкурентоспроможність;

− за рахунок високої ефективності використання основного капіталу забезпечувати сталий розвиток підприємства.

Техніко-технологічну безпеку підприємства можна проаналізувати за допомогою наступних показників:

* темп відновлення основних виробничих засобів (ОВЗ);
* реальний рівень завантаження виробничих потужностей;
* ступінь зносу ОВЗ;
* частка НДДКР у загальному обсязі робіт;
* динаміка обсягів виробництва в діючих цінах;
* частка НДР у загальному обсязі НДДКР;
* стабільність виробничого процесу; питома вага виробництва у ВВП;
* оцінка конкурентоспроможності продукції;
* вікова структура й технічний ресурс парку машин і устаткування;
* фактичний і необхідний обсяг інвестицій;
* рівень інноваційної активності;
* рівень рентабельності виробництва та інші.

Техніко-технологічна безпека передбачає здійснення кількох, послідовних етапів. Перший етап охоплює аналіз ринку технологій стосовно виробництва продукції, аналогічної профілю даного підприємства чи організації проектувальника. Другий етап− це аналіз конкретних технологічних процесів і пошук внутрішніх резервів поліпшення використовуваних технологій.

На третьому етапі здійснюється:

а) аналіз товарних ринків за профілем продукції, що виготовляється підприємством, та ринків товарів-замінників;

б) оцінка перспектив розвитку ринків продукції підприємства;

в) прогнозування можливої специфіки необхідних технологічних процесів для випуску конкурентоспроможних товарів.

Четвертий етап присвячується переважно розробці технологічної стратегії розвитку підприємства. На п’ятому етапі оперативно реалізуються плани технологічного розвитку підприємства в процесі здійснення ним виробничо-господарської діяльності. Шостий етап є завершальним, на якому аналізуються результати практичної реалізації заходів щодо охорони техніко-технологічної складової соціально-економічної безпеки на підставі спеціальної карти розрахунків ефективності таких заходів.

Для забезпечення техніко-технологічної складової соціальноекономічної безпеки треба розрахувати ефективність заходів з відокремлюванням прогнозованих необхідних показників.

Виробнича безпека на підприємстві. Виробнича безпека – безпека від нещасних випадків та аварій на виробничих об’єктах і від їх наслідків забезпечується комплексом організаційних та технічних заходів та засобів, спрямованих на запобігання або зменшення дії на працюючих небезпечних виробничих факторів.

Основними напрямками виробничої безпеки є:

· безпека технологічного обладнання;

· безпека вантажно-розвантажувальних робіт;

· безпека при експлуатації посудин та систем під тиском;

· безпека при експлуатації обладнання з високими чи низькими температурами;

· електробезпека;

· інші напрямки.

Охорона праці – це система забезпечення безпеки життя і здоров’я працівників у процесі трудової діяльності, що включає правові, соціальноекономічні, організаційно-технічні, санітарно-гігієнічні, лікувальнопрофілактичні, реабілітаційні та інші заходи. Умови праці − це сукупність чинників виробничого середовища, що впливають на здоров’я і працездатність людини в процесі праці. На формування і зміну умов праці впливають три групи чинників:

1. Соціально-економічні:

1.1. Нормативне і законодавче регулювання соціально-економічних і виробничих умов праці (тривалість робочого часу, режими праці і відпочинку, санітарні норми і вимоги, система контролю за дотриманням діючих законів, вимог і правил в області умов праці).

1.2. Соціально-психологічні чинники, що характеризують відношення працівника до праці і її умов, психологічний клімат у виробничих колективах, ефективність пільг і компенсацій за роботу, пов’язану з несприятливими впливами.

2. Організаційно-технічні:

2.1. Засоби праці (виробничі будинки і спорудження, санітарно-побутові пристрої, технологічне устаткування, інструменти, пристосування);

2.2. Предмети і продукти праці (сировина, матеріали, заготівлі, напівфабрикати, готові вироби);

2.3. Технологічні процеси (фізичні, механічні, хімічні і біологічні впливи на оброблювані предмети праці, способи їхнього транспортування і збереження);

2.4. Організаційні форми виробництва, праці і управління (рівень спеціалізації виробництва, його масштаби і масовість, змінність роботи підприємства, перерви, безперервність виробництва, форми розподілу і кооперації праці, її прийоми, режими праці і відпочинку протягом робочої зміни, тижня, року, організація обслуговування робочого місця, структура підприємства і його підрозділів, співвідношення функціонального і лінійного управління виробництвом та ін.).

3. Природні чинники. Вони мають особливе значення при формуванні умов праці на підприємствах харчової промисловості, в сільськогосподарському виробництві, на транспорті, у будівництві тощо.

Види нормативних правових актів з охорони праці:

1. Стандарти системи стандартів безпеки праці. 2. Санітарні правила і норми, гігієнічні нормативи. 3. Правила з охорони праці (міжгалузеві і галузеві). 4. Правила безпечної експлуатації. 5. Правила безпеки (пожежної, по вибухах, електричної, ядерної, радіаційної, лазерної, біологічної, технічної). 6. Правила захисту (наприклад, від статичної електрики). 7. Будівельні норми і правила. 8. Інструкції з охорони праці, у тому числі типова галузева. 9. Організаційно-методичні документи (міжгалузеві і галузеві): положення, вказівки, рекомендації.

Ґрунтуючись на нормативах, що наводяться у цих документах, працівники служби управління персоналом підприємства повинні здійснювати роботу щодо:

• визначення рівня безпеки праці на кожному робочому місці;

• прийняття рішень щодо підвищення рівня безпеки праці до нормативного;

• ліквідації робочих місць з несприятливими умовами праці.

Якщо рівень безпеки не відповідає нормативному в силу специфіки виробництва, вирішують питання про компенсацію за роботу у таких умовах і вчать працівників методам захисту здоров’я на даних робочих місцях. Небезпечні за умовами праці робочі місця повинні знаходитися під постійним контролем служби управління персоналом. Організована система управління виробничою безпекою на підприємстві регулює взаємовідносини між структурними підрозділами підприємства, стосунки роботодавця з найнятими робітниками.

Управління виробничою безпекою − це чітка взаємодія усіх структур виробництва, спрямована на дотримання нормативних вимог з охорони праці і виконання посадових обов’язків щодо забезпечення безпеки виробничих процесів. На підприємстві координація діяльності усіх служб підприємства у рамках системи управління виробничою безпекою здійснюється генеральним директором і службою охорони праці.

Щорічно плануються і виділяються засоби на впровадження заходів щодо досягнення встановлених нормативів безпеки, гігієни праці і виробничої санітарії. Планування заходів передбачає визначення умов праці і реалізацію основних напрямів роботи з охорони праці, визначають потребу в новій техніці, технологіях, інженерно-технічних засобах безпеки. Щорічне виділення коштів в обсязі не менше 0,5 % фонду оплати праці за попередній рік. Освоєння засобів з виробничої безпеки повинно бути закладене в колективному договорі, що дозволить планомірно впроваджувати у виробництво технічні засоби, організаційні заходи щодо забезпечення безпеки праці і здійснювати контроль з боку колективу підприємства.

**Лекція №3**

**Тема 5. Інтелектуальна та кадрова складові соціально-економічної безпеки підприємства** (1 год)

ПЛАН ЛЕКЦІЇ

Вступ

1.Поняття інтелектуальної та кадрової складової безпеки підприємства.

*2.* Суб’єкти скоєння економічних злочинів.

3. Основні методи профілактики правопорушень персоналу.

# **РЕКОМЕНДОВАНА ЛІТЕРАТУРА**

1. Пуйда Г.В. Комплексний аналіз філософсько-економічної дефініції «інтелектуальна безпека підприємства» [Текст] / Галя Володимирівна Пуйда // Економічний аналіз: зб. наук. праць / Тернопільський національний економічний університет; редкол.: О. В. Ярощук (голов. ред.) та ін. – Тернопіль: Видавничо-поліграфічний центр Тернопільського національного економічного університету «Економічна думка», 2017. – Том 27. – № 4. – С. 261-272. – ISSN 1993-0259.

2. Ревак І.О. Інтелектуальний потенціал у системі економічної безпеки України. 08.00.03 – економіка та управління національним господарством 21.04.01 – економічна безпека держави (економічні науки). Дисертація на здобуття наукового ступеня доктора економічних наук. Львів. 2016. - 474 с.

3. Касич А.О., Медвідь Г.С. Управління кадровою безпекою на українських підприємствах через призму макроекономічних процесів. Електронне наукове фахове видання «Ефективна економіка». №1. - 2019.

**МЕТА ЛЕКЦІЇ**

Метою лекції є надання необхідних теоретичних знань здобувачам вищої освіти юридичного факультету, що навчаються на магістерському рівні вищої освіти, щодо основних понять інтелектуальної та складових кадрової безпеки підприємства, найважливіші питання скоєння економічних злочинів на підприємстві, а такожметоди профілактики правопорушень персоналу.

**ВСТУП**

На сучасному етапі розвитку підприємництва перед суб’єктами господарювання постає проблема безпеки підприємства. В останні роки все більше уваги звертають саме на забезпечення економічної безпеки. Незважаючи на значні наробки вчених з цієї проблематики, в літературних джерелах досі існуєнеоднозначнетлумачення поняття «економічна безпека», про що свідчать визначення.

Найменш досліджуваною та водночас складною категорією економічної безпеки є інтелектуальна безпека. Її можна розглядати з двох позицій: як захист інтелектуального потенціалу (трудових кадрів), та власне об’єктів інтелектуальної власності (нематеріальних активів). Інтелектуальна безпека з точки зору захисту кадрової складової – це захищеність інтелектуальних ресурсів соціально-економічного розвитку, їх продукування, обміну, використання на макро- та мікроекономічних рівнях.Інтелектуальна безпека з точки зору захисту інтелектуальної власності– це захищеність знань як інтелектуальних ресурсів суспільства, що охоплює забезпечення працівників знань та їх інтелектуальної праці, інтелектуального продукту, інтелектуальної власності, інтелектуального капіталу.

**І. ПИТАННЯ**

**Поняття та складові кадрової безпеки підприємства**

Належний рівень соціально-економічної безпеки залежить від складу кадрів, їхнього інтелекту та професіоналізму. Забезпечення кадрової складової соціально-економічної безпеки охоплює взаємопов’язані і водночас самостійні напрями діяльності, які спрямовані на роботу з персоналом. Кадрова складова СЕБ має на меті збереження стратегічно важливої ланки персоналу (топ менеджмент, працівників, що мають відношення до інтелектуальної власності, інноваційних розробок та конфіденційної інформації).

З кадрами підприємства пов’язані основні внутрішні, а також зовнішні ризики, адже від економічних злочинів своїх співробітників сьогодні страждають більше 40% компаній, втрачаючи в результаті крадіжки до 7% свого доходу, тільки 20% спроб злому мереж і отримання несанкціонованого доступу до комп’ютерної інформації виникає ззовні, інші 80% випадків спровоковані за участі персоналу компанії. 95% збитків на підприємствах США утворюється за особистої участі персоналу підприємств і тільки 5 % – унаслідок дій клієнтів та інших осіб. Статистичні дані Європейського Союзу показують, що приблизно 58% відомих випадків шахрайства й зловживань припадає на частку службовців, 30% – менеджерів, а 12% – топ-менеджерів і власників.

Кадрова безпека є поняттям складним і багатогранним, тому вітчизняні та зарубіжні автори виокремлюють різні підходи до його трактування. Кадрова безпека є уніфікованою категорією, яка виявляється на всіх рівнях від окремо взятого підприємства до національної економіки. Кадрова безпека − це процес запобігання негативним впливам на економічну безпеку підприємства через ризики і погрози, пов’язані з персоналом, його інтелектуальним потенціалом і трудовими відносинами.

Змістом категорії «кадрова безпека» є характеристика стану економічної системи при якому відбувається ефективне функціонування всіх її функціональних складових, забезпечення захищеності та здатність протистоянь внутрішнім і зовнішнім впливам і загрозам пов’язаних з персоналом, змістовний та структурний аналіз, діагностика та прогнозування впливу діяльності персоналу на внутрішні та зовнішні показники економічної системи.

До питань кадрової безпеки зараховують:

· забезпечення підприємства необхідними співробітниками, заповнення вакансій; утримання співробітників, їх розвиток;

· розробка мотиваційних схем і схем оплати праці;

· усунення збитку у зв’язку з трудовими суперечками;

· підвищення лояльності співробітників;

· аналіз ситуації у конкурентів; · робота із сайтами вакансій, кадровими агентствами; · аналіз ситуації на ринку праці в регіоні;

· оцінювання підприємства як працедавця (погляд з боку співробітника);

· способи проектування кар’єри (також погляд з боку співробітника).

Кадрова безпека є комбінацією складових пов’язаних між собою складними і часто завуальованими зв’язками:

1)Безпека життєдіяльності, яка включає: а) безпека здоров’я (створення певних умов праці працівникам по запобіганню травматизму, захворювання на підприємстві); б) фізична безпека (виконання комплексу заходів, щодо недопущення порушень правил безпеки).

2)Соціально-мотиваційна безпека, яка включає: а) фінансова безпека (фінансова, грошово-кредитна платоспроможність працівників; впевненість в своєму робочому місці; оплата праці, яка враховує обсяг, кваліфікацію, професіоналізм і якість виконаної роботи); б) кар’єрна безпека (професійно-кваліфікаційне та посадове просування працівників, заохочення в пристосуванні своєї кваліфікації до вимог робочого місця, в гарантіях виробничого зростання (планування кар’єри): підвищення особистої мобільності на ринку робочої сили; отримання шансівдля самореалізації на робочому місці; в) естетична безпека (проведення загальноосвітніх семінарів, конференцій,групових дискусій; мотивація задоволення персоналу своєю роботою; поліпшення власного іміджу кожного працівника); г) адміністративно-незалежна безпека (створення умов для відсутності можливості призначення непідготовлених і некомпетентних кадрів, що знаходяться у «родинних» стосунках з власниками, засновниками, акціонерами підприємства до керівництва трудового колективу персоналу);

3)Професійна безпека, яка включає: а) безпеку праці (система принципів, підходів, дій направлена на створення певних умов праці (рівень оплати праці, посада, обладнання робочого місця), з урахуванням новітнього, передового досвіду на ринку праці); б) інформаційну безпека (прогнозування структури персоналу, визначення потреби в кадрах, планування, залучення та розміщення персоналу; оцінювання результатів праці для виявлення потенціалу кожного працівника); в) пенсійно-страхова безпека (соціальний захист працівників (страхування, медичне обслуговування); г) інтелектуальна безпека (безпека володіння сучасними знаннями, впровадження новітніх технологій урозвиток персоналу, удосконалення рівня професійних знань, навичок, умінь, здібностей у зв’язку з розвитком науково-технічного прогресу).

4) Антиконфліктна безпека, яка включає: а) патріотична безпека (створення психологічного клімату в колективі на основі позитивного відношення до підприємства, що характеризується психологічними показниками об’єднаності працівників, яка забезпечує узгодженість, безконфліктність спілкування, відповідальність та обов’язок, товариську допомогу, вимогливість до себе та іншого в інтересах виробництва); б) психолого-комунікаційна безпека (сприяння міжособистісним комунікаціям істворенню сприятливого мікроклімату; врахування інтересів і побажань працівників, його особистого потенціалу; задоволеність міжособистісними стосунками по вертикалі (керівник-підлеглі) та горизонталі (виконавці)).

