Львівський державний університет внутрішніх справ

Живко З. Б.

Сучасні методи забезпечення надійності персоналу

Навчальний посібник
у схемах і таблицях

Львів
2019

УДК 331.108(075.8)
Ж66

Рекомендовано до друку та поширення через мережу Інтернет
Вченою радою Львівського державного університету внутрішніх справ
(протокол від 30 жовтня 2019 року № 3)

Р е ц е н з е н т и:
Мартин О. М. – кандидат економічних наук, доцент,
доцент права та менеджменту у сфері цивільного захисту
Львівського державного університету безпеки життєдіяльності;
Васильчак С. М. – доктор економічних наук, доцент,
декан факультету управління та економічної безпеки
Львівського державного університету внутрішніх справ.

Живко З. Б.

Ж66 Сучасні методи забезпечення надійності персоналу: навчальний посібник у схемах і таблицях. Львів: ЛьвДУВС, 2019. 128 с.
ISBN 978-617-511-301-1

Розкрито теоретичні основи та практичні засади забезпечення кадрової безпеки організації. Визначено проблематику кадрової безпеки, яка на початку XXI століття набула першочергового значення, поширилася на сфери соціальних, економічних, правових, культурних, екологічних та інформаційних відносин. Висвітлено особливості сучасних методів забезпечення надійності персоналу.

Для студентів, курсантів, аспірантів економічних та юридичних спеціальностей закладів вищої освіти, фахівців у галузі безпеки держави, співробітників правоохоронних органів та практичних працівників кадрової сфери, власників і керівників комерційних структур, керівників та менеджерів служб безпеки цих структур, а також осіб, які цікавляться питаннями безпеки бізнесу.

Рекомендовано для вивчення таких дисциплін, як «Банківське безпекознавство», «Управління персоналом», «Кадрова безпека», «Управлінські рішення», «Кадрове консультування», «Конкурентна розвідка», «Економічна безпека бізнесу», «Управління економічною безпекою підприємства», «Фінансова безпека СГД», «Менеджмент безпеки персоналу», «Організація та управління системою економічної безпеки підприємства» тощо.

Zhyvko Z. B.

Modern methods of ensuring the reliability of personnel: tutorial in diagrams and tables. Lviv: LSUIA, 2019. 128 p.

The manual reveals of «Modern methods of ensuring the reliability of personnel» the theoretical and practical principles of ensuring the personnel security of organization. The author defines the problems of «personnel security», which at the beginning of the 21st century became of primary importance, spread to the sphere of social, economic, legal, cultural, environmental, and information relations. The guide will allow you to get acquainted with the features of modern methods of ensuring the reliability of personnel.

For students, cadets, postgraduate students in economic and legal specialties of higher education institutions, state security specialists, law enforcement officials and practitioners of personnel, for owners and heads of commercial structures, heads and managers of security services of these structures, as well as other persons who interested in business security issues.

May be recommended for the study of such disciplines as: «Banking Security», «HR», «Personnel Security», «Management Solutions», «Personnel Consulting», «Competitive Intelligence», «Business Economic Security», «Enterprise Economic Security Management», «Financial Security of a business entity», «Personnel Security Management», «System Organization and Management economic security of the enterprise», etc.

УДК 331.108(075.8)

ISBN 978-617-511-301-1

Зміст

Передмова

Персонал традиційно є неодмінним ресурсом функціонування суб'єктів господарювання різних видів економічної діяльності. На кожному етапі роботи з кадрами у керівників компаній виникає чимало проблем, що стосуються безпеки бізнес-структури. В ідеалі практичні аспекти забезпечення кадрової безпеки мають вирішуватися в тісній співпраці зі службою економічної безпеки суб'єкта господарювання. Але на прикладному рівні цей процес зазвичай відбувається хаотично, а взаємодія служб – якщо вона все ж виникає – рідко буває ефективною. Причина криється у нерозумінні кадровиками і менеджментом суб'єктів господарювання власної ролі у процесі забезпечення кадрової безпеки. Подібна практика сприяє активізації проявів численних загроз економічній безпеці від власного персоналу, таких як шахрайство, розголошення конфіденційної інформації, тощо.

У стратегії і тактиці роботи підприємств дедалі частіше зважають на набір, звільнення, роботу та відносини з персоналом, а також різні професійно-кваліфікаційні групи працівників, які є невід'ємною частиною всієї виробничо-економічної діяльності та безпеки будь-якого підприємства. Від підбору, адаптації, мотивації, забезпечення безпечної діяльності та убезпечення персоналу від типових робочих конфліктів, а також задовільних соціально-трудових відносин залежить не тільки виживання, а й успішний розвиток підприємства.

В навчальному посібнику запропоновано шість тем: кадрова безпека підприємств і основи забезпечення надійності персоналу; контррозвідка як спосіб забезпечення надійності персоналу сучасних підприємств; інформація як об'єкт загрози у системі забезпечення надійності персоналу підприємств; особливості прийому персоналу на роботу та його звільнення; мотивування персоналу та контроль за його діяльністю; конфлікти на підприємствах і вплив їх на стан надійності персоналу.

Метою вивчення навчальної дисципліни «Сучасні методи забезпечення надійності персоналу» є набуття теоретичних

знань і практичних навичків з основ кадрового менеджменту та надійності персоналу, формування у здобувачів освітнього ступеня «магістр» системи фундаментальних теоретичних знань у сфері економічної та кадрової безпеки, оволодіння необхідними навичками для локалізації та усунення загроз, попередження небезпек об'єктивного чи суб'єктивного характеру, для формування і розвитку системи запобігання загрозам кадрової безпеки та формуванню лояльності й надійості персоналу.

Відповідно до освітньо-професійної програми, здобувачі вищої освіти повинні вміти:

1) проявляти здатність до професійної самоосвіти, особистого зростання, вміння діяти на основі професійних етичних міркувань;

2) обґрунтовувати напрями удосконалення антикорупційної політики держави;

3) систематизувати й аналізувати інформацію для вирішення професійних і наукових завдань, застосовувати методи, прийоми систематизації та обробки економічної інформації для вирішення типових проблем у сфері кадрової безпеки;

4) адаптувати положення та методи дослідження інших наук для розв'язання професійних і наукових задач у сфері кадрової безпеки;

5) виявляти злочинні технології, схеми і механізми злочинної діяльності персоналу з метою їх розкриття та/або передання зібраної інформації у відповідні органи у формі аналітичних висновків чи рекомендацій;

6) об'єктивно оцінювати дію загроз на всіх суспільних рівнях та формувати відповідні засоби й заходи протидії;

7) використовувати фундаментальні закономірності розвитку персоналу у поєднанні з дослідницькими та управлінськими інструментами для здійснення професійної та наукової діяльності, усунення конфліктів і забезпечення кадрової безпеки.

Тема 1
КАДРОВА БЕЗПЕКА ПІДПРИЄМСТВ І ОСНОВИ ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ ПЕРСОНАЛУ

1.1. Поняття кадрової та інтелектуальної безпеки сучасних підприємств.

1.2. Загрози кадровій безпеці підприємства.

1.3. Критерії кадрової безпеки.

1.4. Процес забезпечення кадрової та інтелектуальної безпеки.

Ключові поняття: кадрова безпека, інтелектуальна безпека, персонал, загрози персоналу, загрози підприємству у кадровій сфері, надійність персоналу.

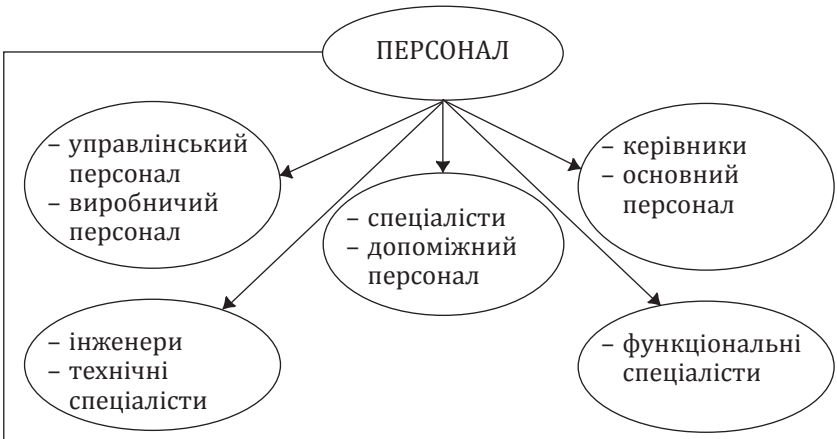
1.1. Поняття кадрової та інтелектуальної безпеки сучасних підприємств

Вище керівництво організації має закріплені статутом організації повноваження (право приймати остаточне рішення, спрямовувати та координувати роботу інших і надавати накази).

Лінійні менеджери уповноважені спрямовувати роботу підлеглих та відповідати за виконання основних завдань організації.

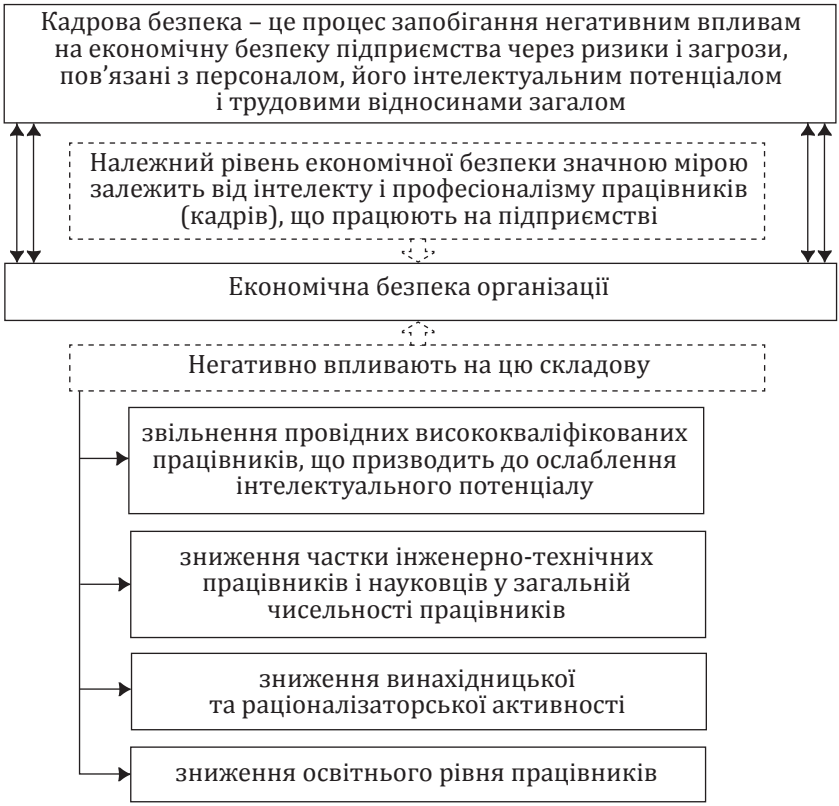
СТРУКТУРА: спискова чисельність персоналу на певну дату (включаючи всіх працівників, також тих, кого прийняли з цієї дати, і всіх звільнених з цієї дати).

За найпоширенішою класифікацією персонал організації поділяється на певні категорії:



Виробничий персонал	здійснює трудову діяльність у матеріальному виробництві з перевагою фізичної праці в загальному обсязі часу, зайнятому на виробництві
Основний персонал	робітники, які займаються виготовленням матеріальних благ або наданням послуг
Допоміжний персонал	робітники, які займаються безпосередньо обслуговуванням виробничих процесів
Управлінський персонал	здійснює свою діяльність у процесі управління виробництвом з переважанням розумової праці
Функціональні спеціалісти	працівники, результатом діяльності яких є управлінська інформація
Інженери	працівники, результатом діяльності яких є конструкторсько-технологічна або проектна інформація в галузі техніки і технології виробництва
Технічні спеціалісти	які виконують допоміжні роботи в процесі управління виробництвом (оператори ЕОМ, комірники)

Якщо розглядати кадрову безпеку в системі економічної безпеки як процес, висновуємо, що кадрова безпека – це процес моніторингу, мінімізації та превенції негативних впливів на економічну безпеку банку через ефективний ризик менеджмент-загроз і небезпек, пов'язаних із персоналом.



Якщо розглядати систему кадрової безпеки банку як стан, то кадрова безпека – це оптимальний стан захищеності персоналу банку від зовнішніх загроз та оптимальний стан економічної захищеності банку від внутрішніх загроз із боку персоналу.

За інтелектуальну складову економічної безпеки на підприємстві відповідають служба з персоналу й особисто головний інженер (якщо таку посаду введено).

Склад кадрів безпосередньо впливає на рівень економічної безпеки на підприємстві.

До найпоширеніших видів порушень належать:

- афери з боку провідних спеціалістів (менеджерів і керівників середньої ланки, відповідальних за конкретний напрям бізнесу підприємства), зазвичай «за стінами» своєї фірми, зокрема у міжнародних організаціях
- «відкат»
- фальсифікація сум «живих грошей» (готівки) у касі й сум на банківських рахунках, підроблення чеків підприємства
- несанкціонований продаж і використання майна (власності) підприємства з корисливою метою
- оплата роботи підставних (фіктивних осіб), так званих «пролісків»
- фальсифікація документації підприємства за допомогою електронної техніки й Інтернету (наприклад, перерахування коштів підприємства на особистий рахунок, внесення «потрібних» змін у звітні документи)
- несанкціоновані операції з цінними паперами, матеріальними й нематеріальними активами підприємства
- фальсифікація звітів про використання коштів, виділених на відрядження, представницькі видатки, на інші потреби підприємства

1.2. Загрози кадровій безпеці підприємства

Негативний вплив на кадрову складову мають внутрішні і зовнішні чинники (табл. 1.1).

Таблиця 1.1

Загрози кадровій безпеці організації

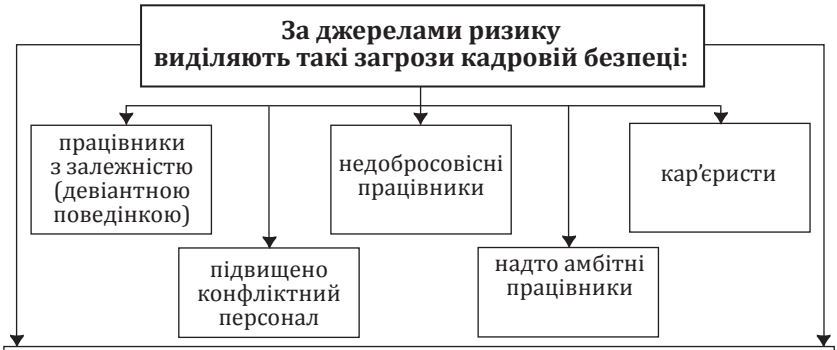
Внутрішні загрози	*Зовнішні загрози*
невідповідність кваліфікації працівників вимогам до них	кращі умови мотивації у конкурентів (нескладно за такого розкладу спрогнозувати перехід фахівців до конкурентів)
недостатня кваліфікація працівників	установка конкурентів на переманювання
слабка організація системи управління персоналом	тиск на працівників ззовні
слабка організація системи навчання	потрапляння працівників у різні узалежнення
неефективна система мотивації	інфляційні процеси (не можна не брати до уваги під час розрахунку заробітної плати і прогнозувати її динаміку); за цю складову економічної безпеки має відповідати служба з персоналу підприємства
помилки в плануванні ресурсів персоналу	прямий підкуп співробітників фірм-конкурентів
зниження кількості раціоналізаторських пропозицій та ініціатив	
відтік кваліфікованих працівників	
відсутність корпоративної політики або вона «слабка»	
неякісна перевірка кандидатів під час приймання на роботу	

Найпоширеніші види порушень із боку персоналу організації:

- фальсифікація сум готівки у касі та коштів на банківських рахунках, підробка фінансових документів підприємств;
- несанкціонований продаж і використання майна підприємства з корисливою метою;
- оплата роботи підставних (фіктивних) осіб;
- фальсифікація документації підприємства за допомогою електронної техніки та Інтернету;
- несанкціоновані операції з цінними паперами, матеріальними й нематеріальними активами підприємства;
- повідомлення конфіденційної та іншої інформації третім особам;
- фальсифікація звітів про використання коштів, виділених на відрядження, представницькі видатки, на інші потреби підприємства;
- порушення техніки безпеки та правил внутрішнього трудового розпорядку.

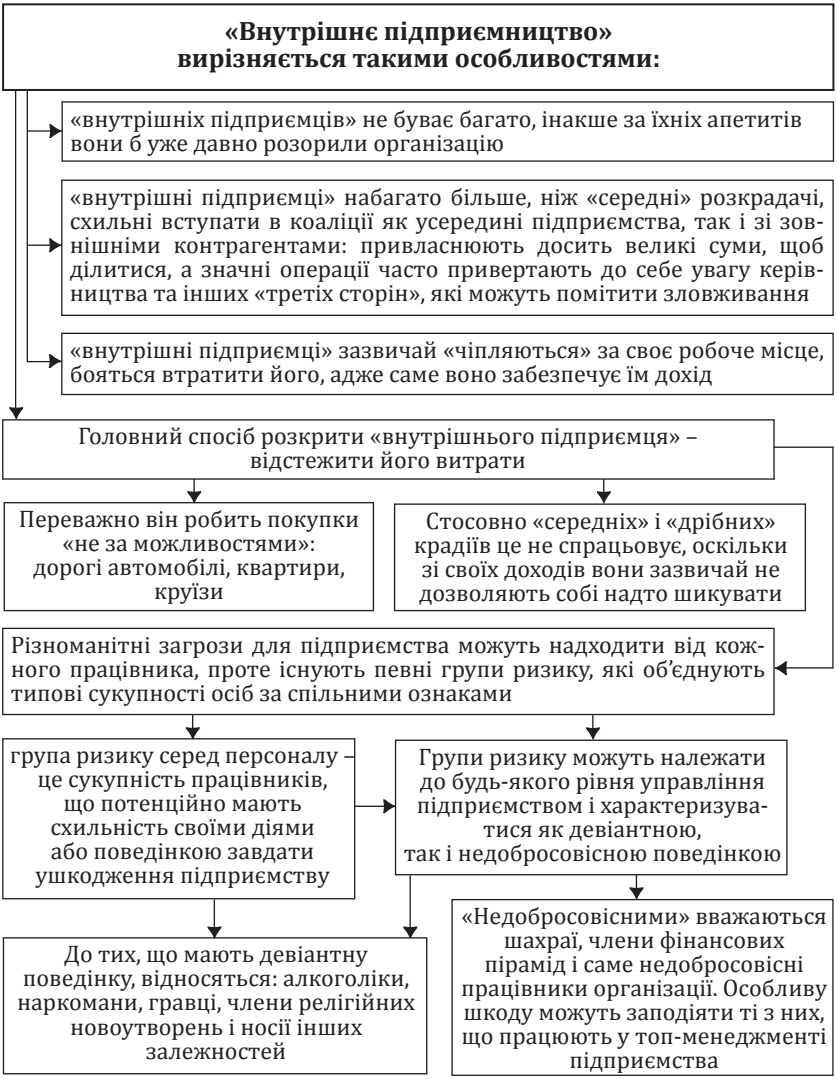
Працівники організації можуть вдаватися до здійснення афер з різних мотивів, серед яких найпоширенішими вважаються:

- особисті фінансові труднощі, неможливість задоволення життєвих потреб
- 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
- слабкий кадровий менеджмент, неефективна персональна робота з кадрами
- наявність слабких місць («дір») у системі управління діяльністю фірми (зокрема в системі бухгалтерського обігу)



Ризики кількісного характеру пов'язані з невідповідною кількістю персоналу на підприємстві поточним потребам. Загрози в роботі з персоналом якісного характеру обумовлені невідповідністю фактичних характеристик персоналу вимогам, що ставляться для нього (недостатністю кваліфікації).

Часто підприємства потерпають від зловживань з боку персоналу. Такими зловживаннями можуть бути дрібні разові розкрадання. Люди схильні іноді здійснювати дрібні крадіжки (наприклад, розкрадання товарів у магазинах самообслуговування). Крім дрібних разових крадіжок, практикуються систематичні розкрадання середнього розміру. Ця група розкрадань відрізняється від першої тим, що здійснюється з економічних мотивів, має систематичний характер, є продуманою та завдає істотних збитків підприємству.



Сьогодні найкращий вибір керівника – це лояльний співробітник.

Лояльність – задоволеність співробітника умовами, винагородою, зростанням і перспективами, колективом, захистом від зовнішніх загроз (наприклад, фізичних загроз співробітникові і його близьким).

Кодовим словом тут є *задоволеність*.

Задля попередження загроз кадровій безпеці потрібно планувати й організовувати заходи для її забезпечення в усіх напрямах кадрової політики організації.

Ці заходи повинні включати:

- аналіз причин виникнення негативних впливів на персонал
- оцінку поточного рівня кадрової безпеки в організації
- виявлення «білих плям»
- пошук шляхів виходу з проблемного стану
- бюджетне планування досягнення кадрової безпеки організації
- розрахунок ефективності запропонованих заходів організації
- оперативну реалізацію запропонованого комплексу заходів у процесі діяльності організації.

Для збереження кадрової безпеки доцільно використовувати сучасні кадрові технології, включаючи такі механізми, як:

- ефективна мотивація
- прискорена адаптація (завдяки наставництву)
- забезпечення контролю з боку служби персоналу
- своєчасне запобігання конфліктним ситуаціям
- атестація
- компенсація
- розумна політика звільнення
- пропаганда корпоративності

Однією з ефективних процедур відбору є **вивчення рекомендацій** з минулих місць роботи кандидата, а також перевірка цих відомостей. Віднедавна працедавці дедалі частіше почали застосовувати цей спосіб отримання додаткової інформації й активно використовувати її під час прийняття рішень.

Існують різні форми отримання характеристик від зовнішніх суб'єктів. Іноді кандидат з власної ініціативи приносить «рекомендацію». Тимчасом її все одно доведеться перевіряти. Або менеджер з персоналу сам звертається до попереднього працедавця (а то й до кількох) з певними запитаннями щодо претендента на посаду.

Варто почати з того, що попросити кандидата на посаду описати три–чотири останні реальні (не за трудовою книжкою) місця роботи зі зазначенням імен керівників, адрес і контактних телефонів. Вже на цій стадії заповнення анкети деякі кандидати починають дивитися в стелю, згадуючи, з ким же вони працювали минулого року, «висмоктувати телефони з пальця» і т. д.

Зазвичай доцільно, щоб менеджери з персоналу отримали усну характеристику на колишнього працівника від різних посадових осіб за рівнями. При цьому менеджер з персоналу зв'язується за місцем колишньої роботи зі своїм колегою і просить стисло описати позитивні й негативні якості претендента. Крім того, менеджер розмовляє з безпосереднім керівником кандидата. У разі приймання на роботу матеріально відповідальних осіб і керівників середньої ланки це робить начальник або працівник служби безпеки, контактуючи зі своїми колегами зі служби безпеки колишнього працедавця.

Отже, характеристики чи рекомендації, компетентна зовнішня і незалежна думка про кандидата є вагомими для ухвалення рішення про його працевлаштування, і нехтувати ними не доречно.

Психологічне тестування

Окрім психологічних тестів професійного відбору, застосовують також певні методи відбору з огляду на претендентів, особливо коли потрібно з'ясувати:

- залежність їх від наркотиків чи алкоголю ↔ пристрасть до азартних ігор
- схильність кандидата до здійснення протиправних дій, зухвалих і необдуманих вчинків у разі виникнення певних обставин ↔ інші ознаки, що свідчать про морально-психологічну нестійкість кандидата

Кадрова служба взаємодіє зі **службою безпеки** під час відбору персоналу тоді, коли потрібно проводити різні перевірки:

- за реєстрами міліції про судимість, істотні адміністративні стягнення, загублені паспорти, наявність розшукових справ та ін. ↔ відповідності реєстрації за місцем проживання (перебування)
- наявності зв'язків у кримінальному світі, зокрема через родичів ↔ кредитної історії через служби безпеки або кредитні відділи банків, що надають кредити
- участі в капіталі (установчому, акціонерному) юридичних осіб ↔ наявності нерухомого і рухомого (автомобілів) майна, зокрема відповідно до заявленого
- документів (диплома, паспорта) на відповідність їхніх форми і змісту дійсності ↔ Особливим різновидом тестування є **перевірка на детекторі брехні (поліграфі)**

За умови використання поліграфа при прийомі нового співробітника на роботу, результат тестування не лише дасть відповіді про минуле кандидата та істинні мотиви працевлаштування у компанію, а й дасть можливість скласти психологічний портрет кандидата, в якому будуть відображені його приховані наміри та схильності. Крім того, проведення поліграфного тесту при працевлаштуванні свідчить про солідність підприємства і серйозність його намірів не допустити потрапляння до своїх лав сумнівних особистостей.

Поліграф на етапі прийому на роботу дозволяє з'ясувати:

- спотворені анкетні дані;
- підроблені документи, що надаються;
- негативні звички і пристрасті;
- кримінальне минуле;
- справжні причини звільнення з попереднього місця роботи;
- істинні мотиви влаштування на роботу й чимало іншого

Періодичні перевірки з використанням поліграфа допомагають:

- виявляти підготовлювані правопорушення і зловживання;
- зв'язки з кримінальним світом або конкурентами;
- змову з метою заподіяння збитку й чимало іншого

При розкритті вчинених правопорушень застосування поліграфа дає змогу:

- виявити осіб, причетних до правопорушення, і ролі кожного з них;
- уточнити обставини і склад правопорушення;
- визначити замовників і виконавців у правопорушеннях та усунути підозру в причетності до них;
- виявити осіб, що ховаються від правосуддя, перебувають у розшуку;
- знайти канали витоку важливої інформації.

Під час роботи потрібно уважно спостерігати за взаєминами в колективі задля виявлення ймовірності негативного впливу. Відповідальність за процеси діяльності на підприємстві та рівень влади рекомендується розподіляти між декількома працівниками з метою зменшення можливості маніпуляцій.

1.3. Критерії кадрової безпеки

Щоби встановити критерії кадрової безпеки, потрібно зробити короткий екскурс у тему про кількісні параметри економічної безпеки організації.

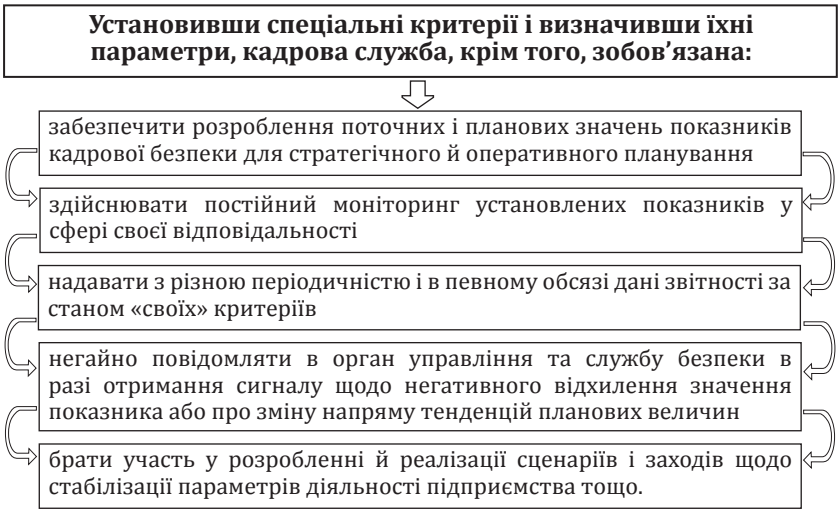
За загальним правилом, концепції і стратегії економічної безпеки практично реалізуються через систему конкретних заходів і механізмів, які, своєю чергою, розробляються на основі аналізу результатів моніторингу якісних критеріїв та їхніх кількісних параметрів.

Для цього іноді вдаються до встановлення певних «сигнальних» показників і вказують їхні граничні значення, тобто граничні величини, вихід за межі яких призводить до формування негативних тенденцій в економічній і, зокрема, в кадровій безпеці.

Подолання граничних значень – сигнал до дії зі запобігання загрозі, зниження збитку або припинення зловмисних атак.
Найвищого ступеня безпеки досягають за умови, якщо весь комплекс показників перебуває в допустимих межах своїх порогових значень.

Головними групами критеріїв безпосередньо в кадровій безпеці є показники:

- чисельного складу персоналу та його динаміки;
- кваліфікації й інтелектуального потенціалу;
- ефективності використання персоналу;
- якості мотиваційної системи.



Моніторинг здійснюється з метою виявлення і прогнозування негативних дій щодо інтересів та об'єктів економічної безпеки (ЕБ). Несприятливі явища і процеси наведені у табл. 1.2.

Таблиця 1.2

Негативні дії щодо інтересів об'єктів ЕБ

№ з/п	Несприятливі явища та процеси
1	Відхилення величин установлених контрольних показників від граничних у негативний бік
2	Збільшення амплітуди динаміки встановлених показників на величини, більші за допустимі
3	Виникнення нез'ясовних фінансових, технологічних та інформаційних явищ і процесів
4	Виникнення форс-мажорних обставин
5	Нез'ясована або негативна поведінка окремих працівників і їхніх груп
6	Виникнення конфліктних ситуацій між внутрішніми й зовнішніми суб'єктами бізнесу
7	Підозрілий інтерес з боку зовнішніх суб'єктів до діяльності компанії, підрозділу, об'єкта, його персоналу, керівництва, інформації, матеріальних засобів і грошових коштів
8	Факти розкрадань, пошкоджень майна, зникнення грошей і документів, інші неправомірні дії
9	Спроби несанкціонованого доступу і використання внутрішньої інформації;
10	Виникнення проблем особистої безпеки працівників та ін.

Зрозуміло, всі посадові особи і працівники зобов'язані негайно повідомляти про такі відхилення в службу безпеки, а іноді – безпосередньо адміністрації. Невжиття належних заходів передбачає встановлену законом відповідальність.

Таблиця 1.3

Перелік критеріїв оцінки кадрового потенціалу організації

№ з/п	Критерії оцінки кадрового потенціалу
1	Кількість працівників з науковим ступенем доктора, кандидата серед науково-дослідного персоналу
2	Кількість наукових публікацій у поточному році (за останні 5 років)
3	Кількість отриманих наукових ступенів у поточному році (за останні 5 років)
4	Досвід роботи в інноваційній сфері науково-дослідного персоналу
5	Частка науково-дослідного персоналу щодо всього персоналу організації
6	Частка працівників з вищою освітою щодо інших груп працівників
7	Кількість нагород, отриманих на конкурсах і виставках за інновації
8	Кількість (вартість) проданих ліцензій у поточному році (за останні 5 років)
9	Кількість зареєстрованих патентів у поточному році (за останні 5 років)

Ці та інші аналітичні показники (коефіцієнти) порівнюють з аналогічними у споріднених підприємствах або аналізують у динаміці.

