**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**Західноукраїнський національний університет**

 **Юридичний факультет**

Кафедра безпеки та правоохоронної діяльності

**ЛУЧКА Арсен Юрійович**

**Система інформаційної безпеки підприємства в Україні сучасний стан та шляхи зміцнення**

спеціальність: 073 – Менеджмент

освітньо-професійна програма – Управління фінансово-економічною безпекою

 Кваліфікаційна робота

 Виконав студент групи МФЕБм-21

 А. Ю. Лучка

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

 Науковий керівник:

 к.е.н., доцент А. П. Колесніков

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

Кваліфікаційну роботу

допущено до захисту

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ р.

В.о. завідувача кафедри \_\_\_\_\_\_\_\_\_\_ Н. Б. Москалюк

 Тернопіль – 2021

ЗМІСТ

|  |  |
| --- | --- |
| Вступ | 3 |
| РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ЕКОНОМІЧНОЇ БЕЗПЕКИ ТА ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПІДПРИЄМСТВА | 5 |
| 1.1. Основи економічної безпеки підприємства та його складових | 5 |
| 1.2. Складові та особливості інформаційної безпеки підприємства | 14 |
| Висновки до розділу 1 | 20 |
| РОЗДІЛ 2 АНАЛІЗ ОСНОВНИХ ПОКАЗНИКІВ ДІЯЛЬНОСТІ ТА ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПІДПРИЄМСТВА | 23 |
| 2.1. Аналіз даних при формуванні інформаційної безпеки підприємства | 23 |
| 2.2. Основи господарської діяльності підприємства | 30 |
| Висновки до розділу 2 | 38 |
| РОЗДІЛ 3 ШЛЯХИ УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА | 40 |
| 3.1. Шляхи управління інформаційною безпекою підприємства | 40 |
| 3.2. Окремі засоби зміцнення інформаційної безпеки підприємства | 46 |
| Висновки до розділу 3 | 55 |
| Висновки  | 57 |
| Перелік використаних джерел | 60 |
|  |  |

**ВСТУП**

**Актуальність теми дослідження.** Економічна безпека будь-якого підприємства залежить від великої кількості факторів, їх взаємозв’язку та вміння реалізувати системний підхід до управління ними. З іншого боку, дія кожного фактора специфічна, а засоби управління для нього мають свої особливості. Одним із важливих інструментів забезпечення економічної безпеки є її інформаційне забезпечення, оскільки кожен елемент і етап забезпечення економічної безпеки передбачає створення системи отримання та обміну інформацією. Це актуалізує вибір теми даного дипломного дослідження.

**Аналіз останніх публікацій.** Проблемам забезпечення економічної безпеки підприємства, і зокрема її інформаційної складової, присвячували свої праці ряд авторів, зокрема: Василішин С. І., Грицишен Д. О., Гусев А., Данілова Е. І., Іванюта Т. М., Заїчковський А. О., Кононенко Є., Мацик О. В., Михальчук В. М., Стовбан М. П. та інші.

**Мета і завдання дослідження.** Метою є дослідження економічної безпеки підприємства, зокрема його інформаційної складової.

Для досягнення мети було поставлено і вирішено наступні завдання:

- охарактеризовано теоретичні основи економічної безпеки підприємства та його складових;

- визначено суть та основні складові інформаційної безпеки підприємства;

- проведено аналіз даних при формуванні інформаційної безпеки підприємства;

- досліджено основи господарської діяльності підприємства;

- визначено шляхи управління інформаційною безпекою підприємства;

- обґрунтовано окремі засоби зміцнення інформаційної безпеки підприємства;

**Об’єктом** дослідження є ТОВ «Детективне агентство «Холмс».

**Предметом** дослідження є інформаційні інструменти забезпечення економічної безпеки підприємства.

**Методи дослідження:** спостереження, порівняння, вимірювання, метод експертних оцінок, екстраполяції, сходження від абстрактного до конкретного, абстрагування, аналіз і синтез, індукція і дедукція, прогнозування інші специфічні прийоми і методи.

**Наукова новизна** дослідження полягає у виробленні рекомендацій щодо підвищення рівня надійності інформаційної складової забезпечення економічної безпеки підприємства.

**Структура і обсяг роботи.** Робота складається з трьох розділів, вступу, висновків, переліку використаних джерел, що містить 45 найменувань та викладена на 59 сторінках.

**РОЗДІЛ 1**

**ТЕОРЕТИЧНІ ОСНОВИ ІНФОРМАЦІЙНО-ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА**

**1.1. Основи економічної безпеки підприємства та його складових**

Основною метою економічної безпеки підприємства є забезпечення його стабільного та максимально ефективного функціонування в сучасному та високого потенціалу розвитку в майбутньому.

Економічна безпека підприємства характеризується сукупністю якісних і кількісних показників, найважливішим з яких є рівень економічної безпеки. Рівень економічної безпеки підприємства — це оцінка стану використання корпоративних ресурсів за критеріями рівня економічної безпеки підприємства. Рівень економічної безпеки підприємства залежить від того, наскільки ефективно його керівництво та спеціалісти зможуть уникнути можливих загроз та ліквідувати шкідливі наслідки окремих негативних компонентів зовнішнього та внутрішнього середовища. Для досягнення найвищого рівня економічної безпеки підприємство повинно проводити роботи з забезпечення максимальної безпеки основних функціональних складових своєї роботи.

Можна виділити внутрішні, зовнішні причини, що впливають на діяльність компанії. До внутрішніх належать такі: вид діяльності підприємства, досвід, відповідна кваліфікація керівництва та персоналу, наявність відповідних комунікацій на підприємстві, форма власності, співвідношення між власним і капіталом, інноваційність, організація виробництво, показники фінансового стану, ефективна маркетингова діяльність. До внутрішніх загроз відносять такі фактори: недоліки виробничого процесу, відсутність фінансування, низька кваліфікація персоналу підприємства, низький рівень управління. До зовнішніх факторів належать: стабільність економічної ситуації в країні, рівень конкуренції, частка ринку, постачальники, споживачі, нові технології, державні органи. До зовнішніх загроз належать: зниження купівельної спроможності споживачів, рівня інфляції, сезонні коливання попиту, кризи окремих галузей [42, с. 171-172].

Серед сукупності авторських інтерпретацій поняття економічної безпеки підприємства чітко виражено її розуміння як «системи захисту економічних інтересів підприємства від загроз [4; 12].

Виходячи з теоретичного змісту економічних відносин, система їх захисту являє собою сукупність економічних, організаційних (адміністративних), управлінських заходів, внутрішньокорпоративних норм, технічних та інформаційних засобів, метою яких є запобігання або мінімізація можливих втрат у процес впровадження системи економічних відносин підприємства. Оскільки збитки виступають як розрахункова величина втрат внаслідок настання загроз, небезпек і ризиків, то весь комплекс методів їх зменшення реалізується в континуумі системи управління економічною безпекою.

У наукових дослідженнях існує трактування економічної безпеки як умови функціонування [11].