Інтелектуальна безпека з точки зору захисту кадрової складової – це захищеність інтелектуальних ресурсів соціально-економічного розвитку, їх продукування, обміну, використання на макро- та мікроекономічних рівнях.Інтелектуальна безпека з точки зору захисту інтелектуальної власності– це захищеність знань як інтелектуальних ресурсів суспільства, що охоплює забезпечення працівників знань та їх інтелектуальної праці, інтелектуального продукту, інтелектуальної власності, інтелектуального капіталу.

Інтелектуально-кадрова безпека підприємства – це найбільш важлива складова економічної безпеки підприємства, яка має на меті виявлення, знешкодження, запобігання, відвернення та попередження загроз, небезпек і ризиків, які спрямовані на персонал та його інтелектуальний потенціал, і ті, які йдуть безпосередньо від нього, що повинно проявлятися в системі управління трудовими ресурсами та в кадровій політиці підприємства.

Інтелектуально-кадрова складоваекономічної безпеки підприємства – синтетична категорія економічної теорії, теорії управління персоналом, економіки праці, соціології, політології. ІКС економічної безпеки є уніфікованою категорією, яка виявляється на всіх рівнях від окремо взятого підприємства до національної економіки і відіграє домінуючу роль у системі безпеки компанії, оскільки ІКС первинна для інших її складових в будь-якій організації. Інтелектуально-кадрова складова включає в себе безпеку життєдіяльності, соціально-мотиваційну безпеку, кар’єрну, професійну, адміністративну безпеку та розглядається як механізм запобігання негативним впливам на економічну безпеку підприємств через ризики і погрози, пов’язані з персоналом, його інтелектуальним потенціалом і трудовими відносинами.

Аналізуючи структуру кадрової безпеки підприємства, доцільно виокремити інші пов’язані з нею ключові проблеми: · розроблення мотиваційних схем та схем оплати праці; · ліквідація збитків, пов’язаних з трудовими спорами; · аналіз ситуації конкурентів, аналіз ринку праці в регіоні; · робота з кадровим резервом, оцінка компанії чи організації як роботодавця; · способи проектування кар’єри; · підвищення лояльності та відповідальності співробітників тощо. Чинники кадрової безпеки підприємства. При прийомі на роботу працівника роботодавець має зважати на низку важливих факторів. Серед них, зокрема, можна виділити наступні: ü відповідність кваліфікації людини посаді, на яку вона претендує, ü освіта за фахом, ü особистісні якості людини, що є дуже важливим фактором тощо.

Серед методів підбору персоналу слід виділити розроблення та проведення тестів на виявлення професійної орієнтації, ерудиції, інтелекту, здібностей і розуміння. Якісна перевірка кандидатів під час прийому на роботу знизить ймовірність зловживань зі сторони решти. Серед зловживань в наш час найчастіше зустрічаються випадки підробки документів, фальсифікації витрат, пов’язаних з виконанням трудових обов’язків (відрядження, представницькі витрати), так звані «відкати» (один із найпоширеніших способів) популярні при несанкціонованих продажах і використаннях майна підприємства і т.п.

Ефективність та продуктивність роботи персоналу залежить насамперед від таких, як: · належні умови праці, · можливість кар’єрного зросту, · гідна винагорода, · гарний колектив, · захист персональних даних та ін. Кадрова безпека організації побудована на трудових та етичних відносинах інтелектуального потенціалу, які забезпечують стабільну і прибуткову роботу підприємства, запобігаючи як внутрішнім, так і зовнішнім загрозам, що сприяє розвиткові людського та соціального потенціалу, підвищення рівня і якості життя населення, що притаманні цивілізованому суспільству.

Кадрова безпека відіграє домінуючу роль у системі безпеки підприємства, оскільки це робота з персоналом, кадрами, а вони в будь-якій організації первинні.

**ІІ. ПИТАННЯ**

**Суб’єкти скоєння економічних злочинів**

Згідно з даними порталу Content Security, наявні у світі внутрішні та зовнішні загрози розподіляються таким чином: розголошення (зайва балакучість працівників) – 32%; несанкціонований доступ шляхом підкупу і схиляння до співпраці з боку конкурентів і злочинних угруповань – 24%; відсутність у компанії належного нагляду і жорстких умов забезпечення конфіденційності інформації – 14%; традиційний обмін виробничим досвідом – 12%; безконтрольне використання інформаційних систем – 10 %; наявність передумов виникнення серед персоналу конфліктних ситуацій, пов’язаних з відсутністю високої трудової дисципліни, психологічною несумісністю, випадковим підбором кадрів, слабкою роботою кадрів зі згуртування колективу – 8%.

За даними дослідження Ernst & Young, рівень зафіксованого в Україні корпоративного шахрайства трохи вищий за середній у розвинених країнах (13%), але кращий за показник країн, що розвиваються (20%). Французька ж компанія Kroll Ontrack серед десяти основних тенденцій у сфері захисту інформаційних даних називає крадіжки за сприяння інсайдерів: сьогодні прогресивні організації роблять ставку на посилення безпеки за допомогою технологій, в той час як злочинці йдуть легшим шляхом – знаходять спільників серед персоналу.

Окрім крадіжок інформації, можна зіштовхнутися і з чорним піаром з боку колишніх підлеглих, і з судовими позовами, що впливають на репутацію компанії, і з некомпетентністю «випадкового» працівника, і з помилками у кадрових документах.

До найпоширеніших видів порушень при недотриманні кадрової безпеки належать:

1) афери з боку провідних спеціалістів (менеджерів і керівників середньої ланки, відповідальних за конкретний напрям бізнесу підприємства), в основному «за стінами» своєї фірми, зокрема у міжнародних організаціях;

2) фальсифікація сум «живих грошей» («готівки») у касі й сум на банківських рахунках, підробка чеків підприємства;

3) несанкціонований продаж і використання майна (власності) підприємства із корисливою метою;

4) оплата роботи підставних («фіктивних осіб»), так званих «пролісків»;

5) фальсифікація документації підприємства за допомогою електронної техніки й Інтернету (наприклад, перерахування коштів підприємства на свій особистий рахунок, внесення «потрібних» змін у звітні документи);

6) несанкціоновані операції із цінними паперами, матеріальними й нематеріальними активами підприємства;

7) фальсифікація звітів про використання коштів, виділених на відрядження, «представницькі видатки», на інші потреби підприємства.

Мотивацію афер персоналу підприємства можна класифікувати так:

· особисті фінансові труднощі, неможливість задоволення життєвих потреб своїх та сім’ї;

· наявність слабких місць («дір») у системі управління діяльністю фірми (зокрема в системі бухгалтерського обігу);

· низька кваліфікація керівництва підприємства;

· нездоровий діловий клімат у колективі підприємства (наявність «скривджених»);

· психологічна готовність (схильність) працівника до зловживання службовим становищем;

· порочні зв’язки, вчинки, захоплення; · відсутність налагодженого контролю з боку керівництва за діяльністю персоналу;

· слабкий кадровий менеджмент, що дає змогу займати відповідальні посади співробітникам-аферистам, неефективна персональна робота з кадрами. Забезпечення кадрової безпеки є найважливішою ланкою роботи менеджера (директора) із персоналу.

Причому варто аналізувати як внутрішню, так і зовнішню небезпеку. Внутрішні кадрові небезпеки такі:

· невідповідність кваліфікації співробітників до займаної посади (небезпека, що спричиняє збитки);

· недостатня кваліфікація працівників (проблема, вирішити яку зобов’язані кадровики); · слабка організація системи управління персоналом (немає філософії підприємства);

· слабка організація системи навчання (відсутня система обліку перспектив розвитку персоналу, що створює соціальну непевність у стабільності свого службового росту);

· неефективна система мотивації (немає аналізу потреб кожної особистості й персональної мотивації);

· помилки в плануванні ресурсів персоналу (найчастіше на просту роботу приймають висококваліфікований персонал);

· відсутність творчих елементів у роботі; · нецільове використання кваліфікованих співробітників;

· працівники орієнтовані на вирішення внутрішніх тактичних завдань;

· співробітники не орієнтовані на дотримання інтересів підрозділу (немає цільового управління);

· відсутність або слабкість корпоративної політики;

· неякісні перевірки кандидатів під час прийому на роботу.

Зовнішні кадрові небезпеки: · умови мотивації в конкурентів кращі, · установка конкурентів на переманювання, · зовнішній тиск на співробітників, · втягування їх у різні види залежності, · інфляційні процеси (їх слід ураховувати під час розрахунку заробітної плати).

Ознаки правопорушення в поведінці співробітника і його неправомірні дії: 1) незвичне поводження працівника (нервозність, дратівливість, занепокоєння, перепади настрою, підозріла покірність тощо); 2) поява нестандартних даних і відхилення від звичайних (середніх) показників у бухгалтерських й/або інших документах; 3) зникнення окремих форм обліку та звітності (зокрема бланків) у бухгалтерській або іншій документації; 4) проведення сторонніх фінансових документів; 5) поява підроблених підписів і підчищень (виправлень) даних у звітній документації; 6) надання ксерокопій документів замість оригіналів; 7) різке поліпшення матеріальних можливостей співробітника, не обґрунтоване його легальною діяльністю.

**ІІІ.ПИТАННЯ**

**Основні методи профілактики правопорушень персоналу**

Основні методи профілактики правопорушень персоналу:

· Висококваліфікований кадровий менеджмент, використання сучасних технологій, персональна робота з кадрами й управління поведінкою персоналу.

· Здійснення зовнішнього й внутрішнього аудиту діяльності керівних кадрів, розподіл їхніх функцій.

· Періодичне відновлення повноважень (анулювання доручень, переділ функціональних обов’язків тощо).

· Доручення комерційних справ не одному фахівцеві, а декільком − на конкурентній основі.

· Розробка й дотримання сучасних методів охорони власності (майна) підприємства, зокрема коштів, інформаційних комунікацій.

· Оптимізація системи фінансового обліку та звітності.

· Обмежити доступ (допуск) співробітників до документів фінансової та бухгалтерської звітності. Для збереження кадрової безпеки варто використовувати сучасні кадрові технології, включаючи такі механізми: ефективну мотивацію; прискорену адаптацію (за рахунок наставництва); своєчасне запобігання конфліктним ситуаціям, атестацію; компенсацію; розумну політику звільнення; пропаганду корпоративності. Адаптація персоналу формується внаслідок психологічної сумісності з етичними цінностями компанії, соціальної сумісності в колективі, комфортності робочих місць, можливості задоволення своїх мотиваційних потреб, уваги керівництва тощо. Час адаптації − це не два місяці випробувального терміну, − вони індивідуальні для кожної особистості й кожної соціальної групи працівників.

Контроль як елемент кадрової безпеки − це комплекс засобів, установлений для персоналу (зокрема й для адміністрації), регламент, обмеження, режими, технологічні процеси, оцінювальні, контрольні та інші операції. Цей комплекс безпосередньо спрямований на ліквідацію можливостей заподіяти збитки. Його регулює, як правило, служба безпеки або інші підрозділи, але меншою мірою служба персоналу. Стимулювання. Насамперед, це матеріальне заохочення. Ефективна фінансова політика щодо співробітників − застава безпеки підприємства. Маленька зарплата фахівця може стати великою втратою для організації. Висока зарплата таїть у собі не менше проблем. Розумна зарплата плюс премія за кожний вдалий крок або за стабільну роботу −найоптимальніше рішення.

Соціальні потреби: · доручення роботи, яка дає змогу співробітникам спілкуватися; · створення особливої атмосфери, духу єдиної команди; · проведення періодичних нарад із підлеглими не тільки для прийняття стратегічних рішень, а й для обговорення поточних питань; · підтримка неформальних відносин, якщо вони не завдають збитків роботі; · створення умов для активного життя працівників поза організацією. Потреба в повазі: · підвищення змістовності роботи співробітників; · організація зворотного зв’язку за результатами роботи (реакція керівництва); · оцінювання й заохочення досягнутих результатів; · залучення підлеглих до формулювання цілей і розробки рішень; · просування підлеглих по службових сходах; · забезпечення навчання та перепідготовки співробітників, що підвищує рівень їхньої компетентності.

Потреба в самовираженні: · визначення та використання потенціалу кожного співробітника; · доручення складних і важливих завдань, що вимагають повної віддачі; · заохочення та розвиток творчих здібностей працівників. Компенсація. Співробітники зазнають стресу, фрустрації, професійних відхилень у психіці через специфіку їхньої діяльності.

Емоційне й психологічне розвантаження співробітників, компенсування всіх незручностей захистить організацію від неадекватних дій персоналу. Для цього можна: · створити кімнати відпочинку; · створити затишну обстановку в робочих приміщеннях; · організувати дозвілля; · урізноманітнити роботу; · звільняти від рутини; · стежити за їхнім здоров’ям; · увести в штат психолога, який знає специфіку роботи, або запрошувати його зі спеціалізованих фірм для моніторингу ситуації за допомогою тренінгів. Вирішення особистих проблем. Іноді особисті проблеми співробітника перестають бути винятково його справою. Часто саме проблеми в родині або загроза близьким стає причиною нелояльності.

Допомогти співробітникові можна тоді, коли керівник має на це моральне право, тобто коли працівник розуміє необхідність втручання у своє особисте життя. Для цього необхідно зробити хоча б кілька кроків:

1) створення атмосфери, що сприяє відкритому вирішенню всіх конфліктів;

2) боротьба з байдужістю як з боку колективу, так і з боку начальства;

3) залучення психолога, який займається проблемами співробітників;

4) культивування певних моральних цінностей, які допоможуть співробітникам встановити для себе певні принципи поведінки. Пропаганда корпоративності. Зміцненню корпоративного патріотизму службовців сприяють: · знання історії створення й розвитку компанії; · постійне нагадування про конкуренцію. Інформація про результати діяльності компанії.

Порівняння з конкурентами, як правило, є потужним імпульсом виховання лояльності; · установлення «неформальних» відносин усередині колективу, нормальних міжособистісних відносин. · Інформаційна політика. Недостача інформації призводить до виникнення чуток, службових інтриг, пліток і домислів. Запобігти або зменшити загрозу негативних тенденцій треба за допомогою: · чіткої інформаційної політики; · коректного ведення справ; · чіткого окреслення компетенції й посадових обов’язків; · профілактичних бесід із тими, кого можна вважати «інтриготворцями».

Комплексну оцінку рівня кадрової безпеки підприємства необхідно здійснювати на основі аналізу показників, які характеризують якість управління і організацію персоналу, розвиток інтелектуального потенціалу.

**Тема 6. Інформаційна безпека підприємства** (1 год)

ПЛАН ЛЕКЦІЇ

Вступ

1. Поняття та класифікація загроз безпеки інформації.

*2.* Методи і принципи забезпечення інформаційної безпеки.

3. Стандарт «Управління інформаційною безпекою».