1.4. Процес забезпечення кадрової та інтелектуальної безпеки

Змістову характеристику всього циклу забезпечення інтелектуальної і кадрової складової економічної безпеки можна подати за схемою:

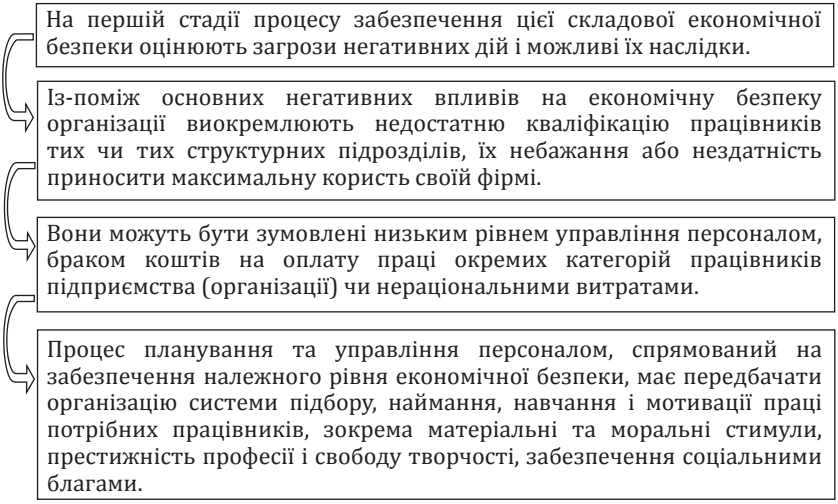
Забезпечення інтелектуальної та кадрової складових економічної безпеки охоплює взаємопов'язані і водночас самостійні напрями діяльності організації:

⇩

перший зорієнтований на роботу з персоналом фірми, на підвищення ефективності діяльності всіх категорій персоналу

⇩

другий – на збереження й розвиток інтелектуального потенціалу, тобто сукупності прав на інтелектуальну власність або на її використання та на поповнення знань і професійного досвіду працівників організації



Деякі ознаки правопорушення в поведінці співробітника і його неправомірні дії наведено в табл. 1.4.

Таблиця 1.4

Ознаки правопорушення в поведінці співробітника і його неправомірні дії

№ з/п	Перелік ознак
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.

Найпоширеніші методи (способи) профілактики правопорушень персоналу перелічено в табл. 1.5.

Таблиця 1.5

Основні методи профілактики правопорушень персоналу

№ з/п	Назва методу
1	Висококваліфікований кадровий менеджмент, використання сучасних технологій, персональна робота з кадрами й управління поведінкою персоналу.
2	Здійснення зовнішнього та внутрішнього аудиту діяльності керівних кадрів, розподіл їхніх функцій.
3	Періодичне відновлення повноважень (анулювання доручень, поділ функціональних обов'язків тощо).
4	Доручення комерційних справ не одному фахівцеві, а декільком – на конкурентній основі.
5	Розроблення й дотримання сучасних методів охорони власності (майна) підприємства, зокрема коштів, інформаційних комунікацій.
6	Оптимізація системи фінансового обліку та звітності.
7	Обмеження доступу (допуску) співробітників до документів фінансової та бухгалтерської звітності.

Наведені загальні положення можуть допомогти керівникам підприємств будь-якої форми власності у питаннях безпеки бізнесу. На практиці характерні неповторні особливості кожного підприємства, окремі положення безпеки бізнесу та профілактики правопорушень персоналу можуть і повинні бути деталізовані й адаптовані до конкретних форм діяльності й організаційної структури підприємства.

Питання для обговорення

1. Роз'ясніть поняття кадрової та інтелектуальної безпеки сучасних підприємств.
2. Які існують загрози кадровій безпеці підприємства?
3. Перелічіть критерії кадрової безпеки.
4. З яких етапів складається процес забезпечення кадрової та інтелектуальної безпеки?
5. Охарактеризуйте кадри як внутрішню загрозу безпеці підприємства.
6. У чому полягають основні моменти відбору персоналу?
7. Які Ви знаєте функції і завдання кадрової служби у сфері забезпечення економічної безпеки?

Домашні завдання

Завдання 1. Здійснити хронологічний аналіз нормативно-правових актів, у яких закладено правове регламентування процесу забезпечення кадрової безпеки підприємств, установ, організацій. Результати аналізу подати у формі таблиці

№ з/п	Документ	Рік прийняття	Положення, що стосуються кадрової безпеки підприємств, установ, організацій
...	...	...	...

Завдання 2. Графічно зобразити структуру системи кадрової безпеки, встановити зв'язки між її елементами.

Форма контролю: Усне опитування, перевірка рефератів, вирішення тестових завдань.

Рекомендована література: 3, 5, 12, 13, 20, 21.

Тема 2

КОНТРРОЗВІДКА ЯК СПОСІБ ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ ПЕРСОНАЛУ СУЧАСНИХ ПІДПРИЄМСТВ

2.1. Поняття системи економічної та конкурентної розвідки на підприємстві.

2.2. Система економічної контррозвідки на сучасному підприємстві.

2.3. Оргструктура контррозвідувального підрозділу.

2.4. Класифікація методів контррозвідувальної діяльності.

Ключові слова: контррозвідувальний підрозділ, економічна контррозвідка, оргструктура підрозділу контррозвідки, система економічної контррозвідки.

2.1. Поняття системи економічної та конкурентної розвідки на підприємстві

Під терміном *«система економічної розвідки»* розуміють організаційну структуру, яка займається питаннями збирання, перевірки (верифікації), опрацювання та аналізу даних з різних аспектів зовнішньоекономічної діяльності підприємства з подальшим використанням отриманої інформації для вирішення конкретних завдань його господарської діяльності.

В умовах ринкової економіки підприємство не може ефективно працювати

без глибокого розуміння її рушійних сил

не маючи у своєму розпорядженні новітньої інформації про те, що ж відбувається у займаному ним сегменті ринку

при цьому обов'язково треба враховувати

що можливості підприємства, обумовлені навколишнім середовищем і балансом інтересів різних співтовариств, угруповань і окремих осіб, часто випливають не з логіки подій, а з емоцій, особистих симпатій і антипатій.

Підрозділ економічної розвідки підприємства – структурний підрозділ, на який покладено завдання єдиного (в рамках господарюючого суб'єкта) інформаційного центру, зі завданнями опрацювання та аналізу інформації, що забезпечує ухвалення вищим керівництвом обґрунтованих рішень із найважливіших для інтересів підприємства питань.

Основні передумови створення системи економічної розвідки на сучасному українському підприємстві

швидка зміна обстановки в країні

політична | соціальна | економічна

обстановка в країні змінюється так різко, що неформальних засобів спостереження за навколишнім середовищем стає недостатньо

Тому для адекватного реагування на вплив навколишнього середовища і забезпечення успіху в конкурентній боротьбі підприємству потрібна ефективна система економічної розвідки.

З метою якісного інформаційного забезпечення керівництва підприємства система економічної розвідки має бути орієнтована на конкретних осіб, що ухвалюють управлінські рішення.

Система економічної розвідки повинна не просто вирішувати питання накопичення даних і видачі звітів.

Головне її завдання – забезпечити осіб, що ухвалюють управлінські рішення, такою інформацією, яка допомагала би вибрати найбільш оптимальний варіант вирішення проблеми, що стоїть перед підприємством.

Цілеспрямований збір загальнодоступної інформації з різних відкритих джерел з подальшим порівнянням і аналізом часто допомагає приймати важливі, але непомітні за поверхневого підходу рішення.

Система економічної розвідки мусить працювати легітимно, тобто не використовуючи незаконних і неетичних методів збору інформації.

Завжди слід зважати на те, що конкуренти також можуть мати розвідувальні органи і за потреби вдатися до незаконних способів отримання інформації, що цікавить їх.

Розглядаючи можливу модель реалізації системи економічної розвідки на підприємстві, слід враховувати, що масштаби й кількість засобів, які залучаються до її створення і експлуатації, багато в чому визначаються можливостями самого підприємства і завданнями, що стоять перед ним.

Планування розвідувальної діяльності і систематизація розвідувальної інформації.

Будь-яка діяльність має ґрунтуватися на певних принципах, не є винятком і розвідувальна діяльність.

Принципи – це керівні ідеї, основоположні аспекти, вироблені оперативно-розвідувальною практикою і виражені в нормах законодавчих актів; політичні, економічні й соціальні закономірності розвитку українського суспільства; етичні і правові уявлення громадян України про суть, мету, завдання і процедури здійснення оперативно-розвідувальної діяльності.

Першим і найважливішим принципом організації будь-якої розвідувальної діяльності, зокрема економічної, ***є неупередженість у відборі, систематизації, обробленні й передачі адресатові здобутої інформації.***

У підприємницьких організаціях найбільший інтерес і, відповідно, кількість загроз виникають у сфері економіки. Тому оперативно-розвідувальна діяльність із гарантування економічної безпеки є пріоритетною.

Іншими важливими принципами планування розвідувальної діяльності в економіці є:

– визначення мети проведення розвідувальної діяльності

– визначення потреби суб'єкта економічної діяльності в інформації для досягнення цих цілей

– визначення джерел отримання необхідної інформації.

Для продуктивного ведення господарської діяльності керівництво підприємства має ухвалювати різнорівневі рішення, інформаційну підтримку яких забезпечує система економічної розвідки.

Управління будь-якою організацією має як мінімум два рівні:

управління поточною діяльністю підприємства

управління його стратегічним розвитком

Результати ухвалених рішень з цих питань виявляються по-різному:

поточні – найближчим часом

стратегічні – в майбутньому

Слід зазначити, що характер інформації для кожного рівня ухвалених рішень є різним.

У роботі підрозділу економічної розвідки підприємства доцільно виокремити дві складові:

Стратегічна (макроекономічна) складова економічної розвідки → збирання й аналіз стратегічної інформації про глобальні процеси в економіці, політиці, технології тощо, які можуть впливати на розвиток підприємства.

Мета стратегічного рівня ухвалення рішення (відкриття нового виробництва, впровадження на ринок нового товару або послуги) полягає у визначенні напряму подальшого розвитку підприємства. → Ці рішення зумовлюють потребу зорієнтуватися на ринку та проаналізувати перспективи його розвитку, розгледіти ще не заповнені конкурентами ринкові ніші.

Оперативно-тактична (мікроекономічна) складова економічної розвідки → збирання й аналіз оперативно-тактичної інформації для ухвалення керівництвом обґрунтованих рішень з поточних проблем підприємства.

Мета оперативно-тактичного рівня ухвалення рішення (будівництво або придбання будівлі під новий цех, навчання персоналу для випуску нової продукції або надання нової послуги), відповідно до напряму подальшого розвитку, – вибрати оптимальний шлях його досягнення і мінімізувати витрати розвитку цим шляхом. → Попереднє планування розвідувальної діяльності потрібне ще й для того, аби в майбутньому не захлинутися в потоках накопичуваної інформації.

Кожне підприємство має власну специфіку, тож та інформація, яка для одного підприємства є життєво необхідною, для іншого – даремний «інформаційний шум». Доцільність збору інформації треба розглядати через потребу в ній для дії на довколишнє середовище з метою отримання конкретним підприємством максимального прибутку.

Цілі створення системи економічної розвідки підприємства

Основне призначення системи економічної розвідки полягає у:

забезпеченні керівництва фірми достовірною, об'єктивною і повною інформацією про наміри партнерів, суміжників, клієнтів і контрагентів, про сильні і слабкі сторони конкурентів

збиранні даних, що дають змогу впливати на позицію опонентів у ділових переговорах

сповіщенні про можливе виникнення кризових ситуацій

моніторингу та контролі реалізації укладених договорів і досягнутих раніше домовленостей

Цілі розвідувальної діяльності в економіці та на підприємстві:

1. своєчасне забезпечення керівництва надійною й усебічною інформацією про навколишнє середовище для підприємства. Виявлення ризиків, які можуть стосуватися економічних інтересів підприємства і перешкодити його нормальному функціонуванню;
2. організація максимально ефективної роботи з інформацією, що запобігає дублюванню структурними підрозділами підприємства функцій один одного;
3. вироблення коротко- і довгострокових прогнозів впливу навколишнього середовища на господарську діяльність підприємства. Розроблення рекомендацій щодо локалізації і нейтралізації чинників, які активізують ризики;
4. посилення сприятливих і локалізація несприятливих чинників впливу навколишнього середовища на господарську діяльність підприємства (управління ризиками).

Потреби в розвідувальній інформації на підприємстві

Підрозділ економічної розвідки іноді повинен ефективно працювати в умовах, коли ще не відомо, які рішення і на основі чого потрібно буде ухвалювати. Щоб максимально зменшити кількість таких робочих моментів, варто разом із керівництвом підприємства дійти єдиного розуміння проблеми і шляхів її вирішення, а також домовитися про уніфікацію використовуваної в роботі термінології.

Єдино можливий шлях виконання цього непростого завдання полягає в проведенні докладних інтерв'ю з керівництвом підприємства і з керівниками його структурних підрозділів про їх інформаційні потреби.

Краще зробити це за допомогою спеціально розробленої анкети, у якій керівництво вищої і середньої ланок висловить свої зауваження з приводу того:

– яку інформацію воно має у своєму розпорядженні;
– як і де ці дані накопичуються;
– яка інформація, за їхніми даними, є в інших підрозділах підприємства;
– яка інформація, що циркулює поза підприємством і в його структурних підрозділах, потрібна їм для повсякденної роботи.

На основі такого анкетування розробляють рубрикатор, за яким відбуватимуться накопичення і систематизація інформаційних масивів.

Будь-яке підприємство постійно розвивається, виникають нові цілі, змінюється сам ринок і навколишнє середовище для підприємства. Тому рубрикатор доцільно періодично переглядати і за потреби змінювати його на основі повторного аналізу цілей та інформаційних потреб підприємства.

Впровадження розвідувальних технологій на практиці зазвичай пов'язане зі специфічною психологічною протидією, відомою як «інформаційний монополізм». Ще до початку впровадження системи економічної розвідки на конкретному підприємстві там уже склався баланс інтересів, який ґрунтується на тому, що кожен працівник, який володіє певним обсягом інформації за напрямом своєї діяльності, прагне якомога менше ділитися нею зі своїм оточенням.

Інформаційний монополізм обумовлюється тим, що статус працівника, його необхідність для підприємства і відповідно отримувані ним матеріальні блага визначаються ступенем доступу до цієї інформації.

Тому перед початком реалізації програми щодо створення системи економічної розвідки потрібні глибоке осмислення ситуації, що склалася, вивчення інтересів усіх учасників подій та їх можливого балансу, і тільки тоді – створення сприятливих умов для проведення відповідних робіт.

У штатному розписі підрозділу економічної розвідки можуть бути підрозділи

зв'язків з громадськістю | економічного аналізу | маркетингових досліджень

Можливе також працевлаштування в різні відділи

відділ збуту | відділ кадрів | юридичний відділ | відділ ЗЕД | відділ постачання

Вони мають щоденні робочі контакти зі зовнішнім оточенням підприємства через працівників підрозділу економічної розвідки, що працюють під офіційним прикриттям і виконують як розвідувальні, так і контррозвідувальні функції.

Трапляються і такі витончені ходи, як виділення розвідувального підрозділу в комерційну інформаційну (юридичну) фірму, оформлену через підставних осіб і юридично ніяк не пов'язану зі своїм працедавцем.

2.2. Система економічної контррозвідки на сучасному підприємстві

Робота підрозділу економічної контррозвідки служби безпеки господарюючого суб'єкта пов'язана:

- з виявленням, попередженням, припиненням спроб інфільтрації і вербуванням агентури конкурентами, партнерами та кримінальними структурами
- зі запобіганням просочуванню конфіденційної інформації про діяльність підприємства з боку його працівників, партнерів і клієнтів
- з профілактичною перевіркою лояльності його співробітників, службовим розслідуванням фактів фальсифікації і розкрадань
- з оперативним прикриттям персоналу, будівель і об'єктів підприємства

Проте варто ще раз нагадати, що в разі виявлення ознак підготовлюваного або здійснюваного злочину підрозділ економічної контррозвідки підприємства повинен налагодити тісну взаємодію з органами внутрішніх справ, СБУ і прокуратури.

Разом зі зазначеним вище підрозділ контррозвідки мусить приділяти достатню увагу запобіганню в колективі підприємства негативним процесам, як-от:

- трудові конфлікти з адміністрацією;
- загострення міжнаціональних відносин;
- погрози у проведенні страйків;
- групові порушення громадського порядку і т. ін.

Виявляти й усувати причини та умови перелічених кризових ситуацій можна:

- спеціальними (адміністративними, дисциплінарними);
- соціально-психологічними методами (погоджуючи інтереси конфліктуючих сторін).

Значення і роль контррозвідки служби безпеки підприємства нині обумовлені принаймні двома обставинами:

1) прагненням деяких підприємців усунути або нейтралізувати своїх конкурентів за допомогою засобів економічного шпигунства;

2) розширенням масштабу криміналізації населення, що створює живильний ґрунт для бажання його певних прошарків задовольняти свої потреби злочинним шляхом.

Мета контррозвідувального підрозділу

протидія розвідувальним заходам конкурентів і припинення правопорушень з боку протиправних груп або окремих осіб, що вчиняли замах на інтереси підприємства або його окремих співробітників

Призначення

контррозвідка займається переважно захистом і оборонною діяльністю

На відміну від розвідки, об'єктом контррозвідувальної діяльності є не зовнішнє, а внутрішнє середовище функціонування підприємства, у складі якого діють:

- керівники (директор, його заступники, головний бухгалтер і т. ін.) як потенційні об'єкти розвідувальних заходів і/або злочинів з боку конкурентів;
- особи з допоміжного персоналу, що мають доступ до комерційної таємниці (друкарки, працівники канцелярії та ін.);
- працівники, з боку яких існує потенційна небезпека надання злочинним елементам таких відомостей, які допоможуть їм скоїти злочини (варта, охоронці, водії персональних машин керівників та ін.);
- працівники самої служби безпеки;
- раніше судимі особи серед працівників підприємства;
- працівники підприємства, родичі яких працюють у конкурентів;
- працівники, що раніше були звільнені з підприємства;
- особи, які через свої посадові обов'язки регулярно приймають відвідувачів підприємства.

Завдання підрозділу контррозвідки

- боротьба з економічним шпигунством
- припинення злочинів проти окремих груп працівників (або всіх працівників на їхніх робочих місцях)
- сприяння правоохоронним, судовим і контрольно-наглядовим органам в документуванні протиправних дій осіб, що скоюють кримінальні злочини і мають адміністративну провину

Функції контррозвідки

- збирання відомостей і документів із цивільних і кримінальних справ
- регулярне інформування керівництва підприємства про причини створення умов та сприяння вчиненню правопорушень з боку персоналу; документування дій осіб, затриманих за адміністративні правопорушення
- виявлення осіб серед персоналу, які сприяють злочинним елементам (що не працюють на підприємстві) у здійсненні ними злочинів
- викриття економічних (промислових) шпигунів серед персоналу
- інформування керівників підприємства й охоронців (якщо вони є) про заплановані стосовно них злочини
- пошук безвісти зниклих працівників підприємства
- створення умов, що запобігають підслуховуванню розмов у службових кабінетах
- з'ясування обставин розголошування відомостей, що становлять комерційну таємницю
- з'ясування біографічних та інших даних про працівників підприємства (за їх письмовою згодою) при підписанні з ними трудових контрактів
- консультування персоналу з питань гарантування безпеки підприємства

Коротко охарактеризуємо кожну з перелічених функцій.

Працівник контррозвідки може займатися збиранням відомостей як до початку, так і в процесі судового розгляду цивільної справи. Те саме стосується збирання відомостей з кримінальних справ.

Проте, на відміну від цивільної справи, керівник контррозвідки зобов'язаний одночасно з цим направити до правоохоронного органу, що проводить розслідування, письмове повідомлення.

Слід також зазначити, що підрозділ контррозвідки може брати участь у збиранні даних з усіх цивільних справ підприємства-засновника, натомість із кримінальних справ, розпочатих проти працівників підприємства, – тільки із санкції його керівництва.

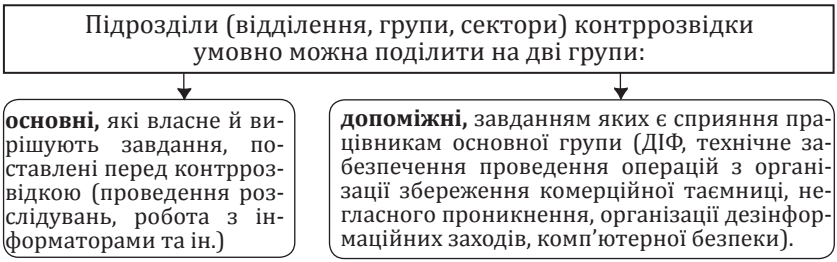
Основні напрями діяльності контррозвідки:

- регулярне інформування керівництва підприємства про причини виникнення умов, які сприяють здійсненню правопорушень з боку персоналу
- документування дій осіб, затриманих за адміністративні правопорушення
- виявлення осіб серед персоналу, що сприяють злочинним елементам (які не працюють на підприємстві) в здійсненні ними злочинів
- викривання економічних (промислових) шпигунів серед персоналу
- інформування керівників підприємства й охоронців (якщо вони є) про заплановані стосовно них злочини
- пошук безвісти зниклих співробітників підприємства
- створення умов, що запобігають підслуховуванню розмов у службових кабінетах
- визначення обставин розголошення відомостей, що становлять комерційну таємницю
- з'ясування біографічних та інших даних про працівників підприємства (за їх письмовою згодою) при підписанні з ними трудових контрактів
- пошук утраченого працівниками майна, що належить підприємству
- консультування з питань забезпечення безпеки підприємства і його персоналу

Цілі, завдання, функції та інші основні питання діяльності контррозвідки зазвичай відображають у положеннях про контррозвідувальні підрозділи.

2.3. Оргструктура контррозвідувального підрозділу

На основі затверджених керівництвом служби безпеки і підприємства цілей, завдань і функцій контррозвідки можна формувати її оргструктуру.



Чіткіше уявлення про розмежування структурних підрозділів контррозвідки можна мати, знаючи їх завдання і форми подання результатів роботи (табл. 2.1).

Таблиця 2.1

Розмежування діяльності структурних підрозділів контррозвідки

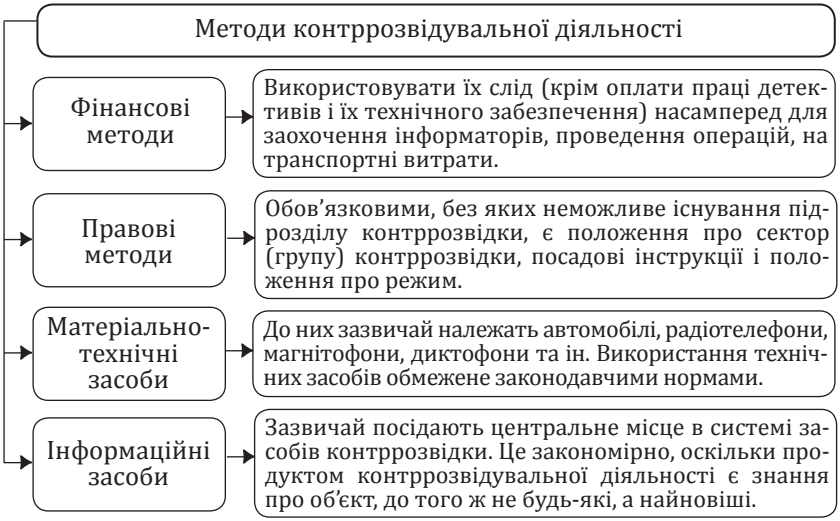
Назва підрозділу	Завдання	Форма подання результатів роботи
1	2	3
1. Відділення (група, сектор) власної безпеки	Документування протиправних і аморальних дій працівників служби безпеки	Рапорт, довідка, протокол спостереження, огляди
2. Відділення (група, сектор) проведення розслідувань	Збирання й аналіз інформації про правопорушення і надзвичайні ситуації	Рапорт, аналітична довідка, справа (досьє)
3. Відділення (група, сектор) роботи з інформаторами	Залучення до співпраці інформаторів і отримання від них регулярної інформації про перебування на об'єкті, що охороняється, і серед його персоналу	Справа (досьє), аналітичні огляди, довідка щодо кожного повідомлення інформатора

Закінчення табл. 2.1

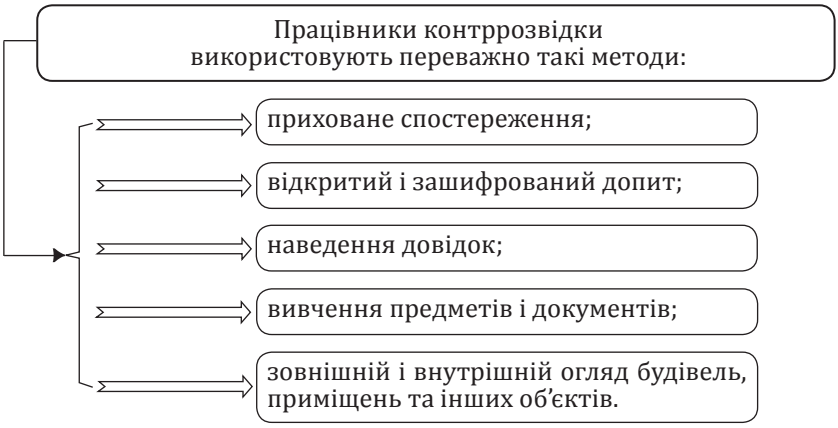
1	2	3
4. Довідково-інформаційний фонд	Ведення звітів, зберігання і видача співробітникам необхідної інформації (досьє) тощо	Довідки, аналітичні огляди, облікові картки, меморандуми
5. Відділення (група, сектор) із запобігання правопорушенням	Аналіз правопорядку на підприємстві та пропозиції керівництву підприємства про усунення причин та умов виникнення правопорушень на об'єкті, що охороняється	Досьє (справа), аналітичні довідки
6. Відділення (група, сектор) з технічного забезпечення проведення операцій	Установлення та експлуатація технічних засобів, надання їх співробітникам інших груп	Акти, кіно-, фотокадри, звукозапис, т. ін.
7. Відділення (група, сектор) організації збереження комерційної таємниці	Створення технічних умов, що запобігають витоку комерційної таємниці	Акти перевірок, протоколи обстеження приміщень, інструкції для персоналу підприємства тощо
8. Відділення (група, сектор) негласного проникнення	Висвітлення стану правопорядку і трудової дисципліни в колективі підприємства	Рапорти, огляди, аналітичні записки
9. Відділення (група, сектор) організації дезінформаційних заходів	Організація заходів, що вводять в оману конкурентів і злочинців	Плани дезінформаційних заходів, звіти, довідки
10. Відділення (група, сектор) комп'ютерної безпеки	Захист комп'ютерних мереж від несанкціонованого доступу до них	Звіти, довідки

До сил контррозвідки належать її кадрові співробітники; поділяються вони на тих, які мають ліцензію на детективну діяльність, і тих, котрі її не мають (друкарки, водії, секретарі й та ін.).

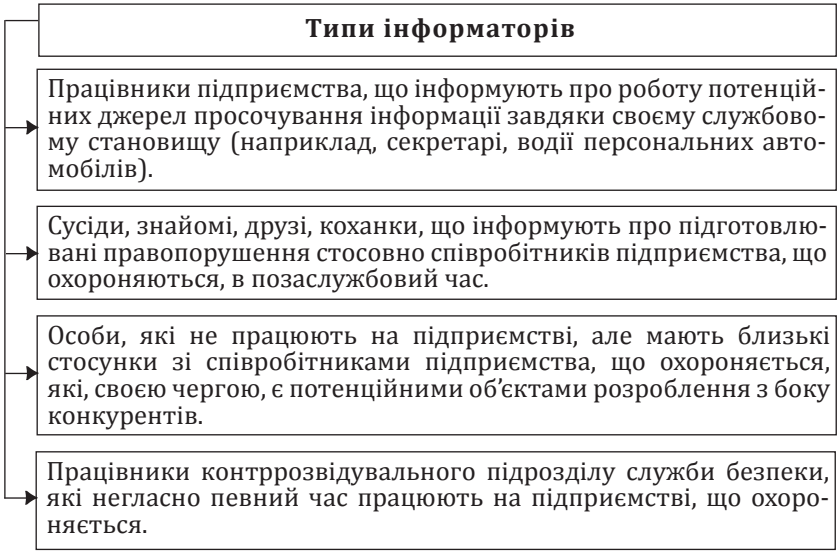
2.4. Класифікація методів контррозвідувальної діяльності



До інформаційних засобів належать різні реєстри, що допомагають детективам контррозвідки у їхній роботі (причому не завжди доцільно вводити їх у комп'ютерні системи).



Перелічені методи можна ефективно застосовувати як окремо, так і в комплексі. Проте найефективнішим методом слід визнати допит, оскільки під час нього можна використовувати інформаторів.



Можлива й інша класифікація методів контррозвідувальної діяльності. Наприклад, у межах тріади «особа–документ–виріб (процес)» методи отримання контррозвідувальної інформації розрізняють за джерелами інформації (табл. 2.2).

Таблиця 2.2

Основні методи отримання розвідувальних відомостей (за джерелами інформації)

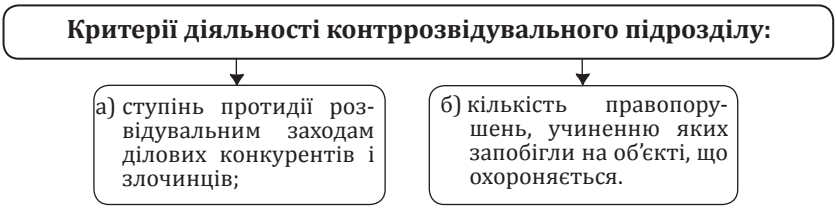
Людина	Документ	Виріб (процес)
1	2	3
1. Допит співробітників свого підприємства	1. Вивчення документів судових, правоохоронних і контрольно-наглядових органів	Створення сприятливих умов для крадіжки непридатного зразка (виробу), що видається за придатний, і документальна фіксація цього злочину
2. Поширення помилкових чуток через балакучих працівників свого підприємства з метою дезінформації конкурентів	2. Аналіз документації з дотримання пропускного режиму	

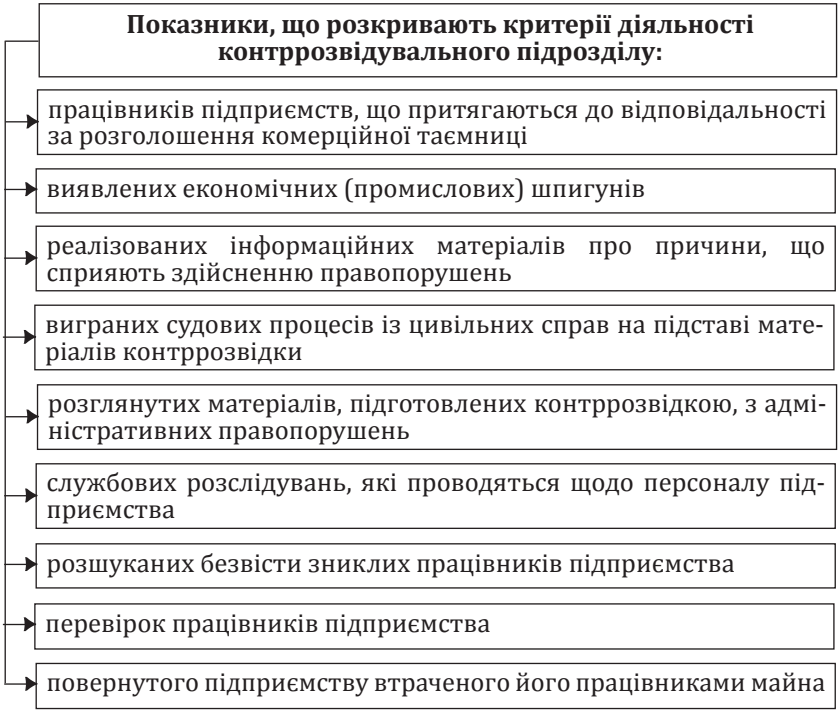
Закінчення табл. 2.2.