Найпоширенішим із трактувань «економічної безпеки» є її тлумачення як «системи захисту від негативних впливів зовнішнього та внутрішнього середовища». Така інтерпретація економічної безпеки ґрунтується на захисній властивості сукупності засобів, методів і засобів, що використовуються для забезпечення реалізації поставлених цілей, та визначенні сукупності загроз, небезпек і ризиків та визначенні напряму їх впливу на діяльності підприємства.

Крім усталених або найбільш типових підходів до тлумачення економічної сутності поняття «економічна безпека підприємства», існують також підходи, які ставлять поняття на основі не захисної функції існуючої системи, але функція використання внутрішніх можливостей для забезпечення ефективної реалізації корпоративних і функціональних цілей компанії.

В економічній літературі зустрічаються трактування економічної безпеки як «рівень використання економічного потенціалу, при якому реальний та/або можливий збиток нижче встановлених підприємством меж» та умов функціонування.

Економічна безпека підприємства - це поняття, що утворилося внаслідок поєднання трьох самостійних економічних категорій: економіка, безпека, підприємство, які в змістовному сенсі слід тлумачити як систему економічних відносин, що виникають у процесі захисту від небезпеки. підприємства. Причому кожна зі складових частин має свої атрибутивні характеристики, що впливають на формування атрибутів цілісного поняття «економічна безпека підприємства».

Отже, теорія формування економічної безпеки підприємства базується на синтезі теорії трьох галузей знання: економіки, організації підприємства та ризиків. Тому методологія управління економічною безпекою базується на методології економіки, методології управління підприємством та методології управління ризиками.

Крім того, за структурним змістом концепції економічна безпека підприємства узгоджується з теорією систем, згідно з якою кожен із самостійних елементів системи має хоча б одну властивість, що забезпечує реалізацію поставлених цілей.

Отже, відповідно до семантичного аналізу, в основу концепції економічної безпеки підприємства різні автори відносять різні пріоритети його елементів, які є визначальними у формуванні його сутності.

Морфологічний опис існуючих наукових інтерпретацій цього поняття дозволяє формалізувати такі логічно послідовні поєднання його складових елементів:

- економіка-безпека-підприємство [12; 20];

- безпека-економіка-підприємство [18];

- охоронно-підприємство [24].

Морфологічний аналіз дозволяє зробити висновок про використання різної послідовності змістовних поєднань елементів поняття «економічна безпека підприємства». Таким чином, перша група авторів вважає безпекою на підприємстві ефективне використання ресурсів і підприємницьких можливостей. Друга група — це специфічна система захисту ресурсів та економічних інтересів. Третя група — це специфічна система безпеки підприємства.

Все це дозволяє розглядати економічну безпеку підприємства як систему, що складається з елементів зі своїми специфічними властивостями. Проте кожен з елементів системи створює нову якість як властивостей всієї системи, так і економічну безпеку підприємства.

Використання семантичного (аналіз сутності понять) та морфологічного аналізу (поділ та поєднання елементів у системі) дозволило узагальнити основні підходи до тлумачення сутності поняття економічної безпеки підприємства, а також результати дослідження були наочно представлені у вигляді таблиці 1.1.

Таблиця 1.1.

Морфологічний аналіз авторських трактувань поняття «економічна безпека» [7, с. 94].

|  |  |  |  |
| --- | --- | --- | --- |
| Об’єкт захисту | Інструменти захисту | Мета захисту | Спосіб захисту |
| Підприємство. Економічні інтереси. Стан корпоратив­них ресурсів та підприємницьких можливостей. Економічний потенціал.Умови діяльності. | Ефективне використання ресурсів та підприємницьких можливостей.Економічні, організаційні, правові, внутрішньо-корпоративні норми, заходи та засоби.Внутрішні чинники.Стан використання економічного потенціалу. | Стабільність функціонування. Досягнення цілей. Убезпечення від за­гроз.Реалізаціяекономічних інтересів. Розвиток. | Усунення небезпек. Пристосування до ризиків.Зменшення негатив­ного впливу небезпек та ризиків. Зменшення збитків. |

Морфологічний аналіз авторських інтерпретацій поняття «економічна безпека підприємства» представлено в таблиці 1.1. Саме візуальний формат основних елементів змісту, визначених авторами, складають сутність цього поняття. Як зазначалося вище, авторські трактування розрізняються повнотою підходу до дослідження економічної безпеки як об’єкта системи: від дослідження окремих елементів системи (ресурсів, відносин, потужностей тощо) до повного дослідження. всієї системи (підприємства).

За результатами семантико-морфологічного аналізу окремих підходів до тлумачення сутності економічної безпеки підприємства з’ясовано, що об’єктом економічної безпеки підприємства є сукупність основних засобів, бізнес-процесів, система відносин, персонал, середовище та результати діяльності підприємства (бренд, частка ринку, імідж тощо) тощо). Відповідно до методологічних основ управління економічні об’єкти перетворюються на агреговані об’єкти управління, які є сукупністю ресурсів, процесів, функцій і структур підприємства. Інструменти економічної безпеки — це сукупність засобів, заходів, процесів, спрямованих на виявлення загроз, усунення небезпек та зниження ризиків.

Що стосується мети економічної безпеки, то слід підкреслити її методологічну відповідність напряму наукових досліджень. Отже, метою економічної безпеки в авторських інтерпретаціях є стабільність функціонування, досягнення цілей, захист від загроз, реалізація економічних інтересів. Стабільність функціонування, поняття, назва якого визначає його приналежність до діяльності, пов’язаної з оперативним управлінням компанією (функціонуванням). Розвиток є категорією стратегічного управління. Метою підприємницької діяльності та створення підприємства є реалізація економічних інтересів.

Крім того, слід відзначити ієрархію цілей підприємства, як логічно підпорядкованої системи загальнокорпоративних і функціональних цілей (цілі першого порядку, цілі другого порядку тощо). У методології управління підприємством управління економічною безпекою реалізує функціональні цілі, які підпорядковуються і формуються виходячи з загальнокорпоративних цілей підприємства (табл. 1.2).

Отже, виходячи з семантико-морфологічного аналізу сутності поняття «економічна безпека підприємства» та з урахуванням методології управління нею, її змістовна сутність трактується як сукупність засобів, засобів і заходів для формування системи захисту всіх видів ресурсів, процесів, функцій і структур підприємства з метою запобігання збиткам шляхом виявлення, запобігання та зменшення негативного впливу небезпек і ризиків.

Таблиця 1.2.