# **РЕКОМЕНДОВАНА ЛІТЕРАТУРА**

1. Рибальченко Л.В., Гребенюк А.М. Стандарти управління інформаційною безпекою / Кібербезпека в Україні: правові та організаційні питання: матеріали міжн. наук. практ. конф., м. Одеса, 22 листопада 2019 р. Одеса : ОДУВС, 2019. 108 с. ISBN 678-717-70204
   1. Кавун С.В. Економічна та інформаційна безпека підприємств у системі консолідованої інформації : навчальний посібник / С. В. Кавун, А. А. Пилипенко, Д. О. Ріпка. – Х. : Вид. ХНЕУ, 2015. – 364 с
   2. Управління фінансовою безпекою економічних суб’єктів. [Текст] : навчальний посібник для студентів вищих навчальних закладів економічних і юридичних спеціальностей усіх форм навчання / Державний вищий навчальний заклад “Українська академія банківської справи Національного банку України” ; за заг. ред. д-ра екон. наук, проф. С. М. Фролова ; [С. М. Фролов, О. В. Козьменко, А. О. Бойко та ін.]. – Суми : ДВНЗ “УАБС НБУ”, 2015. – 332 с.
   3. Рябушка Л.Б. Тіньова економіка та доходи бюджету в системі економічної безпеки держави / Л. Б. Рябушка, Т. Г. Кубах // Економічна ДВНЗ “Українська академія банківської справи НБУ” 331 безпека в умовах глобалізації світової економіки: колективна монографія у 2 т. – Дніпропетровськ : “ФОП Дробязко С. І.”, 2016. – Т. 1. – С. 202–215.
   4. Орлик О.В. Економічна безпека підприємства: властивості, стратегія та методи забезпечення [Текст] / О. В. Орлик // Економічна безпека в умовах глобалізації світової економіки : у 2 т. : колективна моногр. – Дніпропетровськ : "ФОП Дробязко С.І.", 2016. – Т. 2. – С. 176–182.
   5. Кім Ю.Г. Формування системи фінансової безпеки транспортноекспедиційного підприємства: Монографія / Ю. Г. Кім. - К.: ЗАТ «Дорадо», 2017. - 170 с.

**МЕТА ЛЕКЦІЇ**

Метою лекції є надання необхідних теоретичних знань здобувачам вищої освіти юридичного факультету, що навчаються на магістерському рівні вищої освіти, щодо основних понять інформаційної безпеки на підприємстві, методів і принципів забезпечення інформаційної безпеки підприємства.

**ВСТУП**

В інформаційному праві інформаційна безпека – це одна із сторін розгляду інформаційних відносин у межах інформаційного законодавства з позиції захисту життєво важливих інтересів особистості, суспільства, держави і акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами.

**Об’єктами інформаційної безпеки**можуть бути: свідомість, психіка людини; інформаційні системи різного масштабу й різного призначення. До соціальних об’єктів інформаційної безпеки відносять особистість, колектив, державу, суспільство, світове товариство.

До **суб’єктів інформаційної безпеки** належать: держава, що здійснює свої функції через відповідні органи; громадяни, суспільні або інші організації і обʹєднання, що володіють повноваженнями щодо забезпечення інформаційної безпеки відповідно до законодавства.

**І. ПИТАННЯ**

**Поняття та класифікація загроз безпеки інформації**

**Інформаційна безпека підприємства**− це захист інформації, якою володіє підприємство (виробляє, передає або отримує) від несанкціонованого доступу, руйнування, модифікації, розкриття і затримок при надходженні.

**Інформаційна безпека підприємтва** − це суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб’єкта господарської діяльності.

**Інформаційна безпека** − це захищеність інформації та підтримуючої її інфраструктури від будь-яких випадкових або зловмисних дій, результатом яких може з’явитися нанесення збитку самої інформації, її власникам або підтримуючої інфраструктури.

Інформаційна безпека включає в себе заходи щодо захисту процесів створення даних, їх введення, обробки і виведення.

Метою комплексної інформаційної безпеки є збереження інформаційної системи підприємства в цілісності, захист і гарантування повноти і точності інформації, яку вона видає, мінімізація руйнувань і модифікація інформації, якщо такі трапляються.

Досягнення цієї метипотрібно вирішення наступних задач:

· віднесення інформації до категорії обмеженого доступу (службової таємниці);

· прогнозування і своєчасне виявлення загроз безпеці інформаційних ресурсів, причині умов, що сприяють нанесенню фінансового, матеріального і морального збитку;

· створення умов функціонування з найменшою вірогідністю реалізації загроз безпеці інформаційних ресурсів;

· створення механізму і умов оперативного реагування на загрози інформаційній безпеці з використанням правових, організаційних і технічних засобів забезпечення безпеки;

· створення умов для максимально можливого відшкодування і локалізації збитку, що виникає внаслідок дії фізичних і юридичних осіб.

**Інформаційна безпека** − це комплекс заходів, які забезпечує для охоплюваної ним інформації наступні фактори:

─ *конфіденційність* − властивість, яка гарантує, що інформація недоступна і не може бути розкрита несанкціонованими особами, об’єктами чи процесами. Можливість ознайомитись з інформацією мають лише ті особи, які володіють відповідними повноваженнями;

─ *цілісність* − властивість, яка гарантує, що система повноцінно виконує свої функції без навмисних чи випадкових несанкціонованих втручань.

Можливість внести зміни в інформацію повинні мати лише ті особи, які на це вповноважені;

─ *доступність* − можливість отримання авторизованого доступу до інформації з боку вповноважених осіб в відповідний санкціонований для роботи період часу.

Облік ведеться засобами електронних реєстраційних журналів, які використовуються в основному лише вповноваженими службами.

Забезпечення незмінності функціонування інформаційних систем має відбуватися на трьох рівнях: адміністративному − за допомогою політики безпеки організації, локальному − шляхом формування специфічних правил та рекомендаційних норм для персоналу, об’єктному – використання сертифікованих, легальних засобів програмного та апаратного забезпечення.

**4.2. Поняття та класифікація загроз безпеки інформації**

Сутність загроз інформаційної безпеки зводиться до нанесення того чи іншого збитку підприємству (організації).

Прояви можливого збитку можуть бути найрізноманітнішими:

· моральна і матеріальна шкода діловій репутації організації;

· моральний, фізичний чи матеріальний збиток, пов’язаний з розголошенням персональних даних окремих осіб;

· матеріальний (фінансовий) збиток від розголошення конфіденційної інформації;

· матеріальний (фінансовий) збиток від необхідності відновлення порушених інформаційних ресурсів, які захищаються;

· матеріальні збитки (втрати) від неможливості виконання взятих на себе зобов’язань перед третьою стороною;

· моральний і матеріальний збиток від дезорганізації в роботі всього підприємства.

Джерела зовнішніх загроз можуть бути випадковими і запланованими та мати різний рівень кваліфікації. До них відносяться:

─ кримінальні структури;

─ потенційні злочинці і хакери;

─ нечесні партнери;

─ технічний персонал постачальників послуг, тощо.

*Внутрішні суб’єкти* (джерела), як правило, представлені висококваліфікованими фахівцями у галузі розробки та експлуатації програмного забезпечення і технічних засобів, знайомі зі специфікою розв’язуваних завдань, структурою та основними функціями та принципами роботи програмно-апаратних засобів захисту інформації, мають можливість використання штатного устаткування і технічних засобів мережі. До них відносяться:

─ основний персонал (користувачі, програмісти, розробники);

─ представники служби захисту інформації;

─ допоміжний персонал (прибиральники, охорона);

─ технічний персонал;

Технічні засоби, що є джерелами потенційних загроз безпеці інформації, також можуть бути :

а) *зовнішніми:* засоби зв’язку; мережі інженерних комунікації; транспорт;

б) *внутрішніми:* неякісні технічні засоби обробки інформації; неякісні програмні засоби обробки інформації; допоміжні технічні засоби (охорони, сигналізації, телефонії); інші технічні засоби, що застосовуються в установі.

Дії, які можуть завдати шкоди інформаційній безпеці організації, можна

також розділити на 4 категорії:

1. *Дії, які здійснюються авторизованими користувачами*. У цю категорію потрапляють: цілеспрямована крадіжка або знищення даних на робочій станції або сервері; пошкодження даних користувачів у результаті необережних дій;

2. «*Електронні» методи* впливу, які здійснюються хакерами. До таких

методів відносяться: несанкціоноване проникнення в комп’ютерні мережі, атаки;

3. *Комп’ютерні віруси*. Окрема категорія електронних методів впливу - комп’ютерні віруси та інші шкідливі програми. Проникнення вірусу на вузли корпоративної мережі може призвести до порушення їх функціонування, втрат робочого часу, втрати даних, викраденні конфіденційної інформації і навіть прямим розкраданням фінансових коштів. Вірусна програма, яка проникла в корпоративну мережу, може надати зловмисникам частковий або повний контроль над діяльністю підприємства.

4*. «Природні» загрози.* На інформаційну безпеку підприємства можуть впливати різноманітні зовнішні фактори (неправильне зберігання, крадіжка комп’ютерів і носіїв, форс-мажорні обставини тощо).

У сучасних умовах наявність розвиненої системи інформаційної безпеки стає однією з найважливіших умов конкурентоспроможності і навіть життєздатності будь-якого підприємства (організації).

**ІІ.ПИТАННЯ**

**Методи і принципи забезпечення інформаційної безпеки**

Завдання забезпечення інформаційної безпеки повинно вирішуватися системно − різні засоби захисту (апаратні, програмні, фізичні, організаційні і т.д.) застосовуються одночасно і під централізованим управлінням. При цьому компоненти системи повинні «знати» про існування один одного, взаємодіяти і забезпечувати захист як від зовнішніх, так і від внутрішніх загроз.

Методи забезпечення інформаційної безпеки:

·засоби ідентифікації і аутентифікації користувачів;

·засоби шифрування інформації, що зберігається на комп’ютерах і що передається по мережах;

·міжмережеві екрани;

·віртуальні приватні мережі;

·засоби контентної фільтрації;

·інструменти перевірки цілісності вмісту дисків;

·засоби антивірусного захисту;

·системи виявлення вразливостей мереж і аналізатори мережевих атак.

Кожний з перерахованих засобів може використовуватись як самостійно, так і в інтеграції з іншими. Це робить можливим створення систем інформаційного захисту для систем будь-якої складності та конфігурації, незалежно від використовуваних платформ.

Комплекс включає аутентифікацію (або ідентифікацію), авторизацію і адміністрування. Ідентифікація та авторизація - це ключові елементи інформаційної безпеки. При спробі доступу до інформаційних активів функція ідентифікації дає відповідь на питання: чи ви є авторизованим користувачем мережі. Функція авторизації відповідає за те, до яких ресурсів конкретний користувач має доступ. Функція адміністрування полягає у наділенні користувача певними ідентифікаційними особливостями в рамках даної мережі і визначенні обсягу допустимих для нього дій.

Системи шифрування дозволяють мінімізувати втрати у випадку несанкціонованого доступу до даних, що зберігаються на жорсткому диску або іншому носії, а також перехоплення інформації при її пересилання по електронній пошті або передачу з мережних протоколах. Завдання данного засобу захисту − забезпечення конфіденційності. Основні вимоги, що пред’являються до систем шифрування − високий рівень криптостійкості та легальність використання на території держави.

*Міжмережевий екран* − це система або комбінація систем, що утворить між двома чи більш мережами захисний бар’єр, якій захищає від несанкціонованого потрапляння в мережу або виходу з неї пакетів даних.

Основний принцип дії міжмережевих екранів − перевірка кожного пакету даних на відповідність вхідної та вихідної IP адреси базі дозволених адрес. Таким чином, міжмережеві екрани значно розширюють можливості сегментації інформаційних мереж та контролю за циркулюванням даних.

Ефективний засіб захисту від втрати конфіденційної інформації − фільтрація вмісту вхідної і вихідної електронної пошти. Перевірка поштових повідомлень на основі правил, встановлених в організації, дозволяє також забезпечити безпеку компанії від відповідальності за судовими позовами і захистити їх співробітників від спаму.

Засоби контентної фільтрації дозволяють перевіряти файли всіх розповсюджених форматів, у тому числі стислі і графічні. При цьому пропускна здатність мережі практично не змінюється.

Всі зміни на робочій станції або на сервері можуть бути відслідковані адміністратором мережі або іншим авторизованим користувачем завдяки технології перевірки цілісності вмісту жорсткого диска. Це дозволяє виявляти будь-які дії з файлами (зміна, видалення або ж просто відкриття) і ідентифікувати активність вірусів, несанкціонований доступ або крадіжку даних авторизованими користувачами. Контроль здійснюється на основі аналізу контрольних сум файлів (CRC сум).

Сучасні антивірусні технології дозволяють виявити практично всі вже відомі вірусні програми через порівняння коду підозрілого файлу із зразками, що зберігаються в антивірусній базі. Крім того, розроблені технології моделювання поведінки, що дозволяють виявляти новостворювані вірусні програми. Виявлені об’єкти можуть піддаватися лікуванню, ізолюватися (міститися в карантин) або видалятися. Захист від вірусів може бути встановлено на робочі станції, файлові і поштові сервера, міжмережеві екрани, що працюють під практично будь-якою з поширених операційних систем (Windows, Unix-і Linux-системи, Novell) на процесорах різних типів.

Фільтри спаму значно зменшують невиробничі затрати праці, пов’язані з розглядом спаму, знижують трафік і завантаження серверів, покращують психологічний фон в колективі і зменшують ризик залучення співробітників компанії в шахрайські операції. Крім того, фільтри спаму зменшують ризик зараження новими вірусами, оскільки повідомлення, що містять віруси (навіть ще не включені до бази антивірусних програм) часто мають ознаки спаму і фільтруються.

Для протидії природним загрозам інформаційної безпеки в компанії має бути розроблений і реалізований набір процедур щодо запобігання надзвичайних ситуацій (наприклад, щодо забезпечення фізичного захисту даних від пожежі) та мінімізації збитків у тому випадку, якщо така ситуація все-таки виникне. Один з основних методів захисту від втрати даних – резервне копіювання з чітким дотриманням встановлених процедур (регулярність, типии носіїв, методи зберігання копій тощо.

*Основними принципами інформаційної безпекипідприємства* є:

- забезпечення цілісності і збереження даних, тобто надійне їх

зберігання в неспотвореному вигляді;

- дотримання конфіденційності інформації (її недоступність для тих

користувачів, які не мають відповідних прав);

- доступність інформації для всіх авторизованих користувачів за

умови контролю за всіма процесами використання ними отриманої інформації;

- безперешкодний доступ до інформації в будь-який момент, коли

вона може знадобитися підприємству.

Ці принципи неможливо реалізувати без особливої інтегрованої системи

інформаційної безпеки, що виконує наступні функції:

─ вироблення політики інформаційної безпеки;

─ аналіз ризиків (тобто ситуацій, в яких може бути порушена нормальна

робота інформаційної системи, а також втрачені або розсекречені дані);

─ планування заходів щодо забезпечення інформаційної безпеки;

─ планування дій в надзвичайних ситуаціях;

─ вибір технічних засобів забезпечення інформаційної безпеки.

Етапи проведення робіт із забезпечення інформаційної безпеки підприємства:

1. Проведення обстеження підприємства на предмет виявлення реальних загроз несанкціонованого доступу до конфіденційної інформації;

2. Розробка політики безпеки, організаційно-розпорядчих документів і заходів щодо забезпечення інформаційної безпеки системи відповідно до вимог по захищеності технічних і програмних засобів від витоку конфіденційної інформації;

3. Проектування системи інформаційної безпеки;

4. Створення прототипу системи інформаційної безпеки;

5. Розробка зразка системи інформаційної безпеки;

6. Впровадження системи інформаційної безпеки в діючу структуру

підприємства;

7. Навчання персоналу;

8. Атестація системи інформаційної безпеки підприємства.

Метою комплексної інформаційної безпеки є збереження інформаційної системи підприємства, захист і гарантування повноти і точності виданої нею інформації, мінімізація руйнувань і модифікація інформації, якщо такі трапляються.