1	2	3
3. Умови недбалого зберігання документів (виробів) з одночасним негласним контролем за цим з метою установлення особи, зацікавленої в їх придбанні	3. Збирання та аналіз інформації про відхилення, порушення охоронної служби	
4. Інформація, яка суворо дозується і негласно контролюється серед працівників підприємства з метою виявлення джерела просочування конфіденційної інформації	4. Випуск сфальсифікованої проектної документації	
5. Бесіда із працівниками правоохоронних і контрольно-наглядових органів		

Проте перелічені методи будуть ефективними тільки тоді, коли доповнюватимуть один одного.

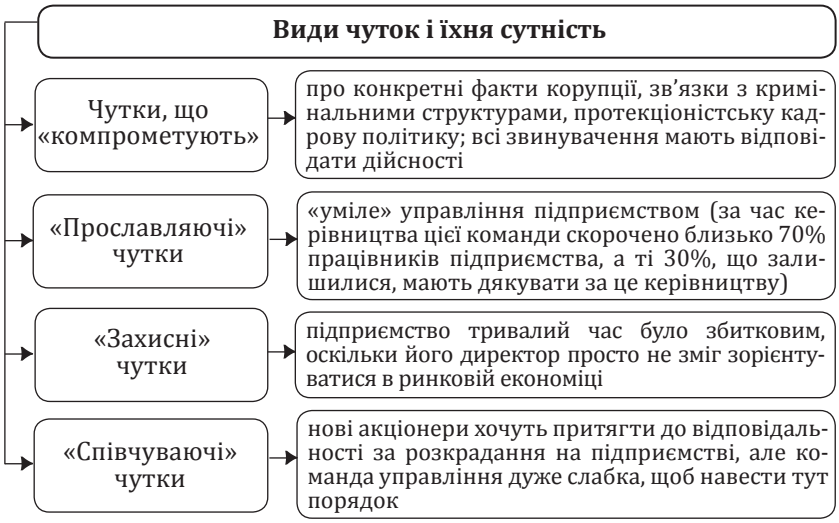
Для об'єктивного оцінювання діяльності контррозвідки потрібно розробляти відповідні критерії і показники її діяльності.





Існує типова схема дій розвідувальних органів стосовно дестабілізації господарюючого суб'єкта.

Поширення компрометуючих чуток з метою підриву авторитету керівництва господарюючих суб'єктів є достатньо складною технологією дії, що полягає у формуванні й поширенні єдиного за своєю спрямованістю блоку чуток, який зазвичай містить інформацію, що ганьбить об'єкт дискредитації і/або «прославляє», «захищає» і «співчуває».



Тому усунення чуток полягає в усуненні двозначності. Повна (і своєчасна недвозначна) інформація про подію перетворює другий співмножник на величину, яка близька або дорівнює нулеві. Це робить функцію від утворення двох співмножників надто мізерною. Тобто чуток не буде, якщо не буде приводу для них.

Питання для обговорення

1. Чим займається контррозвідка на підприємстві?
2. З яких елементів складається середовище, з яким працює розвідувальний підрозділ?
3. У чому полягає мета діяльності та функції розвідувального підрозділу?
4. Що передбачає робота контррозвідувального підрозділу зі збору відомостей і документів з цивільних і кримінальних справ?
5. У чому полягає робота контррозвідувального підрозділу із регулярного інформування керівництва підприємства про причини, що породжують умови, які сприяють здійсненню правопорушень з боку персоналу?
6. У чому полягає робота контррозвідувального підрозділу із документування дій осіб, затриманих за адміністративні правопорушення?

7. У чому полягає робота контррозвідувального підрозділу із виявлення осіб з числа персоналу, що сприяють злочинним елементам (які не працюють на підприємстві) в здійсненні ними злочинів?

8. У чому полягає робота контррозвідувального підрозділу із викривання економічних (промислових) шпигунів з числа персоналу?

9. У чому полягає робота контррозвідувального підрозділу з інформування керівників підприємства й охоронців (якщо вони є) про заплановані щодо них злочини?

10. У чому полягає робота контррозвідувального підрозділу з пошуку безвісти зниклих співробітників підприємства?

Домашнє завдання

Дослідити публікації вітчизняних та зарубіжних учених, у яких надаються пропозиції щодо оптимізації діяльності контррозвідувального підрозділу підприємства (у формі презентації).

Форма контролю: усне опитування, перевірка рефератів, перегляд презентації, вирішення тестових завдань.

Рекомендована література: 1–13, 17–19, 22–25, 28–30, 52–60, 71–76.

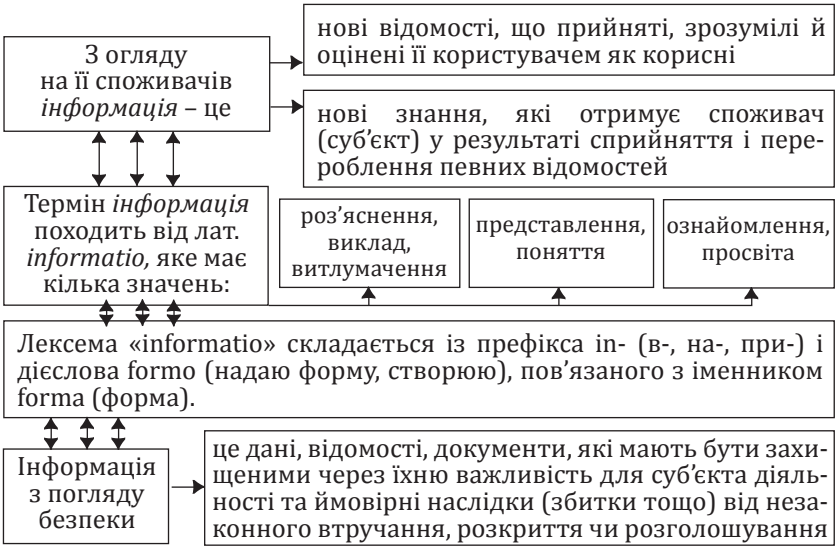
Тема 3
ІНФОРМАЦІЯ ЯК ОБ'ЄКТ ЗАГРОЗИ У СИСТЕМІ ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ ПЕРСОНАЛУ ПІДПРИЄМСТВ

3.1. Суть і поняття інформації та інформаційної безпеки.
3.2. Класифікація і характеристика різних видів інформації.
3.3. Методи і способи захисту інформації.

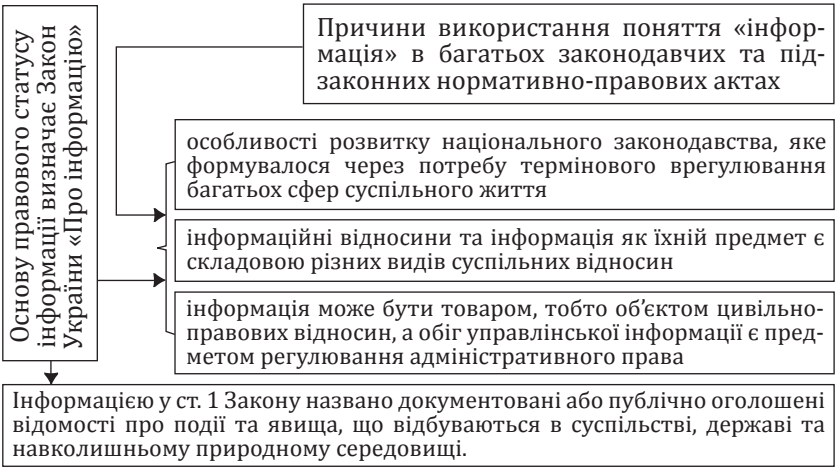
Ключові поняття: інформація як об'єкт загрози у системі забезпечення надійності персоналу, категорії інформації, види інформації, джерела інформації, інформаційна безпека, система інформаційної безпеки, класифікація інформації, методи захисту інформації, способи захисту інформації.

3.1. Суть і поняття інформації та інформаційної безпеки

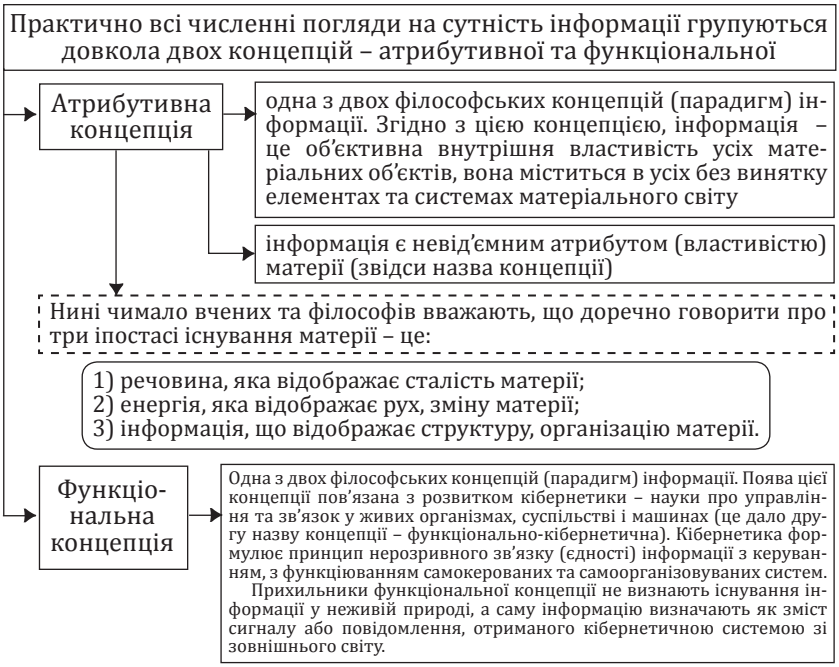
Загальне поняття інформації позиціонується у філософії, де під нею розуміють відображення реального світу. Як філософську категорію її вважають одним із атрибутів матерії, що відображає її структуру.



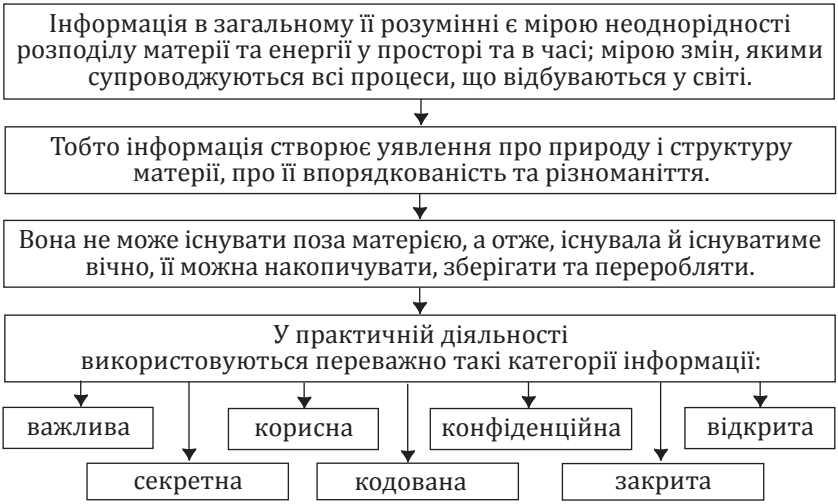
Найповнішу характеристику поняття «інформація» подано у визначеннях нормативно-правових актів.



Існують також інші, переважно несумісні між собою, визначення поняття «інформація».



Інформація, згідно з цією концепцією, міститься у формі властивих матеріальним об'єктам структур (така інформація називається структурною, потенційною, апріорною, внутрішньою, інформацією «в собі»). З цим підходом пов'язане визначення інформації як відображення різноманітності.



Для кращого розуміння суті інформації та її особливостей розглянемо загрози, які виникають під час збирання, опрацювання, використання інформації та ухвалення управлінських рішень.

Фахівці науково-технічних, виробничих, економічних та інших служб підприємства повинні визначати загрози безпеці та навчитися правильно й конкретно (у вартісній формі) оцінювати передбачувані і реальні втрати компанії внаслідок просочування інформації, яка віднесена до категорії комерційної таємниці.

Під загрозою безпеці розуміють потенційні дії або події, які можуть прямо чи опосередковано спричинити втрати – призвести до розладу системи, спотворення інформації чи несанкціонованого використання ресурсів мережі, включаючи інформацію, що зберігається, передається або опрацьовується, а також програмні й апаратні засоби. Загрози бувають двох видів:

- **випадкові** – Джерелом випадкових загроз можуть бути помилки в програмному забезпеченні, вихід із ладу апаратних засобів, неправильні дії користувачів або адміністрації локальної обчислювальної мережі тощо.
- **навмисні** – Навмисні загрози, на відміну від випадкових, пов'язані зі завданням шкоди користувачам (абонентам) локальної обчислювальної мережі і поділяються на пасивні й активні.

Компрометація інформації здійснюється внесенням несанкціонованих змін у бази даних, внаслідок чого її користувач змушений або відмовитись від неї, або докласти додаткових зусиль до виявлення змін і відновлення справжніх відомостей. У разі використання скомпрометованої інформації користувач може прийняти неправильні рішення з усіма подальшими наслідками.

Засобами реалізації загрози розкриття конфіденційної інформації може бути:

- несанкціонований доступ до баз даних (БД)
- прослуховування каналів локальної обчислювальної мережі

Щоразу отримання інформації, яка є власністю якоїсь особи (або групи осіб), завдає її власникам істотної шкоди.

Помилково санкціоноване використання ресурсів локальної обчислювальної мережі теж може призвести до знищення, розкриття або компрометації цих ресурсів. Така загроза є зазвичай наслідком помилок програмного забезпечення локальної обчислювальної мережі.

Несанкціоноване використання ресурсів локальної обчислювальної мережі, з одного боку, є засобом розкриття або компрометації інформації, а з другого – має самостійне значення, оскільки, навіть не торкаючись користувальної або системної інформації, може завдати певних збитків абонентам або адміністрації локальної обчислювальної мережі. Зміна розміру збитків коливається в широкому діапазоні: від скорочення надходжень фінансових ресурсів до повного виходу мережі з ладу.

Несанкціонований обмін інформацією між абонентами локальної обчислювальної мережі може призвести до отримання одним із них відомостей, доступ до яких йому заборонено, що за наслідками прирівнюється до розкриття інформації.

Відмова в обслуговуванні – дуже істотна й досить поширена загроза, джерелом якої є сама локальна комп'ютерна мережа.

Така відмова особливо небезпечна в ситуаціях, коли затримка з наданням ресурсів мережі абонентові може призвести до тяжких для нього наслідків.

Відсутність в абонента даних, необхідних для прийняття рішень, може бути причиною його нераціональних або неоптимальних дій.

Відмова від інформації полягає у невизнанні адресатом чи відправником цієї інформації, фактів її отримання або відправки.

Це, зокрема, може спричинити аргументовану відмову однієї зі сторін від раніше підтриманої угоди (фінансової, торгової, дипломатичної тощо) «технічним шляхом», коли формально від неї не відмовляються, що завдасть іншій стороні значних збитків.

Формування економічного середовища – створення економічно сприятливих умов для виробництва, запровадження й інвестування у сферу ІКТ з метою розвитку інформаційного суспільства.

Інформаційна безпека – стан захищеності інформаційного простору, який забезпечує формування й розвиток цього простору в інтересах особистості, суспільства та держави.

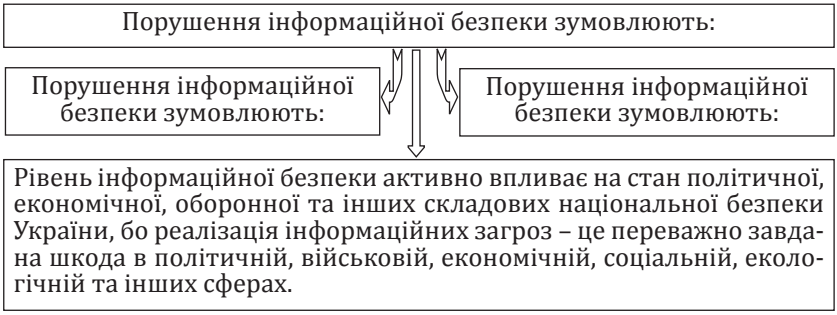
Метою забезпечення інформаційної безпеки в Україні є створення розгалуженого, захищеного інформаційного простору, захист національних інтересів України в умовах формування світових інформаційних мереж, захист економічного потенціалу держави від незаконного використання інформаційних ресурсів, реалізація прав громадян, установ та держави на отримання, поширення й використання інформації.

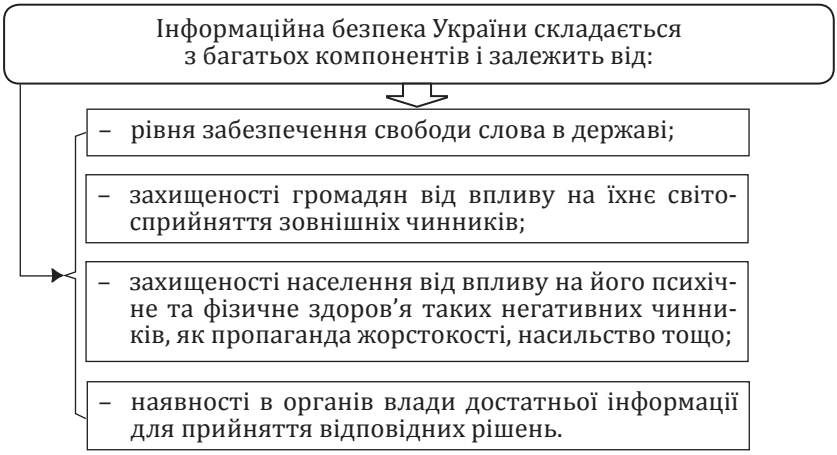
Загрози інформаційній безпеці – фактор або сукупність їх, що створюють небезпеку функціонуванню та розвитку інформаційного простору, інтересам особистості, суспільства, держави.

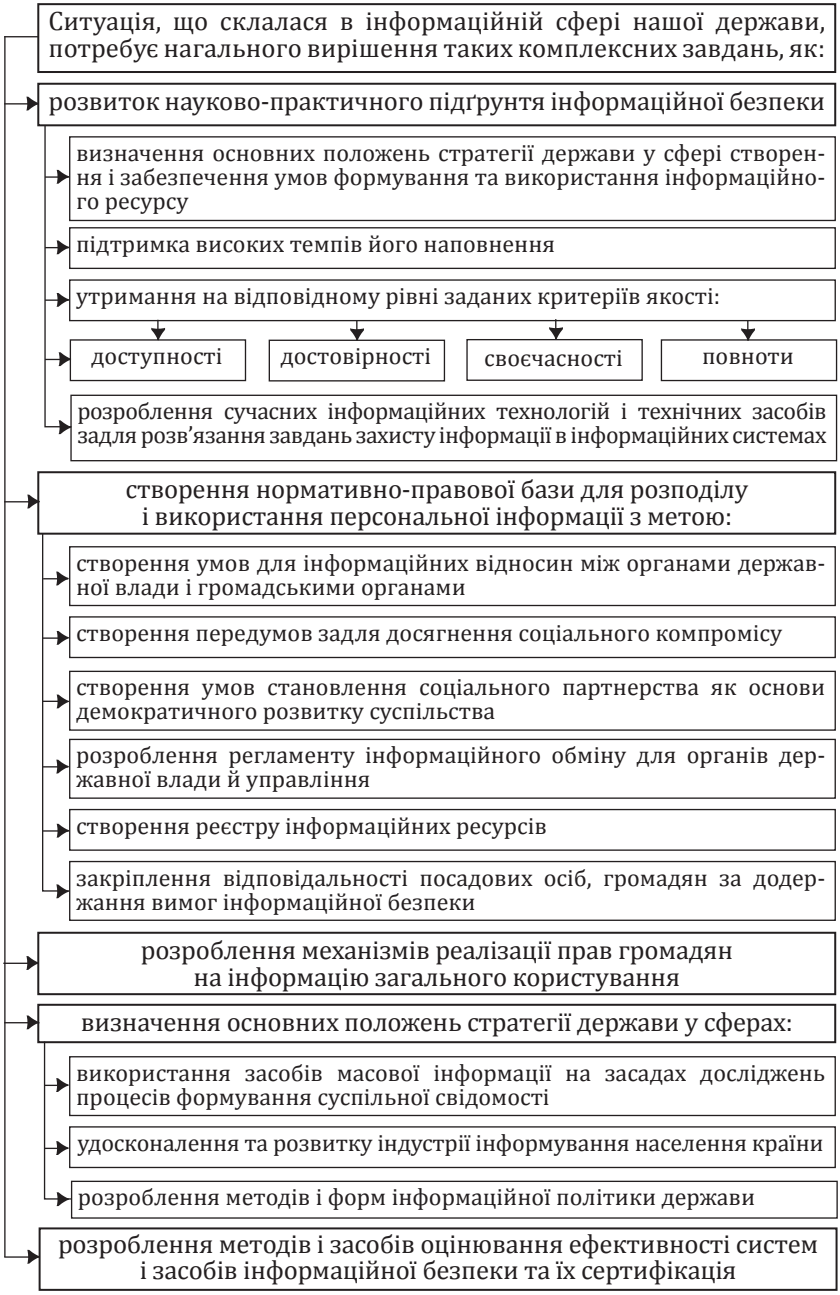
Захист інформації – сукупність засобів, методів, організаційних заходів зі запобігання можливим випадковим або навмисним впливам природного чи штучного характеру, наслідком яких можуть бути збитки чи шкода, завдані власникам інформації або її користувачам, інформаційному простору.

Система захисту державної таємниці – сукупність органів захисту державної таємниці, які функціонують у взаємодії та координації відповідно до наданої законодавством компетенції, використовуваних ними форм, методів і засобів захисту відомостей, що становлять державну таємницю, їхніх носіїв та заходів, що проводяться в їхніх інтересах.

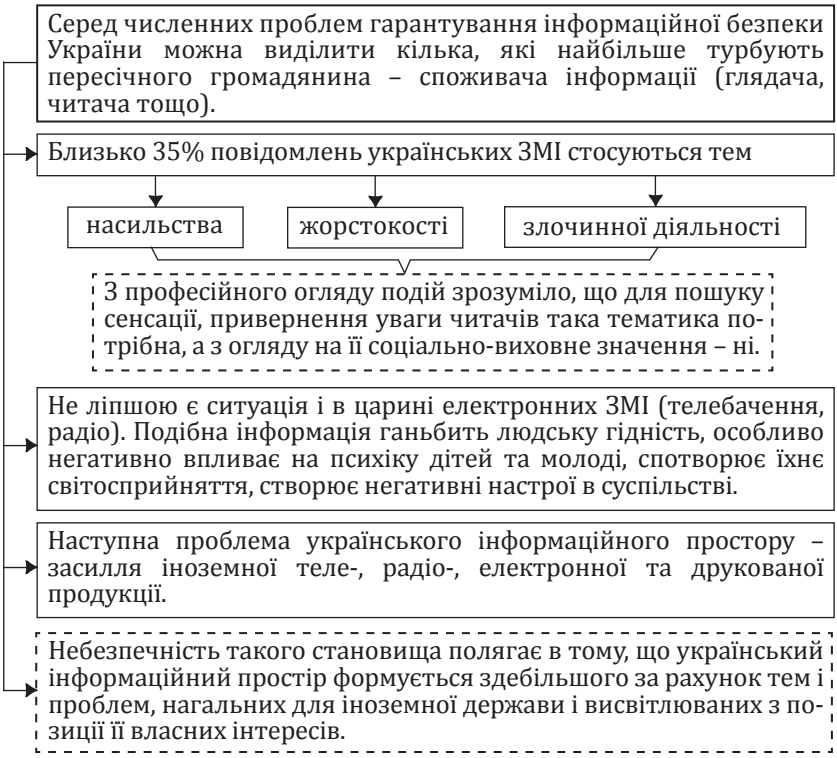
Захист інформації полягає в забезпеченні її доступності при збереженні цілісності та гарантованої конфіденційності.






Ситуація, що склалася в інформаційній сфері нашої держави, потребує нагального вирішення таких комплексних завдань, як:
розвиток науково-практичного підґрунтя інформаційної безпеки
визначення основних положень стратегії держави у сфері створення і забезпечення умов формування та використання інформаційного ресурсу
підтримка високих темпів його наповнення
утримання на відповідному рівні заданих критеріїв якості:
доступності
достовірності
своєчасності
повноти
розроблення сучасних інформаційних технологій і технічних засобів задля розв'язання завдань захисту інформації в інформаційних системах
створення нормативно-правової бази для розподілу і використання персональної інформації з метою:
створення умов для інформаційних відносин між органами державної влади і громадськими органами
створення передумов задля досягнення соціального компромісу
створення умов становлення соціального партнерства як основи демократичного розвитку суспільства
розроблення регламенту інформаційного обміну для органів державної влади й управління
створення реєстру інформаційних ресурсів
закріплення відповідальності посадових осіб, громадян за додержання вимог інформаційної безпеки
розроблення механізмів реалізації прав громадян на інформацію загального користування
визначення основних положень стратегії держави у сферах:
використання засобів масової інформації на засадах досліджень процесів формування суспільної свідомості
удосконалення та розвитку індустрії інформування населення країни
розроблення методів і форм інформаційної політики держави
розроблення методів і засобів оцінювання ефективності систем і засобів інформаційної безпеки та їх сертифікація

Отже, інформаційна безпека України залежить від розв'язання проблем формування суспільної свідомості, процесів виробництва та репродукції інформаційних ресурсів і доступу до них, створення цивілізованого ринку інформаційних продуктів та послуг, реалізації прав громадян на інформацію.



А оскільки українські громадяни мають невеликий вибір, надто серед теле- і радіопрограм, їм просто прищеплюються позиції, які далеко не завжди відповідають дійсності та національним інтересам України. Крім того, зарубіжна інформаційна продукція створює серйозну конкуренцію вітчизняним ЗМІ і заважає їх нормальному розвитку. Останні втрачають прибутки не тільки через зменшення кількості передплатників, покупців, а й через зменшення обсягів реклами, поширення якої їм замовляють.

3.2. Класифікація і характеристика різних видів інформації

Відповідно до ст. 28 Закону України «Про інформацію», інформація поділяється на *відкриту* та *з обмеженим доступом.* Питання належного правового регулювання обігу інформації з обмеженим доступом особливо цікавить службу конкурентної розвідки.

Визначаючи зміст поняття «інформація з обмеженим доступом», слід врахувати положення чинного законодавства України, які закріплюють правові підстави та процедури обмеження доступу до інформації певних категорій.

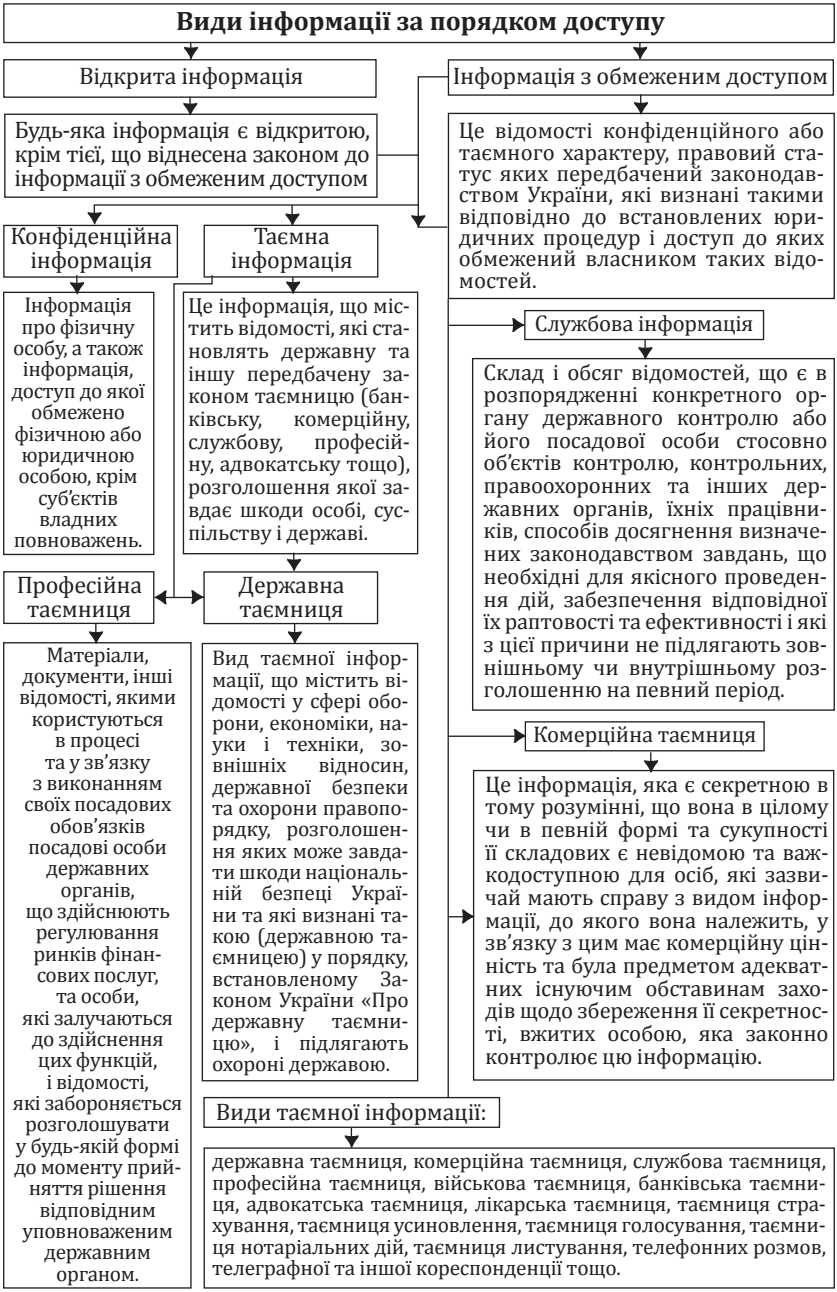
Адже всі громадяни України, юридичні особи і державні органи мають право на інформацію, що передбачає можливість вільного одержання, використання, поширення та зберігання відомостей, необхідних їм для реалізації ними своїх прав, свобод і законних інтересів, здійснення завдань і функцій.

При цьому кожному громадянину забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законами України. Гарантіями ж охорони права на інформацію є норми, закріплені у статті 47 Закону України «Про інформацію», згідно з якими відповідальність за порушення зако-нодавства про інформацію несуть особи, винні у необґрунтованому віднесенні окремих видів інформації до категорії відомостей з обмеженим доступом.

Громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційної, та встановлюють для неї систему (способи) захисту.