Семантико-морфологічний аналіз сутності поняття «економічна безпека підприємства» [7, с. 96]

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Економічні об’єкти за­хисту | Об’єкти управлінняекономічноюбезпекою | Інструментизахисту | Метаекономічноїбезпеки | Мета управління підприємством |
| Тактичнийрівень | Стратегічнийрівень |
| капітальні блага; бізнес-процеси; система відносин; персонал; середовище та результати діяльності підприємства | ресурси;функції;процеси;структурапідприємства | засоби, заходи, проце­си (контроль, аудит, аналіз, прогнозуван­ня ресурсів, процесів та результатів діяльності) виявлення, попередження та зменшення негативного впливу небезпек та ризиків | недопущеннявтрат | стабільність | розвиток |

На завершення семантичного аналізу авторських інтерпретацій економічної безпеки слід зазначити, що теоретичні основи економічної безпеки (з точки зору визначення змістовної сутності поняття) визначають методологічні основи формування економічної безпеки. системи, а остання - методологія управління економічною безпекою.

Концепція управління економічною безпекою, залежно від економічної сутності концепції, повинна мати відмінності в описі проблеми, що потребує вирішення (проблеми, джерело якої це загрози, небезпеки та ризики реалізації економічних відносин, проблеми використання корпоративних ресурсів і підприємницьких можливостей, проблема реалізації внутрішніх факторів тощо), вибір методів її вирішення, визначення ресурсів. беруть участь у реалізації методів вирішення проблеми та оцінки економічних показників та ефективності концепції.

Методичним підходом до оцінки рівня економічної безпеки є комплексний (розрахований на основі адитивної згортки часткових показників) і мультиплікативний (розрахований на основі середнього геометричного з добутку часткових показників) індекси. Слід зазначити, що на сьогодні відсутня методологічна єдність між сутністю поняття економічної безпеки, концептуальними побудовами системи економічної безпеки та управління нею та методичним інструментарієм оцінки рівня економічної безпеки.

Теоретичне дослідження змістовної сутності економічної безпеки також виявило мовні відмінності в її розумінні. Так, вона не знайшла єдності та визнання економічної безпеки як категорії чи поняття. Отже, «у когнітивній лінгвістиці категорія — це когнітивна структура, що складається з елементів, об’єднаних сімейною схожістю і відображають універсальні властивості, загальні закономірності розвитку всіх матеріальних, природних і духовних явищ» [2]. За мовним змістом «поняття» — це істотні ознаки предметів і явищ, один із елементів категорії [2]. Отже, виходячи з вищесказаного, категорія «безпека» відображає універсальні властивості, які проявляються в усіх явищах і об’єктах навколишнього світу, у всіх його суб’єктах і на всіх рівнях світової еволюції. Поняття економічної безпеки характеризує явища і процеси, які пов’язані з розподілом економічних ресурсів і реалізуються з метою реалізації економічних інтересів.

Щодо розуміння економічної безпеки як системи, то Терещенко визначає систему як «сукупність окремих самостійних елементів, кожен з яких має хоча б одну властивість, що забезпечує досягнення поставленої перед нею мети» [35]. Академічний тлумачний словник української мови визначає стан як ситуацію, зумовлену певними обставинами, умовами.

Властивості системи - сукупність її ознак, що характеризують систему.

Властивість слід тлумачити як сукупність проявів, що відображають загальні, характерні та специфічні ознаки досліджуваного поняття.

На основі узагальнення проведених до цього часу досліджень розвитку економічної безпеки визначено, що до основних властивостей економічної безпеки, як її відмінності від інших понять, належать:

- існує в нерозривній єдності з небезпекою;

- економічна безпека ґрунтується на загрозі конфлікту інтересів щодо володіння ресурсами чи контролю над ресурсами;

- існує сукупність елементів, об'єднаних єдиною метою;

- має ієрархічну структуру формування;

- є моделлю взаємодії із зовнішнім середовищем;

- ефективність захисту залежить від внутрішніх можливостей підприємства;

- формується під впливом управлінських дій суб'єктом управління;

- пов'язані з економічним інтересом суб'єкта управління;

- набір засобів захисту змінюється залежно від джерела та сили впливу ризику.

Отже, наявність різноманітних інтерпретацій економічної сутності категорії зумовлена багатогранністю проявів її економічних властивостей.

Структуру механізму управління в системі економічної безпеки підприємства доцільно будувати на основі функціонально-ресурсного підходу, що дозволить: розпізнавати загрози; визначити, коли, за яких обставин і в яких напрямках необхідно здійснити агресивний наступ (реалізувати контрзагрози), застосувати еволюційний підхід (метод ретельної методичної підготовки та розширення житлового простору), застосувати метод пристосування чи вичікування.

Розглянемо структуру економічної безпеки підприємства як сукупність взаємопов’язаних організаційно-фінансово-економічних та адміністративно-правових складових цілеспрямованого впливу на об’єкт управління, результат якого має контролюватися динамікою, що не впливає допускають затяжні кризові явища та банкрутство підприємства. Цьому сприяють прогнозування та планування діяльності, регулярний моніторинг та аналіз рівня економічної безпеки в поточному та майбутньому періодах. У рамках моніторингу та аналізу рівня економічної безпеки підприємства необхідно використовувати систему показників і критеріїв як єдину інформаційну базу для прийняття управлінських рішень щодо зміцнення економічної безпеки підприємства. Для досягнення найвищого рівня економічної безпеки підприємство повинно проводити роботи із забезпечення високого рівня безпеки основних функціональних компонентів [16, с. 137].

Фінансова безпека серед функціональних елементів економічної безпеки вважається провідною і визначальною, оскільки в ринковій економіці фінанси є «двигуном» будь-якої економічної системи.

Інтелектуальна складова включає рівень сучасних знань, інноваційність у розвитку співробітників, удосконалення професійних знань, умінь, навичок, стимулювання ініціативи та здібностей шляхом створення гнучкої системи преміювання відповідно до розвитку науково-технічного прогресу.[30, с. 264].

Людська складова – це процес запобігання впливу на економічну безпеку підприємства шляхом усунення або зменшення ризиків і загроз, пов’язаних з працівниками, їх інтелектуальним потенціалом та трудовими відносинами в цілому. Безпека персоналу - це поєднання компонентів, з'єднаних складними зв'язками.

Соціальне страхування — це стан розвитку держави, за якого держава здатна забезпечити гідний і якісний рівень життя населення незалежно від віку, статі, рівня доходів, підтримувати розвиток людського капіталу, як найважливіша складова економічного потенціалу країни.

Екологічна безпека – це стан навколишнього середовища у світовому господарстві, в країні в цілому і в регіонах зокрема, а також на підприємствах, який не загрожує здоров’ю населення в процесі праці та життя. Екологічна безпека, пов'язана з екологічною небезпекою. Про величезну екологічну небезпеку в Україні свідчить те, що майже 10% її території перебуває в стані глибокої екологічної кризи, близької до катастрофи, майже 70% загальної площі наближається до цього стану.

Енергетична безпека — це захищеність енергетичного потенціалу підприємства від зовнішніх і внутрішніх загроз у різних формах, що забезпечує його стабільний розвиток відповідно до його статутних цілей і здатність протистояти і відтворювати його структуру та організаційний статус.