Для оцінки рівня інформаційної безпеки можуть бути використані коефіцієнти:

- *коефіцієнт повноти інформації (Кпі)* – розраховується як відношення обсягу інформації, що є в розпорядженні особи, яка приймає рішення (ОПР), і обсягу інформації, необхідної для ухвалення обґрунтованого рішення;

- *коефіцієнт точності інформації (Кті)* – розраховується як відношення обсягу релевантної інформації до загального обсягу наявної в розпорядженні ОПР інформації;

- *коефіцієнт суперечливості інформації (Ксі)* – розраховується як відношення кількості незалежних свідчень на користь ухвалення рішення до загальної кількості незалежних свідчень у сумарному обсязі релевантної інформації.

Рівень інформаційної безпеки може бути визначений на основі добутку трьох згаданих коефіцієнтів:

*Кі = Кпі\*Кті\*Ксі.*

При цьому, якщо:

*Кі* ≥ 0,7 – рівень інформаційної безпеки високий;

0,3 ≤ *Кі*<0,7 – рівень інформаційноїбезпеки середній;

*Кі<*0,3 – рівень інформаційної безпеки низький.

**ІІІ. ПИТАННЯ**

**Стандарт «Управління інформаційною безпекою»**

В наш цифровий час дуже швидкими темпами розвиваються різноманітні інформаційні технології, але на жаль разом з ними розвивається і кіберзлочинність.

Ключовим моментом захисту від кіберзлочинності є підготовка і виявлення вразливих місць, а також стійкість з точки зору взаємодії з загальними системами управління. Керувати інформаційною безпекою, а також визначити злочинців і притягнути їх до відповідальності допоможуть стандарти серії **ISO/IEC 27000**, розроблені спільним технічним комітетом Міжнародної організації з стандартизації (ISO) та Міжнародної електротехнічної комісії (IEC)  - ISO/IEC JTC 1.

Перший стандарт серії, **ISO/IEC 27001** щодо систем управління інформаційною безпекою (ISMS), опубліковано вже більше 20 років тому.  З того часу у серії видано понад  40 міжнародних стандартів, що охоплюють все: від  створення спільного словника (**ISO/IEC 27000**), управління ризиками (**ISO/IEC 27005**), безпеки у хмарних технологіях (**ISO/IEC 27017 і ISO/IEC 27018**) до методів судової експертизи, що використовують для аналізу цифрових доказів та  розслідування інцидентів I**SO/ IEC 27042 та ISO/IEC 27043** відповідно).

Наприклад, **ISO/IEC 27043** пропонує настанови, що описують процеси та принципи, які  застосовують до різних видів досліджень, включаючи несанкціонований доступ, пошкодження даних, збої в системі або корпоративні порушення інформаційної безпеки, а також будь-які інші цифрові дані розслідування.

Розробники  стандартів серії  **ISO/IEC 27000** зазначають,  що основоположний стандарт серії **ISO/IEC 27001** постійно вдосконалюється, що дає можливість підприємствам постійно оновлюватися у боротьбі з кіберзлочинністю. Завдяки впровадженню стандарту **ISO/IEC 27001** організація може оцінювати свої ризики, впроваджувати засоби контролю щодо їх пом’якшення, а потім контролювати та переглядати свої ризики та контроль за ними, покращуючи, за необхідності, захист. Таким чином, вона завжди готова  до атак.

Системи управління інформаційною безпекою ISMS  застосовують до всіх типів організацій та всіх видів підприємницької діяльності,  зокрема для малих та середніх підприємств (SMEs), які є частиною ланцюгів постачання, і тому дуже важливо, щоб вони контролювали та керували своєю інформаційною безпекою та кібер-ризиками, щоб захистити себе та інших.

А нещодавно почалась розробка нового стандарту у сфері інформаційної безпеки - **ISO/IEC 27552 «Методи захисту. Розширення ISO/IEC 27001 та ISO/IEC 27002 для управління інформацією про конфіденційність. Вимоги та керівні вказівки»**,  який додатково розширює **ISO/IEC 27001** для вирішення конкретних потреб у сфері конфіденційності. Наразі, на стадії проекту, документ визначає вимоги та надає настанови щодо підтримання та постійного вдосконалення управління приватним життям у контексті організації.

Таким чином, стандарти серії ISO/IEC 27000 дійсно допомагають зробити безпечнішими усі сфери інформаційного життя, захищаючи приватність, фінанси, індивідуальну або корпоративну репутацію, при цьому постійно розвиваючись і вдосконалюючись.

**Лекція №4**

**Тема 7. Ринкова та зовнішньоекономічна безпека** (1 год)

ПЛАН ЛЕКЦІЇ

Вступ

* + 1. Ринкова складова економічної безпеки підприємства (РБП).
    2. Експортна безпека як важлива складова зовнішньоекономічної безпеки.

3*.* Аналітична оцінка конкурентів як важлива складова ринкової безпеки.

# **РЕКОМЕНДОВАНА ЛІТЕРАТУРА**

* 1. Управління фінансовою безпекою економічних суб’єктів. [Текст] : навчальний посібник для студентів вищих навчальних закладів економічних і юридичних спеціальностей усіх форм навчання / Державний вищий навчальний заклад “Українська академія банківської справи Національного банку України” ; за заг. ред. д-ра екон. наук, проф. С. М. Фролова ; [С. М. Фролов, О. В. Козьменко, А. О. Бойко та ін.]. – Суми : ДВНЗ “УАБС НБУ”, 2015. – 332 с.
  2. Рябушка Л. Б. Тіньова економіка та доходи бюджету в системі економічної безпеки держави / Л. Б. Рябушка, Т. Г. Кубах // Економічна ДВНЗ “Українська академія банківської справи НБУ” 331 безпека в умовах глобалізації світової економіки: колективна монографія у 2 т. – Дніпропетровськ : “ФОП Дробязко С. І.”, 2016. – Т. 1. – С. 202–215.
  3. Орлик, О. В. Економічна безпека підприємства: властивості, стратегія та методи забезпечення [Текст] / О. В. Орлик // Економічна безпека в умовах глобалізації світової економіки : у 2 т. : колективна моногр. – Дніпропетровськ : "ФОП Дробязко С.І.", 2016. – Т. 2. – С. 176–182.
  4. Кім Ю. Г. Формування системи фінансової безпеки транспортноекспедиційного підприємства: Монографія / Ю. Г. Кім. - К.: ЗАТ «Дорадо», 2017. - 170 с.

**МЕТА ЛЕКЦІЇ**

Метою лекції є надання необхідних теоретичних знань здобувачам вищої освіти юридичного факультету, що навчаються на магістерському рівні вищої освіти, щодо основних понять ринкової складової економічної безпеки підприємства, оцінка конкурентів та експортна безпека.

**ВСТУП**

Ринкова складова економічної безпеки підприємства (РБП) - це захист від неефективно обраної моделі поведінки на ринку, помилок у товарній збутовій політиці, політиці ціноутворення, виготовлення неконкурентоспроможної продукції. Ця складова економічної безпеки характеризує ступінь відповідності внутрішніх можливостей розвитку підприємства зовнішнім можливостям, які генеруються ринковим середовищем. За ринкову складову безпеки на підприємстві має відповідати служба маркетингу. Ця складова відображає рівень відповідності внутрішніх виробничих можливостей підприємства зовнішнім, які формуються в ринковому середовищі, тобто наскільки науково-дослідна робота, виробнича і збутова діяльність відповідають запитам ринку і конкретним потребам споживачів.

Значущість РБП полягає в тому, що вона відповідає за доведення виготовленої продукції до конкретного споживача. Відомо, що всі зусилля з виробництва будуть зведені нанівець, якщо продукція не буде продана.

Неузгоджена робота маркетологів, дизайнерів, конструкторів, економістів, фінансистів, низька якість виготовленої продукції, невчасне реагування на зміну кон'юнктури ринку, неефективна збутова мережа, низький рівень культури підприємства - це чинники внутрішнього середовища, які створюють загрозу ринковій безпеці підприємства.

**І. ПИТАННЯ**

**Ринкова складова економічної безпеки підприємства (РБП)**

*Ринкова складова економічної безпеки підприємства (РБП)*− це захист від неефективно обраної моделі поведінки на ринку, помилок у товарній збутовій політиці, політиці ціноутворення, виготовлення неконкурентоспроможної продукції. Ця складова економічної безпеки характеризує ступінь відповідності внутрішніх можливостей розвитку підприємства зовнішнім можливостям, які генеруються ринковим середовищем. Про ослаблення ринкової безпеки свідчать:

· зменшення частки ринку, яку займає підприємство;

· ослаблення конкурентних позицій і спроможності протидіяти конкурентному тиску;

· зниження адаптаційних можливостей підприємства до змін ситуації на ринку, відставання від вимог ринку і т. ін.

За ринкову складову безпеки на підприємстві має відповідати служба маркетингу. Ця складова відображає рівень відповідності внутрішніх виробничих можливостей підприємства зовнішнім, які формуються в ринковому середовищі, тобто наскільки науково-дослідна робота, виробнича і збутова діяльність відповідають запитам ринку і конкретним потребам споживачів.

Значущість РБП полягає в тому, що вона відповідає за доведення виготовленої продукції до конкретного споживача. Відомо, що всі зусилля з виробництва будуть зведені нанівець, якщо продукція не буде продана.

Неузгоджена робота маркетологів, дизайнерів, конструкторів, економістів, фінансистів, низька якість виготовленої продукції, невчасне реагування на зміну кон’юнктури ринку, неефективна збутова мережа, низький рівень культури підприємства - це чинники внутрішнього середовища, які створюють загрозу ринковій безпеці підприємства.

*Зовнішній чинник*− це неконтрольоване підприємством середовище, яке складається з покупців, посередників, конкурентів, фінансових установ, рекламних агентств, митних і податкових організацій.

На ринкову безпеку впливають: нечесні дії конкурентів, рівень платоспроможності покупців, часті зміни податків, курсу валют, політична ситуація в країні і світі.

Що більше уваги приділяє підприємство вивченню навколишнього середовища, стежить за ним, аналізує всі зміни, то швидше можна передбачити небезпеку, вигідніше використати внутрішні можливості, прибутковіше вести бізнес.

Ринкова безпека підприємства характеризується наступними показниками:

*Коефіцієнт ринкової віддачі активів* розраховується за формулою

https://pidruchniki.com/imag/econom/ort_eb/image057.jpg

де Пч − чистий прибуток підприємства, грн.; А - активи підприємства, грн.

*Конкурентоспроможність продукції (послуг)* розраховується за

формулою

https://pidruchniki.com/imag/econom/ort_eb/image058.jpg

де Ц виробу − ціна виробу підприємства, грн.;

Цеталон− ціна еталонного виробу, грн.

*Частка фірми на ринку*розраховується за формулою

https://pidruchniki.com/imag/econom/ort_eb/image059.jpg

де Пч − чистий прибуток підприємства, грн.;

Опродажу− обсяг продажу галузі, грн.

Коефіцієнт інноваційних витрат розраховується за формулою

https://pidruchniki.com/imag/econom/ort_eb/image060.jpg

де Він − інноваційні витрати підприємства, грн.;

Взаг −загальні витрати підприємства, грн.

*Ритмічність збуту* розраховується за формулою

https://pidruchniki.com/imag/econom/ort_eb/image061.jpg

де Оплан − плановий обсяг продажу за і-й період, грн.;

Офакт− фактичний обсяг продажу за той самий період, грн.

*Коефіцієнт ефективності рекламної політики підприємства (організації)* розраховується за формулою

https://pidruchniki.com/imag/econom/ort_eb/image062.jpg

де Врек − витрати на рекламу, грн.;

ВП − валовий прибуток, грн.

Західні комерційні структури використовують таке поняття, як **бенчмаркінг** − це вивчення досвіду, стратегії, рішень, ділової практики кращих компаній галузі з метою використання в адаптованому вигляді для поліпшення якості роботи своєї компанії.

**Бенчмаркінг** − це метод управління, орієнтований на відтворення еталона, якій передбачає збирання інформації про чужі еталони і ключові параметри бізнес-операцій (бенчмарках) та їх відтворення у своїх компаніях.

**Бенчмаркінг** − це порівняння ефективності системи з якимось установленим, прийнятим значенням. У США, Японії та інших країнах програми бенчмаркінгу розвиваються за державної підтримки; діють також індустріальні бюро знайомств, мета яких − пошук партнерів з бенчмаркінгу.

**Бенчмаркінг** − це система методів і способів вивчення позитивного досвіду партнерів та конкурентів, розроблення взаємозв’язаної системи показників ефективності й рентабельності, вивчення особливостей досягнення кожного з них окремо і в сукупності, в основі чого лежить свідоме відтворення та впровадження у власному бізнесі необхідного комплексу бізнес-рішень.

**ІІ.ПИТАННЯ**

Експортна безпека як важлива складова зовнішньоекономічної безпеки

Комплекс факторів, пов’язаних із станом та перспективами розвитку експорту, необхідно сформувати у цілісну систему заходів державного стимулювання експорту з метою створення сприятливих економічних, правових, організаційних та інших умов для розширення експорту та надання вітчизняним експортерам відповідної допомоги в фінансовій, правовій, інформаційній, дипломатичній, маркетинговій сферах.

Важливо, щоб Україна інтегрувалася у світову економіку як рівноправний партнер, що можливо лише за умов кардинального поліпшення структури зовнішньоекономічної діяльності за рахунок поставок готової продукції, використання інвестицій виробничої та науково-технічної кооперації тощо. Необхідно ефективно використовувати для розвитку експортного потенціалу різні форми міжнародного економічного співробітництва. Йдеться про створення спільних підприємств, міжнародний лізинг, створення вільних економічних зон, прикордонну торгівлю, розвиток міжнародного туризму.

Стимулювання розвитку експорту та забезпечення експортної безпеки підприємств повинно включати насамперед економічні та організаційно-правові заходи.

*Економічні заходи* експортної безпеки повинні полягати у забезпеченні:

- страхування експортних кредитів від комерційних та політичних ризиків;

- надання урядом гарантій щодо залучення кредитних ресурсів в експортоорієнтовані виробництва, запровадження спеціальної системи кредитування обігових коштів виробництв;

- надання державної фінансової підтримки експортерам промислової продукції;

- податкового заохочення експортерів (повернення податку на добавлену вартість у разі експорту продукції тощо);

- митно-тарифного стимулювання.

Серед *організаційно-правових заходів експортної безпеки* доцільно виділити:

- вдосконалення правової бази розвитку експортної діяльності;

- створення системи зовнішньоторговельної інформації;

- державну підтримку просування української продукції на зовнішні ринки;

- організацію ефективної системи сертифікації експортної продукції;

- підвищення ролі закордонних українських представництв у дипломатичній підтримці ними важливих експортних операцій, попередніх маркетингових досліджень, зусиль щодо організації зарубіжних виставок, ярмарків тощо;

- проведення наукових досліджень у зовнішньоекономічній сфері, зокрема досліджень кон’юнктури товарів на зовнішніх ринках;

- підготовка кваліфікованих кадрів для діяльності в зовнішньоекономічній сфері;

- здійснення ефективного державного контролю за зовнішньо-економічними операціями з метою попередження порушень, збір інформації щодо ділової репутації та фінансового стану учасників зовнішньоекономічної діяльності, обмін нею з органами безпеки інших країн;

- створення та підтримка об’єднань експортерів, координація їх діяльності на зовнішніх ринках з метою ефективного використання кон’юктури та дотримання правил конкуренції.