Слід зазначити, що положення Закону України «Про інформацію» були доповнені Законом № 676-IV від 03.04.2003 р. нормою такого змісту: «Інформація з обмеженим доступом може бути поширена без згоди її власника, якщо ця інформація є суспільно значимою, тобто якщо вона є предметом громадського інтересу і якщо право громадськості знати цю інформацію переважає право її власника на її захист». Питання практичного застосування зазначеної норми є доволі проблематичним. Якщо предмет громадського інтересу ще можна визначити з певною часткою імовірності, то перевага права громадськості знати інформацію з обмеженим доступом над правом її власника на захист такої інформації визначається не так легко. У будь-якому разі лише органи судової влади уповноважені приймати остаточне рішення стосовно співвідношення права громадськості знати інформацію з обмеженим доступом і права її власника на захист такої інформації.


Види інформації за змістом
(ст. 10 Закону України «Про інформацію»)
Інформація про фізичну особу
відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована
Інформація довідково-енциклопедичного характеру
систематизовані, документовані, публічно оголошені або іншим чином поширені відомості про суспільне, державне життя та навколишнє природне середовище
Інформація довідково-енциклопедичного характеру
відомості та/або дані про:
– стан складових довкілля та його компоненти, включаючи генетично модифіковані організми, та взаємодію між цими складовими;
– фактори, що впливають або можуть впливати на складові довкілля (речовини, енергія, шум і випромінювання, а також діяльність або заходи, включаючи адміністративні, угоди в галузі навколишнього природного середовища, політику, законодавство, плани і програми);
– стан здоров'я та безпеки людей, умови життя людей, стан об'єктів культури і споруд тією мірою, якою на них впливає або може вплинути стан складових довкілля;
– інші відомості та/або дані.
Інформація про товар (роботу, послугу)
відомості та/або дані, які розкривають кількісні, якісні та інші характеристики товару (роботи, послуги).
Науково-технічна інформація
будь-які відомості та/або дані про вітчизняні та зарубіжні досягнення науки, техніки і виробництва, одержані в ході науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.
Податкова інформація
сукупність відомостей і даних, що створені або отримані суб'єктами інформаційних відносин у процесі поточної діяльності і необхідні для реалізації покладених на контролюючі органи завдань і функцій у порядку, встановленому Податковим кодексом України.
Правова інформація
будь-які відомості про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо.
Статистична інформація
документована інформація, що дає кількісну характеристику масових явищ та процесів, які відбуваються в економічній, соціальній, культурній та інших сферах життя суспільства.
Соціологічна інформація
будь-які документовані відомості про ставлення до окремих осіб, подій, явищ, процесів, фактів тощо.


Види інформації за порядком доступу
Відкрита інформація
Будь-яка інформація є відкритою, крім тієї, що віднесена законом до інформації з обмеженим доступом
Інформація з обмеженим доступом
Це відомості конфіденційного або таємного характеру, правовий статус яких передбачений законодавством України, які визнані такими відповідно до встановлених юридичних процедур і доступ до яких обмежений власником таких відомостей.
Конфіденційна інформація
Інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень.
Таємна інформація
Це інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю (банківську, комерційну, службову, професійну, адвокатську тощо), розголошення якої завдає шкоди особі, суспільству і державі.
Службова інформація
Склад і обсяг відомостей, що є в розпорядженні конкретного органу державного контролю або його посадової особи стосовно об'єктів контролю, контрольних, правоохоронних та інших державних органів, їхніх працівників, способів досягнення визначених законодавством завдань, що необхідні для якісного проведення дій, забезпечення відповідної їх раптовості та ефективності і які з цієї причини не підлягають зовнішньому чи внутрішньому розголошенню на певний період.
Професійна таємниця
Матеріали, документи, інші відомості, якими користуються в процесі та у зв'язку з виконанням своїх посадових обов'язків посадові особи державних органів, що здійснюють регулювання ринків фінансових послуг, та особи, які залучаються до здійснення цих функцій, і відомості, які забороняється розголошувати у будь-якій формі до моменту прийняття рішення відповідним уповноваженим державним органом.
Державна таємниця
Вид таємної інформації, що містить відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані такою (державною таємницею) у порядку, встановленому Законом України «Про державну таємницю», і підлягають охороні державою.
Комерційна таємниця
Це інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та важкодоступною для осіб, які зазвичай мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію.
Види таємної інформації:
державна таємниця, комерційна таємниця, службова таємниця, професійна таємниця, військова таємниця, банківська таємниця, адвокатська таємниця, лікарська таємниця, таємниця страхування, таємниця усиновлення, таємниця голосування, таємниця нотаріальних дій, таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції тощо.

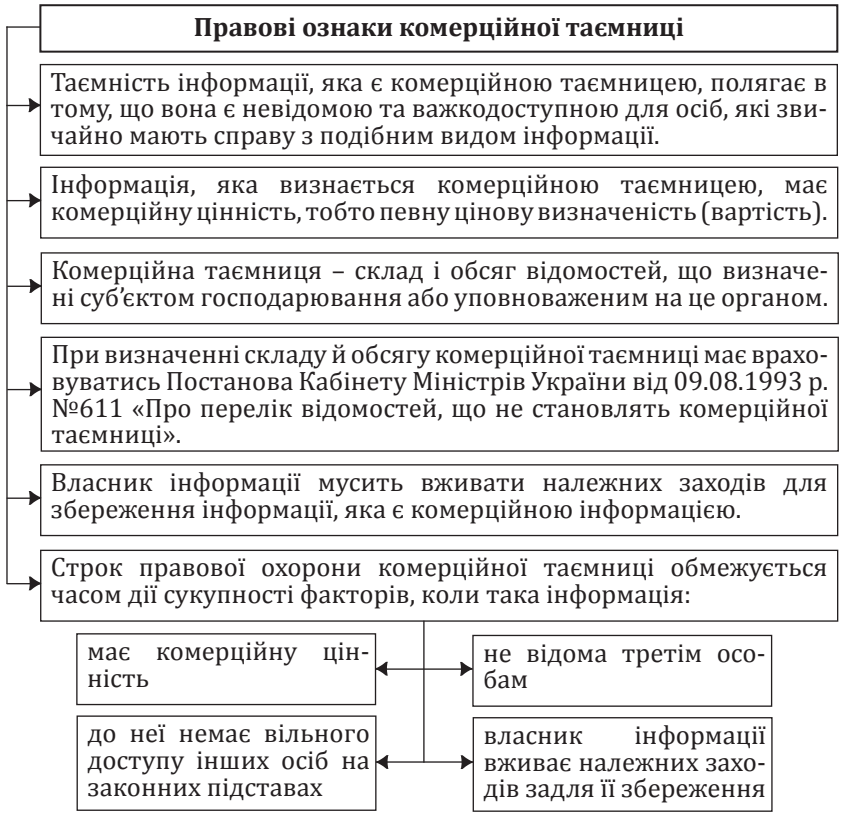
Господарський кодекс України (ГКУ) також частково наводить особливості комерційної таємниці, включаючи останню до об'єктів прав інтелектуальної власності. При цьому ГКУ визначає повноваження суб'єктів господарювання щодо комерційної таємниці, зокрема, «суб'єкт господарювання, що є власником технічної, організаційної або іншої комерційної інформації, має право на захист від незаконного використання цієї інформації третіми особами, за умов, що ця інформація має комерційну цінність у зв'язку з тим, що вона не відома третім особам і до неї немає вільного доступу інших осіб на законних підставах, а власник інформації вживає належних заходів для збереження її конфіденційності».

Відповідно до Постанови Кабінету Міністрів України від 09.08.1993 р. № 611, комерційну таємницю не становлять:

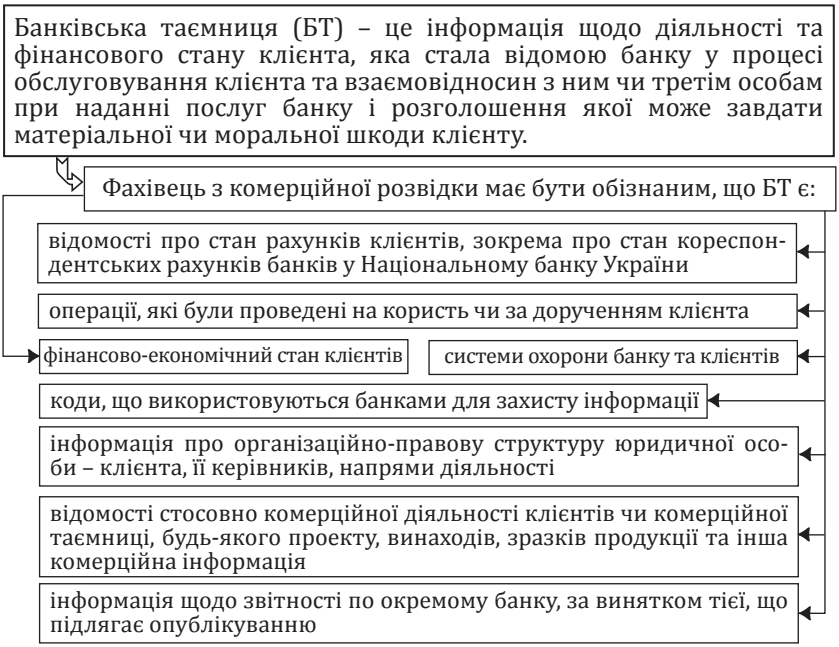
- установчі документи, документи, що дозволяють займатися підприємницькою чи господарською діяльністю та її окремими видами
- інформація за всіма встановленими формами державної звітності
- дані, необхідні для перевірки обчислення і сплати податків та інших обов'язкових платежів
- відомості про чисельність і склад працюючих, їхню заробітну плату загалом та за професіями й посадами, а також наявність вільних робочих місць
- документи про сплату податків і обо'язкових платежів
- інформація про забруднення навколишнього природного середовища, недотримання безпечних умов праці, реалізацію продукції, що завдає шкоди здоров'ю, а також інші порушення законодавства України та розміри завданих при цьому збитків
- документи про платоспроможність
- відомості про участь посадових осіб підприємства в кооперативах, малих підприємствах, спілках, об'єднаннях та інших організаціях, які займаються підприємницькою діяльністю
- відомості, що підлягають розголошенню, відповідно до чинного законодавства

Підприємства зобов'язані подавати перелічені у зазначеній Постанові відомості органам державної виконавчої влади, контролюючим і правоохоронним органам, іншим юридичним особам за їх вимогою відповідно до чинного законодавства. Особа, яка протиправно використовує комерційну інформацію, що належить суб'єкту господарювання, зобов'язана відшкодувати завдані йому такими діями збитки згідно зі законом.

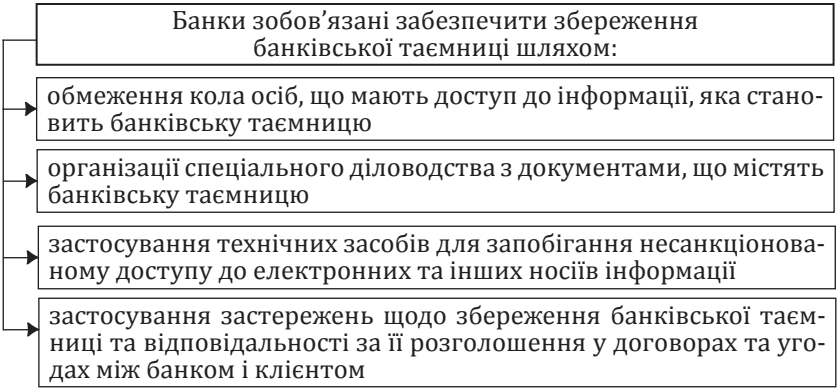
Особа, яка самостійно і добросовісно одержала інформацію, що є комерційною таємницею, має право використовувати цю інформацію на свій розсуд. Це положення є «наріжним каменем» конкурентної розвідки.



Правовий статус банківської таємниці визначається Законом України «Про банки і банківську діяльність», а також ЦКУ.



Інформація про банки чи клієнтів, яка збирається під час проведення банківського нагляду, теж становить банківську таємницю.



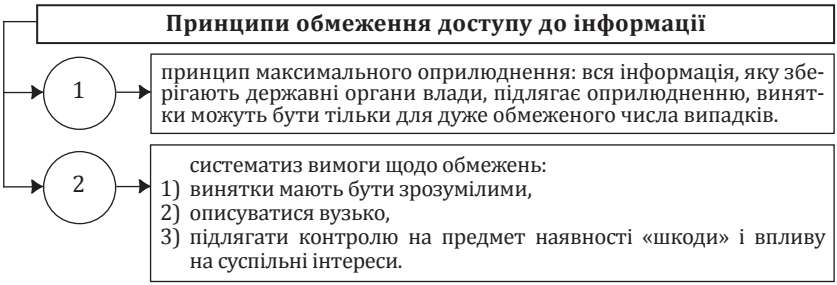
Особливості збереження банківської таємниці

- Службовці банку, вступаючи на посаду, підписують зобов'язання про збереження банківської таємниці.
- Керівники та службовці банків зобо'язані не розголошувати та не використовувати з вигодою для себе чи для третіх осіб конфіденційну інформацію, яка стала відома їм під час виконання своїх службових обов'язків.
- Приватні особи та організації, які при виконанні своїх функцій або наданні послуг банку безпосередньо чи опосередковано отримали конфіденційну інформацію, зобов'язані не розголошувати цю інформацію і не використовувати її на свою користь чи на користь третіх осіб.
- У разі заподіяння банку чи його клієнту збитків шляхом витоку інформації про банки та їхніх клієнтів з органів, які уповноважені здійснювати банківський нагляд, збитки відшкодовуються винними органами.
- Фахівці з КР також мають усвідомлювати, що особи, винні в порушенні порядку розкриття та використання банківської таємниці, несуть відповідальність згідно зі законами України.

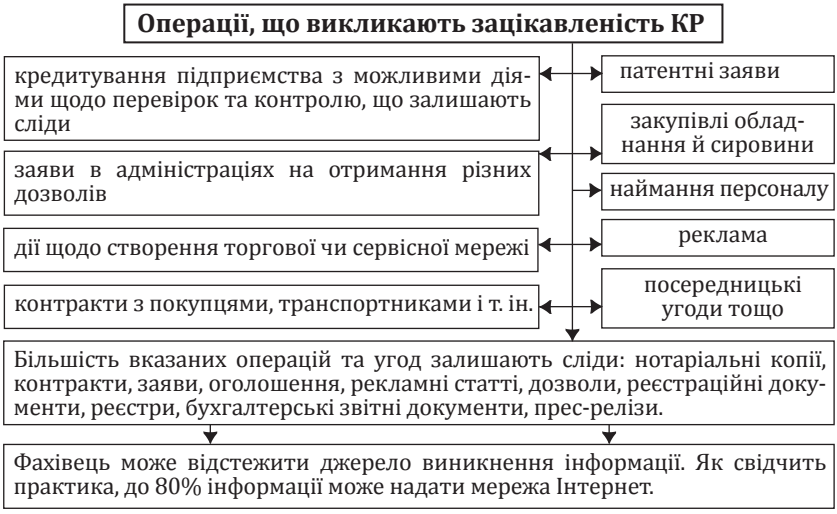
Предмет адвокатської таємниці

- питання, з яких громадянин або юридична особа зверталися до адвоката, сутність консультацій, порад, роз'яснень та інших відомостей, одержаних адвокатом при здійсненні професійної діяльності
- окремими передбаченими законодавством видами таємної інформації також є таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції, таємниця заповіту тощо.

Слід пам'ятати, що підстави та процедури обмеження доступу до інформації є предметом широких наукових дискусій. Приміром, необхідно чітко визначити законом інформацію, доступ до якої обмежується, і мету обмеження; перелік відомостей, які входять до кола обмежень, має бути вичерпно визначений і оприлюднений. Пропонуються два принципи обмеження доступу до інформації.



Позитивний аспект конкурентної розвідки (КР) полягає в тому, що від неї повністю захиститися неможливо. Будь-яке підприємство, яке працює, залишає чимало слідів. Треба тільки знати, де вони знаходяться, як їх побачити й оцінити, не порушуючи закону та етичних норм.



3.3. Методи і способи захисту інформації

Створення систем інформаційної безпеки (СІБ) в ІС і ІТ ґрунтується на принципах, описаних нижче.

Вирішення питань інформаційної безпеки організацій сьогодні стало надважливим. Адже нині інформація – це один із найбільш цінних та критичних активів бізнесу, а гарантії її безпеки – ключове завдання будь-якої компанії, котра прагне провадити успішну діяльність на ринку та підтримувати свою конкурентоспроможність.

1. Системний підхід до побудови системи захисту означає оптимальне поєднання взаємозв'язаних організаційних, програмних, апаратних, фізичних та інших властивостей, підтверджених практикою створення вітчизняних і зарубіжних систем захисту і вживаних на всіх етапах технологічного циклу оброблення інформації.

2. Принцип безперервного розвитку системи є одним з основоположних для комп'ютерних інформаційних систем та актуальним для СІБ. Способи уникнення загроз інформації в ІТ безперервно вдосконалюються, тому гарантування безпеки ІС не може бути одноразовим актом.

Безперервний процес полягає в:

- обґрунтуванні та реалізації найраціональніших методів, способів і шляхів удосконалення СІБ; безперервному контролі; виявленні її вузьких і слабких місць;
- установленні потенційних каналів просочування інформації; визначенні нових способів несанкціонованого доступу.

3. Розмежування і мінімізація повноважень з доступу до оброблюваної інформації та процедур оброблення – це надання як користувачам, так і працівникам ІС мінімуму певних повноважень, достатніх для виконання ними своїх службових обов'язків.

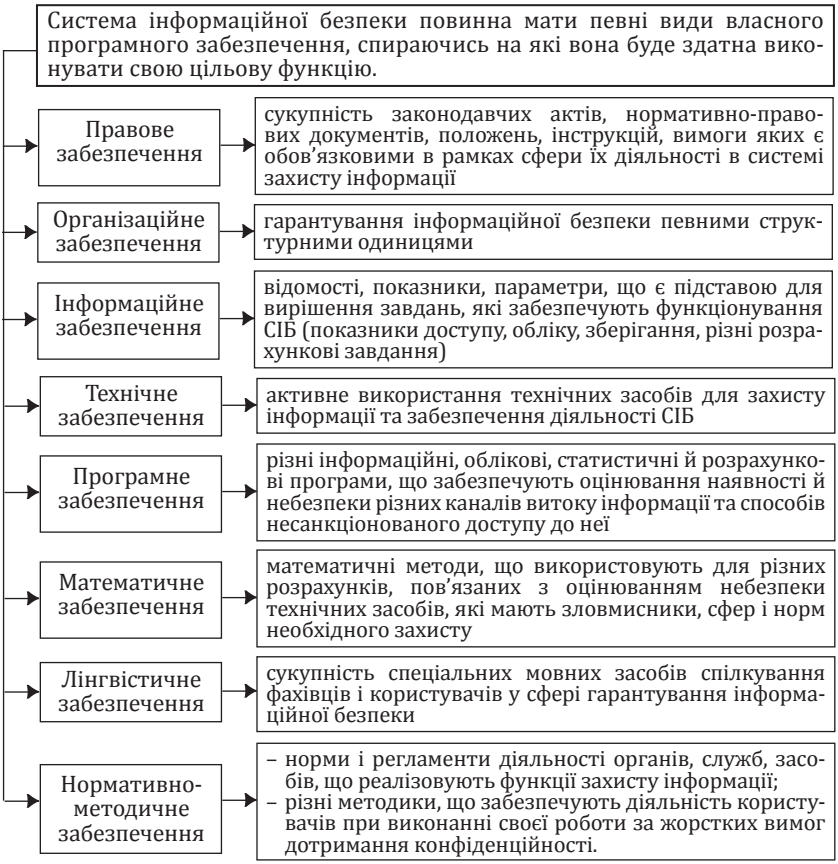
4. Повнота контролю і реєстрації спроб несанкціонованого доступу означає необхідність точно встановлювати ідентичність кожного користувача і протоколювання його дій задля проведення ймовірного розслідування, а також неможливість здійснювати будь-яку операцію з оброблення інформації в ІТ без її попередньої реєстрації.

5. Забезпечення надійності системи захисту полягає в неможливості зниження рівня надійності у разі виникнення в системі збоїв, відмов, навмисних дій зломлювача або ненавмисних помилок користувачів та обслуговуючого персоналу.

Забезпечення контролю за функціонуванням системи захисту – це створення засобів і методів контролю працездатності механізмів захисту.

Забезпечення економічної доцільності використання системи захисту виражається в перевищенні можливого збитку ІС та ІТ від реалізації загроз над вартістю розроблення й експлуатації СІБ.

Маючи системний і цілеспрямований характер, зовнішній негативний інформаційний вплив призводить у підсумку до появи загроз національній безпеці України в інформаційній сфері, які завдають державі відчутних збитків. Особливо це стосується виконання завдань оборони країни, оскільки ця діяльність безпосередньо спрямована на захист національних інтересів держави від зовнішніх загроз і пов'язана з підготовкою та веденням війни з можливим агресором.



Особливості видів та методів забезпечення

Нормативно-методичне забезпечення дотичне з правовим.

Провідну роль відіграють організаційні заходи захисту інформації. Тому виникає питання щодо організації служби безпеки.

Реалізація політики безпеки потребує налаштування засобів захисту, управління системою захисту та здійснення контролю функціонування ІС. Завдання управління і контролю зазвичай вирішуються адміністративною групою, склад і розмір якої залежать від конкретних умов. Часто така група працює у складі адміністратора безпеки, менеджера безпеки та операторів.

У найбільшій мережі світу Інтернеті атаки на комп'ютерні системи особливо актуальні, вони не знають державних кордонів, не враховують расових чи соціальних відмінностей. Відбувається постійна боротьба інтелекту, а також організованості системних адміністраторів і винахідливості хакерів.

Правові методи передбачають розроблення комплексу нормативно-правових актів і положень, що регламентують інформаційні відносини в суспільстві, керівних і нормативно-методичних документів щодо гарантування інформаційної безпеки.

Програмно-технічні методи – це сукупність засобів:

- запобігання витоку інформації;
- усунення можливості несанкціонованого доступу до інформації;
- запобігання впливам, які призводять до знищення, руйнування, переключення інформації, або збоям чи відмовам у функціонуванні засобів інформатизації;
- виявлення вмонтованих пристроїв;
- запобігання перехопленню інформації технічними засобами;
- використання криптографічних засобів захисту інформації під час передачі каналами зв'язку.

Організаційно-економічні методи передбачають:

- формування і забезпечення функціонування систем захисту секретної і конфіденційної інформації;
- сертифікацію цих систем відповідно до вимог інформаційної безпеки;
- ліцензування діяльності у сфері інформаційної безпеки;
- стандартизацію способів і засобів захисту інформації;
- контроль за діями персоналу в захищених інформаційних системах.

Важливими у запобіганні інформаційним загрозам є мотивація, економічне стимулювання і психологічна підтримка діяльності персоналу, який забезпечує інформаційну безпеку.

Методи і засоби забезпечення безпеки інформації:

метод фізичного втручання на шляху зловмисника до захищеної інформації (до документів, апаратури, носіїв інформації тощо)

Управління доступом – методи захисту інформації регулюванням усіх ресурсів ІС та ІТ. Ці методи протистоять можливим способам несанкціонованого доступу до інформації. Управління доступом виконує такі функції захисту:

- ідентифікацію користувачів, персоналу й ресурсів системи;
- впізнання об'єкта або суб'єкта за пред'явленим ним ідентифікатором;
- перевірку повноважень;
- дозвіл і створення умов роботи в межах установленого регламенту;
- реєстрацію звернень до конфіденційних ресурсів;
- реагування у разі спроб несанкціонованих дій.

Механізми шифрування – криптографічне закриття інформації. Цей метод захисту дедалі ширше застосовується під час опрацювання та при зберіганні інформації на магнітних носіях. У разі передавання інформації каналами зв'язку великої протяжності цей метод є єдино надійним.

Протидія атакам шкідливих програм припускає комплекс різних організаційних заходів і використання антивірусних програм.

Мета протидії атакам:

- зменшення вірогідності інфікування АІС;
- виявлення фактів зараження системи;
- зменшення наслідків інформаційних інфекцій;
- локалізація або знищення вірусів;
- відновлення пошкодженої інформації в ІС.

Регламентація – створення таких умов автоматизованого опрацювання, зберігання і передавання інформації, що піддягає захисту, за яких норми і стандарти захисту найбільш ефективні.

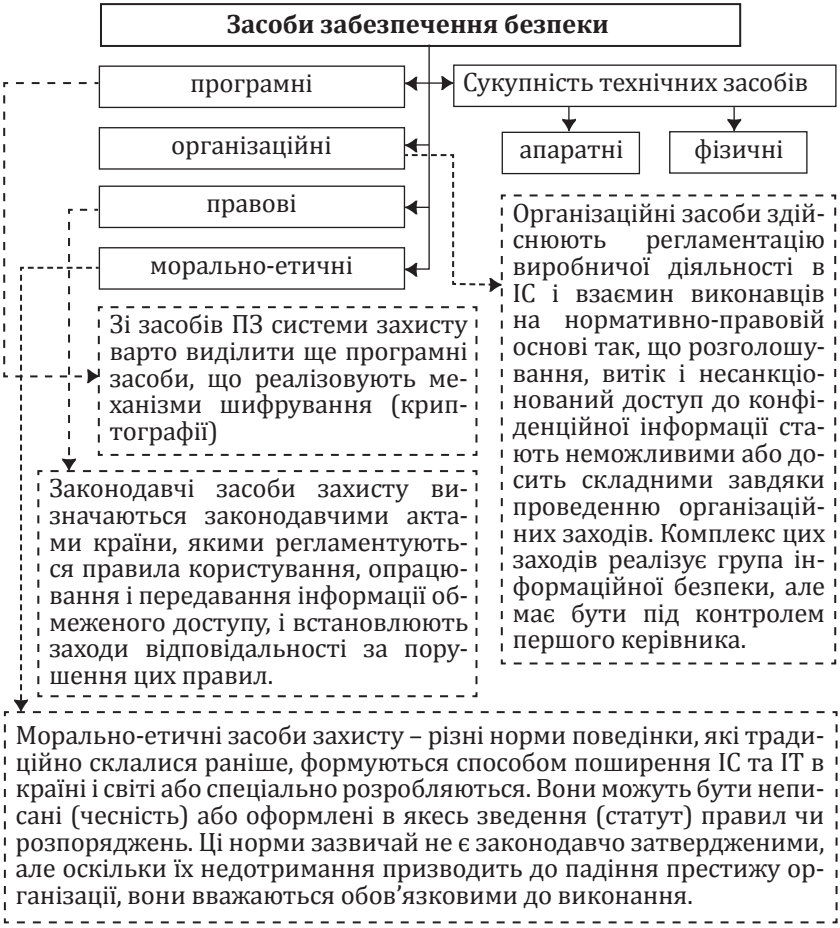
Примус – метод захисту, за якого користувачі і персонал ІС змушені дотримуватися правил опрацювання, передавання і використання конфіденційної інформації через загрозу матеріальної, адміністративної або кримінальної відповідальності.

Спонука – метод захисту, що спонукає користувачів і персонал ІС не порушувати встановлених порядків завдяки дотриманню моральних і етичних норм, що склалися.

Апаратні засоби – пристрої, які вбудовують безпосередньо в обчислювальну техніку, або пристрої, котрі з'єднують із нею за стандартним інтерфейсом.

Фізичні засоби – це різні інженерні пристрої і споруди, що перешкоджають фізичному проникненню зловмисників на об'єкти захисту і здійснюють захист персоналу, матеріальних засобів і фінансів, інформації від протиправних дій.

Програмні засоби – спеціальні програми і програмні комплекси, призначені для захисту інформації в ІС.



За допомогою спеціального лазера можна прослуховувати офіс через зачинене вікно з відстані до кілометра.

Розвиток нових інформаційних технологій і загальна комп'ютеризація зробили інформаційну безпеку обов'язковою та однією з характеристик ІС.

Існує доволі поширений клас систем опрацювання інформації, при розробленні яких чинник безпеки відіграє першочергову роль, зокрема банківські інформаційні системи.

! *Безпека ІС* – це захищеність системи від випадкового або навмисного втручання в нормальний процес її функціонування, від спроб розкрадання (несанкціонованого отримання) інформації, модифікації або фізичного руйнування її компонентів. Тобто це здатність протидіяти різним протизаконним діям на ІС.

! *Загроза безпеці інформації* – події або дії, які можуть призвести до спотворення, несанкціонованого використання чи руйнування інформаційних ресурсів керованої системи, а також програмних і апаратних засобів.

Зняти інформацію з комп'ютера можна за допомогою:

«хакерського» мистецтва | «хакерського» мистецтва

спеціального радіоприймача,
який приймає паразитичні випромінювання комп'ютера
з подальшим детектуванням корисної інформації

Існує безліч методів боротьби з несанкціонованим зняттям інформації. Але найважче протистояти новим, нестандартним методам зняття інформації. Скажімо. складно звичними методами знайти напівактивний мікрофон, котрий працює через резонатор з вібратором, без джерела живлення, що налаштований на частоту зовнішнього джерела електромагнітного випромінювання.

Питання для обговорення

1. У чому полягає суть поняття «інформація»?
2. Що розуміють під поняттям «інформаційна безпека»?
3. Чим зумовлено поширене використання поняття «інформація» різними нормативними документами?
4. З чим пов'язане філософське визначення інформації?
5. Як Ви розумієте поняття «інформаційна система»?
6. У чому криється зміст захисту інформації?
7. Які Вам відомі категорії інформації?
8. Які Ви знаєте види інформації та основні класифікаційні ознаки?
9. Які є основні ознаки класифікації загроз безпеки інформації?
10. Які є основні етапи захисту інформації?
11. У чому полягають особливості структури системи захисту інформації?

12. Як функціонує система захисту інформації?
13. Які є напрями інформаційної безпеки?
14. З яких компонентів складається інформаційна безпека?
15. Які комплексні проблеми в інформаційній сфері України потребують невідкладного вирішення?
16. Чому інформація є важлива для діяльності компанії?
17. Які Ви знаєте види інформації про ринкову кон'юнктуру?
18. Які види інформації та їхні джерела Вам відомі?
19. Які бувають методи і способи захисту інформації?
20. Які функції виконує система інформаційної безпеки?
21. Що таке політика безпеки і в чому суть її реалізації?
22. Які є методи технічного захисту інформації?
23. Хто виступає суб'єктами системи технічного захисту інформації?
24. У чому полягає завдання підрозділу захисту інформації?

Домашнє завдання

Розробити посадові інструкції працівників служби (підрозділу) захисту інформації підприємства, установи, організації.

Форма контролю: усне опитування, перевірка рефератів, розв'язання тестових завдань, підготовка презентацій.

Рекомендована література: 1–6, 9–11, 17–19, 21, 34–42, 48–64, 72–76.

Тема 4
ОСОБЛИВОСТІ ПРИЙОМУ ПЕРСОНАЛУ НА РОБОТУ ТА ЙОГО ЗВІЛЬНЕННЯ

4.1. Попередня перевірка при прийомі на роботу.

4.2. Особливості оцінки кандидата за зовнішнім виглядом і поведінковими ознаками («face-control»).

4.3. Особливості оцінки кандидата за документами.

4.4. Роль служби економічної безпеки при прийнятті працівників на роботу та їх звільненні.