Теоретичне та практичне значення результатів дослідження полягає в тому, що структура економічної безпеки підприємства виражається забезпеченістю підприємства якісними ресурсами, їх хорошими запасами з урахуванням ймовірних ризиків господарської діяльності. При цьому всі ресурси повинні ефективно використовуватися в рентабельному виробництві для забезпечення прибутку і підтримки ліквідності підприємства. Це дасть змогу виконати планові показники розвитку підприємства економічної безпеки.

**1.2. Складові та особливості інформаційної безпеки підприємства**

У зв’язку зі стрімким розвитком інформаційних технологій та глобальною цифровізацією соціально-економічних відносин значно зросла значення інформації для економіки. У сучасних умовах процес успішного функціонування та економічного розвитку підприємства залежить від прийняття якісних і своєчасних управлінських рішень, сформованих на основі ретельного і всебічного аналізу інформації, що надходить як із внутрішнього, так і з зовнішнього середовища. Фактично інформація стала одним із найважливіших управлінських ресурсів. Його накопичення та споживання є основою ефективного функціонування та розвитку як економіки в цілому, так і підприємництва в цілому.

Водночас із зростанням ролі інформації виник інформаційний простір, який потребує захисту від несанкціонованого чи ненавмисного впливу на рівні держави і окремих підприємств. А з розвитком інформаційного суспільства, в якому функціонує більшість суб’єктів ринкової економіки, все більшого значення набуває інформація та всі основні складові процесу інформатизації. У господарській діяльності максимальний та ефективний захист інформації дозволяє отримувати високі доходи, укладати вигідні договори з контрагентами, значно підвищує рівень конкурентоспроможності підприємства, а також дозволяє значно підвищити ефективність діяльності організації в цілому.

Загрози збереження, цілісності та конфіденційності інформаційних ресурсів обмеженого доступу практично реалізуються через ризик формування каналу несанкціонованого отримання (вилучення) кимось цінної інформації та документів. Відповідно, забезпечення інформаційної безпеки має починатися з визначення суб’єктів господарських відносин, пов’язаних із використанням інформаційних систем. Спектр їх інтересів можна розділити на такі основні категорії: доступність (можливість отримати необхідну інформаційну послугу в розумний час), цілісність (актуальність і несуперечливість інформації, її захист від знищення та несанкціонованого зміни), конфіденційність (захист від несанкціонованого знайомства). У зв'язку з цим інформаційна безпека є невід'ємним елементом системи економічної безпеки. Відповідно, комплексна інформаційна безпека є запорукою забезпечення економічної безпеки підприємства.

Інформаційна безпека з точки зору економічної безпеки – це стан захищеності діяльності організації та її інформаційного середовища від негативного впливу дестабілізуючих факторів, що забезпечує збереження основних властивостей інформації та досягнення соціально-економічних цілей. створення організації. До об'єктів інформаційної безпеки в організації належать [15]:

- інформаційні ресурси, що містять відомості, віднесені до комерційної таємниці, та конфіденційну інформацію, представлену у вигляді інформаційних масивів та баз даних;

- засоби та системи інформатизації - засоби обчислювальної та організаційної техніки, мережі та системи, загальне системне та прикладне програмне забезпечення, автоматизовані системи керування, системи зв'язку та передачі даних, технічні засоби збору, реєстрації, передачі, обробки та відображення інформації.

До основних загроз безпеці належать [15]:

- розголошення конфіденційної інформації;

- несанкціоноване використання інформаційних ресурсів;

 - неправильне використання ресурсів;

- несанкціонований обмін інформацією;

- злом системи.

Система захисту інформації — це організована сукупність спеціальних органів, засобів, методів і заходів, що забезпечують захист інформації від внутрішніх і зовнішніх загроз. З точки зору системного підходу до захисту інформації, висуваються певні вимоги:

- забезпечення безпеки інформації

- це безперервний процес, який полягає в обґрунтуванні та впровадженні найбільш раціональних методів, методів і способів удосконалення та розвитку системи захисту, постійному моніторингу її стану, виявленні вузьких і слабких місць та протиправних дій;

- планування інформаційної безпеки здійснюється шляхом розробки детальних планів захисту кожною службою у сфері її компетенції;

- конкретні дані підлягають захисту, об'єктивно підлягають захисту, втрата яких може завдати певної шкоди організації;

- методи та засоби захисту повинні надійно блокувати можливі шляхи незаконного доступу до інформації;

- ефективність захисту інформації означає, що витрати на її реалізацію не повинні перевищувати можливих втрат від реалізації інформаційних загроз;

- чіткість визначення повноважень і прав користувачів на доступ до окремих видів інформації;

- забезпечення контролю цілісності засобів захисту та негайного реагування на їх вихід з ладу.

Система захисту інформації, як і будь-яка система, повинна мати певні види власної підтримки, спираючись на які вона буде виконувати свою цільову функцію. З огляду на це, система захисту інформації може мати:

- юридичний супровід. Сюди входять нормативні акти, положення, інструкції, вказівки, вимоги яких є обов'язковими в межах сфери дії;

- організаційне забезпечення. Мається на увазі, що здійснення захисту інформації здійснюється певними структурними підрозділами, такими як: служба безпеки, режимна служба, служба захисту інформації технічними засобами тощо;

- апаратне забезпечення. Передбачається, що технічні засоби будуть широко використовуватися як для захисту інформації, так і для забезпечення функціонування самої системи захисту інформації;

- інформаційна підтримка. Вона включає документовану інформацію (індикатори, файли), що лежить в основі вирішення завдань, що забезпечують функціонування системи;

- програмне забезпечення. До нього належать антивірусні програми, а також програми (або частини програм постійного користування), що реалізують контрольні функції при вирішенні бухгалтерських, статистичних, фінансових, кредитних та інших завдань;

- програмне забезпечення. Це передбачає використання математичних методів для різноманітних розрахунків, пов'язаних з оцінкою небезпеки технічних засобів зловмисників, зон і норм необхідного захисту;

- нормативно-методичне забезпечення. Сюди входять норми та положення діяльності органів, служб, засобів, що реалізують функції охорони;

- ергономічна підтримка. Набір інструментів, що забезпечують зручність користувачів засобів інформаційної безпеки.

Зрозуміло, що робота будь-якої системи заснована на певних принципах. І система інформаційної безпеки підприємства, організації чи установи не є винятком. Принципи, які будуть наведені нижче, є вихідними положеннями, нормами та правилами поведінки, які формують та забезпечують якісне функціонування системи інформаційної безпеки. Український учений М.В. Верескун виділяє такі принципи забезпечення інформаційної безпеки компаній, організацій та установ: простота використання, повний контроль, загальна заборона, відкрита архітектура, контроль доступу, невеликі переваги, достатня стабільність, мінімізація [6]. Варто відзначити, що кожен із цих принципів заслуговує на особливу увагу, тому коротко зупинимося на аналізі.