Цікавою для України видається експортна політика Південної Кореї, що передбачає різноманітні пільги для експортерів, зведення до мінімуму різних бюрократичних перешкод і навіть запровадження святкування Дня експортера, яке відзначається щорічно в останній день листопада.Для успішної інтеграції України у світову економіку слід ураховувати нинішнє її становище у міжнародному розподілі праці, а також характер політичних відносин з окремими країнами та групами країн. Важливо також враховувати тенденції розвитку сучасного світового господарства, щоб формувати науково обгрунтовану і ефективну зовнішньоекономічну політику України.

**ІІІ.ПИТАННЯ**

**Імпортна безпека як важлива складова зовнішньоекономічної**

**безпеки**

**Імпортна безпека –** є важливою складовою зовнішньоекономічної безпеки, яка визначається як раціональна товарна та географічна збалансованість імпорту, що позитивно впливає на розвиток національної економіки, захищає внутрішній ринок і національного товаровиробника, сприяє зміцненню конкурентоспроможності вітчизняної продукції та економічної незалежності України.

Оптимальний обсяг імпорту та його регіональний поділ повинні визначатися для кожного виду товару з урахуванням найважливіших зовнішніх та внутрішніх факторів зовнішньоекономічної діяльності.

Держава може впливати на імпорт за допомогою тарифних та нетарифних методів.

Тариф на імпорт є найпоширенішим видом обмеження торгівлі, що являє собою державний грошовий збір із ввезених товарів, які пропускаються через кордон країни під контролем митного відомства.

Існують два основні види митних тарифів:

*специфічні*, які визначаються у вигляді фіксованої суми з одиниці виміру (наприклад, ваги, площі, кількості тощо);

*адвалорне мито*, яке встановлюється у вигляді відсотка з митної вартості товару.

Введення імпортного тарифу призводить до збільшення ціни імпортованих товарів, скорочення обсягу імпорту, збільшенню цін на подібні товари вітчизняного виробництва і, як результат, зростання вітчизняного виробництва даного товару.

Щодо нетарифних методів регулювання державою імпорту, то найбільш поширеною формою їх є квотування, яке являє собою обмеження в кількісному або вартісному вираженні обсягу продукції, дозволеної до ввозу в країну за визначений період.

Вплив квоти на рівень добробуту ідентичний впливові тарифу. Різниця полягає в тому, що при введенні тарифу держава завжди одержує додатковий дохід, а при встановленні квоти частина цього доходу може дістатися імпортеру. Однак квота дає гарантію, що імпорт не буде перевищувати визначену величину, оскільки позбавляє іноземних конкурентів можливості розширювати продаж за рахунок зниження цін.

Для забезпечення імпортної безпеки країни слід здійснити низку заходів, а саме:

• привести товарну структуру імпорту у відповідність із потребами національної економіки;

• забезпечити спрямування імпорту на структурну перебудову економіки, передусім на створення замкнених технологічних циклів;

• активно залучати передові технології для модернізації національного виробництва;

• здійснювати географічну диверсифікацію імпорту з метою зменшення ресурсної, фінансової та технічної залежності України;

• надавати підтримку вітчизняним виробникам у сфері освоєння продукції, що дозволяє зменшити імпорт закордонних аналогів;

• вдосконалити чинне законодавство для ефективного регулювання імпорту;

• розробити економічно обґрунтовану систему тарифного регулювання імпорту з метою насичення внутрішнього ринку необхідними товарами;

• законодавчо оформити внесення змін до переліку країн (у бік їхнього зменшення), на які поширюється преференційний режим;

• здійснювати сертифікацію імпортної продукції відповідно до норм міжнародної практики і національного законодавства з метою запобігання ввезенню в Україну недосконалої, застарілої та екологічно небезпечної продукції;

• здійснювати імпорт дефіцитної сировини з метою збереження обмежених власних ресурсів;

• у разі необхідності здійснювати обмеження імпорту з метою захисту вітчизняних товаровиробників та споживчого ринку.

Насамперед доцільно здійснювати імпорт таких передових технологій, які сприятимуть технічному переозброєнню та модернізації вітчизняної промисловості, припиненню нераціонального імпорту і зростанню експорту високотехнологічної та наукоємної продукції.

**ІV. ПИТАННЯ**

**Аналітична оцінка конкурентів як важлива складова ринкової безпеки**

Метою аналітичної оцінки конкурентів є визначення напрямів діяльності та способів ведення конкурентної боротьби.

***Конкурент*** (від лат. сопсигго −«стикатись») − товаровиробник, розширення або збереження обсягів діяльності якого призводить до зменшення ринкової частки іншого товаровиробника – суб’єкта цього ринку або ринку взаємозамінюваного товару. Це зовнішній фактор, вплив якого неможливо оскаржувати і в багатьох випадках не споживачі, а саме конкуренти визначають, якого роду діяльності результати можливо продати, яку ціну запросити. Визначення головних конкурентів дозволяє більш ефективно будувати свою конкурентну стратегію і тактику, економить час та гроші на проведення аналізу конкурентів.

Підходи до аналізу конкурентів. Для чіткого аналізу і отримання високих результатів принципово важливим є вільний вибір об`єктивної бази аналізу. Об’єктами аналізу конкурентів можуть виступати:

· майбутні цілі конкурентів;

· поточна стратегія;

· можливості (сильні та слабкі місця конкурента);

· характер реакції конкурента;

· стратегічна орієнтація організації та її економічна політика;

· рівень якості продукту;

· організація збуту та реалізації продукції;

· маркетингові можливості;

· виробничий потенціал, забезпеченість енергією та сировиною;

· фінансова ситуація;

· рівень наукових досліджень і розробок;

· географічна локалізація системи виробництва та збуту;

· рівень витрат на виробництво;

· якість підготовки керівників і персоналу;

· наявність торгової марки/імідж фірми (за А. Роу).

Найчастіше використовується функціональний підхід до оцінювання потенціалу конкурента та стратегій його використання. Зіставлення об’єктів аналізу під час оцінювання рівня конкурентоспроможності дає змогу зосередити увагу на більш або менш глибокому проникненні у функціональні підсистеми конкурента. Відповіді на ці запитання можна дістати, якщо проводити поглиблений аналіз конкурентів, які опинилися всередині однієї «стратегічної групи».

При аналізі конкурентів створюється величезна потреба в достатній і повній інформації для проведення попередніх аналітичних процедур.

Ефективність процесу збору інформації залежить від організованого механізму - певного типу системи дослідження конкурента, елементи якої можуть змінюватися залежно від потреб конкретної фірми, що випливають із специфіки галузі, можливостей її персоналу, інтересів та здібностей її керівництва.

**Тема 8. Фінансова безпека** (1 год)

ПЛАН ЛЕКЦІЇ

Вступ

1. Формування системи фінансової безпеки.

2. Зовнішні та внутрішні загрози фінансової безпеки

3. Валютна складова фінансової безпеки

4.Індикатори фінансової безпеки підприємства

# **РЕКОМЕНДОВАНА ЛІТЕРАТУРА**

* 1. Управління фінансовою безпекою економічних суб’єктів. [Текст] : навчальний посібник для студентів вищих навчальних закладів економічних і юридичних спеціальностей усіх форм навчання / Державний вищий навчальний заклад “Українська академія банківської справи Національного банку України” ; за заг. ред. д-ра екон. наук, проф. С. М. Фролова ; [С. М. Фролов, О. В. Козьменко, А. О. Бойко та ін.]. – Суми : ДВНЗ “УАБС НБУ”, 2015. – 332 с.
  2. Рябушка Л. Б. Тіньова економіка та доходи бюджету в системі економічної безпеки держави / Л. Б. Рябушка, Т. Г. Кубах // Економічна ДВНЗ “Українська академія банківської справи НБУ” 331 безпека в умовах глобалізації світової економіки: колективна монографія у 2 т. – Дніпропетровськ : “ФОП Дробязко С. І.”, 2016. – Т. 1. – С. 202–215.
  3. Орлик, О. В. Економічна безпека підприємства: властивості, стратегія та методи забезпечення [Текст] / О. В. Орлик // Економічна безпека в умовах глобалізації світової економіки : у 2 т. : колективна моногр. – Дніпропетровськ : "ФОП Дробязко С.І.", 2016. – Т. 2. – С. 176–182.
  4. Кім Ю. Г. Формування системи фінансової безпеки транспортноекспедиційного підприємства: Монографія / Ю. Г. Кім. - К.: ЗАТ «Дорадо», 2017. - 170 с.
  5. Рибальченко Л.В., Сауліна А.І., Піжак В.М., Заходи боротьби та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом в сфері економічної безпеки України / The 4th International scientific and practical conference “Scientific achievements of modern society” (December 4-6, 2019) Cognum Publishing House, Liverpool, United Kingdom. - 2019. С. 555-559.

6. Кокарєв І.В., Е.В. Рижков, Рибальченко Л.В., Сидоренко К.Г., Тютченко С.М. Методичні рекомендації з документування та викриття діяльності організованих злочинних груп, пов’язаної з мінімізацією доходів та легалізацією коштів / Дніпро: Дніпропетровський державний університет внутрішніх справ, 2019. – 36 с.

7. І.В. Кокарєв, Е.В. Рижков, Рибальченко Л.В., Сидоренко К.Г. Методичні рекомендації з виявлення конвертаційних центрів / Дніпро: Дніпропетровський державний університет внутрішніх справ, 2019. – 34 с.

**МЕТА ЛЕКЦІЇ**

Метою лекції є надання необхідних теоретичних знань здобувачам вищої освіти юридичного факультету, що навчаються на магістерському рівні вищої освіти, щодо основних понять фінансової та валютної складових безпеки підприємства, а також індикаторів фінансової безпеки підприємства.

**ВСТУП**

У сучасних економічних умовах діяльність підприємств, незалежно від форми власності та організаційно-правової форми господарювання, схильна до постійного ризику та загроз, що пов'язані з посиленням впливу факторів зовнішнього та внутрішнього середовища на їх функціонування. Постійне підвищення ризиковості господарської діяльності може спричинити значне зниження рівня фінансового стану підприємства, а в майбутньому призвести до банкрутства, і потребує від кожного суб'єкта господарювання розробки та реалізації системи фінансово-економічної безпеки.

Фінансово-економічна безпека підприємства є досить складною системою, що включає певний набір внутрішніх характеристик, спрямованих на забезпечення ефективності використання матеріальних, трудових, інформаційних і фінансових ресурсів.

**І. ПИТАННЯ**

Формування системи фінансової безпеки. Основні поняття

***Фінансова безпека підприємства*** − це захищеність його діяльності від негативних впливів зовнішнього середовища, а також спроможність швидко усунути різноманітні загрози або пристосуватися до існуючих умов, що не позначаються негативно на його діяльності. Зміст даного поняття містить у собі систему засобів, що забезпечують конкурентоспроможність і фінансову стабільність підприємства, а також сприяють підвищенню рівня добробуту робітників.

***Фінансова безпека підприємства*** − це такий стан корпоративних фінансових ресурсів і підприємницьких можливостей, за якого гарантується найбільш ефективне їхнє використання для стабільного функціонування та динамічного розвитку, запобігання внутрішнім і зовнішнім негативним впливам (загрозам).

***Фінансова безпека підприємства*** − це захист життєво важливих інтересів підприємства, за якого забезпечуються його сталий розвиток, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз економічним інтересам.

Необхідність постійного дотримання фінансової безпеки зумовлюється об’єктивно наявним для кожного суб’єкта господарювання завданням забезпечення стабільності функціонування та досягнення головних цілей своєї діяльності. Рівень фінансової безпеки підприємства залежить від того, наскільки ефективно її керівництво і спеціалісти (менеджери) будуть спроможні уникнути можливих загроз і ліквідувати шкідливі наслідки окремих негативних складових зовнішнього і внутрішнього середовища.

Джерелами негативних впливів на фінансову безпеку можуть бути:

1) свідомі чи несвідомі дії окремих посадових осіб і суб’єктів господарювання (органів державної влади, міжнародних організацій, підприємств-конкурентів);

2) збіг об’єктивних обставин (стан фінансової кон’юнктури на ринках

даного підприємства, наукові відкриття та технологічні розробки, форс мажорні обставини тощо).

Залежно від суб’єктної обумовленості негативні впливи на фінансову безпеку можуть мати об’єктивний і суб’єктивний характер.

Об’єктивними вважаються такі негативні впливи, які виникають не з волі конкретного підприємства, або його окремих працівників.

Суб’єктивні впливи мають місце внаслідок неефективної роботи підприємства в цілому або окремих його працівників (передовсім керівників і функціональних менеджерів).

**ІІ.ПИТАННЯ**

**Зовнішні та внутрішні загрози фінансової безпеки**

*Зовнішні загрози фінансової безпеки* підприємства складають:

· несприятливі макроекономічні умови: загальноекономічна ситуація в країні і регіоні, кризи;

· урядові кризи;

· нестабільність нормативно-правової бази;

· нестабільність податкової, кредитної і страхової політики країни;

· рівень інфляції і прогноз інфляції;

· нестабільність валютної політики держави;

· брак коштів для інвестування в регіоні, низький рівень інвестиційної активності;

· несприятливі умови кредитування підприємств, зміна процентних ставок за кредитами;

· недобросовісна конкуренція на ринку;

· несприятлива криміногенна обстановка в регіоні, поширення кримінальних і фінансових злочинів у фінансово-кредитній сфері;

· природні катаклізми.

*Внутрішні загрози фінансової безпеки*підприємства включають:

· некваліфіковане управління, помилки в стратегічному плануванні і ухваленні тактичних рішень;

· слабке маркетингове опрацювання ринку;

· недостатня ліквідність активів підприємства;

· низький рівень кваліфікації основного персоналу;

· неконкурентна цінова політика;

· слабке технічне озброєння підприємства;

· перебої в роботі устаткування і комунікацій;

· помилки в організації збереження фінансових і матеріальних цінностей;

· просочування стратегічної і фінансової інформації підприємства, недоліки в організації роботи служби безпеки підприємства;

· низький рівень бізнес репутації підприємства;

· відсутність планування діяльності підприємства в аварійних ситуаціях;

· недотримання контрактів і договірних зобов’язань.

Аналіз внутрішніх і зовнішніх загроз фінансової безпеки підприємства потрібен при стратегічному плануванні діяльності підприємства і дозволяє прийняти правильні тактичні рішення для забезпечення успішної фінансової діяльності підприємства.

*Головна мета фінансової безпеки підприємства* полягає в тім, щоб гарантувати його стабільне та максимально ефективне функціонування тепер і високий потенціал розвитку в майбутньому.

До основних функціональних цілей фінансової безпеки належать:

• забезпечення високої фінансової ефективності роботи;

• підтримка фінансової стійкості та незалежності підприємства;

• забезпечення високої ліквідності активів;

• підтримка належного рівня ділової активності;

• забезпечення захисту інформаційного поля і комерційної таємниці;

• ефективна організація безпеки капіталу та майна підприємства, а також його комерційних інтересів.

Головна та функціональні цілі зумовлюють формування необхідних структуроутворюючих елементів і загальної схеми організації фінансової безпеки.

Загальна схема процесу організації фінансової безпеки включає такі дії (заходи), що здійснюються послідовно або одночасно:

1) Формування необхідних фінансових ресурсів.

2) Прогнозування та планування фінансової безпеки.

3) С тратегічне планування фінансово-господарської діяльності

підприємства.