Ключові поняття: кадри підприємства, потенційний працівник, трудовий договір, Кодекс законів про працю України, нерозголошення комерційної таємниці, «face-control», прийом на роботу, звільнення з роботи, служба економічної безпеки (СЕБ).

4.1. Попередня перевірка при прийомі на роботу

Менеджер фірми розмовляє з кандидатом:

М. *Найбільше у працівниках ми цінуємо охайність. Скажіть, Ви витерли ноги об килимки на вході?*

К. *Звісно, витер.*

М. *Більше, ніж охайність, ми цінуємо чесність, а в нас немає на вході килимка…*

Скажімо, кандидат уже стоїть на порозі з твердим бажанням влаштуватися на роботу. Тож природно, що починати завжди треба з попередньої бесіди.

До бесіди з потенційним працівником, або, як це прийнято називати, інтерв'ю, необхідно ретельно підготуватися. Адже саме з інтерв'ю можна дізнатися найбільше.

Доречно залучити на допомогу психолога. Професійний психолог, просто поговоривши з людиною, зможе з високою вірогідністю зробити висновок про її професійні та особисті якості, про те, наскільки він чесний, чи зможе він нормально вписатися в колектив фірми.

Сьогодні вже існують спеціальні послуги з психологічного тестування кандидатів, які допомагають отримати об'єктивні результати. Але якщо такі послуги не доступні, доведеться самим ставати психологом.

По-перше, в жодному разі не варто створювати атмосферу допиту. Так тільки нашкодите собі. Чесна і порядна людина відчує негативне до себе ставлення і може відмовитися від роботи. А зловмисник, навпаки, зачаїться і насторожиться, уміло приховуючи свої наміри.

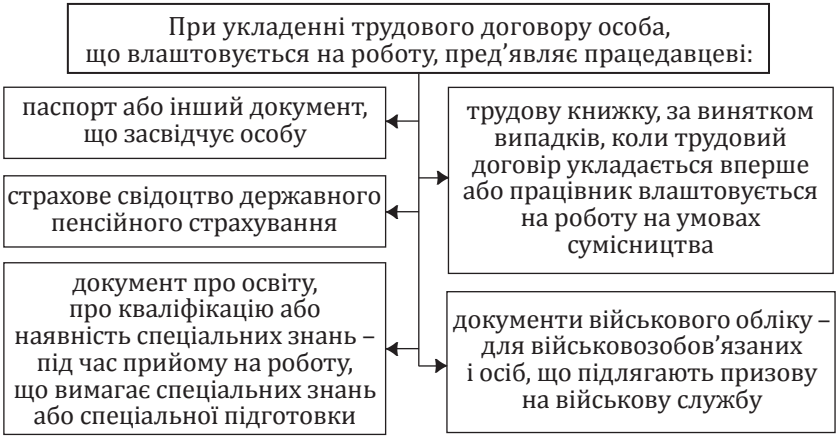
По-друге, не поводьтеся зарозуміло, вважаючи, що якщо людина прийшла до вас влаштовуватися, то вона вже вам зобов'язана і терпітиме ваші витівки.

По-третє, ніколи заздалегідь нічого не обіцяйте, говоріть лише про реальні речі.

Найліпше створити дружню атмосферу взаєморозуміння. У такій атмосфері кандидат почуватиметься розкуто і зможе розмовляти відвертіше. Варто уважно стежити, як людина поводиться, що і як говорить, наскільки вона скута чи, навпаки, розкріпачена.

Деякі працедавці влаштовують кандидатам на роботу докладну екскурсію по підприємству, розповідаючи йому про всі особливості майбутньої роботи. Наступним кроком є перевірка достовірності документів і минулого кандидата.

Насамперед слід встановити особу працівника.



В окремих випадках з урахуванням специфіки роботи чинним Кодексом законів про працю України, іншими законами, указами Президента України і постановами Кабінету Міністрів може передбачатися необхідність пред'явлення при укладенні трудового договору додаткових документів.

Забороняється вимагати від особи, що влаштовується на роботу, документи, крім передбачених Кодексом, іншими законами, указами Президента і постановами Уряду.

При укладенні трудового договору вперше трудова книжка і страхове свідоцтво державного пенсійного страхування оформляються працедавцем.

Потім потрібно з'ясувати робоче минуле кандидата. Все робоче минуле працівника можна дізнатися з трудової книжки, де вказані попередні місця роботи, заохочення, причини звільнення і таке інше. Проте тут треба бути обережним, бланки трудових книжок зараз можна з легкістю купити на будь-якому ринку і заповнити, як спаде на думку. Крім того, подекуди працівник тільки формально був на підприємстві, насправді ж не виконував ніякої роботи. А завдяки «зв'язкам» або дружнім взаєминам отримував необхідні записи в трудовій книжці.

Також не завадить самостійно з'ясувати думку про кандидата у його попередніх працедавців і людей, з якими він працював або вчився.

Тому незайве попросити у кандидата заповнити картку обліку кадрів і надати автобіографію, характеристику з останнього місця роботи або рекомендації. Так само необхідно упевнитися в професійній придатності працівника – попросити подати документ, що засвідчує рівень освіти (диплом про вищу освіту, диплом про закінчення коледжу, СПТУ, ПТУ, атестат і т. ін.).

Сформуйте анкету працівника так, щоб дізнатися про нього щонайбільше відомостей, зокрема, про його близьких родичів, особисті інтереси, спортивні й наукові досягнення тощо.

Не зайвим буде з'ясувати, чи не мав кандидат раніше судимостей, чи перебував на обліку в психо- або неврологічному диспансері. Впевнені, що немає сенсу пояснювати, як можна отримати таку інформацію. Якщо ж такої змоги нема, можна попросити кандидата надати належні довідки.

Припустимо, Ви перевірили всі відомості про кандидата і тепер мусите прийняти одне з таких рішень: узяти його на роботу або відмовити. Розглянемо обидва ці варіанти. Отже, людина Вам з якихось причин не підходить і Вам потрібно відмовити в прийомі на роботу. Як це зробити без шкоди для людини, якій Ви відмовляєте, але найголовніше – без шкоди для Вашого підприємства? Доцільно розрахувати, яку шкоду може заподіяти відмова прийняти кого-небудь на роботу.

Якщо ви відмовляєте людині в різкій формі в прийомі на роботу, кажете, що вона – кандидат недостатньо розумний, що у нього диплом не того формату, вам не підходить колір його волосся або щось схоже. Будь-яка нормальна людина після такої відмови затаїть на Вас образу, прийде додому, розповість про все своїй дружині, друзям, знайомим, а ті, своєю чергою, своїм друзям і знайомим. І поширеться негативна інформація, як кола по воді від кинутого каменя. Адже не слід забувати, що все це Ваші потенційні клієнти. Про Ваше підприємство можуть піти погані розмови, які здатні негативно позначитися на Вашій діловій репутації. Як результат – зниження кількості клієнтів, обсягів замовлень, тобто прямий матеріальний збиток у вигляді недоотриманого прибутку. А це, можливо, тисячі і тисячі гривень. Отож, як бачите, такі «дрібниці» мають величезне значення.

Крім того, не забувайте, що у працівника при прийомі на роботу існують певні гарантії, передбачені трудовим законодавством.

Так, відповідно до КЗпП України, забороняється необґрунтована відмова в укладенні трудового договору.

Крім того, як би там не було, одне пряме чи непряме обмеження, або встановлення прямих чи непрямих переваг при укладенні трудового договору залежно від статі, раси, кольору шкіри, національності, мови, походження, майнового, соціального і посадового положення, місця проживання, а також інші обставини, не пов'язані з діловими якостями працівників, не допускаються, за винятком випадків, передбачених законом.

І ще одна важлива гарантія полягає в тому, що на вимогу особи, якій відмовлено в укладенні трудового договору, працедавець зобов'язаний повідомити причину відмови у письмовій формі. І ця відмова в укладенні трудового договору може бути оскарженою в судовому порядку. А це додаткові витрати на адвоката, додаткова витрата часу і нервів, до того ж погана реклама для підприємства.

Тому відмову в прийомі на роботу необхідно робити в м'якій і делікатній формі. При цьому краще виключити особистий контакт з кандидатом. Найліпше послати йому відмову у письмовій формі поштою, ввічливо подякувавши за співпрацю і вибачившись за час, що відняли. Якщо причиною відмови є негативна інформація про кандидата, яку отримали в ході попередньої перевірки, не слід повідомляти його про це. Чимало бізнесменів, бажаючи показати свою обізнаність, розповідають про кандидата все, що їм вдалося дізнатися, таким чином насторожуючи його і примушуючи краще приховувати інформацію про себе. Тому при вказівці причин відмови доречніше залишити кандидата в здогадках про дійсні мотиви, створивши враження, що він не влаштував працедавця через інші причини.

Проте скажімо, працівник за діловими (трудовими) і людськими якостями підходить, і Ви хочете прийняти його на роботу. Тож потрібно оформити прийом на роботу так, щоб убезпечити себе від можливого розголошення Вашої конфіденційної комерційної інформації працівником в період його роботи і після його можливого звільнення.

Можна запропонувати такі способи:

1. Оформити прийом на роботу наказом, виданим на підставі поданої заяви працівника про прийом на роботу.

По-перше, дача будь-якого зобов'язання зазвичай супроводжується сильним морально-психологічним впливом на людину. Більшість людей прагнуть дотримуватись навіть формальних зобов'язань.

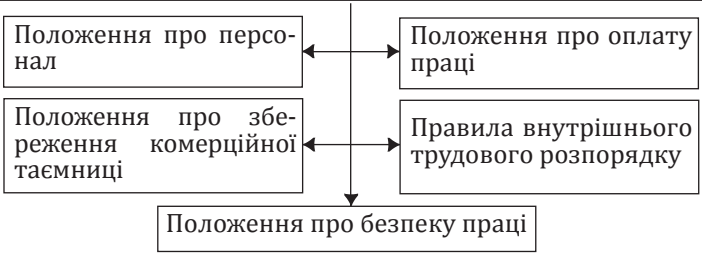
По-друге, у разі якщо працівник порушить ці зобов'язання, то, відповідно до закону, він нестиме і дисциплінарну відповідальність і цивільну, зокрема з відшкодуванням заподіяного збитку.

По-третє, можна нагадати, що відповідальність за розголошування комерційної таємниці настає тільки за умови, що відомості зберігалися господарюючим суб'єктом в таємниці, що вони були в установленому порядку впевнені в особі, яка розголосила їх без згоди на розголошення.

2. Оформити прийом на роботу наказом, виданим на підставі укладеного з працівником індивідуального трудового договору.

В цьому випадку Ви вносите до трудового договору окремий пункт або положення про те, що працівник ознайомлений з положеннями, що діють на підприємстві, і зобов'язується їх дотримуватись, а в разі їх порушення нестиме відповідальність.

Перед укладенням трудового договору необхідно провести інструктаж і надати працівникові для ознайомлення всі положення, що стосуються його, які діють на Вашому підприємстві.



Після прийому на роботу працівник повинен протягом певного часу (від 1 до 6 місяців) знаходитися на негласному контролі. Для чого це потрібно? У цей період часу працівник влаштовується в колективі, між ним і рештою працівників починають формуватися міжособистісні зв'язки.

Тому необхідно поспостерігати, як працівник влаштувався на новому місці, як він поводиться, як справляється зі своїми трудовими обов'язками, хто приходить до працівника зі сторонніх осіб (родичі, знайомі).

Незайве після спливу 1–3 місяців викликати працівника на бесіду, дізнатися, що він думає про своє місце роботи, чи все його влаштовує. Здійснення таких нехитрих заходів допомагає вчасно виявити на підприємстві неблагонадійного працівника.

Проте слід пам'ятати, що більшість нових працівників знають або здогадуються про те, що попервах вони перебувають на контролі. Тому в цей період вони прагнутимуть показати себе зі щонайліпшого боку.

4.2. Особливості оцінки кандидата за зовнішнім виглядом і поведінковими ознаками («face-control»)

Часто цей контроль проводиться в досить короткий період – від моменту, коли кандидат переступив поріг кабінету кадрової служби (служби персоналу), до моменту отримання ним анкети для заповнення.

Дійсно, досвідчені співробітники служби з першого погляду на відвідувача отримують які-небудь сигнали на підсвідомому рівні або прямо уловлюють певні зовнішні ознаки, інтерпретація яких не на користь претендента може поставити

під сумнів доцільність подальшої роботи з ним. Звісно, часто це відбувається інтуїтивно. Проте видається правильним, щоб це дійство було визнано однією з відбіркових процедур, з постановкою відповідних цілей і грамотним їх досягненням.

Цілі формуються доволі просто:

1. Експрес-оцінка зовнішньої підготовленості кандидата до спілкування з потенційним працедавцем або його співробітниками
2. Оцінка готовності до спілкування
3. Виявлення зовнішніх і мовних ознак, характерних для різного виду залежностей і відхилень (що зловживають алкоголем, наркомани, психічно нестійкі і т. ін.)

Цей перелік є неповним і абстрактним, оскільки тут неможливо описати всю інформацію, яку можна отримати з аналізу зовнішніх ознак претендентів. Завданням менеджера з персоналу є чітка постановка цілей, властивих «фейс-контролю», і їх подальше відпрацювання підлеглими.

Прийоми встановлення нещирості кандидата

- Перехресне опитування – претендента одночасно опитують два кадровики. Вони формулюють практично аналогічні запитання. Якщо кандидат на посаду обманює, то раніше чи пізніше він втратить контроль над собою і відповідатиме по-різному, врешті-решт спіймається.
- Питання на уточнення – в цьому разі претенденту ставлять багато запитань щодо уточнення тих чи інших подробиць. Співбесіда може тривати кілька годин. Як правило, вона застосовується щодо висококваліфікованих фахівців. Зазвичай триває співбесіда 20–30 хвилин.
- Психологічний тиск – його застосовують на тих, хто ловиться на брехні. Кадровик робить довгі паузи, заглядає у вічі, уважно все оцінює, вивчає ваші документи, ставить питання особистого характеру.
- Перевірка отриманої від претендента інформації – кадровики перевіряють відомості резюме, телефонують колишнім роботодавцям.
- Перевірка на стресостійкість – полягає у тому, що кадровики підвищують на вас голос, ставлять питання особистого характеру, заглядають в очі. Цей прийом застосовують до претендентів на посади, пов'язані зі спілкуванням – секретарів, менеджерів з продажу, продавців-консультантів тощо. Порада претенденту – не слід панікувати, не відповідайте на грубість грубістю.

Будь-яка підозра, що виникла стосовно кандидата, має бути з'ясованою. При цьому необхідно звернути особливу увагу на додаткове навчання співробітників служби персоналу, які першими зустрічають і працюють з кандидатами. І йдеться тут не про вивчення психології питання, а лише про правильне трактування ознак і їх сукупностей. Абсолютно очевидно, що ніяка поодинока ознака не може бути покладена в основу висновків про людину – тільки їх комплекс.

Аналізуючи нормативну базу стосовно закладів громадського харчування та ресторанів, слід зазначити, що поняття «face-control» є неконституційним та незаконним. Поняття «dress-kod» у більшості випадків не має юридичного підґрунтя.

На перше місце виходять такі якості особистості, як загальна ерудованість, високий коефіцієнт емоційного інтелекту, усвідомлене ставлення до свого життя, прагнення до особистісного зростання, розвитку, вміння ставити собі високі цілі і досягати їх. Однак неабиякого значення керівники компаній надають сьогодні зовнішній відповідності кандидата своїм уявленням про сучасну успішну людину.

Здоровий спосіб життя як принцип: відсутність шкідливих звичок, правильне харчування, рухливий спосіб життя і, як наслідок, чудова фізична форма і свіжий вигляд.

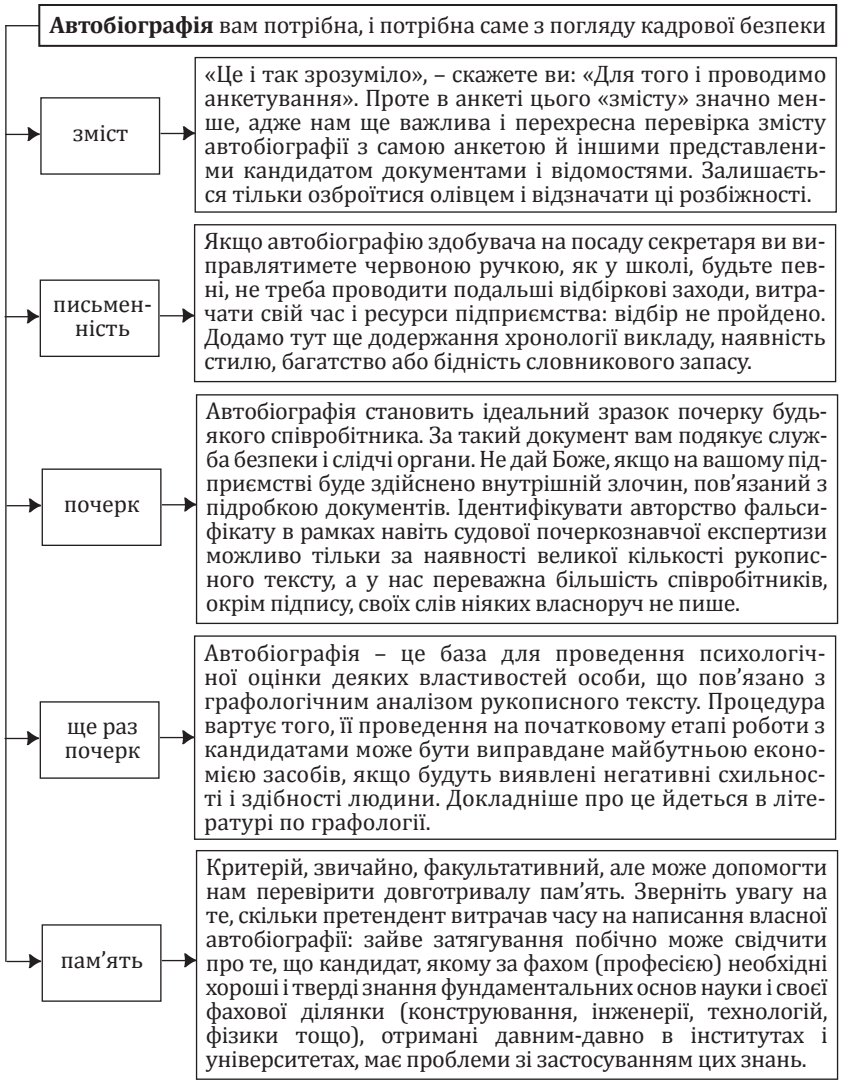
Якості особистості передбачають:

- відчуття відповідальності за своє життя (відсутність таких установок, як «вони там на верху ...», «ці керівники ...», «у всьому винна фінансова криза ...» і т. д.
- почуття емоційної залученості і смаку до життя (відсутність таких установок, як «якби я зміг повторити своє життя ...», «день минув – і добре ...», «а раптом завтра остеохондроз мене схопить...»)
- демонстрація відкритого, доброзичливого ставлення до оточуючих людей, де б ви не знаходилися (неправду іноді це буває непросто)
- прагнення до особистісного розвитку, постійна робота над собою (зазвичай у таких людей є цікаві захоплення, вони читають цікаві книги, цікавляться мистецтвом)
- стриманість у проявах емоцій, особливо негативних
- повагу до моральних цінностей, до інших культур і народів, повагу до родини, до старшого покоління, прийняття молоді та багато іншого
- зовнішню доглянутість (акуратний одяг, підібраний зі смаком, доглянуті волосся, шкіра, нігті, стрункa фігура, відсутність стоптаного взуття, зношеної сумки і т. ін.).

4.3. Особливості оцінки кандидата за документами

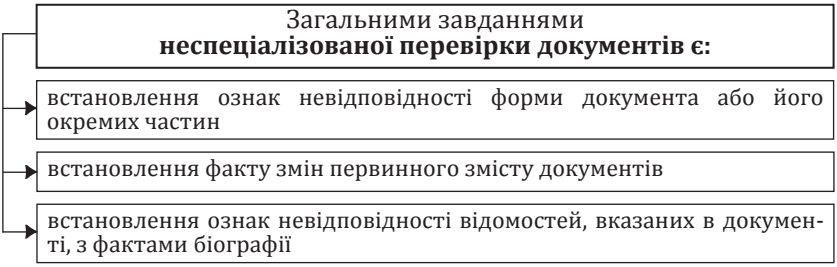
Автобіографія. А навіщо?

Ви не просите кандидатів заповнювати автобіографію? Марно: не позбавляйте себе цікавої подорожі в світ каліграфії і відчуття гумору, щирості спроб пригадати день народження чоловіка і додаткової інформації, незліченної кількості помилок і вишуканості стилю, ламаної послідовності опису власного життя і згризених ручок.



З метою досягнення цілей кадрової безпеки потрібно для написання автобіографії давати чистий лінійований бланк з переліком через кому в його шапці основних моментів біографії, виділяти для цього місце або приміщення і необхідний час. Заповнення автобіографії краще проводити на наступних після анкетування етапах роботи з кандидатом, попередньо попрохавши підготуватися до цього.

Фахівці служби персоналу не часто стикаються з підробленими документами, але і рідкістю це не назвеш.



Існують і інші способи введення в оману потенційного працедавця шляхом підробки документів. Цілі, яких при цьому

хочуть досягти кандидати, різні, але всі вони несуть певну небезпеку для кадрової безпеки підприємства.

Способи підробки документів

Найпоширенішим способом підробки документів є внесення змін до змісту справжнього документа шляхом стирання, дописки, заміни окремих листів документа або фотографії (часткова підробка). Ознаки цих підроблень визначаються за допомогою лупи і потужної лампи.

Переклеювання фотокарток зазвичай проводиться в документах, що засвідчують особу. Ці документи виготовлені на спеціальних бланках, які містять друкарський текст, захисні сітки, лінії графлення. При цьому способі підробки документа або переклеюється картка, що раніше була в іншому документі, або наклеюється нова фотографія, або проводиться монтаж фотокартки з відтисненням друку шляхом підклеювання до неї нової фотографії зі зрізаним кутом. У всіх випадках залишаються ознаки, що допомагають встановити факт заміни фотографії.

Нерідко виявляється і заміна частин документа, яка може бути вироблена в документах, що складаються з декількох листів. Ознаками заміни листів у документі є відмінності в нумерації сторінок, серії і номерів, ступінь забруднення, відмінності розмірів листів, їхні кольори, наявність зайвих слідів проколу від скріпок, сліди переробки нумерації сторінок шляхом підмальовування, підклеювання тощо.

Таким чином, використовуючи елементарні технічні засоби і нескладні навички, співробітник служби безпеки персоналу, що працює з документами кандидатів, здатний проводити первинну оцінку документів і при виявленні ознак підробки зобов'язаний повідомляти про це керівнику служби безпеки. Навчитися виявляти такі ознаки цілком можливо, освоївши декілька профільних розділів з будь-якого підручника з криміналістики.

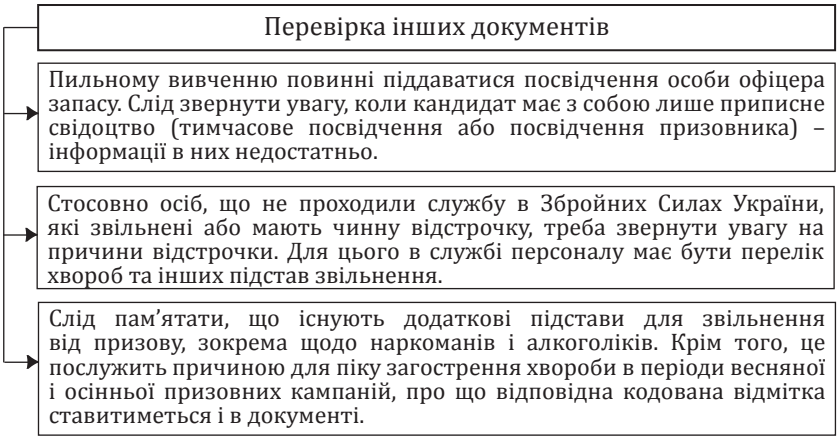
Приблизний **перелік моментів,** на які варто звернути увагу

Використовуючи тільки паспорт, вже можна будувати результативну співбесіду з претендентом, «випробовуючи» його на встановлених в компанії заборонах та обмеженнях.

Не вклеєна вчасно фотографія робить паспорт недійсним. Окрім цього, кандидат може влаштовуватися на роботу, пред'являючи паспорт, заявлений ним раніше як загублений, після чого той паспорт став також недійсним.

Перевірку з метою з'ясування дійсності документа може проводити служба безпеки. Вона ж запитає у кандидата, з якою метою він прийшов з недійсним паспортом.

Отже, розглядаючи ретельність вивчення документів на прикладі паспорта, ми проілюстрували, що ця процедура відбору є результативною тільки за умови якісного підходу і дає працедавцям достатньо корисної інформації.

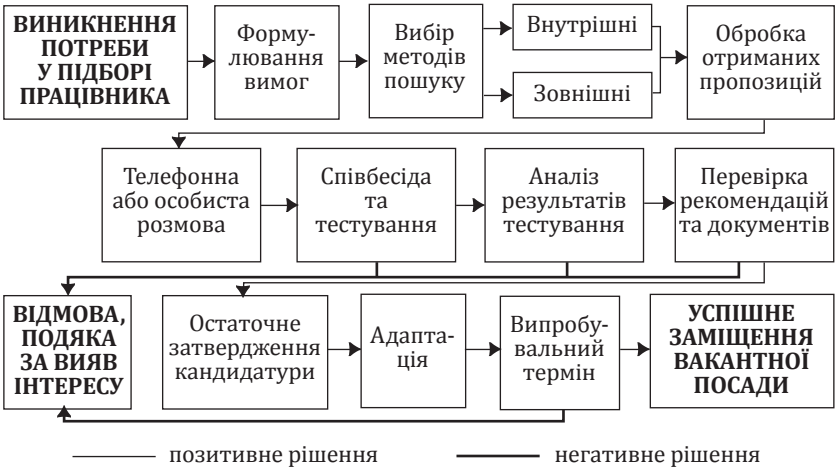


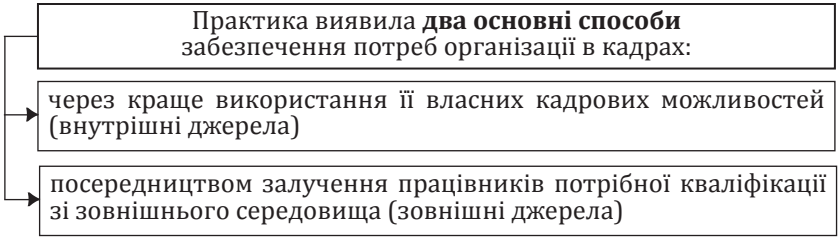
Кадрова служба займається веденням військового обліку. Її ігнорування не тільки не додасть вам упевненості при спілкуванні з військово-обліковими столами комісаріатів – покарання за таку провину розцінюватиметься як заподіяння збитку кадровій безпеці організації.

4.4. Роль служби економічної безпеки при прийнятті працівників на роботу та їх звільненні

Співбесіда кандидата зі співробітниками СБ – обов'язковий етап при прийомі на роботу. Бесіда має бути побудована так, щоб налаштувати на вільне спілкування та певний рівень довіри.

Алгоритм процесу підбору персоналу на підприємстві наводить у своєму посібнику І. І. Мігус.





Під час першого особистого контакту з кандидатом потрібно оцінити його зовнішній вигляд і манеру поведінки. При цьому важливо відзначати негативні ознаки – розгнузданість, недбалість в одязі, помітний макіяж, татуювання, особливо з кримінальною символікою, та ін. Стиль поведінки та одягу людини повинен відповідати вимогам посади, на яку вона претендує.

Метою проведення співбесіди співробітником СБ є отримати максимум відомостей біографічного характеру від самого кандидата, а також перевірити достовірність поданої в документах інформації (рівень освіти, досвід роботи і т. ін.). Якщо на вимогу надати будь-які додаткові документи кандидат відповідає відмовою, важливо проаналізувати причини такої поведінки.

Суть політики передбачає такі елементи:

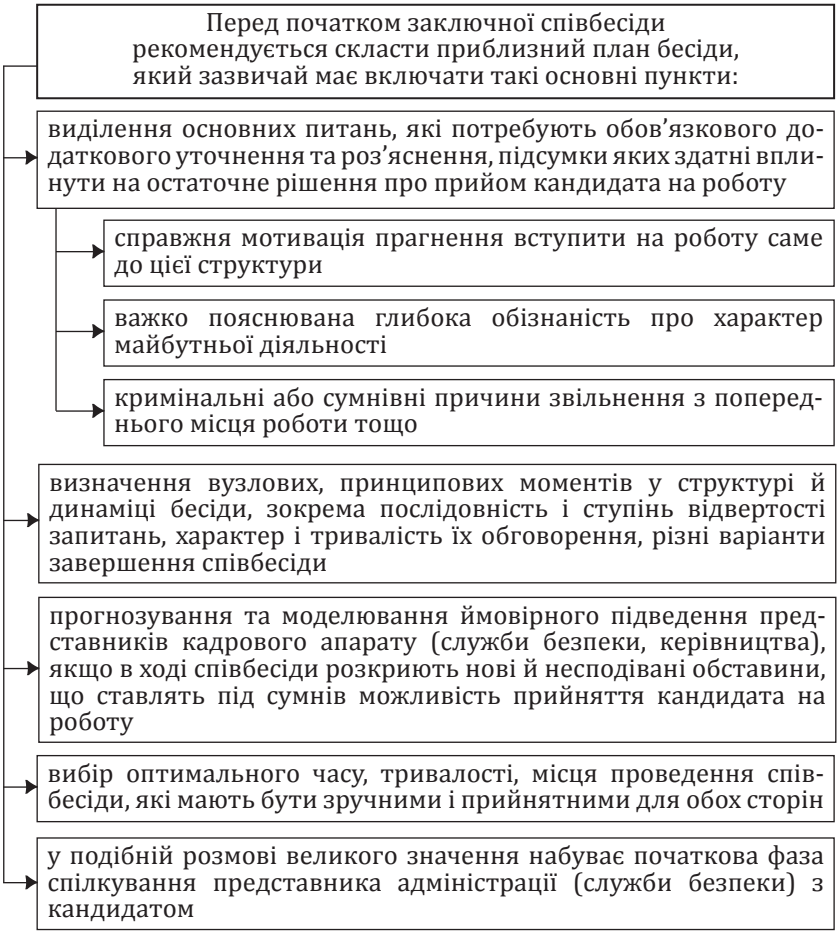
- професійний і грамотний підбір персоналу
- розгляд кандидатур
- навчання нових співробітників особливостям роботи
- створення належних умов праці
- визначення критеріїв морального й матеріального заохочення та стимулювання в роботі
- турбота про професійний ріст та перспективне просування по службі
- створення у колективі здорового морально-психологічного клімату
- визначення функціональних обов'язків для кожної категорії співробітників
- розробка критеріїв навантаження та оцінка віддачі (результатів)
- визначення раціонального співвідношення кількості працівників різних категорій
- розробка системи перевірки (на наявність компромату, лояльність, чесність) співробітників
- визначення політики відносин зі звільненими працівниками (з різних причин)

Методи підбору персоналу зі зовнішніх джерел

Етичні методи	Неетичні методи
використання особистих контактів	переманювання працівника з компанії-конкурента (хедхантинг)
пошук резюме в Інтернеті	пряме переманювання
розміщення оголошення в Інтернеті, ЗМІ, на сайті компанії	переманювання за допомогою приватних служб безпеки
звернення до ДСЗ	переманювання шляхом отримання нелегальним способом бази персональних даних компанії-конкурента
звернення до спеціалізованих агентств	співпраця з інсайдерами компанії-конкурента
пошук претендентів безпосередньо у ЗВО	
участь у ярмарках вакансій	

Наступним етапом у процесі прийняття співробітника на роботу вважається ***заключна співбесіда***. Ця співбесіда може відбуватися з керівником або іншою уповноваженою на те особою і є основним моментом заключної фази роботи з кандидатом.