Принцип простоти. Саме він акцентує увагу на тому, що завдяки простоті роботи інформаційної системи ймовірність помилки зводиться до мінімуму. Висока складність операції та процедури, яку мають виконати користувачі та адміністратори, в рази збільшують ризик помилитися. Тож чим простіше буде процес використання системи, тим менше помилок доведеться згодом нейтралізувати. Однак простоту використання не слід плутати з простотою архітектури системи, оскільки складність останньої необхідна для забезпечення її безпеки.

Принцип контролю. Його суть полягає в організації постійного нагляду за справністю системи інформаційної безпеки та в моніторингу факторів, які можуть на неї впливати. Цей принцип вимагає від системи архітектури контролювати доступ до кожного зі своїх об’єктів, швидко справлятися з блокуванням небажаних дій і відновлювати нормальну роботу системи інформаційної безпеки.

Принцип загальної заборони. Вона полягає в тому, що заборонено все, що заборонено. Для ознайомлення та роботи з об’єктами інформаційної системи необхідно мати відповідний дозвіл. Вони її забезпечують, дотримуючись усіх інструкцій, прописаних у нормативних документах, що регулюють організацію інформаційної системи. Однак насправді мета системи полягає в тому, щоб дозволити, а не заборонити дію. Суть цього принципу полягає в тому, що в інформаційній системі можуть виконуватися лише відомі безпечні дії.

Принцип відкритої архітектури інформаційної системи. Відповідно до цього принципу, безпека системи може бути забезпечена лише завдяки неоднозначності. Дійсно, з такими маніпуляціями, як ускладнення, плутанина і спроби приховати недоліки інформаційної системи, хакерська, вірусна або інсайдерська атака рано чи пізно впорається.

Принцип контролю доступу. Він наголошує, що людина отримує доступ до системи в тій мірі, в якій їй дозволяють її повноваження. Кожна роль / посада / група повинна мати власні повноваження для роботи з певними об'єктами інформаційної системи.

Принцип найменших привілеїв. Коли ми говоримо про цей принцип, ми говоримо про те, що кожен користувач повинен бути наділений найменшими правами і доступом до мінімальної кількості процесів і програмних операцій. Про перешкоду для виконання трудових обов’язків мова не йде. Слід подбати про те, щоб цього не сталося.

Принцип достатньої стійкості. Цей принцип виражається в тому, що на шляху потенційних зловмисників має бути достатньо перешкод. Для цього ідеально підходять обчислювальні задачі. Так, можна організувати захист таким чином, щоб проникнення в систему хакерів вимагало від них нереально великої кількості часу або обчислювальної потужності.

Принцип мінімізації дублювання. Повинні бути хоча б ідентичні операції. Бажано, щоб усі або принаймні більшість процедур були різними для кожного користувача [37].

Отже, принципи забезпечення інформаційної безпеки підприємств, організацій та установ є важливим елементом системи інформаційної безпеки, саме вони разом із цільовими характеристиками системи, її завданнями, основними загрозами та заходами нейтралізації загроз, складають його основу. Сама ж система інформаційної безпеки є невід'ємною частиною будь-якого підприємства, і нехтування нею може коштувати йому занадто великої шкоди або навіть загрожувати самому його існуванню.

Враховуючи той факт, що досягнення певного рівня інформаційної безпеки гарантує належний рівень економічної безпеки, можна зробити висновок, що поняття «інформаційно-економічна безпека» об’єднує тісно пов’язані різні стани діяльності організації, що гарантують її стабільність. Відповідно до цього можна відзначити, що інформаційно-економічна безпека – це стан захищеності діяльності організації та її інформаційного середовища від негативного впливу дестабілізуючих факторів, що забезпечує збереження основних властивостей інформації та дозволяє досягти соціально-економічні цілі створення організації.

**Висновки до розділу 1**

Аналіз теоретичних основ забезпечення економічної безпеки підприємства, зокрема його інформаційної складової, дав змогу зробити ряд висновків.

Економічна безпека підприємства характеризується сукупністю якісних і кількісних показників, найважливішим з яких є рівень економічної безпеки. Рівень економічної безпеки підприємства — це оцінка стану використання ресурсів підприємства за критеріями рівня економічної безпеки підприємства.

Рівень економічної безпеки підприємства залежить від того, наскільки ефективно його керівництво та спеціалісти зможуть уникнути можливих загроз та ліквідувати шкідливі наслідки окремих негативних компонентів зовнішнього та внутрішнього середовища. Для досягнення найвищого рівня економічної безпеки підприємство повинно проводити роботи з забезпечення максимальної безпеки основних функціональних складових своєї роботи.

Найпоширенішим із визначень «економічної безпеки» є її тлумачення як «системи захисту від негативних впливів зовнішнього та внутрішнього середовища». Така інтерпретація економічної безпеки ґрунтується на захисній властивості сукупності засобів, методів і засобів, що використовуються для забезпечення реалізації поставлених цілей, та визначенні сукупності загроз, небезпек і ризиків та визначенні напряму їх впливу на діяльності підприємства.

Загрози збереження, цілісності та конфіденційності інформаційних ресурсів обмеженого доступу практично реалізуються через ризик формування каналу несанкціонованого отримання (вилучення) кимось цінної інформації та документів. Відповідно, забезпечення інформаційної безпеки має починатися з визначення суб’єктів господарських відносин, пов’язаних із використанням інформаційних систем. Спектр їх інтересів можна розділити на такі основні категорії: доступність (можливість отримати необхідну інформаційну послугу в розумний час), цілісність (актуальність і несуперечливість інформації, її захист від знищення та несанкціонованого зміни), конфіденційність (захист від несанкціонованого знайомства). У зв'язку з цим інформаційна безпека є невід'ємним елементом системи економічної безпеки. Відповідно, комплексна інформаційна безпека є запорукою забезпечення економічної безпеки підприємства.

**РОЗДІЛ 2**

**АНАЛІЗ ОСНОВНИХ ПОКАЗНИКІВ ДІЯЛЬНОСТІ ТА ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПІДПРИЄМСТВА**

**2.1. Аналіз даних при формуванні інформаційної безпеки підприємства**

Основною метою інформаційної безпеки є балансування захисту конфіденційності, цілісності та доступності даних.

Як зазначає д-р Г. Я. Аніловська, на сучасному етапі зі стрімким розвитком інформаційних технологій та їх широким впровадженням в облікові процеси постає проблема взаємодії цих систем обліку з іншими системами та між собою, а також проблема конфіденційності. Крім того, ці проблеми існують на технічному, програмному та інформаційному рівнях. Їх можна вирішити методом розробки та впровадження єдиних, загальних та обов’язкових правил побудови та використання облікових інформаційних систем [1]. У світлі розвитку нових ІТ-технологій поняття «інформаційна безпека» значно розширилося. Сьогодні від захисту процесів, інформації та діяльності кіберпростору залежить набагато більше, ніж просто втрата інформації. Це означає, що втрата інформації призводить до багатьох інших складних ускладнень. Нині комплекс заходів із захисту інформації має включати, зокрема, антивірусний захист, захист від хакерських атак, підробки даних тощо. Наприклад, дія комп’ютерних вірусів може не тільки стерти чи викрасти дані, але й вплинути на роботу і продуктивність працівників, і навіть зупинити виробництво.