4) Загально-тактичне планування фінансової безпеки.

5) Тактичне планування фінансово-господарської діяльності підприєм-

ства.

6)Оперативне управління фінансово-господарською діяльністю підприємства.

7) Здійснення функціонального аналізу рівня фінансової безпеки.

8) Загальна оцінка досягнутого рівня фінансової безпеки.

*Оцінювання безпеки грошового обігу*

Ринкова економіка може ефективно функціонувати лише за умови існування досконалої грошової системи, яка полегшує економічний розвиток.

Незаперечним є вплив характеру формування грошової маси як одного з

найважливіших елементів фінансової системи на рівень фінансової безпеки

країни, у тому числі і підприємства.

***Грошова маса в обігу*** є кількісною характеристикою руху грошей на

певну дату і за певний період й означає всю сукупність грошових коштів, що перебувають у розпорядженні юридичних та фізичних осіб.

***Інфляційне таргетування грошей*** − це режим монетарної політики, згідно з яким офіційно проголошуються кількісні цільові орієнтири (або допустимі межі коливання цільових орієнтирів) рівня інфляції на один чи більше горизонти прогнозування, а також офіційно визнається, що низький, незмінний рівень інфляції є першочерговою кінцевою метою монетарної політики.

Існує тісний взаємозв’язок між обсягом грошової маси в обігу, темпами її зростання та рівнем інфляції. Так, уповільнення темпів зростання грошової маси в обігу сприяє зниженню темпів інфляції. Разом з тим стримування темпів інфляції та реальне підвищення обмінного курсу національної грошової одиниці забезпечує збільшення питомої ваги коштів у національній валюті порівняно з коштами в іноземній валюті.

У свою чергу, зниження темпів інфляції викликає збільшення реального рівня відсоткових ставок та зменшення інфляційних очікувань. Окрім того, планування кількості грошей в обігу ускладнюється ще й через те, що достеменно невідома дійсна величина вексельно-бартерно-залікового обігу в Україні, а також доларової готівки.

Особливо слід зазначити, що ступінь впливу наявної грошової маси в обігу на рівень фінансової безпеки фізичних і юридичних осіб та держави загалом багато в чому визначається характером декларованої монетарної політики (як найважливішої складової грошово-кредитної політики) та практичними кроками щодо її реалізації. Характер такої політики зумовлений потенціалом країни, станом соціально-економічного розвитку держави.

Вибір того чи іншого виду грошово-кредитної політики − важливий, але не визначальний фактор подолання глибокої соціально-економічної кризи. Для досягнення позитивних зрушень необхідним є поєднання реалізації виваженої грошово-кредитної політики з проведенням структурної перебудови народногосподарського комплексу країни.

Водночас дієвість грошово-кредитної політики та її вплив на безпеку грошового обігу як важливу складову фінансової безпеки держави визначається, по-перше, змістом, складовими і пріоритетами, характером розроблення основних засад грошово-кредитної політики та здійснення контролю за її проведенням, надання цьому дуже важливому документу законного статусу. Це зумовлюється тим, що від змістовного наповнення засад залежить сутність політики, що має провадитися у сфері грошового обігу, а від статусу зазначеного документа − обов’язковість чи необов’язковість дотримання встановлених у ньому параметрів, а також відповідальність за невиконання намічених рубежів.

По-друге, рівень безпеки грошового обігу залежить від характеру взаємозв’язку і взаємозумовленості монетарної та фіскальної політики. При цьому можуть виникати ситуації, коли монетарна та фіскальна політика тісно переплетені між собою, або коли між ними існує чітке розмежування.

По-третє, безпека грошового обігу зумовлюється наявністю (відсутністю) стимулів (обмежень) грошово-кредитної політики щодо рівня життя населення, наявності (відсутності) достатніх фінансових ресурсів держави, напруженості (чи відсутності такої) балансу надходження та використання валютних ресурсів, можливості (неможливості) стискання реальної грошової маси тощо, які прямо пропорційно позначаються на параметрах такої політики.

По-четверте, на рівень безпеки грошового обігу впливає наявність (відсутність) замкненого циклу обігу національної грошової одиниці.

Відсутність замкненого циклу обігу національної валюти є одним з вагомих

факторів платіжної кризи.

По-п’яте, безпека грошового обігу характеризується структурою

грошової маси і кредитної емісії, системою контролю динаміки грошової маси, практикою стимулювання процесів збільшення обсягів вкладів населення в банківську систему.

По-шосте, на рівні безпеки грошового обігу безпосередньо позначається

застосування в обороті грошових сурогатів. Як свідчить досвід країн СНД,

емісія грошових сурогатів попри очікувані наслідки спричиняє зниження

частки грошей у виручці емітентів, зростання невиплат ними заробітної плати, значне викривлення ціноутворення, собівартості і прибутку, збільшення темпів зростання номінальної кредиторської заборгованості емітентів, формування замкнених регіональних і галузевих фінансових систем, створення систем нераціонального перехресного субсидування, платіжну дискримінацію з боку монополій, перерозподіл багатства, встановлення неекономічного контролю над підприємствами, розквіт корупції, подальше зростання неплатежів, зниження рівня централізованого контролю над грошовим обігом.

По-сьоме, на безпеку грошового обігу впливає курс національної валюти. Так, знецінення останньої призводить до зростання обсягу грошової маси, необхідної для обслуговування наявного натурально-речового колообігу матеріальних цінностей, тобто для незмінного обсягу створеного продукту необхідна значно більша кількість грошей. Разом з тим стримувати валютні коливання і одночасно нарощувати грошову масу неможливо.

По-восьме, про безпеку грошового обігу можна судити з огляду на наявну в державі кредитну і відсоткову політику. Так, труднощі при отриманні суб’єктами господарювання банківських кредитів сприяють нарощуванню взаємних заборгованостей в економіці. При цьому необхідно враховувати, що

подорожчання гривневих ресурсів призводить до перерозподілу ринку депозитів, який може спричинити погіршення ліквідності ряду комерційних банків, а відтак − їх фінансової безпеки.

По-дев’яте, безпека грошового обігу визначається стабільністю грошової одиниці − відносною незмінністю вартості, яку представляє грошова одиниця в обігу, що виражається в купівельній спроможності грошей.

По-десяте, безпека грошового обігу зумовлюється ефективністю управління грошовими потоками на державному рівні.

І, нарешті, безпека грошового обігу перебуває у прямій залежності від організації захисту економічних інтересів суб’єктів грошово-кредитного ринку.

*Загрозами безпеці грошового обігу* є:

• зростання неплатежів;

• слабкий рівень регулювання цін у природних монополіях, цінові

диспропорції;

• погіршення структури платіжних засобів; штучне обмеження грошової

маси в обігу, що призводить до поглиблення платіжної кризи та зростання

масштабів тіньової економіки;

• рух доларових потоків всередині країни (з огляду на те, що такий рух

має дуалістичний характер: з одного боку, долари є іноземною валютою для

обслуговування експортно-імпортних операцій і перепливу капіталу, а з іншого − це внутрішня грошова одиниця, що суттєво ускладнює регулювання

внутрішнього грошового обігу та ефективне застосування важелів монетарної політики);

• збільшення питомої частки позабанківського грошового обігу.

Фінансова небезпека виникає також через наявність поряд з іменними

грошима, тобто грошима на іменних рахунках, неіменних грошей, що

зберігаються на анонімних і номерних рахунках.

*Стан грошового ринку* характеризується цілою низкою специфічних

індикаторів, зокрема:

• рівень монетизації;

• грошовий мультиплікатор (відношення грошового агрегату М2 у

національній валюті до грошової бази);

• співвідношення між ціновою масою товарів та їх грошовим

забезпеченням;

• співвідношення між темпами зростання грошової маси і споживчих

цін;

• середньорічні темпи приросту грошової маси;

• величина номінальної і реальної облікової ставки;

• середньорічні темпи приросту банківських резервів;

• ставки за гривневими і валютними депозитах;

• ставки по операціях SWAP;

• кредитні і депозитні ставки на міжбанківському ринку;

• міжнародні міжбанківські кредитні ставки (LIBOR, FIBOR, PIBOR).

**Оцінювання безпеки інфляційних процесів**

Вплив інфляції на господарську діяльність підприємства мають на увазі всі економісти, що зустрічаються у своїх дослідженнях із цим поняттям. У процесі інфляції відбувається:

·відносне заниження вартості окремих матеріальних активів, використовуваних підприємством, зниження реальної вартості грошових і інших фінансових активів;

·зниження собівартості виробництва продукції, що викликає штучний зріст суми прибутку й, що приводить до зростання податкових відрахувань з нього;

·падіння реального рівня майбутніх доходів підприємства;

·особливо сильно фактор інфляції позначається на проведенні дострокових фінансових операцій.

Розробка системи фінансової безпеки підприємства, вимагає попереднього моніторингу факторів інфляції і їхніх впливів на фінансову безпеку підприємства. Забезпечення фінансової безпеки підприємства, на нашу думку, не повинне бути питанням, що вирішується винятково силами самих підприємств.

***Антиінфляційна політика*** має підпорядковуватися досягненню стану

інфляційної безпеки, тобто таких рівнів насиченості економіки грошовою масою, зростання цін споживчого ринку і знецінення національної валюти, які не впливали б руйнівно на соціально-економічні процеси в державі, а стимулювали б розвиток виробництва і споживання.

Комплексний аналіз розвитку інфляційних процесів повинен включати порівняння індексу споживчих цін з індексом відпускних цін промислових виробників. Окрім того, одним із показників інфляційної безпеки є співвідношення темпів інфляції і темпів зростання номінальної заробітної плати.

**ІІІ. ПИТАННЯ**

**Валютна складова фінансової безпеки**

В Україні відсутні: стале валютне законодавство, чітка національна

валютна система, належний обсяг і склад валютних резервів, нормальний

валютний паритет, умови конвертованості, продумана валютна політика, дієвий валютний контроль, обґрунтоване курсоутворення.

**Валютна складова фінансової безпека держави** – це ступінь забезпеченості її валютними коштами, достатній для додержання позитивного сальдо платіжного балансу, виконання міжнародних зобов’язань, накопичення необхідного обсягу валютних резервів, підтримання стабільності національної грошової одиниці; стан курсоутворення, який створює оптимальні умови для поступального розвитку вітчизняного експорту, широкомасштабного припливу в країну іноземних інвестицій, інтеграції України до світової економічної системи і максимально захищає від потрясінь на міжнародних валютних ринках.

**Валютна безпека суб’єктів господарювання** – це оптимально

можливий за умов існуючих нормативно-правової бази, валютної стратегії і

політики держави, механізму валютного регулювання, інфраструктури

валютного ринку рівень забезпеченості валютними коштами, достатній для

розрахунків з бюджетною системою, своїми контрагентами, а також власного

споживання (соціально-економічного розвитку) та накопичення з урахуванням

досягнення валютної ефективності (оптимального рівня валютних витрат і

виручки).

**Валютна безпека громадян** – це стан, за якого їх валютні надходження

та заощадження перевищують особисті витрати іноземної валюти.

Визначено, що чинниками, які визначають рівень валютної безпеки в

Україні, є:

· валютна стратегія;

· чинна валютна політика;

· стандартизація валютного обігу;

· зняття обмежень на конвертованість гривні за поточними операціями;

· наявність (відсутність) валютної заборгованості (боргів держави і

господарюючих суб’єктів країни в іноземній валюті) та її розмір;

· рівень ліцензування здійснення валютних операцій;

· організація валютного контролю в країні.

З’ясовано, що валютній безпеці України загрожують:

· внутрішня втеча іноземної валюти;

· масове правомірне вивезення нерезидентами і неправомірне вивезення

резидентами валютних коштів за межі країни; “відмивання брудних грошей” на

території нашої держави;

· неповернення в Україну іноземної валюти у визначені чинним

законодавством строки;

· зростання валютної заборгованості держави і вітчизняних

господарюючих суб’єктів;

· порушення інструкцій НБУ по роботі з валютними коштами;

проведення незаконних валютних операцій;

· порушення у переведенні безготівкових коштів в іноземній валюті у

готівку;· розвиток кризових явищ на світовому валютному ринку;

· можливість запровадження валютної блокади; недостатній рівень

офіційних валютних резервів;

· наявність валютних ризиків;

· фальшування іноземної валюти.

***Рівень валютної безпеки*** визначається: обсягом валютного ринку,

загальним обсягом і структурою валютних надходжень, ступенем доларизації

національної економіки, номінальним і реальним курсом національної валюти,

показником її девальвації (ревальвації), відхиленням обмінного курсу валюти і

показником відхилення розподілу іноземної валюти, доларовою відсотковою

ставкою, вартістю підтримання одного пункту курсу національної валюти,

наявністю достатніх валютних резервів, покриттям резервами

середньомісячного імпорту, щоденним обсягом обігу іноземної валюти, рівнем

наповненості вартості національної валюти резервами в іноземній валюті,

купівельною спроможністю іноземної валюти, співвідношенням вартості

національної валюти і паритету купівельної спроможності, різницею ставок по

цінних паперах одного типу (емітованих в іноземній і національній валюті),

межею коливань валютних курсів.

**ІV. ПИТАННЯ**

**Індикатори фінансової безпеки підприємства**

Оцінювання фінансової безпеки підприємства необхідно почати з розрахунку значень множини показників, які дадуть змогу зробити висновокстосовно умов функціонування підприємства – стабільна робота підприємства чи кризова ситуація в діяльності підприємства. Методики визначення умов функціонування підприємства є загальновідомими.

Найбільш оптимальним і об’єктивним є метод визначення типу фінансової стійкості підприємства, сутність якого полягає в такому: абсолютнимипоказниками фінансової стійкості є показники, що характеризують міру забезпеченостізапасів джерелами їхнього фінансування.

Існують різні погляди на визначення множини показників (індикаторів) фінансової безпеки. Основним критерієм включення показника до множини індикаторів фінансової безпеки, з нашого погляду, є забезпечення реалізації пріоритетних фінансових інтересів підприємства (як і господарськихзагалом). Ці інтереси визначаються станом функціонування підприємства.

Використання системи індикаторів для оцінювання фінансової безпеки підприємства прийнято й у світовій практиці. Згідно зі світовою практикою, вимоги до значень індикаторів не мають обов’язкового характеру, а лише рекомендаційний у разі оцінювання стану фінансової безпеки підприємства.

**Лекція №5**

**Тема 9. Політико-правова, силова та екологічна складові соціально-економічної безпеки підприємства** (1 год)

ПЛАН ЛЕКЦІЇ

Вступ

1. Поняття та сутність екологічної безпеки.

2. Поняття політико-правової безпеки.

*3.* Сутність силової безпеки.

# **РЕКОМЕНДОВАНА ЛІТЕРАТУРА**

1.Управління ризиками у підприємництві: навчальний посібник \ І. М. Посохов. – Харків : НТУ «ХПІ», 2015. – 220 c.

2. Опорний конспект лекцій з дисципліни «Управління ризиками» для студентів вищої освіти : другий (магістр) / укладач Дядюк М.А. – Харків: «Видавництво «Форт», 2017. – с. 165.

3.Економічний ризик: методи оцінки та управління [Текст] : навч. посібник / [Т. А. Васильєва, С. В. Лєонов, Я. М. Кривич та ін.] ; під заг. ред. д-ра екон. наук, проф. Т. А. Васильєвої, канд. екон. наук Я. М. Кривич. – Суми : ДВНЗ “УАБС НБУ”, 2015. – 208 с.