Співробітникам кадрових підрозділів рекомендується виходити на підсумкову співбесіду з кандидатом не будучи заангажованим заздалегідь на позитивне рішення, оцінювати об'єктивно співрозмовника, прагнути уточнення і повторної перевірки раніше отриманої про нього інформації.


Перед початком заключної співбесіди рекомендується скласти приблизний план бесіди, який зазвичай має включати такі основні пункти:
виділення основних питань, які потребують обов'язкового додаткового уточнення та роз'яснення, підсумки яких здатні вплинути на остаточне рішення про прийом кандидата на роботу
справжня мотивація прагнення вступити на роботу саме до цієї структури
важко пояснювана глибока обізнаність про характер майбутньої діяльності
кримінальні або сумнівні причини звільнення з попереднього місця роботи тощо
визначення вузлових, принципових моментів у структурі й динаміці бесіди, зокрема послідовність і ступінь відвертості запитань, характер і тривалість їх обговорення, різні варіанти завершення співбесіди
прогнозування та моделювання ймовірного підведення представників кадрового апарату (служби безпеки, керівництва), якщо в ході співбесіди розкриють нові й несподівані обставини, що ставлять під сумнів можливість прийняття кандидата на роботу
вибір оптимального часу, тривалості, місця проведення співбесіди, які мають бути зручними і прийнятними для обох сторін
у подібній розмові великого значення набуває початкова фаза спілкування представника адміністрації (служби безпеки) з кандидатом

Особливості випробувального терміну

- після проведення попередньої перевірки кандидата і прийому на роботу йому призначається випробувальний термін, під час якого він перебуває під особливим наглядом з метою виявлення його негативних якостей
- у час випробувального терміну нові працівники мають отримувати мінімум інформації про підприємство і, природно, їх небажано знайомити з конфіденційною інформацією підприємства. Вони повинні мати доступ тільки до необхідної для виконання їх функціональних обов'язків інформації, а будь-які спроби дізнатися більше мають присікатися керівництвом або службою безпеки
- випробувальний термін – період посиленого контролю за працівником

На ринок праці потрапляє велика кількість безробітних, що пов'язано зазвичай з політикою, яку провадять підприємства стосовно оптимізації чисельності персоналу, тобто зведення загальної кількості працівників до мінімуму з метою мінімізації витрат.

Тимчасом, звільняючи працівників, роботодавець має пам'ятати про соціальну відповідальність, яку він взяв на себе, наймаючи персонал. Усунути основні негативні сторони процесу звільнення як для роботодавця, так і для працівників може відносно новий метод звільнення – аутплейсмент.

Аутплейсмент (з англ. *outplacement*) – це форма розірвання трудових відносин між підприємством та працівниками, що передбачає залучення спеціалізованих організацій з метою надання працівникам, які підпадають під скорочення, консультацій з працевлаштування за кошти колишнього роботодавця.

Аутплейсмент – комплексний пакет кваліфікованих послуг, таких як юридична допомога, психологічна підтримка, пошук адекватної посади, які сприяють подальшому працевлаштуванню звільненого працівника.

Зазвичай ця послуга надається кадровими та рекрутинговими агентствами. Залежно від способу реалізації розрізняють такі основні види аутплейсменту: *відкритий* – працівники знають про те, що їх звільняють, а роботодавець за допомогою кадрової служби компанії або посередника надає їм допомогу в подальшому працевлаштуванні; *закритий* – працівник про звільнення не знає, як правило, це стосується топ-менеджерів і керівників відділів, відкритий конфлікт з якими для роботодавця дуже небажаний; *масовий* – застосовується в умовах численних звільнень персоналу через обмежений бюджет компанії.

Вивільнення персоналу – це вид діяльності, який передбачає комплекс заходів щодо дотримання правових норм і організаційно-психологічної підтримки з боку адміністрації при звільненні працівників підприємства.

Звільнення персоналу підприємства вимагає:

– дотримання трудового законодавства;
– чітких, максимально об'єктивних критеріїв добору;
– прив'язки до робочих місць;
– мінімізації витрат і одержання економії;
– запобігання наступним і пов'язаним із вивільненням витрат;
– відкритості;
– інформування;
– компенсацій і допомоги у працевлаштуванні.

Гнучка політика зайнятості підприємства полягає в її підтримці та раціоналізації й передбачає:

припинення наймання, коли на місце, що вивільняється, не наймаються нові працівники. При цьому скорочується лише загальна чисельність, а не конкретні робочі місця;

скорочення робочого часу шляхом зниження тривалості робочого дня і (або) робочого тижня, скасування або скорочення масштабів внутрішнього сумісництва і понаднормових робіт;

припинення видачі замовлень на сторону;

направлення на навчання з відривом від основних занять і надання неоплачуваних відпусток;

використання внутрішніх венчурів (з англ. *venture* – ризиковане підприємство) – груп ентузіастів, що мають свої ідеї, бажають працювати як їхні розробники, збутовики або вкладати в них кошти на додаток до первісного фінансування підприємством цих проектів. Реалізуючи проект, кожен учасник венчуру просувається службою в його межах;

стимулювання звільнень за власним бажанням

- на основі пропозиції грошових компенсацій
- пропозиції дострокового виходу на пенсію (принцип «зелених вікон») і за додаткову винагороду («золоте рукостискання»)

аутплейсмент – сукупність методів, за допомогою яких кадрові служби забезпечують зацікавленим особам, що звільняються, допомогу у працевлаштуванні коштом підприємства в оптимальний термін і при найбільш сприятливих умовах;

звільнення окремих працівників за різні порушення;

масові звільнення (є останнім засобом при недостатності індивідуальних заходів).

Головна мета аутплейсменту – сформувати у звільненого працівника загальне розуміння ситуації, що склалася на ринку праці, і спрямувати його поведінку на ефективний та правильний пошук нової роботи.

Отже, для співробітника, якого звільняють, аутплейсмент – це життєво важлива підтримка, а для компаній, що розлучаються з ключовими працівниками і керівниками, – це найкращий спосіб підтримки своєї репутації, адже фірма показує, що цінує своїх співробітників, незважаючи на вимушені звільнення.

Відповідно до трудового законодавства, при звільненні за скороченням штатів переважне право залишитися на роботі надається:

- працівникам з вищою продуктивністю праці і кваліфікацією;
- сімейним працівникам (тим, що мають двох і більше дітей, і тим, у родині яких немає інших осіб зі самостійним заробітком) – у випадку рівної продуктивності праці;
- працівникам, що мають тривалий стаж безупинної роботи в цьому підприємстві;
- працівникам, що отримали у підприємстві професійне захворювання;
- працівникам, що підвищують свою кваліфікацію без відриву від виробництва у вищому і середньому спеціальному навчальному закладах відповідно до виконуваної роботи.

Працівники, що вивільняються, поділяються на дві частини:

- особи, які не пройшли атестацію, систематично порушують дисципліну або ті, які не «вписуються» у підприємство з тієї причини, що функції, які виконувалися ними колись, стали непотрібними;
  - вони підлягають звільненню незалежно від заслуг, але навіть їм спочатку потрібно запропонувати поліпшити свою роботу і звільняти лише в тому випадку, якщо це не допоможе.
- працівники, яких підприємство хоче залишити, але вже у новій якості.
  - Роботу працівникам, що вивільняються, доцільно пропонувати в письмовому виді, називаючи усі наявні вакансії.
  - Уперше це робиться у день оголошення про майбутнє звільнення, оскільки працівник має право бути переведеним на вакантне робоче місце.
  - Вдруге – у день звільнення, тому що судові органи перевіряють законність розірвання трудового договору саме на цей момент. Крім того, думка людини про ту чи іншу роботу може змінитися або у підприємстві можуть відкритися нові вакансії.
  - Крім того, думка людини про ту чи іншу роботу може змінитися або у підприємстві можуть відкритися нові вакансії.

Обов'язок адміністрації підприємства – довести суду факт необхідності скорочення чисельності або штатів. У разі прийняття судом рішення про неправильні або незаконні дії адміністрації покладається як адміністративна, так і матеріальна відповідальність на посадову особу.

Не можна попереджати працівника про майбутнє вивільнення у період тимчасової непрацездатності або чергової відпустки.

Менеджер з персоналу повинен проводити заняття з працівниками, які звільняються, щодо правильного складання резюме, проходження інтерв'ю у різних підприємствах; допомагати в пошуку роботи; пояснювати, як стати на облік у Службу зайнятості, і т. ін.

Можна виокремити рекомендації щодо організації звільнення працівників з підприємства

Не слід повідомляти працівникові про звільнення у четвер або п'ятницю, або за день до свята, коли в них буде додатковий час для міркувань. Це не стосується звільнень у випадках, коли потрібна негайна дія. Потрібно бути делікатним і не звільняти людину в день його народження, річницю весілля або річницю роботи у підприємстві.

Повідомлення про звільнення слід робити в присутності щонайменше заступника директора з кадрових питань.

Не можна виражати причину звільнення своїми словами, її слід повідомляти офіційно, з точними й аргументованими фактами (поганого виконання роботи або складного становища підприємства). Не допускається принижувати людину, незалежно від причини звільнення.

Не слід повідомляти суперечливу інформацію: працівникові, що звільняється, говорити про одну причину, а іншим працівникам – про іншу. Щоб уникнути конфлікту, деякі менеджери повідомляють своїм службовцям, що їхня посада скорочена (ліквідована), а всім іншим повідомляють, що людина просто не виконувала свою роботу. Але така поведінка змушує працівників, що залишилися, замислитися, чи чесний керівник з ними.

Не слід говорити нікому, крім тих, хто повинен знати, про те, що людина буде звільнена. Якщо така інформація пошириться, це може викликати паніку на підприємстві.

Не бажано повідомляти занадто рано про звільнення через відсутність роботи або ліквідацію посади.

Не потрібно просити людину негайно звільнити робочий стіл і залишити офіс. Час після роботи – найоптимальніший для цього.

За винятком випадків шахрайства або крадіжки, не доречно вдаватися до послуг фірмової служби безпеки, для того щоб провести звільненого з будівлі.

Слід доручити одному зі своїх найближчих працівників контактувати зі звільненим доти, допоки він не знайде інше місце роботи.

Обов'язково необхідно дотримуватися вимог трудового законодавства.

Таким чином виникає дилема: скорочувати треба, але використовувати традиційні способи впливу на персонал (адміністративні, економічні й силові) неефективно.

Вирішити проблему можна, застосовуючи недирективні (нежорсткі) форми скорочення. Вони пов'язані з доведенням до індивідуальної свідомості кожного працівника необхідності змінити свою поведінку, місце у структурі, замислитися про потребу залишатися саме на цьому підприємстві. Основний інструмент недирективного скорочення – емоційно-ціннісні мотиви при формуванні рішення про звільнення і, зрештою, прийняття кожним рішення або подолання негативного ставлення до рішення керівництва про можливості виходу з підприємства. Саме недирективні методи дають змогу одержати економічний і психологічний ефект від скорочення персоналу.

Питання для обговорення

1. Як здійснюється попередня перевірка при прийомі на роботу?
2. У чому криється специфіка оцінки кандидата за зовнішнім виглядом і поведінковими ознаками («face-control»)?
3. Які особливості перевірки документів при прийомі на роботу?
4. Перелічіть способи підроблення документів.
5. Охарактеризуйте особливості звільнення працівників.
6. Наведіть рекомендації щодо звільнення персоналу.

Домашні завдання

Завдання 1. Розробити Положення про службу (підрозділ) кадрової безпеки підприємства, установи, організації.

Завдання 2. Розробити посадові інструкції працівників служби (підрозділу) кадрової безпеки підприємства, установи, організації.

Завдання 3. Проведіть оцінювання. Покладіть перед собою який-небудь рукопис (лист) і оцініть характер його автора за поданими нижче показниками:

1. Часті тире, особливо подовжені і з натиском, вказують на агресивність характеру.

2. Довгі петлі, особливо в нижній частині букв (в результаті отримуються довгі вузькі літери) вказують на діловитість і схильність радше до матеріального, ніж до духовного.

3. Незакінчені петлі нижніх частин букв свідчать про консерватизм.

4. Важкі петлі нижніх частин букв часто вказують на нерішучий характер.

5. Непропорційно великі заголовні літери є ознакою егоїзму.

6. Витіюваті закрутки вказують на метушливість, педантичність і егоцентричність.

7. Незграбні великі літери нерідко належать допитливому розуму.

8. Завершені нижні петлі букв «д», «у», «з» вказують на задоволеність життям і схильність до веселощів.

9. Незвичайні закрутки верхніх частин букв можуть належати «ідеалістам».

10. Екстравагантно виписані заголовні букви можуть вказувати на екстравагантність характеру.

11. Якщо друга і третя вертикальна риса великих літер «н», «п», «т», «ж», «м» вищі, ніж перша, – це може вказувати про невротичність характеру.

12. Різні за розміром букви в рядку, а особливо в одному слові, підкреслюють неуважність в різних аспектах життя.

13. Простота і легкість написання великих літер може бути ознакою спокійного, безтурботного і задоволеного характеру.

14. Непомірно великий почерк вказує на непристосованість до життя і навіть конфліктність.

15. Плавний потік рівних букв у словах є ознакою логічного та здорового глузду.

16. Довгі закрутки букв останнього слова можуть бути показником екстравагантності.

17. Відкриті верхні частини літер А, О, Д вказують на схильність до балакучості.

18. Крупний незграбний почерк може бути показником збудженості характеру.

19. Тяжкий (великий) і неохайний почерк вказує на негнучкість фантазії.

20. Якщо літери «деруться» догори або, навпаки, «збігають» донизу, це є ознакою романтичності і невгамовності.

21. Якщо кінцеві літери слів виразні і за розміром більші від початкових – перед вами відкрита особистість.

Форма контролю: усне опитування, перевірка рефератів, вирішення тестових завдань.

Рекомендована література: 1, 2, 3, 5–7, 11–17, 20, 21.

Тема 5
МОТИВУВАННЯ ПЕРСОНАЛУ ТА КОНТРОЛЬ ЗА ЙОГО ДІЯЛЬНІСТЮ

5.1. Мотивування і стимулювання персоналу.

5.2. Організація мотивації праці та управління нею.

5.3. Захист від протиправних дій працівників.

5.4. Особливості попередження і виявлення протиправних дій працівників.

5.5. Внутрішнє шахрайство на підприємстві та шляхи його виявлення.

Ключові поняття: мотивація персоналу, стимулювання персоналу, особливості мотивації праці, матеріальна мотивація, моральна мотивація, мотиваційний моніторинг, протиправні дії, захист від протиправних дій працівників, шахрайство персоналу, розслідування та протидія шахрайству.

5.1. Мотивування і стимулювання персоналу

Мотивація трудової діяльності не може бути дієвою без застосування сучасних форм і методів матеріального стимулювання персоналу.

Мотиви праці різноманітні. Вони різняться за:

- потребами, які людина хоче задовольнити своєю трудовою діяльністю
- цінностями, які потрібні людині для задоволення своїх потреб
- ціною, яку працівник готовий заплатити за свої погреби

Виділяють декілька груп мотивів праці, які в сукупності створюють єдину систему. Це мотиви змістовності праці, її корисності, статусні мотиви, пов'язані з визнанням трудової діяльності, мотиви одержання матеріальних цінностей, а також мотиви, зорієнтовані на певну інтенсивність роботи.

Мотивація – це довготерміновий вплив на працівників з метою зміни за заданими параметрами структури ціннісних орієнтацій та інтересів, формування відповідної мотиваційної системи і розвиток на цій основі трудового потенціалу.

Стимулювання як тактика вирішення проблем є ставкою на фактичну структуру ціннісних орієнтацій та інтересів працівника, на більш повну реалізацію наявного трудового потенціалу.

Мотивація і стимулювання як методи управління працею є протилежними за напрямами: перший направлений на зміну існуючого стану, другий – на його закріплення, проте вони доповнюють один одного.

Стимулювання мусить відповідати потребам, інтересам і здібностям працівника.

Мотивація – це процес свідомого вибору людиною того чи іншого типу поведінки, що визначається комплексним впливом зовнішніх (стимули) і внутрішніх (мотиви) чинників.

Стимулювання праці передбачає створення умов, при яких активна трудова діяльність дає певні, раніше зафіксовані результати, стає необхідною і достатньою умовою задоволення значних і соціально обумовлених потреб працівника, формування у нього мотивів до праці.

Стимулювання праці ефективне тільки у тому випадку, коли органи управління вміють добиватися і підтримувати той рівень роботи, за який платять. Ціль стимулювання – не взагалі спонукати людину працювати, а зацікавити її працювати краще, продуктивніше, ніж це обумовлено трудовими відносинами.

Мотивація праці формується до початку професійної трудової діяльності, шляхом засвоєння людиною цінностей і норм трудової моралі та етики, а також через особисту участь у трудовій діяльності, в сім'ї та школі.

Матеріальна мотивація – це прагнення певного рівня добробуту, певного матеріального стандарту життя.

Матеріальна мотивація трудової діяльності залежить від цілої низки чинників, а саме:

- рівня і структури особистого доходу
- матеріального забезпечення наявних грошових доходів
- дієвості системи стимулів, що застосовуються в організації

Зв'язок мотивації результатів праці опосередкований природними здібностями і набутими навиками праці, тільки мотивація є джерелом діяльності людини.

Трудова мотивація пов'язана як зі змістовністю, корисністю праці, так і з самовираженням, самореалізацією працівника. Велику роль у практиці управління персоналом відіграє і статусна мотивація, вона є рушійною силою поведінки, пов'язаної з бажанням людини зайняти вишу посаду, виконувати складнішу, відповідальнішу роботу, працювати в сфері діяльності, яка вважається суспільно корисною.

Для мотивації праці, а по суті, для забезпечення потрібного рівня трудової активності персоналу **доцільно**:

визначити набір цінностей, які будуть закладені в основу мотивування персоналу

- Цей набір повинен включати основні потреби та інтереси людей, які занотовують у формі пільг, переваг, видів заохочення в «Правилах внутрішнього трудового розпорядку організації» і закріплюють в інших локальних нормативно-правових актах.

з'ясувати рівень потреб кожного працівника, його інтереси і можливості задоволення

конкретизувати види трудової діяльності, які потрібні організації і які доцільно мотивувати

організувати працю так, щоби переконати працівника в можливості задовольнити його інтереси з доступними для нього витратами фізичних і моральних сил, часу та можливості відтворити свою працездатність

узгодити певні види діяльності з набором цінностей і переваг

наймаючи працівника, з'ясувати, які в нього мотиви, інтереси, яка система цінностей

встановити доходи працівника в організації, щоби були достатніми, аби покривати його витрати.

Умовами ефективного використання мотивації праці є:

- високий рівень оплати
- використання високопрофесійної праці
- відсутність зрівняйлівки в оплаті
- високий престиж праці в державі, висока купівельна спроможність людини та її зацікавленість у підвищенні кваліфікації

Щоб мотиваційний процес був керованим, потрібно створити певні умови:

- мати повну й достовірну інформацію про об'єкт управління
- мати уявлення про стан і динаміку мотиваційної спрямованості персоналу
- ретельно стежити за соціально-економічними наслідками управлінських рішень
- вміти прогнозувати наслідки управлінських рішень

Досвід свідчить, що традиційні методи збирання даних стосовно мотиваційної спрямованості персоналу вже не задовольняють потреби практики управління; необхідно запровадити в кожній організації систему мотиваційного моніторингу, яка би створила нову інформаційну базу для прийняття управлінських рішень у сфері мотивації трудової діяльності.

Мотиваційний моніторинг – це система постійного спостереження і контролю за станом мотивації трудової діяльності з метою його оперативної діагностики й оцінки в динаміці, прийняття кваліфікованих управлінських рішень задля підвищення ефективності виробництва.

Запровадження мотиваційного моніторингу є актуальним для більшості підприємств України, адже вивчення потреб, інтересів мотиваційної спрямованості персоналу здійснюється в Україні епізодично і вкрай поверхово.

Винагороди ідентифікуються в такій послідовності:

Повне визнання та адекватна оцінка виконаної роботи.
Почуття належності до справ.
Співчутливе ставлення з боку менеджерів (інтерес до особистих проблем працівників, бажання допомогти).
Стабільність зайнятості.
Добра оплата.
Цікава робота.
Особисті контакти з менеджерами.
Просування по службі.
Сприятливі умови праці.
Дисципліна праці.

5.2. Організація мотивації праці та управління нею

Мотиваційний моніторинг передбачає проведення регулярних опитувань та аналіз наявної економічної, соціологічної та психологічної інформації.

Для оцінки мотивації трудової діяльності в динаміці взаємозумовленості та взаємозв'язку зі соціально-економічними процесами важливо мати набір ключових характеристик (показників), до яких належать:

а) характеристика трудової діяльності та якості трудового потенціалу

- професійно-кваліфікаційний склад працівників;
- якість професійної підготовки та перепідготовки робочої сили;
- стан зайнятості;
- оцінка конкурентоспроможності працівників;
- форми і методи матеріального стимулювання трудової діяльності та їх дієвість;
- форми і методи негативної мотивації та їх ефективність;
- умови й організація праці;
- рівень продуктивності праці;
- рівень задоволення працею та результатами трудової діяльності; роль і місце праці в ціннісних орієнтаціях працівників;
- основні мотиви трудової діяльності і зміни в їхній структурі;

б) показники рівня життя

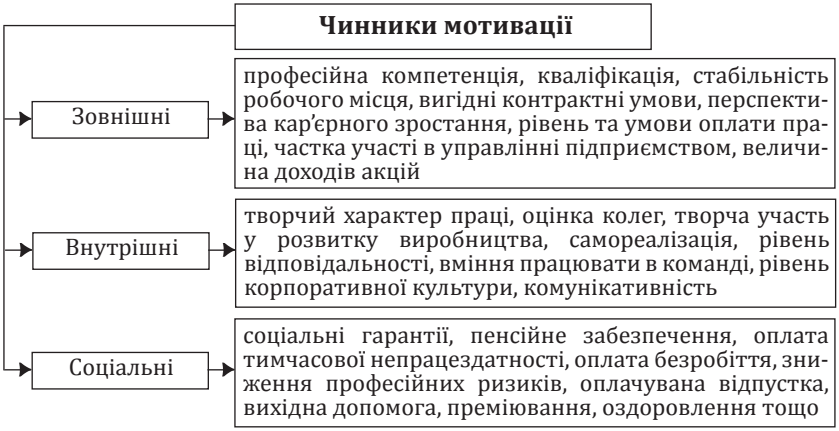
- номінальна заробітна плата;
- структура доходів;
- диференціація доходів;
- структура витрат;
- реальний бюджет працівників та їхніх сімей;
- рівень забезпечення житлом, послугами медицини, освіти, культури, екологічна ситуація, особиста безпека;

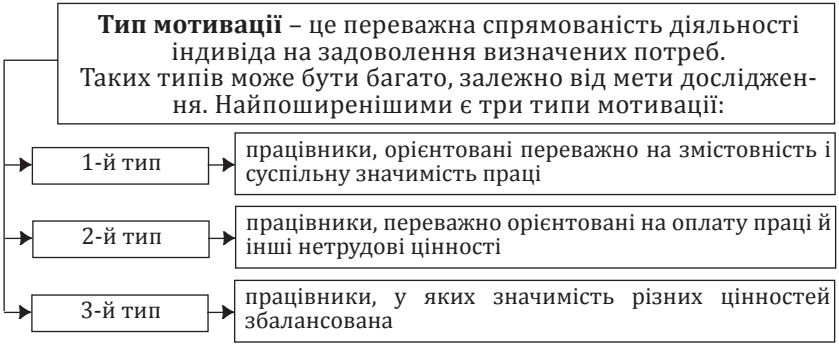
в) характеристики стану суспільної думки щодо ефективності соціально-економічної політики держави, соціальної спрямованості ринкових перетворень

Система моніторингу мотивації трудової діяльності має ґрунтуватись на таких принципах:

системність	формування набору оціночних показників для кожного напрямку мотивації трудової діяльності
комплексність	отримання й обробка соціально-економічної, соціологічної та психологічної інформації, яка характеризує стан і зміни в мотивації трудової діяльності
аполітичність	аналіз основних причин зміни стану мотивації трудової діяльності з урахуванням впливу як внутрішніх, так і зовнішніх чинників
періодичність	регулярне поповнення інформаційної бази, необхідної для розробки ключових характеристик мотивації трудової діяльності
виробничо-територіальний підхід	досягнення оптимального поєднання виробничих і територіальних принципів проведення моніторингу службами мотивації

Управління мотивацією – це процес стимулювання працівників до здійснення ефективної діяльності, спрямованої на досягнення цілей підприємства.





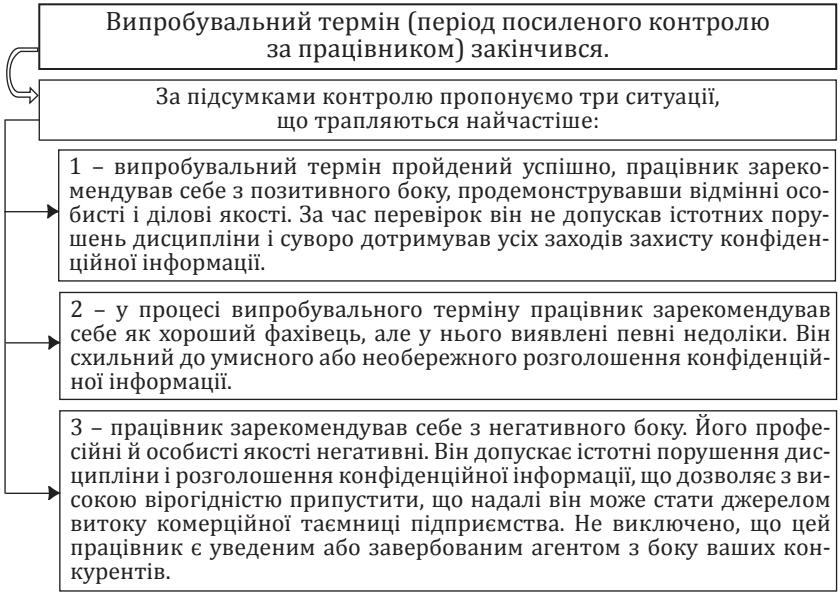
Основна маса працівників у нашій країні (не менше 80%) належить до другого типу мотивації: мотиваційне ядро базується на високій (у їхньому розумінні) заробітній платі.

5.3. Захист від протиправних дій працівників

Спостерігайте за людиною,
вникайте в причини її вчинків,
придивляйтеся до неї в час її дозвілля.
Чи залишиться вона тоді для вас загадкою?
Конфуцій

Після проведення попередньої перевірки кандидата і прийому на роботу йому призначається випробувальний термін, під час якого він перебуває під особливим спостереженням з метою виявлення його негативних якостей. Слід наголосити, що в цей час нові працівники мають отримувати мінімум інформації про підприємство і, природно, їх небажано знайомити з конфіденційною інформацією підприємства.

Вони повинні мати доступ тільки до необхідної для виконання їхніх функціональних обов'язків інформації, а будь-які спроби дізнатися більше повинні присікатися керівництвом або службою безпеки (до речі, якщо ці спроби вельми наполегливі і постійні – доречно приділити цьому працівникові особливу увагу).



Такої людини, звісно, потрібно щонайшвидше позбутися, оскільки вона становить серйозну загрозу і може завдати непоправного збитку підприємству. Як позбуватися – вирішувати вже Вам, головне, аби це все відбувалося в правових рамках. У виняткових випадках, якщо Ви впевнені в своїх силах, таку людину можна використовувати для дезінформації, даючи їй свідомо помилкову або непотрібну інформацію.

Потрібно пам'ятати, що не можна повністю керуватися тільки результатом попередньої перевірки і випробувального терміну.

По-перше, практично всім працівникам відомо, що попервах вони перебуватимуть під наглядом. Тому протягом випробувального терміну працівники намагаються поводитися позитивно, дотримуватися всіх інструкцій.

По-друге, спершу у нового працівника є період адаптації. Він ще не знає про взаємини, що склалися у фірмі, правила і порядки, відчуває себе невпевнено і прагне справити сприятливе враження. У подальшому, після облаштування на новому місці, його поведінка може кардинально змінитися.

По-третє, не виключено, що попередня перевірка і випробувальний термін були проведені неефективно, і людині з негативними якостями вдалося успішно пройти контроль з добрим результатом.

Отже, персонал повинен постійно бути під пильним спостереженням і регулярно проходити спеціальні перевірки, які мають проводити фахівці (співробітники служби безпеки) або, в крайньому разі, менеджери з персоналу чи експерти, що працюють за контрактом.

Перевірки можуть бути:

1) регулярні (проводяться за графіком, наприклад, першого числа кожного місяця, 15 числа кожного місяця тощо).

1) оперативні (проводяться за плаваючим графіком, несподівано для тих, що перевіряються, крім того, обов'язково проводяться у разі НП, розголошення інформації або виникнення підозри стосовно конкретних співробітників).

Перевірки можуть проводитися:

а) гласно – перевірка дотримання інструкції, режиму зберігання, користування і знищення документації і джерел конфіденційної інформації, обліку вхідної / вихідної кореспонденції і т. ін., теоретичного знання спеціальних інструкцій, заслуховування пропозицій і зауважень від тих, що перевіряються, і їхніх керівників тощо.

б) негласно – проводяться таємно від тих, що перевіряються співробітниками СБ або особами, які спеціально залучаються. Такі перевірки дають змогу з високою ефективністю отримати необхідний результат, оскільки особа, яка перевіряється, не підозрює про те, що знаходиться під контролем, тож поводиться розкуто і природно.

Окрім перевірок, служба безпеки підприємства регулярно має здійснювати певні заходи зі збору інформації та перевірки персоналу.

Найвикористовуванішими заходами є:

1) спостереження

2) агентурна робота

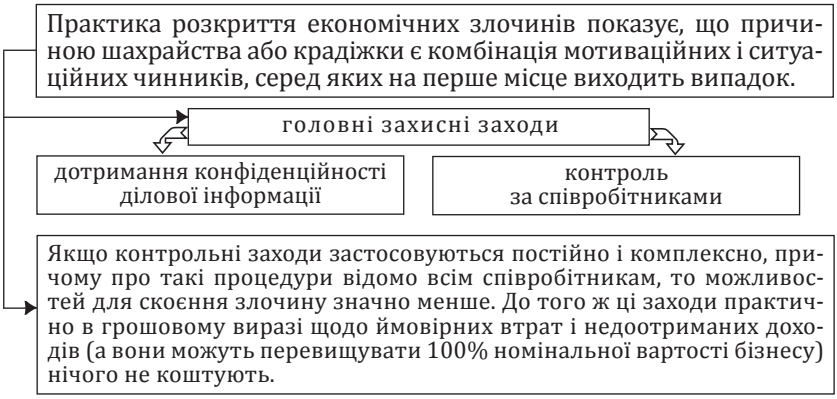
3) провокації

Таким чином, спеціально створена система контролю за персоналом дозволяє відсіяти неблагонадійних осіб уже на першому етапі, а в разі успішного проходження попередньої перевірки – виявити і вчасно нейтралізувати загрозу безпеці підприємства.