Розглянемо типи інформації, що підлягає захисту. Сьогодні держава забезпечує захист інформації з обмеженим доступом, у тому числі секретної інформації [29], конфіденційної інформації, конфіденційної інформації (у тому числі персональних даних); а також захист в інформаційно-телекомунікаційних системах має бути відкритою інформація, що належить до державних інформаційних ресурсів і відноситься до статистичної, правової, соціологічної інформації, інформації довідкового та енциклопедичного характеру та «використовується для забезпечення діяльності державних органів або органів місцевого самоврядування, а також інформацію про діяльність цих органів, яка публікується в Інтернеті, інших глобальних інформаційних мережах і системах або передається по телекомунікаційних мережах» [28].

В законі України «Про інформацію» зазначено, що «конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною чи юридичною особою, крім суб’єктів владних повноважень. Конфіденційна інформація може поширюватися на вимогу (згоду) заінтересованої особи у визначеному нею порядку на передбачених нею умовах, а також в інших випадках, визначених законом». Іншими словами, кожне підприємство може визначити, яка інформація є конфіденційною і щодо якої, відповідно, вжити заходів захисту. Єдине застереження полягає в тому, що така інформація не може бути класифікована як інформація з обмеженим доступом:

1) про стан навколишнього середовища, якість продуктів харчування та предметів побуту;

2) про аварії, катастрофи, небезпечні природні явища та інші надзвичайні ситуації, що виникли або можуть статися і загрожують безпеці людей;

3) про стан здоров'я населення, рівень його життя з урахуванням харчування, одягу, житла, медичного обслуговування та соціального забезпечення, а також за соціально-демографічними показниками, станом правопорядку, освіти і культури; населення;

4) про факти порушення прав і свобод людини з урахуванням відомостей, що містяться в архівних документах колишніх радянських органів державної безпеки щодо політичних репресій, Голодомору 1932-1933 років в Україні та інших злочинів, вчинених представниками комуністичний та/або націонал-соціалістичний (нацистський) тоталітарний режими;

5) про неправомірні дії органів державної влади, органів місцевого самоврядування, їх посадових і службових осіб;

6) про діяльність державних і комунальних унітарних підприємств, господарських товариств, у статутному капіталі яких більше 50 відсотків акцій (часток) належать державі або територіальній громаді, а також господарських товариств, 50 і більше відсотків акції (частки) яких належать господарському товариству, державній частці або територіальному товариству, в якому вона становить 100 відсотків, підлягають обов’язковому оприлюдненню відповідно до закону;

7) іншу інформацію, доступ до якої не може бути обмежений згідно із законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України. У приватному секторі ми можемо визначити захист конфіденційної та певних видів відкритої інформації. За формою подання інформація, що підлягає захисту, може бути на матеріальних носіях (папір, машина тощо), у вигляді сигналу чи повідомлення, а також озвучена інформація. Наступним кроком є класифікація загроз інформаційної безпеки. Загрози інформаційної безпеки можна класифікувати за різними критеріями (рис. 2.1).

Рис. 2.1. Класифікація загроз інформаційній безпеці [21, С. 40]

За аспектом інформаційної безпеки, на який спрямовані загрози:

- погрози конфіденційності (несанкціонований доступ до інформації). Такі загрози полягають у тому, що інформація стає відомою тому, хто не має повноважень на доступ до неї. Виникнення таких загроз може бути викликано людським фактором або несправністю програмного або апаратного забезпечення;

- загрози цілісності (незаконна зміна даних). Такі загрози пов’язані з можливим впливом на дані з метою їх знищення або пошкодження. Причинами порушення цілісності інформації можуть бути як збій програмного забезпечення, так і навмисні дії персоналу або сторонній вплив (наприклад, вірусні атаки);

- загрози доступності (вжиття дій, що унеможливлюють або ускладнюють доступ до ресурсів інформаційної системи). Для реалізації таких загроз створюються умови, за яких доступ до інформації або блокується, або обмежується на час, що виключає можливість виконання певних бізнес-цілей.

За локалізацією джерела загрози можна розділити на внутрішні - перш за все, це персонал і програмне забезпечення, що використовуються на підприємстві; а зовнішні — будь-який вплив сторонніх, апаратних, програмних засобів тощо.

За розміром заподіяної шкоди загрози поділяються на загальні - такі, які можуть завдати значної шкоди об'єкту, що охороняється в цілому, або заподіяти критичний збиток; місцеві - такі, які можуть завдати шкоди окремим частинам об'єкта охорони; приватні - ті, які можуть завдати шкоди окремим властивостям елементів охоронного об'єкта.

За ступенем впливу на інформаційну систему виділяють пасивні, при яких структура і зміст системи не змінюються; і активні загрози, вплив яких змінює структуру чи зміст системи в цілому чи окремих її елементів.

За характером загрози їх можна поділити на природні та об’єктивні – загрози, спричинені впливом на систему природних явищ чи елементів і не залежать від волі людини; і штучні, тобто суб’єктивні – загрози, викликані так званим людським фактором, тобто впливом людини на інформаційну систему. До штучних загроз, у свою чергу, належать: ненавмисні (випадкові) загрози, помилки програмного забезпечення та персоналу, системні збої, відмови обладнання для обробки або передачі інформації; Навмисні погрози – це навмисні дії персоналу або сторонніх осіб з метою порушення конфіденційності, цілісності або доступності інформації. Основні проблеми реалізації політики безпеки будь-якого підприємства пов'язані з свідомими загрозами.

Для деталізації можливого зловмисника інформаційної безпеки необхідно розробити специфічну для кожного підприємства модель такого зловмисника. При цьому необхідно вирішити, що має відображати ця модель. Залежно від потреб, модель зловмисника може бути:

- змістовна - відображає цілі правопорушника, його мотивацію, а також загальний характер його дій при підготовці та здійсненні порушень інформаційної безпеки;

- математичний - визначає послідовність дій порушника, використовуючи кількісні показники, що характеризують результати та наслідки порушень, а також функціональні зв'язки порушника з елементами об'єкта охорони;

- сценарій впливу порушника - визначає види порушень і конкретний алгоритм дій порушника на кожному етапі.

При цьому для найкращої характеристики зловмисника та його дій необхідно розробити комплексну модель з урахуванням усіх рівнів деталізації. Для якісного аналізу можливих дій правопорушника його слід класифікувати (рис. 2.2).