4. Лук’янова В. В. Економічий ризик: Навч. посіб./ В. В. Лук’янова, Т. В. Головач. – К.: Академвидав, 2017. – 462 с.

**МЕТА ЛЕКЦІЇ**

Метою лекції є надання необхідних теоретичних знань здобувачам вищої освіти юридичного факультету, що навчаються на магістерському рівні вищої освіти, щодо основних понять та особливостей екологічної, політико-правової та силової безпеки підприємства*.*

**ВСТУП**

Охорона довкілля, раціональне використання природних ресурсів, забезпечення екологічної безпеки життєдіяльності людини – невід’ємна умова сталого економічного та соціального розвитку країни. З цією метою Україна здійснює на своїй території екологічну політику, спрямовану на збереження безпечного для існування живої та неживої природи, довкілля, захисту життя та здоров’я населення від негативного впливу, зумовленого забрудненням довкілля, досягнення гармонійної взаємодії суспільства і природи, охорону, раціональне використання і відтворення природних ресурсів.

Чинне законодавство визначає правові, економічні та соціальні основи організації охорони довкілля в інтересах нинішнього і майбутніх поколінь. Завданням законодавства про охорону довкілля є регулювання відносин у галузі охорони, використання та відтворення природних ресурсів, забезпечення екологічної безпеки, запобігання та ліквідації негативного впливу господарської та іншої діяльності на довкілля, збереження природних ресурсів, генетичного фонду живої природи, ландшафтів та інших природних комплексів, унікальних територій та природних об’єктів, пов’язаних з історикокультурною спадщиною.

**І. ПИТАННЯ**

**Поняття та сутність екологічної безпеки**

**Екологічна безпека** – такий стан навколишнього середовища, при якому стає неможливим погіршення екологічного стану i виникнення небезпеки для здоров’я людей. Екологічна безпека – це компонент національної безпеки, що забезпечує захищеність життєво важливих інтересів людини, суспільства, довкілля та держави від реальних чи потенційних загроз, які створюються антропогенними чи природними чинниками відносно навколишнього середовища.

Під державною системою екологічної безпеки розуміють сукупність державних заходів (правових, економічних, технічних, гуманітарних і медичних), спрямованих на підтримку рівноваги між її екосистемами та антропогенними й природними навантаженнями.

Система екологічної безпеки створюється і розвивається відповідно до Конституції України, указів Президента України, постанов Уряду, державних програм у цій сфері.

**Екологічна безпека** – це :

– сукупність дій, станів і процесів, що прямо чи побічно не призводять до серйозних збитків (або загроз таких збитків), що завдаються природному середовищу, окремим людям і людству загалом;

– комплекс станів, явищ та дій, що забезпечують екологічний баланс на Землі і у будь-яких її регіонах на рівні, до якого фізично, соціальноекономічно, технологічно та політично готове (може без серйозних збитків адаптуватися) людство.

*До зовнішніх загроз* екологічної безпеки підприємства слід віднести особливості природних ресурсів конкретного регіону, зміни клімату, егативні

трансформації водних ресурсів та біосистем, забруднення довкілля, природні

катаклізми та техногенні аварії.

Зрозуміло, що дію зовнішніх загроз господарюючі суб’єкти не в змозі призупинити, але в коаліції з державою та шляхом прикладання цілеспрямованих зусиль, можливим є суттєве зменшення та нівелювання їх дії.

*Внутрішні загрози* екологічній безпеці підприємства формують, перш за все, застосовувані (переважно застарілі) технології та залежні від них інші

складові виробничої системи підприємства – сировина, матеріали, комплектуючі, енергоносії, вироблювана продукція, відходи, викиди тощо. Окремо слід вказати на таке джерело внутрішньої загрози як персонал, здатний порушувати технологічні регламенти та правила безпеки.

**Екологічна безпека підприємства** – це стан захищеності економічних

інтересів підприємства від реальних і потенційних екологічних загроз, що

створюються в результаті виробничої діяльності господарюючих суб’єктів

внаслідок екологічно необумовленого господарювання, за умови мінімізації

негативного впливу виробничої діяльності самого підприємства на навколишнє природне середовище і суб’єктів виробничого процесу.

Алгоритм процесу охорони екологічної складової економічної безпеки

полягає в проведенні таких послідовних дій:

1) розрахунок карти ефективності здійснюваних заходів для охорони екологічної складової економічної безпеки на підставі звітних даних про фінансово-господарську діяльність підприємства;

2) аналіз виконаних розрахунків і розробка рекомендацій для підвищення ефективності здійснюваних заходів,

3) розробка альтернативних сценаріїв реалізації запланованих заходів;

4) вибір пріоритетного сценарію на засаді порівняння розрахунків ефективності запланованих заходів;

5) передача вибраного планового сценарію в складі загального плану охорони економічної безпеки в підрозділи, які здійснюють функціональне планування фінансово-господарської діяльності підприємства;

6) практичне здійснення запланованих заходів у процесі діяльності відповідного суб’єкта господарювання.

**Особливості екологічної безпеки на харових підприємствах**

Підприємства харчової промисловості в ході здійснення своєї діяльності здійснює прямий та опосередкований вплив на довкілля.

*Прямий вплив* обумовлений викидами в атмосферу, скидами стічних вод, утворенням та розміщенням твердих відходів, Також виробництво харчових продуктів здійснює суттєвий вплив на соціальне середовище,забезпечуючи населення продуктами харчування та робочими місцями.

*Опосередкований вплив* на довкілля має місце на попередніх стадіях,пов’язаний із забезпеченням виробництва сировиною, енергетичними

матеріальними, інформаційними та людськими ресурсами в процесі виробництва, пов’язаний із вилученням земельних ресурсів, вторинним

забрудненням продуктами трансформації первинного забруднення, впливом на здоров’я людини через знижену якість оточуючого природного середовища та фактори небезпеки продуктів харчування та на стадії використання готової продукції, вплив на етапах транспортування, зберігання та утилізації відходів харчової продукції, включаючи перш за все утилізацію неякісної продукції, тари та упаковки.

Як наслідок зазначеного, позитивно змінюється кваліфікація і структура персоналу, соціальна складова виробничої системи підприємства,

формується сучасна соціальна інфраструктура, що відповідає прогресивним

екологічним нормативам та законодавству.

**ІІ.ПИТАННЯ**

**Поняття політико-правової безпеки**

**Політико-правова складова СЕБ** − правове забезпечення діяльності підприємства і дотримання чинного законодавства.

Основними загрозами політико правові й безпеціпідприємства є:

· недостатня правова захищеність інтересів підприємства в договірній та іншій діловій документації;

· порушення юридичних прав підприємства та його працівників;

· умисне або ненавмисне розголошування комерційно важливих відомостей;

· порушення норм патентного права.

Політико-правову безпеку визначають за такими показниками:

– питома вага судових й арбітражних справ у загальній сумі господарських договорів підприємства (Кс.ар.):

– частка виграних судових й арбітражних справ у загальній кількості юридичних справ, що розглядалися (Квю):

– питома вага одержаних і сплачених штрафних санкцій в загальній сумі зобов’язань за господарськими договорами підприємства (Кш):

– частка витрат на юридичне забезпечення діяльності підприємства в загальній структурі його виробничих витрат (Кв.юр.).

Чим вище значення показників частки виграних судових й арбітражних справ, у тому числі й тих, що розглядалися раніше, та частки витрат на юридичне забезпечення діяльності підприємства в загальній структурі його виробничих витрат і чим нижче значення показників питомої ваги судових й арбітражних справ загальній сумі господарських договорів підприємства та питомої ваги одержаних і сплачених штрафних санкцій у загальній сумі зобов’язань за господарськими договорами підприємства, тим вище рівень політико-правової безпеки підприємства.

Загальний процес забезпечення політико-правової безпеки здійснюється за схемою, яка охоплює такі елементи (дії) організаційно-економічного спрямування:

1) аналіз загроз негативних впливів;

2) оцінка поточного рівня забезпечення;

3) планування комплексу заходів, спрямованих на підвищення цього рівня;

4) здійснення ресурсного планування;

5) планування роботи відповідних функціональних підрозділів підприємства;

6) оперативна реалізація запропонованого комплексу заходів щодо забезпечення належного рівня безпеки.

Передовсім детально аналізують загрози внутрішніх і зовнішніх негативних впливів на політико-правову безпеку та причини їх виникнення.

Основними причинами виникнення внутрішніх негативних впливів можуть бути:

а) низька кваліфікація працівників юридичної служби відповідного суб’єкта господарювання та помилки у підборі персоналу цієї служби;

б) недостатнє фінансування юридичного забезпечення підприємницької або іншої діяльності;

в) небажання чи нездатність підприємства активно впливати на

зовнішнє політико-правове середовище його діяльності.

Останнє проявляється у слабкому правовому опрацюванні договірних відносин даного суб’єкта господарювання з іншими, невмінні захищати інтереси підприємства в конфліктних ситуаціях, неефективному плануванні юридичного забезпечення бізнесової діяльності.

Причини виникнення зовнішніх негативних впливів здебільшого мають подвійний характер:

1) політичний;

2) законодавчо-правовий.

До першої групи причин можна віднести:

а) зіткнення інтересів суспільних груп населення з економічних, національних, релігійних та інших мотивів;

б) військові конфлікти (дії);

в) економічна й політична блокада, ембарго;

г) фінансові та політичні кризи світового характеру.

У другій групі причин виокремлюють:

а) здійснення власних політичних та інших цілей партіями (суспільними

рухами), що перебувають при владі;

б) зміна положень чинного законодавства з питань власності,

господарського і трудового права, оподаткування тощо.

Оцінка поточного рівня забезпечення політико-правової безпеки

підприємства (організації) провадиться за кількома напрямками:

1) рівень організації та якості робіт із забезпечення цієї складової загального рівня економічної безпеки;

2) бюджетно-ресурсне забезпечення робіт;

3) ефективність діяльності відповідних підрозділів суб’єктів

господарювання.

**ІІІ.ПИТАННЯ**

**Сутність силової безпеки**

**Силова безпека** характеризуєзахищеність інтересів підприємства

від фізичних і моральних негативних впливів. Вона включає:

а) забезпечення фізичної та моральної безпеки співробітників та

керівників підприємства;

б) забезпечення захисту майна підприємства від негативних впливів,

які можуть призвести до втрати цього майна або зниження його вартості;

в) забезпечення силових аспектів інформаційної безпеки

підприємства.

Завдання силової безпеки підприємства:

· забезпечення фізичної та моральної безпеки керівництва,

провідних фахівців, працівників підприємства;

· навчання персоналу розпізнавати небезпеки і вживати заходи

самозахисту;

· забезпечення охорони приміщень, ліній зв’язку й устаткування та

іншого майна підприємства;

· забезпечення захисту від комп’ютерних крадіжок;

· організація пропускного режиму;

· забезпечення захисту від рейдерства;

· розроблення заходів щодо попередження шахрайства, крадіжок.

Дії, що негативно впливають на рівень силової безпеки, зумовлюються

основними причинами є:

· нездатність підприємств-конкурентів досягти переваг коректними методами ринкового характеру;

· кримінальні мотиви одержання злочинними юридичними (фізичними) особами доходів через шантаж, шахрайство або крадіжки;

· некомерційні мотиви посягань на життя та здоров’я керівників і

працівників підприємства (організації), а також на майно підприємства.

Названі спонукальні мотиви можуть зумовити спроби негативного

впливу (фізичного та морального характеру) на працівників підприємства. Спроби фізичного усунення керівників, вищих менеджерів і головних

спеціалістів спричинюються переважно зіткненням комерційних інтересів

підприємств (організацій)-конкурентів, конфліктами керівництва підприємства (організації) з кримінальними організаціями (особами), а також політичними мотивами. Спроби морального тиску на працівників підприємства робляться з метою змусити їх учинити дії, що завдаватимуть шкоди соціально-економічній безпеці та ефективності організації.

Виконавцями таких дій можуть бути представники криміналітету, корумповані чиновники служб безпеки та податкових служб або спеціально найняті для цього люди та організації.

Негативних дії щодо силової безпеки підприємства:

1) фізичні і моральні впливи особистого спрямування (спрямовані проти

конкретної особистості);

2) негативні дії, спрямовані на завдання шкоди майну, включаючи

загрози зменшення активів підприємства (організації) і втрати ним (нею)

фінансової незалежності;

3) негативний вплив на інформаційне середовище суб’єкта

господарювання (так званий промисловий шпіонаж).

Розрахунок силової безпеки підприємства за цими показниками

дозволить оцінити:

1) рівень захищеності підприємства від незаконного проникнення;

2) рівень захищеності підприємства від комп’ютерних крадіжок;

3) рівень захищеності співробітників та керівництва підприємства

від фізичних і моральних негативних впливів;

4) надійність персоналу, що забезпечує силову безпеку;

5) рівень фінансування силових служб підприємства.

**Тема 10. Ризик та його вплив на соціально-економічну безпеку підприємств** (1 год)

ПЛАН ЛЕКЦІЇ

Вступ

# 1. Ризик та його вплив на економічну безпеку підприємства

2.Загрози підприємницькій діяльності

3. Управління економічними ризиками підприємства

# **РЕКОМЕНДОВАНА ЛІТЕРАТУРА**

1.Управління ризиками у підприємництві: навчальний посібник \ І. М. Посохов. – Харків : НТУ «ХПІ», 2015. – 220 c.

2. Опорний конспект лекцій з дисципліни «Управління ризиками» для студентів вищої освіти : другий (магістр) / укладач Дядюк М.А. – Харків: «Видавництво «Форт», 2017. – с. 165.

3.Економічний ризик: методи оцінки та управління [Текст] : навч. посібник / [Т. А. Васильєва, С. В. Лєонов, Я. М. Кривич та ін.] ; під заг. ред. д-ра екон. наук, проф. Т. А. Васильєвої, канд. екон. наук Я. М. Кривич. – Суми : ДВНЗ “УАБС НБУ”, 2015. – 208 с.

4. Лук’янова В. В. Економічий ризик: Навч. посіб./ В. В. Лук’янова, Т. В. Головач. – К.: Академвидав, 2017. – 462 с.

**МЕТА ЛЕКЦІЇ**

Метою лекції є надання необхідних теоретичних знань здобувачам вищої освіти юридичного факультету, що навчаються на магістерському рівні вищої освіти, щодо основних понять ризику та його впливу на економічну безпеку підприємства. Загрози підприємницькій діяльності та управління економічними ризиками.

**ВСТУП**

Управління ризиками включає прогнозування можливості настання потенційно ризикової події, а відповідно дає можливість вчасно вжити заходів щодо запобігання або зниження ступеня наслідків що можуть настати від ризику, який не можна локалізувати.

Управління економічними ризиками, як будь-яка інша система управління, має об'єкт та суб'єкт.

Об'єктом управління ризиками є здійснення економічної діяльності за умов невизначеності і економіко-правові відносини, ще виникають між господарчими суб'єктами у процесі усунення чи реалізації ризику.

Суб'єкт такого управління — це група менеджерів підприємства та/або фахівців спеціалізованих компаній, які через різноманітні варіанти комбінованих дій здійснюють цілеспрямовану диверсифікацію ризиків для ефективної економічної діяльності.