На кожному підприємстві існують внутрішні і зовнішні **джерела небезпеки**

внутрішні – діяльність професійних злочинців, зокрема оганізованих злочинних груп; чиновників – корупціонерів, не рідко пов'язаних з оргзлочинністю; «випадкових» злодіїв; навмисні протиправні дії ділових партнерів;

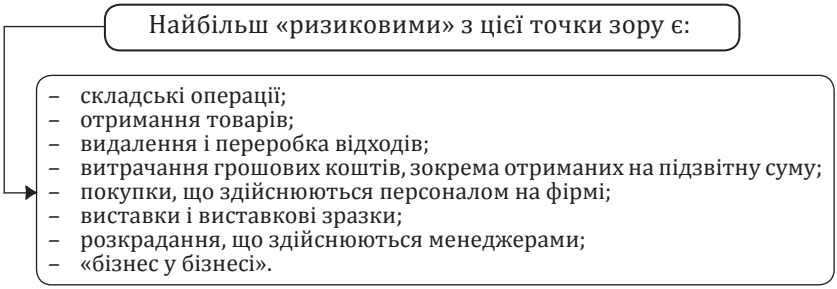
зовнішні – зазвичай персонал, але доцільно включити й відвідувачів.



Слід уникати непотрібних ризиків. Повністю уникнути всіх ризиків, які можуть зустрітися в конкретному виді бізнесу, можна, тільки якщо припинити займатися ним взагалі. Тобто треба на основі наявної перевіреної інформації оцінити ступінь ризику в тій чи іншій ситуації, потім ухвалювати рішення.

Обмеженням ризику може служити страхування, зокрема від настання якихось конкретних подій. Природно, такі рішення приймаються усвідомлено після всебічного оцінювання всіх ризиків і їх можливих наслідків.

Відсутність системи постійного контролю за співробітниками надає можливість нечесним працівникам використовувати своє становище, яке їм дає допуск у компанію, для здійснення крадіжок і розкрадань у ній.



Оперативно-слідча практика свідчить, що саме співробітники (або з їх участю) здійснюють 90% крадіжок усередині організацій, оскільки саме вони найліпше знають «слабкі місця», які можна використовувати в своїх корисливих цілях.

Основна причина розкрадань тут – поганий контроль (приклади)

Передбачалося, що запасні частини, які використовуються для ремонту техніки в автосервісі, повинні списуватися з облікових документів менеджером зі зберігання, який мав робити це наприкінці робочого дня. У такій обстановці і продавці, і механіки брали собі деякі деталі, а в ході розслідування було встановлено, що іноді списанням займався один з механіків. Ця людина «враховувала» не тільки ті запасні частини, які дійсно були необхідні для відновних робіт, що проводяться в майстерні, але і ті, які він відносив до себе додому. Більш того, він зізнався, що деколи забирав собі деталі, які взагалі не враховувалися як використані. Це те, що називається «бардаком» і відсутністю контролю взагалі. Необхідно систематично проводити перевірки виконання обов'язків посадовими особами, звірки складських запасів з даними по закупівлях і продажах, причому такі перевірки мають виконувати співробітники, котрі не працюють безпосередньо на цьому складі.

Один з обов'язків комірника – враховувати видачу і надходження назад устаткування і витратних матеріалів для виконання внутрішніх робіт. Часто записи про це слідують відразу ж один за одним. Розслідування показало, що таке робиться тому, що фактично зворотного надходження не відбувається (навіть якщо диспетчерські документи тимчасового користувача засвідчують інакше). Швидке відображення повернення робиться для того, щоб інший комірник не відмітив, що устаткування не повернуто. Подібні операції проробляються і спільно з постачальниками товарів, коли фактично товар не поставляється, а оформляється як такий, що поступив або вибув. Як подяку за «співпрацю» в шахрайстві комірник отримує різні послуги, зокрема «право безкоштовного придбання» товарів у постачальників.

Шахрайства такого роду зазвичай розкриваються доволі легко, але вірогідні вони тільки там, де за роботою складських працівників немає контролю. Якщо йдеться про шахрайство зі сировиною, факт розкрадання можна встановити, порівнюючи показники, що наводяться, з плановими. В разі істотних розбіжностей необхідна детальніша перевірка.

Значно небезпечніше є тоді, коли менеджер середньої ланки вдається до прямої змови зі сторонніми шахраями або збирає команду з працівників підприємства для систематичного таємного і безоплатного вилучення «фірмових» цінностей.

Достатньо кримінальним вважається і «бізнес усередині бізнесу».

5.4. Особливості попередження і виявлення протиправних дій працівників

Нейтралізація протиправних дій

Недопущення – система засобів адміністративного примусу, спрямованих на перешкоджання здійсненню злочинного наміру конкретною особою на стадії його підготовки.

Припинення – заходи спрямовані на зупинення протиправної діяльності, яка вже почалася, з метою відвернення настання суспільно небезпечних наслідків.

Профілактика правопорушень – обов'язкова діяльність органів державної влади, місцевого самоврядування, підприємств, установ, організацій незалежно від форми власності, зокрема громадських організацій, спрямована на виявлення та усунення причин і умов, які сприяють учиненню правопорушень, а також виявлення осіб, схильних до вчинення правопорушень, та застосування заходів щодо їх виправлення.

Загальна профілактика – заходи, спрямовані на виявлення причин і умов, що сприяють учиненню правопорушень на всій території України, у її окремому регіоні, галузі господарства, стосовно частини населення чи групи осіб, а також на підприємстві, в установі чи організації незалежно від форми власності.

Віктимологічна профілактика правопорушень – система взаємопов'язаних, організаційно забезпечених державних, громадських й індивідуальних заходів, спрямованих на виявлення та усунення або нейтралізацію чинників, які формують особисту чи масову можливість стати жертвою правопорушення.

Жертва правопорушення – особа, що потерпіла від правопорушення, незалежно від того, чи визнана вона такою у встановленому законом порядку і чи усвідомлює себе такою.

Індивідуальна профілактика правопорушень – система спеціальних заходів щодо конкретних осіб, які не скоїли протиправних діянь, але знаходяться в несприятливих умовах і під їх впливом можуть учиняти такі дії, ведуть антисуспільний спосіб життя, скоюють правопорушення, характеризуються формуванням умислу і мотиву на вчинення правопорушень, підготовкою конкретного правопорушення, учинили замах на злочин, але не довели його до кінця, скоїли злочин і можуть допустити рецидив.

Антисуспільна спрямованість особи – виявляється в її аморальних вчинках, дисциплінарних, адміністративних та інших правопорушеннях, які ще не мають злочинного характеру, але при повторенні дедалі більше набирають кримінальних рис.

Інші категорії осіб, схильні до вчинення правопорушень, – це особи:

- визнані в установленому порядку хронічними алкоголіками або зловживають спиртними напоями і двічі протягом року притягалися до адміністративної чи іншої відповідальності за розпиття спиртних напоїв або появу в громадських місцях у нетверезому стані;
- визнані в установленому порядку наркоманами, токсикоманами або вживають наркотичні речовини без призначення лікаря;
- психічно хворі, які страждають на тяжкі психічні розлади і перебувають на спеціальному обліку в закладах охорони здоров'я;
- які вчинили насильство в сім'ї після винесення їм офіційного попередження про неприпустимість учинення насильства в сім'ї;
- неповнолітні, які скоїли адміністративні правопорушення, ведуть антисуспільний спосіб життя, зокрема звільнені із спеціальних виховних установ;
- які двічі протягом року притягалися до адміністративної відповідальності за дрібне хуліганство.

Охорона підприємства – безпосередні дії працівників охорони за місцезнаходженням об'єкта, спрямовані на виявлення, запобігання та припинення:

- несанкціонованих проникнень на об'єкт, що охороняється (на територію, у приміщення);
- перебування осіб, яким не надано відповідних повноважень, на об'єкті, що охороняється;
- протиправного заволодіння майном на об'єкті, що охороняється, шляхом крадіжки, грабежу, розбійного нападу, шахрайства тощо;
- протиправного використання майна на об'єкті охорони особами, яким не надано відповідних повноважень;
- заподіяння майнової шкоди об'єкту, що охороняється, шляхом очевидних порушень промислової безпеки та охорони праці, належних умов зберігання майна або внаслідок стихійного лиха, аварії, катастрофи та інших надзвичайних подій за відсутності протиправних дій щодо об'єктів охорони.

Забезпечення охорони цехів, відділів, лабораторій, інших виробничих і спеціальних приміщень технічними засобами в позаробочий час відповідно до переліку, затвердженого керівником підприємства.

Забезпечення пропускного та внутрішньооб'єктового режимів – контроль за проходженням персоналу та відвідувачів на об'єкт (з об'єкта) охорони, пересуванням його територією, переміщенням майна, яке перебуває на об'єкті, відповідно до порядку, установленого керівником об'єкта, що охороняється, з урахуванням вимог чинного законодавства України, зокрема шляхом:

- застосування контрольно-пропускного та внутрішньооб'єктового режимів;
- використання технічних засобів охоронного призначення;
- використання службових собак.

До заходів індивідуальної профілактики правопорушень слід віднести:

- профілактичну бесіду
- роз'яснення законодавства
- усне попередження про неприпустимість протиправних дій
- офіційне попередження про неприпустимість учинення насильства в сім'ї
- офіційне застереження про неприпустимість протиправної поведінки
- профілактичний облік
- адміністративний нагляд органів внутрішніх справ
- соціальний патронаж осіб, які відбували покарання у виді обмеження волі або її позбавлення на певний строк, та осіб антисуспільної спрямованості

Застосування заходів індивідуальної профілактики не сумісне з приниженням честі й гідності особи, а також не тягне правових наслідків, за винятком передбачених законодавством.

Профілактична бесіда проводиться за наявності інформації про те, що особа вчинила протиправні дії, з метою роз'яснення суспільної небезпечності та усного попередження про неприпустимість протиправних і антигромадських дій, що посягають на громадський порядок і громадську безпеку, а також на встановлений порядок управління.

- Для цього особа викликається до відповідного органу внутрішніх справ чи Служби безпеки України за місцем проживання або роботи.
- Роз'яснення та усне попередження має характер заходу індивідуальної профілактики, якщо воно зроблене службовою особою органу внутрішніх справ чи Служби безпеки України, яка має відповідні повноваження, зі складанням про це письмової довідки.
- У разі неявки правопорушника без поважних причин до органу внутрішніх справ чи служби безпеки за викликом для роз'яснення суспільної небезпечності поведінки та усного попередження про неприпустимість протиправних і антигромадських дій, його може бути піддано приводу.
- Поважними причинами неявки визнаються несвоєчасне одержання повістки, хвороба чи інші обставини, що практично позбавляють можливості своєчасно прибути за викликом.
- Привід здійснюється в денний час, за мотивованою постановою, затвердженою начальником органу, який має намір роз'яснити суспільну небезпечність поведінки та усно попередити про неприпустимість протиправних і антигромадських дій, або його заступником чи начальником територіального підрозділу цього органу. Постанова про привід оголошується особі, щодо якої він має бути застосований.

5.5. Внутрішнє шахрайство на підприємстві та шляхи його виявлення

Жертвою корпоративного шахрайства може стати будь-яке підприємство, незалежно від сфери управління, виду діяльності та країни розташування.

Через інтернаціональність і варіативність способів шахрайських дій, до яких вдаються працівники, стає очевидним, що вжиття заходів запобігання шахрайству на підприємстві є одним із ключових завдань власника бізнесу.

З іншого боку, реалії українського підприємництва є такі, що власник зазвичай активно залучений до операційного управління підприємством і в нього дуже часто створюється ілюзія, що, здійснюючи тотальний контроль за співробітниками, змінюючи тактики й стратегії керування бізнесом, підприємству вдасться уникнути долі жертви шахрайських дій.

Шахрайство

- зовнішнє → здійснюване щодо підприємства контрагентами або третіми особами
- внутрішнє → здійснюване безпосередньо працівниками самого підприємства

При цьому внутрішнє шахрайство значно більше впливає на підприємство, якщо брати до уваги втрату репутації та клієнтів, що рано чи пізно відбувається на підприємстві, де «крадуть».

Шахрайство у вузькому розумінні, згідно з правовою кваліфікацією Кримінального кодексу України (далі – КК України), кваліфікують як дію, спрямовану на заволодіння чужим майном або на набуття права на майно за допомогою обману чи зловживання довірою.

Корпоративне шахрайство – дещо ширше поняття. Сюди, відповідно до КК України, доречно зарахувати й інші злочини проти власності підприємства (інтелектуальна власність та інші немайнові права підприємства також можуть бути об'єктом шахрайських дій).

Причини шахрайства працівників на підприємстві вельми різноманітні.

Дехто називає однією з основних причин шахрайства недостатність фінансової мотивації працівника, що не відкидає шахрайських дій керівництва підприємства.

Хтось одну з основних причин убачає у девіантній поведінці, тобто схильності працівника, який має справу з фінансовими ресурсами, до вчинення злочину.

За соціологічною теорією злочинності для вчинення злочину потрібні три умови:

– воля вчинити злочин, яка залежить від моральності людини;
– сприятливі умови для злочинної діяльності;
– можливість використовувати ці умови.

У будь-якому разі зі складу ніколи нічого просто так не пропадає, завжди для цього потрібен помічник, котрий має необхідні владні повноваження. Найліпший вид попередження таких злочинів – чіткий розподіл обов'язків, наприклад, підпису тільки комірника не повинно бути достатньо для видачі зі складу цінностей.

Деякими несумлінними громадянами крадіжка за місцем роботи розглядається як законний підробіток. Особливо характерно це у сфері будівництва.

Багато «бізнесменів» погано розуміють, наскільки цінні ті або інші відходи виробництва і якими збитками їм загрожує поганий контроль за їх видаленням і переробкою. В ході практично будь-якого виробництва завжди утворюються якісь відходи. Крім того, частина продукції бракується. Досить часто такі відходи і брак зберігаються протягом якогось часу на стихійних складах, чекаючи утилізації.

Розкрадання зазвичай трапляються саме в період зберігання, якщо охорона цих субпродуктів або бракованих виробів не організована. Проте навіть в тому випадку, якщо керівництво усвідомлює дійсну їх цінність і здійснює щодо них операції з іншими організаціями, ці відходи і брак під час зберігання не охороняються, оскільки часто вважається, що тільки сторонні переробні організації можуть вилучати з них споживчу цінність.

Чимало фірм дозволяють працівникам купувати свої вироби за ціною собівартості. Вважається, що це добре впливає на морально-психологічний стан працівників, дає можливість їм заощадити і підвищити свій добробут.

При реалізації таких схем можливі зловживання, пов'язані з тим, що працівники, які купують багато дешевих виробів (від туалетного приладдя, продуктів харчування, іграшок до меблів), легко відшукують канал їх постійного збуту, користуючись тим, що ціна товару набагато нижча від роздрібної. Працівники швидко з'ясовують вигоди таких покупок, і те, що починається як позика для членів сім'ї або друзів, незабаром стає джерелом додаткового заробітку для не дуже педантичних громадян.

Витрати грошей, отриманих на підзвітну суму, як ніякі інші схильні до шахрайських махінацій з боку персоналу. Як правило, їх строго контролюють. Але в цілому практика скоювання подібних злочинів багато в чому залежить від загальної атмосфери, що панує в компанії, від того, чи вважаються серед співробітників спроби поживитися за рахунок компанії нормальними або абсолютно неприпустимими.

Слабкості і пристрасть до наживи властиві не тільки пересічним працівникам, а й тим, хто перебуває на чолі окремих підрозділів, відділів і крупніших структурних підрозділів. Тут можна повторити все, що вже було сказане вище, з обмовкою, що відсутність належного контролю за роботою цього персоналу загрожує значно крупнішим збитком, ніж діяльність рядових працівників. Крім загальних «правил крадіжки» з підприємств, якими керуються взагалі всі шахраї, є деякі види злочинів, які є привілеєм тільки «великих» (або невеликих) начальників.

Зокрема, на одному з м'ясокомбінатів, де фраза «Приготуйте швиденько зразок для дослідження в лабораторії» стала своєрідним паролем для безвідплатного вилучення м'ясних виробів. Саме так постійно говорив заступник начальника цеху, вказуючи на конвеєрі на один або два відмінні шматки м'яса. Дуже скоро всім стало відомо, що до перевірочного столу жоден зразок так і не дійшов. Після цього будь-хто, кому треба було м'яса, супроводжував крадіжку словами начальника.

Роботодавцеві варто звернути увагу на такі ознаки, що характеризують можливе вчинення шахрайства:

- нестандартні (викривлені) дані в бухгалтерських документах;
- відхилення від нормальних значень величин або показників;
- нетиповий для стандартного доходу співробітника спосіб його життя;
- незвична поведінка співробітника;
- надходження сигналів і скарг на співробітника, зокрема й від контрагентів.

Оскільки існує величезна кількість видів і форм підприємницької діяльності, то є й така сама немислима кількість видів шахрайських дій співробітників, класифікувати які немає сенсу через різноманітність і «фантазії» виконавців. Окрім цього, не всі протиправні дії працівників доречно класифікувати як шахрайські.

Шахрайські дії обов'язково мають містити:

- намір на заволодіння чужим майном;
- вилучення та (або) звернення цього майна на користь винного чи інших осіб;
- протиправність (очевидне розуміння працівником незаконності своїх дій);
- безоплатність;
- завдання збитку власнику чи іншому володільцю;
- корисливу мету (зазвичай щоб поліпшити власний добробут).

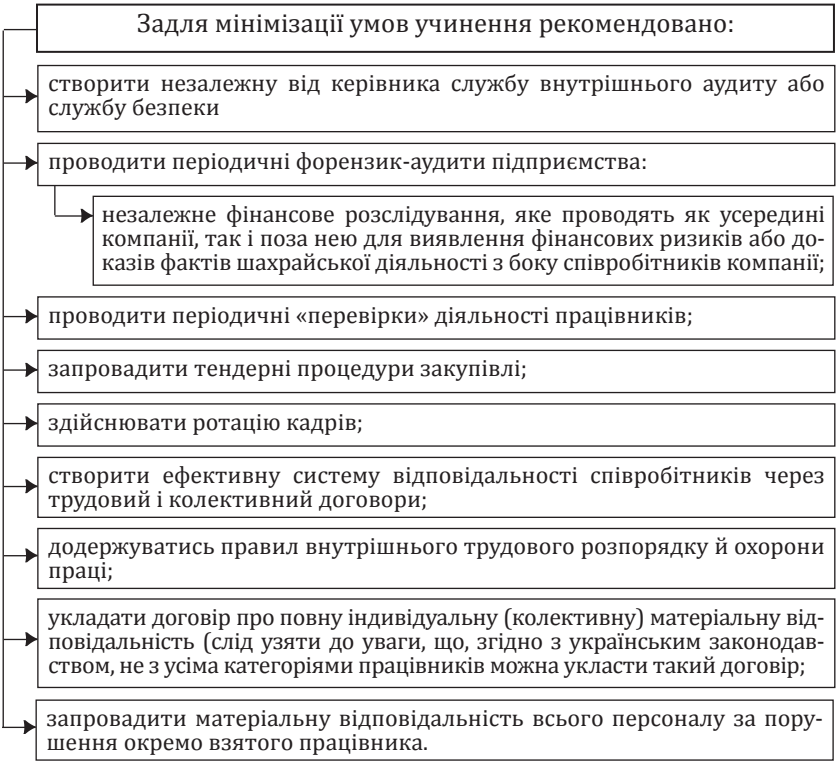
Серед найпоширеніших схем шахрайства – придбання товарів і послуг, яких не існує, надання благодійної допомоги, різноманітні виплати формально не пов'язаним компаніям, а також взаємодія з держорганами через посередників, реалізація інвестиційних проектів, непрозора структура маркетингових витрат, «відкати» за послуги, надані компанії.

Заходи захисту потрібно впроваджувати за двома основними напрямами:

1) мінімізація причин учинення шахрайства;

2) мінімізація умов для вчинення шахрайства.

В інтересах мінімізації причин учинення доцільно підвищувати фінансову мотивацію співробітників, створювати атмосферу соціальної значущості кожного співробітника, що не залишає місця для думок про вчинення якихось правопорушень, подавати загальний приклад керівником. Також дуже важливо викорінювати схеми непрозорого бухгалтерського обліку на підприємстві, можливих фінансових маніпуляцій (наприклад, підписання чистих бланків підприємства «про запас», завищення вартості послуг).



Усі перелічені вище заходи працюватимуть лише в комплексі зі здоровою корпоративною культурою та за умови, що виявлення шахрайства не буде єдиною ціллю власника підприємства. Також потрібно не забувати, що подолати шахрайство стовідсотково неможливо, але розслідувати й виявляти передумови – життєво необхідно для ефективності бізнесу.

Питання для обговорення

1. Хто організовує захист від протиправних дій працівників?
2. Які особливості попередження і виявлення протиправних дій працівників?
3. Як нейтралізувати протиправні дії працівників?
4. Які особливості розслідування внутрішнього та зовнішнього шахрайства на підприємстві?
5. Поясніть сценарні конфлікти на підприємствах і надійність персоналу.
6. Яка роль темпераменту працівника в конфліктології?
7. Кого відносять до основних груп ризику та конфліктів на підприємстві?
8. Як здійснюється захист від протиправних дій працівників?
9. Як виявити і попередити протиправні дій працівників?
10. Перелічіть внутрішні і зовнішні джерела небезпеки для працівників.
11. Які контрольні заходи вживаються для попередження загроз від персоналу?
12. Як належить звільняти працівників?
13. Роз'ясніть забезпечення безпеки підприємства у процесі звільнення працівника.
14. Які особливості звільнення працівника за власним бажанням?
15. Які особливості звільнення працівника за ініціативою адміністрації?
16. Як забезпечити нерозголошення комерційної таємниці звільненими працівниками?
17. Які особливості мотивації персоналу?
18. Чим відрізняється мотивація від стимулювання?

Домашні завдання

Завдання. 1. Розробити карту ризиків для підприємства з боку персоналу.

Завдання 2. Розробити карту ризиків для персоналу щодо його ненадійності на підприємстві.

Завдання 3. Здійснити аналіз існуючих методик оцінювання надійності персоналу. Запропонувати власну методику оцінювання стану надійності персоналу підприємств, установ, організацій. За авторською методикою провести діагностику стану надійності персоналу служби безпеки підприємства.

Завдання 4. Підготувати наказ про звільнення працівника.

Завдання 5. Провести дослідження найрезонансніших випадків звільнення персоналу та встановити його наслідки цього для суб'єкта господарювання.

Ситуація 1. «Умови та вигода залишити працівника, що не пройшов атестацію».

Ситуація 2. «Дії кадрового апарату за умови, якщо рівень професійної кваліфікації співробітника суттєво перевищує вимоги посади, яку він займає».

Ситуація 3. «Дії служби безпеки за умови крадіжок власних речей персоналу».

Ситуація 4. «Дії служби безпеки за умови крадіжок МТЦ підприємства».

Ситуація 5. «Керівник вважає, що він та його підприємство не залежать від обставин».

Ситуація 6. «Керівник повністю ототожнює себе з підприємством, втрачаючи здатність відрізняти особисті інтереси від корпоративних».

Ситуація 7. «Керівник вважає, що він знає відповіді на всі питання».

Ситуація 8. «Керівник без докорів сумління звільняє всіх працівників, які стовідсотково не погоджуються з його позицією».

Рекомендована література: 1, 2, 3, 5, 7, 11–14, 15–17, 20–31, 33–43, 48–52, 56–72.

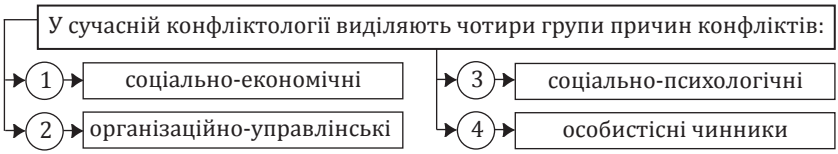
Тема 6
КОНФЛІКТИ НА ПІДПРИЄМСТВАХ І ЇХНІЙ ВПЛИВ НА СТАН НАДІЙНОСТІ ПЕРСОНАЛУ

6.1. Причини та учасники конфліктів.
6.2. Способи вирішення конфліктів.
6.3. Основні групи ризику й типи конфліктів на підприємстві.

Ключові поняття: конфлікт, причини конфліктів, способи вирішення конфліктів, групи ризику, конфліктні ситуації, соціальні суб'єкти, організаційно-управлінські конфлікти, особисті чинники.

6.1. Причини та учасники конфліктів

Для попередження, подолання або конструктивного вирішення конфліктів варто знати їх причини.



2 Організаційно-управлінські причини конфліктів

структурно-організаційні	помилки в розробці організаційної структури органів управління та її невідповідність завданням, що вирішуються; неоднакова технічна оснащеність робочих місць, що знижує темп роботи; проблеми у владних структурах – невідповідність прав і обов'язків, компетенції та відповідальності тощо
функціонально-організаційні	неоптимальні функціональні зв'язки підприємств зі зовнішнім середовищем, між їх структурними підрозділами; неправильний розподіл відповідальності між співробітниками; обмеженість ресурсів, які потрібно ділити між окремими підприємствами й окремими працівниками; відсутність, викривленість або суперечливість інформації; слабкість контактів керівництва з рядовими співробітниками
особистісно-функціональні	неповна відповідність працівника посаді за моральними, професійними або іншими якостями; суперечливість вимог у змісті посадових інструкцій; відмінність формальних професійних і особистих вимог керівництва до окремих працівників
ситуативно-управлінські	помилки в ухваленні та виконанні управлінських рішень

3 Соціально-психологічні причини конфліктів

- зникнення та перекручення інформації в процесі міжособис-тісного та міжгрупового спілкування → відсутність словарного запасу, обмаль часу для спілкування, недостатність уваги до співрозмовників
- існування різних способів оцінки результатів діяльності (існує п'ять способів оцінки):
  1) порівняння досягнутих результатів з ідеальним станом справ;
  2) порівняння діяльності з нормативними вимогами;
  3) порівняння ступеня досягнення мети діяльності з результатами, досягнутими іншими людьми при виконанні тієї ж діяльності;
  4) оцінка залежності результатів діяльності від ставлення до справи;
  5) порівняння досягнутих результатів зі станом справ на початку діяльності (при цьому, оцінюючи інших, люди використовують способи 1–3, оцінюючи ж себе – 4 і 5).
- природне зіткнення інтересів людей у процесі їхньої життєдіяльності
- прагнення окремих особистостей до влади або намагання інших більше отримувати і поменше працювати;
- конфлікт між ціннісними орієнтаціями: свободою та жорсткою дисципліною, справедливістю і несправедливістю, колективізмом та індивідуалізмом, ксенофобією і спрямованістю до використання досягнень світової спільноти, демократією й авторитарністю, прагненням до суспільної власності та відстоюванням особистої приватної власності
- психологічна несумісність членів одного колективу

4 **Особистісні чинники конфліктів**

Конфлікти здебільшого зумовлюються розбіжностями в ціннісних орієнтаціях, цілях, мотивах, інтересах та потребах учасників конфліктів.

Ці розбіжності можуть бути найрізноманітнішими і стають однією з основних причин конфліктів, визначаючи лінію поведінки учасників конфлікту, його стратегію і тактику.

Іншою важливою причиною конфлікту може бути незбігання характерів індивідів.

Якщо холерика і меланхоліка, яким властива емоційна нестабільність, відправити на тривалий час у космос на одному космічному кораблі, то конфлікту їм не уникнути.

Значну роль у виникненні й розвитку конфліктів відіграють неадекватні уявлення, оцінки і самооцінки. Особливо часто вони є причиною конфліктної поведінки в діловому спілкуванні, де не можна застосувати тактику уникнення.

Вагомою причиною конфлікту в цьому контексті є розрив між очікуваним і реальним результатом.

Основними особистісними причинами конфліктів виступають: суб'єктивна оцінка поведінки партнера як неприпустимої; низька конфліктостійкість; поганий розвиток емпатії; неадекватний рівень домагань; акцентуації характеру та ін.

Тому як завищена, так і занижена самооцінка, що пов'язана з неправильним уявленням про свої можливості та місце в групі, спричинятиме постійні непорозуміння й напруженість.

Відмінності в манерах поведінки можуть також стати причиною конфлікту, бо зменшують ступінь взаєморозуміння між людьми.

Груба і безцеремонна людина постійно вступатиме в конфлікт з тими, хто її оточує.

Не меншу небезпеку становить й інший тип – «вибухова людина».

Вона не є злою за своєю природою, але вибухає – як дитина, в якої зненацька зіпсувався настрій. Тому від неї завжди можна чекати неприємностей.

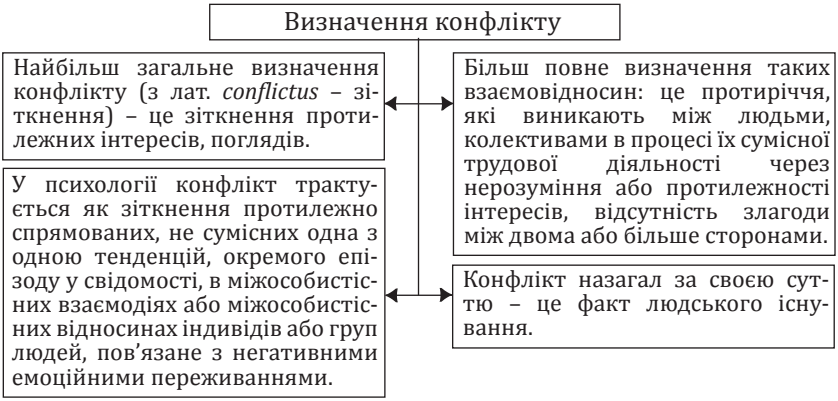
Багато неприємностей у спілкуванні можна чекати і від такого типу важких людей, як «мовчуни».

Ці люди також є потенційно небезпечними стосовно виникнення конфлікту, бо причини їхньої скритності стороннім не відомі.