Рис. 2.2. Класифікація порушника інформаційної безпеки [21, С. 41]

Ознаками класифікації можуть бути:

- за місцем дії порушники можуть бути внутрішніми - всі користувачі системи (працівники підприємства), які мають відповідний рівень доступу до інформації та можуть в тій чи іншій мірі впливати на систему (включаючи адміністратора та адміністратора безпеки). права, мають доступ до конфігурації системи тощо); або зовнішні - суб'єкти несанкціонованого доступу до системи або її елементів (треті особи);

- з причин порушення носії погроз можуть бути спонукані через необережність або безвідповідальність, тобто порушник вчиняє дії, спрямовані на порушення безпеки, ненавмисно або через власні низькі морально-ділові якості («Необережне»); самоствердження або помста, тобто порушник свідомо йде на порушення з метою заподіяння шкоди підприємству або його керівництву. Як правило, такий зловмисник не володіє високим рівнем технічних навичок (Avenger); егоїстичний інтерес, тобто втручання в роботу системи з метою отримання вигоди. Такий зловмисник зазвичай має високий рівень технічної майстерності («Зручність»);

- за рівнем знань про інформаційну систему зловмисник може знати структуру та функціональні особливості системи, принципи її функціонування та безпеки, вміє користуватися технічними засобами, що входять до складу системи («Адміністратор»). ; мати знання та досвід роботи з технічними засобами (елементами системи), їх обслуговування (Технік); як правило, мають високу кваліфікацію в галузі програмування та архітектури інформаційних систем, але не володіють знаннями конкретної системи («Хакер»); володіти високими знаннями та навичками з принципів роботи, проектування та функціонування засобів інформаційної безпеки («Налаштування»);

- за рівнем можливостей порушників можна поділити на тих, хто використовує персонал підприємства (постійних користувачів системи) для отримання доступу до інформації або елементів інформаційної системи («Агент»); використовувати технічні засоби для видалення та перехоплення інформації без впливу на інформаційну систему («Скаут»); використовувати стандартні технічні засоби та недоліки у своїй роботі для обходу засобів захисту, а також переносних комп’ютерних носіїв інформації для проходження постів охорони («Кріт»); застосовувати методи та засоби активного впливу на інформаційні ресурси, їх зміну, використовуючи спеціальні технічні та програмні засоби, технічні пристрої, які підключені до каналів передачі даних, введення програмних закладок, використання спеціального програмного забезпечення (програміст);

- до моменту дії порушники можуть реалізувати загрози інформаційній безпеці безпосередньо під час роботи системи або окремих її компонентів («Час роботи»); в періоди простою системи або її елементів, у тому числі в неробочий час, під час перерв на поточне технічне обслуговування ("Off-Hours"); як під час функціонування системи, так і під час перебоїв у їх роботі («Безперервно»).

Аналіз та запропонована класифікація загроз інформаційної безпеки, а також потенційних носіїв цих загроз є необхідними умовами для подальшої роботи з формування політики інформаційної безпеки на підприємстві. Аналіз вихідних даних, на нашу думку, дозволить продовжити роботу над формуванням політики безпеки на підприємстві.

Вважаємо, що, виявивши всі можливі загрози, які можуть пошкодити інформацію на підприємстві, і тим самим завдати певної шкоди, в першу чергу фінансову, а також проаналізувавши потенційних носіїв цих загроз, керівник підприємства отримає комплекс факторів на основі з яких можна сформувати політику інформаційної безпеки. Таким чином, викладена класифікація покликана спростити роботу з формування чітких моделей загроз і правопорушників, що дає можливість відкинути зайві фактори та зосередитися на тих, хто несе реальну загрозу. При цьому необхідно враховувати потенційно небезпечні впливи, тобто припускати ймовірність різних загроз. Як зазначив М.Ю. Танцюра [34], важливо визначити, чи перевищать витрати на реалізацію політики безпеки можливі фінансові втрати від реалізації тих чи інших загроз.

**2.2. Основи господарської діяльності підприємства**

ТОВ «Детективне агентство «Холмс»за формою власності є товариством з обмеженою відповідальністю. За кодом ЄДР контрагента зареєстрована юридична адреса: 46018, Тернопільська обл., м. Тернопіль, вул. Миру, буд. 2, прим. 65.

Всі співробітники агентства є висококласними професіоналами, колишніми працівниками державних органів правопорядку.

В агентстві є такі фахівці: експерти- криміналісти, оперативні працівники, психологи, графологи, поліграфологи та інші.

Досвід і знання, відповідальне та уважне ставлення до роботи дозволяють розслідувати найскладніші справи, збирати важкодоступну інформацію та шукати людей. Під час роботи приватний детектив збирає інформацію, проводить розслідування та складає протокол, який особисто вручає замовнику, надсилає через Інтернет або іншим зручним для замовника способом.

Детективне агентство забезпечує своїм клієнтам повну конфіденційність.

Послуги приватного детектива розраховані як на юридичних, так і на фізичних осіб. Детективні послуги охоплюють дуже широкий спектр сфер:

- пошук автомобілів і людей, у тому числі за телефоном або даними в Інтернеті;

- збір інформації про організацію чи особу;

- проведення зовнішнього спостереження - за автомобілем, нерухомістю або людиною;

- консультації юристів;

- розкриття крадіжок і крадіжок;

- проведення судово-медичної експертизи будь-якого виду.

Приватний детектив допоможе перевірити потенційного ділового партнера, з’ясувати, чим займається підліток, знайти зниклого.

Агентству можна довірити безпеку компанії на будь-якому рівні: організація охорони на підприємстві, в офісі, перевірка персоналу, спостереження за конкурентами.

Детективне агентство перевіряє майно в Тернополі. Приватний детектив перевірить не лише юридичну чистоту автомобіля чи нерухомості, а й законність угоди, чесність продавця.

Перелік послуг, які надає ТОВ «Детективне агентство Холмс», наведено на рис. 2.3.

Вартість послуг приватного детектива залежить від обсягу та складності роботи, а також пропорційно терміновості її виконання. Ціна робіт відповідає часу та обсягу виконаної роботи. Як підтвердження виконаної роботи приватний детектив надає фільми та фотографії, а також письмовий звіт про виконану роботу.

Досвід країн, де діяльність приватних детективів регулюється законодавством, свідчить, що діяльність приватних детективів, детективних агентств та їх об’єднань значно підвищує відповідальність державної правоохоронної системи за своєчасне та високопрофесійне реагування на потреби громадян та суспільства. . звільняє правоохоронців від необхідності виконання багатьох другорядних нетипових функцій, сприяє загальному покращенню криміногенної ситуації.