Організація управління ризиками економічної діяльності передбачає створення підсистем та інфраструктурних елементів управління ризиками на рівні підприємства. В організаційній структурі підприємства будь-якої форми власності ці функції може бути покладено як на спеціально створені структурні елементи, так і в сукупності на рівні співпраці фахівців аналітичних, юридичних відділів, служб безпеки тощо. Якщо є потреба, можна залучити фахівці спеціалізованих компаній, або ж узагалі функції з управління ризиками можуть передаватися іншим компаніям.

**І. ПИТАННЯ**

# **Ризик та його вплив на економічну безпеку підприємства**

Діяльність підприємств за умов ринку характеризується передусім певним рівнем економічної свободи суб'єктів господарювання. Однак свобода одного учасника ринкових відносин обмежується правами та економічною свободою інших суб'єктів господарювання, які прагнуть насамперед власної вигоди. Таке поняття, як вигода, є майже ключовим у причинно-детермінаційному комплексі виникнення ризиків, оскільки вигода одного учасника ринкових відносин може стати руйнівною силою виникнення ризику, збитків, втрат і навіть банкрутства для інших учасників. Це положення посилюється ще й тим, що підприємства, які виробляють однорідну продукцію або надають подібні послуги, прагнуть у будь-який спосіб витіснити свого конкурента з ринку або хоча б посісти домінуюче положення.

Отже, учасники економічних відносин незалежно від власного бажання протягом своєї діяльності будуть мати справу з певним рівнем невизначеності і, як наслідок цього, відчувати на собі вплив тих видів ризиків, які притаманні ринковій економіці взагалі та конкретним економічним умовам країни в цілому або тому чи іншому напрямку діяльності зокрема.

Умови невизначеності, які існують у будь-яких видах економічної діяльності, е предметом досліджень і об'єктом постійного спостереження фахівців різних галузей науки — юристів, економістів, соціологів, політологів тощо. Комплексність підходу до вивчення цієї проблеми зумовлюється тим, що суб'єкти господарювання у процесі своєї діяльності залежать від цілої низки умов, залежно від їх причинного складу та місця виникнення, а саме: соціально-політичних, адміністративно-управлінських, законодавчих, виробничих, комерційних, фінансових. Поняття ризику як об'єктивного прояву невизначеності з'явилося у військових, економічних, демографічних, медичних, біологічних, правових та інших дисциплінах. У вищих навчальних закладах багатьох країн дедалі більше уваги приділяється проблемі вивчення методів управління ризиками.

Нині категорія "ризик" входить до повсякденного словника керівника, стає складовою частиною та необхідною передумовою процесу здійснення господарської діяльності. Що складнішим та невизначенішим є навколишнє середовище, то актуальнішим є урахування ризику та управління ним.

Сьогодні у наукових та періодичних фахових джерелах можна знайти багато різних за обсягом та багатогранністю визначень "ризику". Це обумовлюється насамперед багатоаспектністю цього явища, а також практично повною відсутністю його законодавчого врегулювання.

Ризик — це ймовірність виникнення збитків або недоодержання прибутків порівняно із варіантом, що прогнозується.

Сутність ризику як феномену характеризує взаємозв'язок таких основних його елементів:

* • можливість відхилення від передбачуваної мети, заради якої здійснюється вибір одного з альтернативних рішень;
* • імовірність досягнення бажаного результату;
* • відсутність упевненості в досягненні поставленої мети;

Можливість матеріальних, моральних та інших втрат, пов'язаних із втіленням у життя вибору, зробленого за наявності альтернативи, за умов невизначеності.

На підставі викладеного можна зробити висновок, що ризик економічної діяльності зводиться до загрози виникнення у період реалізації певного проекту або чинності певної угоди дій або подій, які можуть призвести до додаткових витрат суб'єкта господарювання або отримання менших доходів, ніж ті, на які він розраховував.

Багатогранність імовірних ризиків обумовлюється різноманітністю його джерел — чинників, що зумовлюють невизначеність результатів, а саме:

* • спонтанність природних процесів та явищ, стихійні лиха;
* • випадковість (різні аварії, вихід з ладу обладнання, нещасні випадки на транспорті тощо);
* • наявність антагоністичних тенденцій, зіткнення суперечливих інтересів (від воєн і міжнаціональних конфліктів до конкуренції та звичайної розбіжності інтересів);
* • імовірнісний характер науково-технічного прогресу;
* • неповнота, брак інформації про об'єкт, процес, явище, яких стосується рішення, обмежені можливості людини щодо збирання та перероблення інформації, а також постійне її оновлення;
* • обмеженість, недостатність матеріальних, фінансових, трудових та інших ресурсів, необхідних для прийняття та реалізації рішень;
* • неможливість однозначного пізнання об'єкта за наявних рівні: та методів наукового пізнання.

У найбільш загальному вигляді ризик, основним джерелом якого є внутрішня та зовнішня невизначеність, виникає за таких основних причин:

* • раптове настання непередбачених змін у зовнішньому серед вищі, які відображаються (або можуть відобразитися) на діяльності суб'єкта господарювання (зміна цін, зміни у податковому законодавстві, коливання валютного курсу, зміни соціально-політичної ситуації та ін.);
* • зміни відносин суб'єкта господарювання з його контрагентами. Ці зміни можуть бути викликані як самим суб'єктом, та і безпосередньо його партнерами (можливість укласти вигіднішу угоду, збільшення або зменшення строку угоди, вигідніші умови діяльності, зміни за умов переміщення товарних, фінансових та трудових ресурсів та інші), що призведе до перегляду досягнутих домовленостей або відмови від них;
* • зміни, що відбуваються в межах самого суб'єкта господарювання, або інші причини внутрішнього походження (невідповідність рівня кваліфікації персоналу запланованим завданням, раптовий вихід із ладу основних виробничих фондів та ін.);
* • зміни, що відбуваються внаслідок науково-технічного прогресу, результатом чого є формування нової системи орієнтації (наприклад, зміна ставлення до ручної праці після виникнення машинної).

У літературі, присвяченій вивченню теорії ризиків, висвітлюються різні засади їх класифікації. Вони дозволяють проаналізувати найзагальніші ознаки класифікації ризиків, що можуть виникати під час економічної діяльності.

Існують загальні зовнішні джерела загрози функціонуванню підприємства, а саме:

* • несприятлива для підприємства економічна політика держави. Маніпулювання (з метою регулювання економіки) валютним курсом, ставками митного тарифу, податків і т. ін. можуть вступати у протиріччя виробництву, комерційній і фінансовій політиці держави. Крім вищезгаданого, реальну загрозу для підприємства становлять адміністративні дії влади, насильницьке звуження сфери товарно-грошових відносин, порушення (з боку державних органів) законів, що регламентують підприємницьку діяльність, перевищують встановлену компетенцію у взаємовідносинах із підприємством, необґрунтоване втручання в його виробничу, фінансову і комерційну діяльність, зазіхання на власність підприємства і т. ін.
* • при виході на зовнішні ринки підприємство може також зазнати негативного впливу внаслідок несприятливої економічної політики іноземних держав.
* • джерелом зовнішньої загрози для комерційної діяльності підприємства є дії деяких господарчих суб'єктів. Насамперед ідеться про недобросовісну конкуренцію, яка, до речі, різними джерелами трактується по-різному.
* • руйнації, пов'язані із землетрусом, повінню (затопленням), пожежею, аваріями енергопостачання, радіаційною небезпекою, небезпекою від впливу сильних акустичних і електромагнітних полів.

Загрози приміщенням, устаткуванню, транспорту можуть бути спрямовані або на їх знищення (розплата за щось), або на внесення істотних обмежень у їх нормальне функціонування. У цьому випадку загрози можуть бути реалізовані під виглядом стихійних (аварійних) явищ або під виглядом діянь, що перебувають у полі дії кримінального кодексу, коли передбачене законом покарання незмірно менше завданих збитків.

Загрози персоналу і клієнтам можуть мати як фізичний, так і психологічний характер. Це можуть бути акти насильства, шантажу, замасковані під "гумову" статтю 206 Кримінального кодексу (Хуліганство), а можуть бути і серйозні розборки, про результати яких ми дізнаємося з кримінальної хроніки (з вибухами та вбивствами). Тут також можна простежити дії, спрямовані на примушування виконати визначені умови, або помста за що-небудь (зазвичай вони поєднуються).

Загрози інформації переважно спрямовані на її негласне одержання, знищення (відновлення) і модифікацію. Ці загрози можуть бути реалізовані за допомогою агентів (викрадання, використання сильних світу цього тощо) або за допомогою спеціальних технічних засобів. Як відомо, вартість техніки з приставкою "спеціальна" значно зростає, а заробітна плата потенційних агентів (найманих працівників) такої тенденції не має. Тому вашому потенційному супротивнику у наших умовах вигідніше годувати агента, що працює з вами, ніж купувати техніку з приставкою "спеціальна", залучати осіб, ще її обслуговують, і прокидатися вночі з думкою про те, що вони ще чиїсь агенти. В інших економічних умовах (стабільність, наявність середнього класу (де існує страх найманих працівників втратити роботу назавжди), природно, більш небезпечними є загрози, пов'язані із застосуванням технічних засобів.

**ІІ.ПИТАННЯ**

**Загрози підприємницькій діяльності**

Отже, зробимо маленьке відкриття — одержати повний перелік загроз неможливо.

Пояснюючи його, візьмемо до уваги такі узагальнення:

• фізичні загрози присутні як у середовищі, яке вас оточує (стихія, фізичні і хімічні середовища, аномальні явища, етнічне оточення, економіка, політика, право), так і у вигляді таких самих інших, але спеціально створених і реалізованих людиною явищ, актів у правовому полі кримінального кодексу або поза ним. Повні знання про такі загрози та методи їх здійснення повинні охоронятися державою і застосовуватися тільки у випадках, які зачіпають інтереси держави (питання дуже суперечливе, звичайно, але історія свідчить, що саме так і відбувається).

Говорячи про загрози підприємницькій діяльності, потрібно підкреслити, що найбільше поширення в українських реаліях одержали крадіжки, пограбування, розбої, шахрайства, вимагання, хабарництво, зловживання службовим становищем, службова фальсифікація, а також різні форми недобросовісної конкуренції і такі небезпечні форми, як замовлені вбивства і захоплення заручників.

Не будемо також забувати, що все це відбувається на фоні таких притаманних українському ринку особливостей, як:

* • несприятлива для підприємця економічна політика держави, що виявляється у маніпулюванні з метою регулювання економіки обліковою ставкою, валютним курсом, ставками митного тарифу і податків;
* • руйнування господарських зв'язків;
* • штучно знижений курс гривні;
* • економічна корупція.

Крім цього, при спробі дати повну картину ситуації, що склалася у сфері української національної економіки, слід враховувати такі особливості нашого ринку:

* • розмах промислового і комерційного шпигунства (з боку різних структур, що використовують методи агентурного і технічного проникнення до комерційної таємниці);
* • відсутність єдиної стратеги забезпечення безпеки підприємницьких структур;
* • відсутність цивілізованих юридичних гарантій для реалізації комерційних інтересів.

**ІІІ.ПИТАННЯ**

**Управління економічними ризиками підприємства**

Суб'єкт підприємницької діяльності, який мислить раціо­нально, не повинен покладатися на стихійний хід подій, він мусить навчитися управляти ризиками у підприємництві.

У підприємницькій практиці постійно розробляються і реа­лізуються заходи, спрямовані на зниження величини ризику.

У сукупності вони становлять єдиний механізм управління ри­зиком, так званий ризик-менеджмент. Останній становить со­бою систему управління ризиком і фінансовими відносинами, що виникають у процесі цього управління.

При цьому ризик-менеджмент базується на використанні таких методів зниження його в підприємницькій діяльності, як *диверсифікація ризику; об'єднання ризиків або страхуван­ня; розподіл ризиків; пошук інформації.*

Розглянемо ці методи.

***Диверсифікація ризику***— це метод зниження ризику шля­хом розподілу його між декількома ризикованими товарами. Здійснюється в такий спосіб, що підвищення ризику від купівлі (або продажу) одного означає зниження ризику від купівлі (або продажу) іншого.

***Об'єднання ризиків***— це метод, спрямований на зниження ризику шляхом перетворення випадкових збитків у відносно невеликі постійні витрати. Останні становлять основу страху­вання.

***Розподіл ризику***відбувається під час розробки фінансового плану підприємницького проекту, підготовки контрактів, угод. Значно зменшує потенційний ризик детальна розробка бізнес-плану та прогнозування підприємницької діяльності. У бізнес-план закладаються можливі зміни й проблеми здійснення про­екту, форми контролю поточних операцій, аналітична оцінка стану справ.

Ризик пов'язаний та багато в чому зумовлений невизначені­стю ситуації, що складається на ринку. Методи аналізу ризиків передбачають використання інформації щодо відповідних опе­рацій, запланованих підприємцем. ***Пошук інформації***тим са­мим сприяє зниженню ризику. Для визначення кількості необ­хідної інформації доцільно порівняти очікувані майбутні виго­ди з очікуваними запропонованими витратами, пов'язаними з її одержанням.

Ефективність заходів зі зниження ризику залежить від вирі­шення таких завдань: *обґрунтування надійності ринків збу­ту; міцності матеріально-технічної бази підприємства; захо­дів, спрямованих на зниження ризику; вибору підприємницької стратегії, її інноваційності аналітичної оцінки товару, рин­ків, конкурентів.*

Наприклад, для обґрунтування надійності ринків збуту по­трібно визначити потенційну кількість покупців, виявити їхні споживацькі нахили, бажання. Міцність матеріально-техніч­ної бази підприємства визначається величиною та станом ви­робничих фондів, наявністю сучасних технологій. Інноваційність обраної підприємницької стратегії виражається у пошукові нових форм задоволення потреб споживачів, створенні но­вітніх товарів та послуг. Аналітична оцінка товару, ризиків, конкурентів дасть змогу уникнути зайвих витрат, знайти слуш­ний час для розгортання бізнесу.

Попередня розробка цих заходів допоможе уникнути можливого банкрутства або інших негативних наслідків. Отже, вне­сення правильного рішення, детальне опрацювання підприєм­ницького проекту з використанням засобів блокування та міні­мізації ризиків у процесі його здійснення — основний спосіб вирішення питань ризик-менеджменту.

Таким чином, з цією метою формується ризикова політика фірми. ***Ризикова політика фірми***— це комплекс захисних заходів від основ­них форм ризиків.

Найважливішими захисними антиризиковими заходами є:

- страхування ризику;

- вивчення ринку;

- вивчення клієнтів, зокрема перевірка їх платоспромож­ності;

- здійснення диверсифікації виробництва та постачання;

- поточний контроль;

- використання застави;

- вивчення конкурентів;

- створення фінансових резервів;

- створення страхових запасів найважливіших матеріалів;

- удосконалення цінової політики тощо.

Таким чином, набуття і застосування студентами поглиблених знань з питань раціонального прийняття управлінських рішень в умовах ризику та невизначеності, формування теоретичної та методологічної бази, необхідної для вільного володіння сучасними методиками ідентифікації, оцінки та управління ризиками, а також опанування основними підходами до вибору, обґрунтування та реалізації найбільш ефективних фінансових рішень в нестабільному середовищі, надасть студентам можливості правильного вибору та класифікації щодо видів ризиків за причинами їх виникнення, підбирати методи кількісної оцінки, прийнятні для кожного з видів; отримання студентами теоретичної та практичної підготовки з питань зниження ризиків; засвоєння основних методів і моделей прийняття багатоцільових рішень за умов невизначеності та ризику; розвиток уміння застосовувати методи управління ризиком на вітчизняних підприємствах.