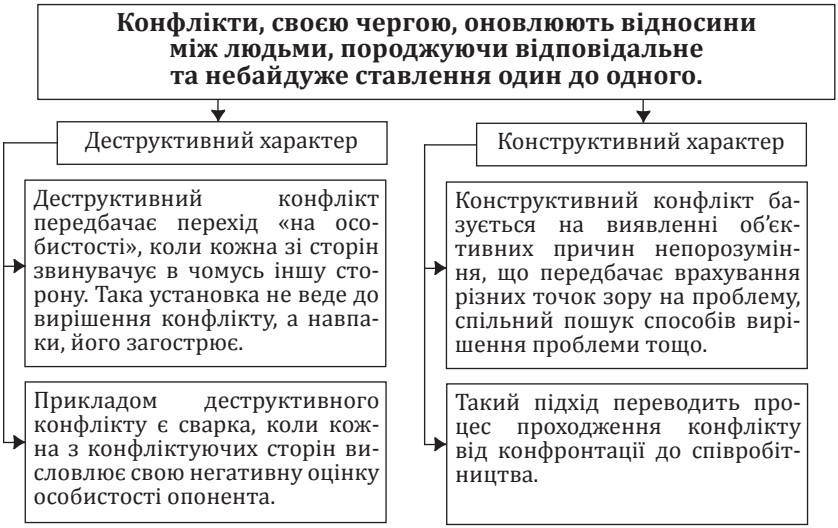
Велику небезпеку становить і такий тип, як «занадто поступливий».

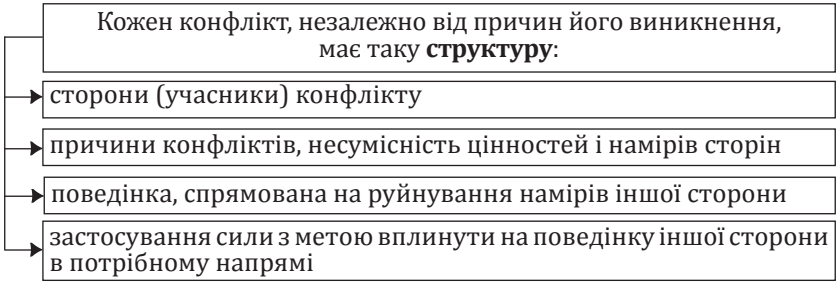
Такі люди можуть не створювати проблем у суто людських відносинах, бо вони завжди й усім поступляться і пообіцяють допомогти в будь-якій справі. Однак щойно доходить до виконання обіцянки, вони можуть створити вам труднощі, бо їхні слова часто розходяться з ділом.

6.2. Способи вирішення конфліктів

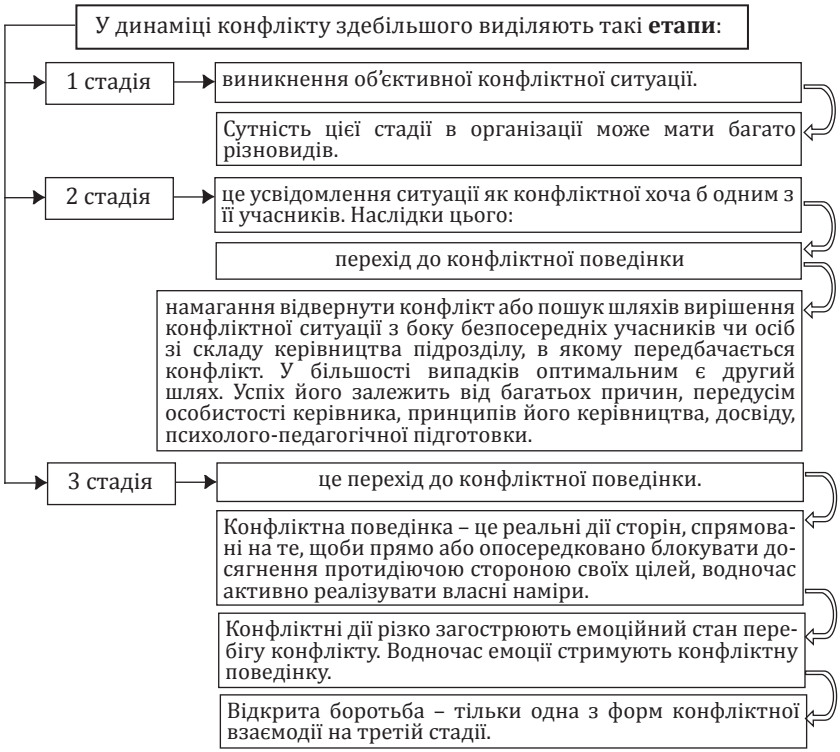


Більшість людей сприймають історію людства як безкінечну розповідь про конфлікти і боротьбу. Виникнення конфліктів є об'єктивним і неминучим явищем. Адже життя – це постійний діалектичний процес, в ході якого постійно виникають нові проблем та з'являються нові варіанти їх вирішення.





Будь-який реальний конфлікт розвивається в часі, тобто це процес. У широкому розумінні динаміка конфлікту – це послідовна зміна певних стадій і станів, які характеризують процес від виникнення конфліктної ситуації до розв'язання конфлікту.



В основі співробітництва, з одного боку, лежить повага до себе, почуття власної гідності, чесність, намагання знайти справжню причину конфлікту, а з іншого, повага до інших, товариськість, визнання права інших на власну точку зору, позицію. Така поведінка в конфлікті призводить до глибшого

розуміння проблеми, взаємодовіри, готовності зрозуміти один одного і зрештою – вирішення (залагодження) конфлікту.

Існує декілька способів (стратегій) вирішення конфліктів:

Способи (стратегії) вирішення конфліктів

Ухиляння	мається на увазі, що людина здатна передбачати наперед та уникати дій, які провокуватимуть загострення конфліктної ситуації. Така роль пасивного спостерігача притаманна особам, які не зацікавлені у змінах та прагнуть уникнути загострення суперечностей.
Згладжування	це тип поведінки, який має багато спільного з попереднім. При цьому людиною не помічаються ознаки майбутнього конфлікту, йде активна профілактика його вияву, ліквідовуються чи завуальовуються суперечності сторін.
Примус	контроль над ситуацією і регулювання її розвитку. В разі небажаного напряму розвитку конфлікту особа, яка наділена владою і повноваженнями, втручається і силовими методами впливає на ситуацію, спрямовуючи конфлікт у бажане русло.
Компроміс	тимчасове чи нейтральне вирішення проблеми, що умовно задовольняє всі сторони, які беруть участь у конфлікті. Суперники (опоненти) йдуть на взаємні поступки, частково приймають точку зору іншої сторони або ж відкладають вирішення питання на майбутнє, залишаючи його відкритим.
Розв'язання конфлікту	найбільш бажаний і радикальний шлях розвитку ситуації. Сторони детально ознайомлюються з аргументацією як «за», так і «проти», йдуть на взаємні поступки, складні питання вирішують спільним прийняттям рішень.

Стиль компромісу вибирають здебільшого у таких випадках:

- коли проблема порівняно проста і зрозуміла
- коли для вирішення конфлікту нема багато часу і хочеться погасити його якомога швидше
- тоді, коли краще досягнути швидко тимчасової угоди, а потім «повернутися» до цієї проблеми знову і проаналізувати приховані причини
- коли для двох сторін їхні інтереси дуже важливі
- коли не вдалося досягнути розв'язання вдавшись до співпраці або не вдалося досягнути бажаного з застосуванням своєї влади.

Ця норма конфліктної взаємодії досліджена найповніше з огляду на практичну значимість виявлення чинників і умов, які сприяють успіху перемовин.

6.3. Основні групи ризику й типи конфліктів на підприємстві

Конфлікт у колективі є суперечкою, яка виникає між людьми внаслідок розбіжностей у їхніх інтересах, поглядах, установках, домаганнях. У діяльності виробничого колективу конфлікти можуть бути найрізноманітнішими, але завжди проявляються як взаємна протидія особистостей, активне їх зіткнення.

Під **конфліктною ситуацією** слід розуміти збіг передумов, умов і причин (потенційного) конфлікту. Це така напружена ситуація, яка може «перерости» у відкритий конфлікт.

В основі кожного конфлікту, незалежно від рівня його перебігу, є:

організаційні причини

Це різновид конфліктів, які виникають у колективі внаслідок неузгодженості формальної організаційної поведінки і реальної поведінки членів колективу:

- по-перше, якщо працівник з якихось причин не виконує, ігнорує вимоги, які ставить до нього організація (порушує дисципліну, неякісно виконує свої обов'язки тощо);
- по-друге, якщо вимоги, котрі ставлять перед працівником, нечіткі, неконкретні, суперечливі, (низька якість посадових інструкцій, непродуманий розподіл посадових обов'язків, недостатнє організаційне забезпечення та ін.).

виробничі причини

виробничий конфлікт здебільшого виникає в колективі, де є низький рівень організації праці й управління.

Причинами такого конфлікту може бути морально застаріла техніка, обладнання, не пристосоване до нормальної роботи приміщення, дефіцит нової техніки (конфлікт між водіями, зумовлений дефіцитом нових автомашин тощо).

міжособистісні причини

з огляду на суб'єкти конфлікту існують такі типи (види) конфліктів:

внутрішньоособистісний – сторонами конфлікту виступають дві або більше складових тієї самої особистості;

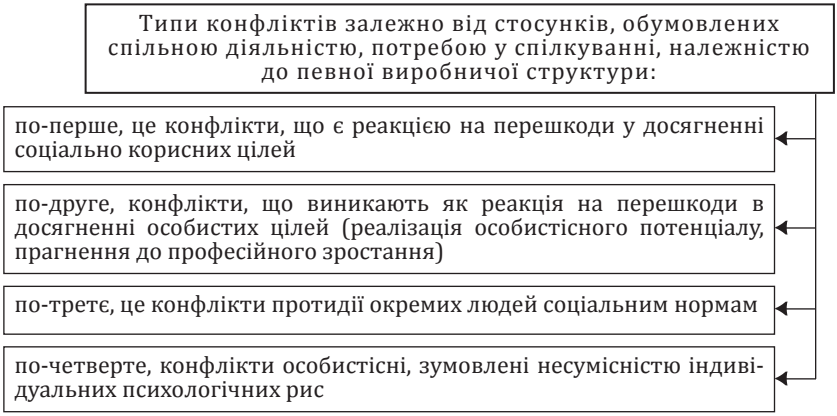
міжособистісний – конфронтація з приводу потреб, мотивів, цілей, цінностей між окремими особами;

особистісно-груповий – невідповідність норм поведінки, цінностей, цілей індивіда та групи;

міжгруповий – зіткнення норм поведінки, цінностей, цілей різних груп.

Шість типів конфлікту

Реальний конфлікт	це конфлікт, який об'єктивно існує й адекватно сприймається
Випадковий, або умовний, конфлікт	залежить від обставин, що можуть змінюватися, але ці обставини не усвідомлюються конфліктуючими сторонами
Зміщений конфлікт	це реальний конфлікт, за яким приховується інший, що є справжнім чинником конфліктуючої сторони
Помилково дописаний конфлікт	конфлікт, що помилково тлумачиться
Латентний конфлікт	конфлікт, який має відбутися, але не виникає тому, що не усвідомлюється
Хибний конфлікт	у цьому разі реальних підстав для конфлікту не існує, об'єктивно його немає, але він виникає у свідомості конфліктуючих сторін через помилкове сприймання та розуміння ситуації



Основними завданнями кадрової служби з удосконалення кадрової безпеки підприємства є:

– участь у формуванні кадрової стратегії компанії, процесах планування людських ресурсів, інформаційній, фінансовій політиці, розвитку й оцінці персоналу;

– складання нормативної документації для співробітників організації в інтересах дотримання кадрової безпеки;

– проведення інформаційно-роз'яснювальної роботи зі співробітниками організації;

– проведення заходів, спрямованих на недопущення осіб до зайняття посад, зловживаючи якими вони можуть завдати своїми діями шкоду підприємству;

– здійснення моніторингу, спрямованого на забезпечення кадрової безпеки підприємства.

Питання для обговорення

1. У чому полягає сутність конфлікту?
2. Назвіть види конфліктів.
3. Поясніть суть соціально-економічних причин конфліктів.
4. Поясніть суть організаційно-управлінських причин конфліктів.
5. Поясніть суть соціально-психологічних причин конфліктів.
6. Поясніть суть особистісних чинників конфліктів.
7. Які відмінності в манерах поведінки можуть стати причиною конфлікту?

8. Перелічіть способи вирішення конфліктів.
9. Наведіть визначення конфлікту.
10. Яка сутність деструктивного характеру конфліктів?
11. Яка сутність конструктивного характеру конфліктів?
12. У чому сутність динаміки конфлікту?
13. Назвіть етапи динаміки конфлікту.
14. Назвіть способи (стратегії) вирішення конфліктів.
15. Який стиль компромісу?
16. Охарактеризуйте типи корпоративних конфліктів.
17. Що розуміється під конфліктною ситуацією?
18. Які шість типів конфліктів вам відомі?
19. Роз'ясніть завдання служби кадрової безпеки.

Домашні завдання

Завдання 1. Підготовка до переговорів: визначення мети, стратегії і тактики переговорів; аналіз учасників переговорів, підготовка групи до переговорів; планування ходу переговорів.

Особистісні риси, вміння і навички учасників переговорів. Уміння слухати і переконувати. Вміння сказати «ні». Вміння «читати» інтонації, жести, міміку партнерів. Прийоми, що можуть покращити взаємини в перемовинах. Підготовка місця для ведення переговорів. Ведення переговорів.

Етапи переговорів: діагностичний, визначення загальних рамок угоди; спільного пошуку рішень; прийняття рішень; складання угоди.

Завдання 2.

І. Спірні питання. Які спірні питання в конфлікті? Яким чином вони змінюються з часом? Чи збільшується їх кількість?

1.1. Чи розуміють сторони суть спірних питань?

1.2. Чи є у сторін єдність думок (якщо є, чи знають вони про це) стосовно ключових питань конфлікту?

ІІ. Основні учасники (сторони) конфлікту. Хто є конфліктуючими сторонами?

2.1. Які їхні офіційні стосунки (керівник-підлеглий, чоловік-дружина, друзі з однаковим статусом)? Як характер цих стосунків впливає на конфлікт?

2.2. Яка історія стосунків? Були вони дружніми, чи ні? Чи є у сторін проблеми, не вирішені раніше? Чи впливають вони на цей конфлікт?

ІІІ. Інші учасники (сторони).

Чи намагаються основні учасники залучити до свого конфлікту інших осіб? Чи вдалі ці спроби?

Завдання 3. Уявіть себе оратором, що пропагує новий науковий напрямок – психологію менеджменту. На цій підставі складіть тези свого публічного виступу серед колег по роботі (колектив до 10 осіб).

1. Під час виконання роботи:
– наведіть визначення поняття «психологія», її засновника;
– назвіть періоди формування психології управління;
– визначте об'єкт і предмет психології;
– наведіть основні складові напрями формування загальної психології;
– з'ясуйте, які основні риси притаманні психології менеджменту.

Завдання 4. 1. Уявіть себе оратором, що пропагує новий науковий напрямок – психологію менеджменту. На цій підставі складіть тези свого виступу по радіо;

2. Під час виконання роботи:
– наведіть визначення поняття «психологія», її засновника;
– назвіть періоди формування психології управління;
– визначте об'єкт і предмет психології;
– наведіть основні складові напрями формування загальної психології;
– з'ясуйте, які основні риси притаманні психології менеджменту.

Завдання 5. 1. Уявіть себе розробником нового наукового напряму – психології управління людиноповедінкою. На цій підставі сформулюйте тези представлення нового напряму невідомій аудиторії (100 і більше осіб).

1. Під час виконання роботи:
– визначте основні школи психології;
– окресліть фундаментальні та спеціальні галузі психології;
– перелічіть основні підходи до визначення предмета психології управління;
– охарактеризуйте поняття «організована діяльність», роль і місце психології в управлінні нею;
– з'ясуйте, які основні риси притаманні управлінню людиноповедінкою.

Рекомендована література: 1–8, 10–21, 25–33, 35–45, 48–56, 58–63, 68–73.

Список рекомендованої літератури та електронних джерел

1. Аутплейсмент в Україні. URL: http://speshiall.blox.ua/2010/06/AUTPLEJSMENT-V-UKRAYiNI.html
2. Бандурка О. М., Духов В. Є., Петрова К. Я., Червяков І. М. Основи економічної безпеки: підручник. Харків: Вид-во Нац. ун-ту внутр. справ, 2003. 36 с.
3. Васенко В. К., Пуш Л. А., Шульга І. П., Зачосова Н. В., Герасименко О. М. Економічна безпека держави, суб'єктів господарювання та тіньова економіка: кол. монографія / за заг. ред. В. К. Васенка. Черкаси: Вид-во ТОВ «Маклаут», 2010. 367 с.
4. Васильців Т. Г., Волошин В. І., Бойкевич О. Р., Каркавчук В. В. Фінансово-економічна безпека підприємств України: стратегія та механізми забезпечення: монографія / за ред. Т. Г. Васильціва. Львів, 2012. 386 с.
5. Веретенникова Г. Б. Економічна безпека підприємства: планування й організація: конспект лекцій. Х.: ХНЕУ, 2008. 83 с.
6. Васильців Т. Г. Економічна безпека підприємництва України: стратегія та механізми зміцнення: монографія. Львів: Арал, 2008. 384 с.
7. Видрін Д. Концепція стратегії безпеки. Україна у посттоталітарний період. *Розбудова держави*. 2005. № 5. С. 36–41.
8. Герасименко О. М. Індикатори оцінки стану системи економічної безпеки торговців цінними паперами: монографія. Черкаси: ТОВ «Маклаут», 2011. 250 с.
9. Головатий М. Ф., Панасюк М. Б. Соціальна політика і соціальна робота: термінологічно-понятійний словник. К.: МАУП, 2005. 560 с.
10. Губарев О. О. Економічна безпека: конспект лекцій. Х.: ХНЕУ, 2007. 59 с.
11. Донець Л. І., Ващенко Н. В. Економічна безпека підприємства: навч. посіб. для студ. ЗВО. К.: ЦУЛ, 2008. 239 с.
12. Драчёв С. С. Основы корпоративной безопасности. СПб.: ООО Изд-во «Полигон», 2000. 240 с.

13. Духов В. Л. Экономическая разведка и безопасность бизнеса. К.: НВФ «Студцентр», 1997. 176 с.

14. Економічна безпека в умовах глобалізації світової економіки: кол. монографія: у 2 т. Дніпропетровськ: ФОП Дробязко С. І., 2014. Т. 2. 349 с.

15. Економічна безпека: навч. посібник. / В. І. Франчук, Л. В. Герасименко, В. О. Гончарова, З. Б. Живко та ін.; за ред. В. І. Франчука. Львів: Вид-во ЛьвДУВС, 2010. 244 с.

16. Економічна безпека: навч. посібник / за ред. З. С. Варналія. К.: Знання, 2009. 647 с.

17. Економічна безпека підприємств, організацій та установ: навч. посіб. для студ. ЗВО / В. Л. Ортинський, І. С. Керницький, З. Б. Живко та ін.. К.: Правова єдність, 2009. 544 с.

18. Економічна безпека держави: навч.-метод. посіб. / З. Б. Живко, О. В. Черевко, М. І. Копитко, Н. В. Зачосова, М. О. Живко, В. В. Середа, В. О. Занора, А. В. Бієвець; за ред. З. Б. Живко. Черкаси: вид. Чабаненко Ю. А., 2019. 240 с.

19. Економічна безпека підприємств: підручник. / В. Л. Ортинський, І. С. Керницький, З. Б. Живко та ін. К.: Алерта, 2011. 704 с.

20. Єпіфанов А. О., Пластун О. Л., Домбровський В. С. Фінансова безпека підприємств і банківських установ: монографія. Суми: ДВНЗ «УАБС НБУ», 2009. 295 с.

21. Єрмошенко М. М. Економічні та організаційні засади забезпечення фінансової безпеки підприємства: препринт наукової доповіді / за ред. М. М. Єрмошенка. К.: Нац. академія управління, 2005. 77 с.

22. Живко З. Б., Сватюк О. Р., Копитко М. І. Корпоративне управління в системі економічної безпеки: навч. посіб. / за заг. ред. З. Б. Живко. Львів: ЛьвДУВС, 2018. 456 с.

23. Живко З. Б. Методологія управління економічною безпекою підприємства: монографія. Львів: Ліга-Прес, 2013. 474 с.

24. Живко З. Б. Рейдерство: фермент ринкової економіки: монографія. Львів: Ліга-Прес, 2009. 270 с.

25. Живко З. Б. Розвідувальна діяльність як функція економічної безпеки підприємства // Соціально-економічний розви-

ток держави, регіону, підприємства в нестабільних ринкових умовах: монографія / З. Б. Живко, С. Б. Князь, В. І. Ляшенко, Н. В. Осадча та ін.; за заг. ред. А. М. Штангрета, А. П. Левітської. Львів: УАД, 2015. С. 372–400.

26. Живко З. Б., Керницька М. І. Соціально-економічна безпека: навч. посіб. для самостійного вивчення дисципліни. Львів: Ліга-Прес, 2008. 345 с.
27. Живко З. Б. Управління системою економічної безпеки підприємства: навч. посіб. Львів: ЛьвДУВС, 2016. 212 с.
28. Живко З. Б. Управління змінами: навч. посіб. Львів: ЛьвДУВС, 2016. 252 с.
29. Живко З. Б. Управлінські інформаційні системи в обліку, аналізі та аудиті: навч. посіб. / В. С. Рудницький, Т. В. Давидюк, С. М. Деньга, І. І. Стецiв, З. Б. Живко. К.: УБС НБУ, 2015. 242 с.
30. Захаров О. І. Організація та управління економічною безпекою суб'єктів господарської діяльності: навч. посіб. К.: КНТ, 2008. 257 с.
31. Зачосова Н. В. Управління системою економічної безпеки фінансових посередників: компанії з управління активами: монографія. Черкаси: Вертикаль: вид. Кандич С. Г., 2011. 240 с.
32. Кавун С. В. Система економічної безпеки: методологічні та методичні засади: монографія. Х.: ХНЕУ, 2009. 299 с.
33. Кавун С. В., Пилипенко Д. О., Репко А. А. Економічна та інформаційна безпека підприємств у системі консолідації інформації: навч. посіб. Х.: В-во ХНЕУ, 2013. 264 с.
34. Кадрова безпека суб'єктів господарської діяльності: менеджмент інсайдерами / за заг. ред. І. П. Мігус. Черкаси: Маклаут, 2012.
35. Кавун С. В. Информационная безопасность в бизнесе: монография. Х.: ХНЭУ, 2007. 408 с.
36. Каламбет С. В., Воропай В. А. Економічна безпека підприємства. К.: Основа, 2008. 224 с.
37. Камлик М. І. Економічна безпека підприємницької діяльності: економіко-правовий аспект: навч. посіб. К.: Атіка, 2005. 432 с.
38. Керницький І. С., Живко З. Б., Копитко М. І. Конкурентна розвідка підприємств: курс лекцій. Львів: Ліга-Прес, 2015. 388 с.

39. Козаченко Г. В., Пономарьов В. П., Ляшенко О. М. Економічна безпека підприємства: сутність та механізм забезпечення: монографія. К.: Лібра, 2003. 280 с.

40. Концепции безопасности. Кн. 1 / С. А. Буришев, И. В. Лутаев, С. Л. Прохоров. К.: А-ДЕПТ, 2005. 363 с.

41. Копан О. В. Забезпечення внутрішньої безпеки України: теоретико-управлінські засади. Введення в поліцейську стратегію: монографія. К.: НАВСУ, 2001. 424 с.

42. Куркін М. В., Понікаров В. Д., Назаренко Д. В. Контроль та захист економічної безпеки діяльності підприємства: навч. посіб. Х.: ІНЖЕК, 2010. 297 с.

43. Менеджмент безпеки масових заходів: конспект лекцій / М.Й.Штангрет, І.С.Керницький, М.І.Копитко, З.Б.Живко; за заг. ред. М. І. Копитко. Львів: Ліга-Прес, 2012. 170 с.

44. Менеджмент безпеки персоналу: конспект лекцій / З. Б. Живко, Л. М. Томаневич, В. С. Дудюк, М. І. Копитко, С. М. Лихолат; за заг. ред. З. Б. Живко. Львів: Ліга-Прес, 2012. 204 с.

45. Менеджмент безпеки персоналу: навч. посіб. / З. Б. Живко, О. Б. Баворовська, М. О. Живко, Л. М. Плахотнюк, Х. З. Босак; за заг. ред. З. Б. Живко. Львів: Ліга-Прес, 2011. 228 с.

46. Менеджмент персоналу: навч. посіб. / З. Б. Живко, І. Ю. Копєлєв, І. Б. Гапій, М. О. Живко, І. М. Горбан. Львів: Ліга-Прес, 2013. 380 с.

47. Мігус І. П. Корпоративне управління в системі економічної безпеки акціонерних товариств України: кол. монографія / І. П. Мігус, Л. М. Худолій, М. П. Денисенко, С. П. Міхно. Черкаси: Маклаут, 2012. 274 с.

48. Мойсеєнко І. П., Марченко О. М. Управління фінансово-економічною безпекою підприємства: навч. посіб. Львів, 2011. 380 с.

49. Організація та управління системою економічної безпеки підприємства: навч. посіб. / З. Б. Живко, Н. В. Зачосова, О. В. Черевко, М. О. Живко, О. Б. Баворовська; за ред. З. Б. Живко. Черкаси: Вид-во ПП Чабаненко Ю. А., 2019. 120 с.

50. Олійник С. У. Теорія та практика менеджменту персоналу: підруч. Х.: Вид-во НУА, 2013. 376 с.

51. Отенко І. П., Іващенко Г. А., Воронков Д. К. Економічна безпека підприємства: навч. посіб. Х.: ХНЕУ, 2012. 251 с.

52. Перхач О. Л., Подольчак Н. Ю. Корпоративні конфлікти та методи їх подолання: навч. посіб. Львів: Вид-во НУ «Львівська політехніка», 2014. 191 с.

53. Подольчак Н., Ковальчук Г. Менеджмент управлінських конфліктів у діяльності машинобудівних підприємств: монографія. Львів: Вид-во НУ «Львівська політехніка», 2015. 190 с.

54. Подольчак Н., Карковська В. Організація та управління системою фінансово-економічної безпеки: навч. посіб. Львів: Вид-во НУ «Львівська політехніка», 2014. 267 с.

55. Правові основи охорони інформації: підручник / З. Б. Живко, В. В. Сердюков, О. М. Стаднік, В. О. Хорошко; за ред. В. О. Хорошка. К.: Вид-во ДУІКТ, 2009. 355 с.

56. Прыгунов П. Л. Психологическое обеспечение специальных операций: ролевое поведение: учеб. пособие. К.: Изд-во Европейского ун-та, 2000. 303 с.

57. Соснин А. С., Прыгунов П. Л. Менеджмент безопасности: учеб. пособие. К.: Изд-во Европейского ун-та, 2002. 367 с.

58. Соціальна економіка: навч. посіб. / кол. авт.: О. О. Бєляєв, М. І. Диба, В. І. Кириленко та ін. К.: КНЕУ, 2005. 196 с.

59. Соціально-економічна захищеність населення України: стан, тенденції, напрями використання. К.: Держкомстат України, 2003. 147с.

60. Технологічні засоби економічних систем: курс лекцій / Т. В. Рудий, З. Б. Живко, Я. Ф. Кулешник, О. І. Руда. Львів: ЛьвДУВС, 2017. 122 с.

61. Тимошенко И. Л., Соснин А. С. Мотивация человеческих ресурсов. К.: Изд-во Европейского ун-та, 2002. 676 с.

62. Управління персоналом: навч. посіб. / С. М. Лихолат, З. Б. Живко, І. Б. Гапій, М. Р. Яцик. Львів: Ліга-Прес, 2014. 428 с.

63. Цимбалюк М. М., Керницький І. С., Живко З. Б., Копитко М. І. Конкурентна розвідка: курс лекцій. Львів: Ліга-Прес, 2013. 264 с.

64. Чурсіна Л. А., Березовський Ю., Тіхосова Г. Сертифікація персоналу: навч. посіб. К.: Ліра-К, 2014. 314 с.

65. Фінансова безпека будівельних підприємств: монографія / Ю. М. Воробйов, О. І. Воробйова, О. Г. Блажевич. Сімферополь: ВД «АРІАЛ», 2013. 180 с.

66. Фінансова безпека підприємства: навч. посіб. / Т. Б. Кузенко, Л. С. Мартюшева, О. В. Грачов, О. Ю. Литовченко. Харків: Вид. ХНЕУ, 2010. 304 с.

67. Франчук В. І. Основи економічної безпеки: навч. посіб. Львів: Вид-во Львівського держ. ун-ту внутр. справ., 2008. 203 с.

68. Франчук В. І., Живко В. І., Керницька М. І. Соціально-економічна безпека: практикум. Львів: Ліга-Прес, 2009. 103 с.

69. Черевко О. В., Мігус І. П., Зачосова Н. В. Стратегічні пріоритети детінізації економіки України у системі економічної безпеки: макро- та мікровимір: монографія. Черкаси: Вид-во ПП Чабаненко Ю. А., 2014. 370 с.

70. Черевко О. В., Мігус І. П. Управління системою економічної безпеки суб'єктів господарювання: обліково-аналітичне забезпечення: монографія. Черкаси: Вид-во ПП Чабаненко Ю. А., 2015. 198 с.

71. Шевчук П. І. Соціальна політика та соціальна безпека людини: навч. посіб. Львів: ЛРІДУ НАДУ, 2003. 171с.

72. Шевчук П. І. Соціальна політика: навч. посіб. Львів: Світ, 2005. 400 с.

73. Шкарлет С. М. Економічна безпека підприємства: інноваційний аспект: монографія. К.: Вид-во Національного авіаційного ун-ту, 2007. 436 с.

74. Шульга І. П. Рейтингова оцінка векселедавців як індикатор фінансової безпеки учасників фондового ринку України: монографія. Черкаси: Вид-во ПП Чабаненко Ю. А., 2009. 220 с.

75. Шульга І. П. Економічна безпека емісійної діяльності акціонерних товариств: монографія. Черкаси: ТОВ «Маклаут», 2010. 425 с.

76. Якубівська Ю. Є. Сучасні методи забезпечення надійності персоналу: навч. посіб. Тернопіль: ТАЙП, 2014. 118 с.

77. Сайт Міністерства фінансів України. URL: www. minfm.gov.ua

78. Сайт Верховної Ради України. URL: www.rada.kiev.ua

79. Сайт Державної служби статистики. URL: www.ukrstat.gov.ua
80. Сайт Ради національної безпеки і оборони України. URL: http://www.rnbo.gov.ua
81. Сайт Національного інституту стратегічних досліджень при Президентові України. URL: http://www.niss.gov.ua
82. Сайт Національного банку України. URL: www.bank.gov.ua

НАВЧАЛЬНЕ ВИДАННЯ

Живко Зінаїда Богданівна,
доктор економічних наук, професор,
професор кафедри менеджменту
Львівського державного університету внутрішніх справ

Сучасні методи забезпечення надійності персоналу

Навчальний посібник у схемах і таблицях

Редагування *Оксана Шмиговська*

Макетування *Галина Шушняк*

Друк *Іван Хоминець*

Підписано до друку 20.12.2019 р.
Формат 60×84/16. Папір офсетний. Умовн. друк. арк. 7,44.
Тираж 100 прим. Зам № 129-19.

Львівський державний університет внутрішніх справ
Україна, 79007, м. Львів, вул. Городоцька, 26.

Свідоцтво про внесення суб'єкта видавничої справи до державного реєстру
видавців, виготівників і розповсюджувачів видавничої продукції
ДК № 2541 від 26 червня 2006 р.