**Послуги юридичним особам**

• [Боротьба з контрафактною продукцією](https://poligraf.lviv.ua/borotba_z_kontrafaktnoiu_produktsiieiu)

• [Компютерна безпека, розслідування злочинів в інтернеті](https://poligraf.lviv.ua/kompiuterna_bezpeka%22%20%5Ct%20%22_self)

• [Поради по безпеці підприємства](https://poligraf.lviv.ua/porady_po_bezpetsi_pidpryiemstva)

• [Перевірка первинних документів на автентичність](https://poligraf.lviv.ua/perevirka_pervynnykh_dokumentiv)

• [Організація контрольних закупівель](https://poligraf.lviv.ua/orhanizatsiia_kontrolnykh_zakupivel)

• [Заходи по захисту інформації](https://poligraf.lviv.ua/zakhody_po_zakhystu_informatsii)

• [Встановлення або спростування факту подружньої зради](https://poligraf.lviv.ua/vstanovlennia_faktu_zrady)

• [Перевірка на вірність жінки (чоловіка)](https://poligraf.lviv.ua/perevirka_na_virnist)

• [Повернення в сім’ю жінки (чоловіка)](https://poligraf.lviv.ua/povernennia_v_simiu_zhinky_chy_cholovika)

• [Допомога наркозалежним, сприяння поверненню людини додому](https://poligraf.lviv.ua/dopomoha_narkozalezhnym)

• [Вивід людини із секти, повернення її до нормального способу життя](https://poligraf.lviv.ua/vyvid_liudyny_iz_sekty)

• [Пошук втрачених родинних звя’зків і біологічних батьків](https://poligraf.lviv.ua/poshuk_vtrachenoi_rodyny)

• [Контроль способу життя **«**важких**»**підлітків](https://poligraf.lviv.ua/kontrol_pidlitkiv)

• [Перевірка охорони, водіїв, персоналу](https://poligraf.lviv.ua/perevirka_okhorony_vodiiv_personalu)

• [Перевірка кримінального минулого, біографії і т. п.](https://poligraf.lviv.ua/perevirka_kryminalnoho_mynuloho_ta_biohrafii)

• [Незалежне розслідування злочинів](https://poligraf.lviv.ua/nalezhne_rozsliduvannia_zlochyniv)

• [Пошук свідків і збір доказів](https://poligraf.lviv.ua/poshuk_svidkiv_i_zbir_dokaziv)

• [Допомога людям, потрапившим в сексуальне рабство](https://poligraf.lviv.ua/dopomoha_potrapyvshym_u_seksualne_rabstvo)

• [Перевірка біографії нареченого (нареченої)](https://poligraf.lviv.ua/perevirka_biohrafii_narechenoho)

**Послуги фізичним особам**

• [Перевірка на **«**жучки**»** приміщень, авто](https://poligraf.lviv.ua/perevirka_na_proslukhovuvannia)

• [Графологічна та генетична експертизи](https://poligraf.lviv.ua/hrafolohichna_ta_henetychna_ekspertyzy)

• [Надання інформаційних довідок **«**Юридичні і фізичні особи**»**](https://poligraf.lviv.ua/nadannia_informatsiinykh_dovidok)

• [Визначення місцезнаходження майна, особи, зниклих людей](https://poligraf.lviv.ua/poshuk_liudyny_ta_mistseznakhodzhennia_maina)

•[Збір інформації, доказів, пошук свідків](https://poligraf.lviv.ua/zbir_informatsii_ta_dokaziv)

•[Сприяння в позасудовому і досудовому примиренні сторін](https://poligraf.lviv.ua/pozasudove_i_dosudove_prymyrennia_storin)

**Інші послуги приватного детектива**

Рис. 2.3. Перелік послуг, що надаються ТОВ «Детективне агентство «Холмс»

В Україні цей вид діяльності тривалий час офіційно не визнавався і не був законодавчо врегульований, хоча фактично приватною детективною діяльністю тривалий час і плідно займаються не лише фізичні, а й юридичні особи. За неофіційними даними, зараз в усіх регіонах України налічується кілька тисяч приватних детективів і приватних детективних агентств, а їхні послуги користуються великим попитом у бізнесу, політиків, юристів.

З 2000 р. існує ряд законопроектів про приватну детективну діяльність, розроблених різними авторами, але не отримали законодавчої підтримки. Але з кінця 2015 року на перший план знову постало питання законодавчого регулювання здійснення приватної детективної діяльності.

13 квітня 2017 року з прийняттям Верховною Радою України Закону України «Про приватну детективну (розшукову) діяльність» завершилося понад двадцятирічне легалізацію приватного розшуку в Україні та новий етап у почався розвиток професії приватного детектива. Закон визначає загальні правові засади організації приватної детективної діяльності в Україні як один із способів забезпечення конституційних гарантій особи та громадянина щодо захисту їх законних прав та інтересів.

Відповідно до Закону така діяльність ґрунтується на принципах верховенства права, законності, обачності, об’єктивності та неупередженості, поваги до прав, свобод та законних інтересів фізичних та юридичних осіб, поваги людської гідності, чесності та незалежності. теми приватної детективної діяльності, конфіденційності та професійної таємниці. взаємодія з правоохоронними органами, органами державної влади та місцевого самоврядування, підприємствами, установами, організаціями та громадянами.

Приватним детективом може бути громадянин України, який досяг 21 року, володіє державною мовою, має вищу юридичну освіту або стаж роботи в оперативних підрозділах чи органах досудового розслідування не менше трьох років, пройшов відповідну підготовку з для здійснення приватної детективної діяльності та отримав відповідне свідоцтво на право займатися такою діяльністю, який не зареєстрований в органах охорони здоров’я у зв’язку з психічними захворюваннями, алкоголізмом чи наркоманією, не має судимості.

Приватна детективна діяльність в Україні визначається як підприємницька. Послуги приватного детектива надаються на платній договірній основі.

Приватні детективи зможуть працювати самостійно як індивідуальний підприємець, а також створювати об’єднання приватних детективів. При цьому діяльність приватних детективів буде дозволена як в Україні, так і за кордоном.

Слід зазначити, що детективам заборонено видавати себе за співробітників правоохоронних органів або представників інших державних органів. Крім того, ви не можете збирати інформацію, пов’язану з особистим життям, політичними та релігійними переконаннями осіб без надання їх письмової згоди на це.

Законодавець надав можливість приватним детективам вирішувати досить широкий спектр питань, які були лише у компетенції правоохоронних органів, але тепер приватна та державна системи будуть доповнювати одна одну. Головне, що детективи можуть збирати та фіксувати інформацію, яка згодом може бути використана в цивільному, господарському, адміністративному та кримінальному судочинстві, що надасть громадянам додаткові можливості для захисту своїх прав та особистих інтересів у судах. Інформація, отримана приватними детективами, згідно з документом, є професійною таємницею, яка не підлягає розголошенню, конфіденційна, крім випадків, коли в ній є факти підготовки чи замаху на вчинення кримінального правопорушення (детективи зобов’язані повідомити про такі факти правоохоронні органи з передача допоміжних матеріалів).

Щоб зрозуміти сутність приватної детективної діяльності, слід детальніше зупинитися на таких аспектах, як: 1) професіоналізм; 2) самостійність професійної діяльності; 3) пошук і пошуковий характер; 4) договірні основи виконання; 5) співвідношення з оперативно-розшуковою та розшуковою діяльністю.

Оскільки робота приватного детектива — це не хобі, а професійна діяльність, у сучасних країнах поширеною практикою є створення спеціальних навчальних закладів для підготовки та перепідготовки приватних детективів. Дистанційне навчання та екстернат для них зазвичай не допускаються.

Наприклад, у США функціонує 14 коледжів приватного розшуку, які випускають спеціалістів із ступенем бакалавра та 5 коледжів – зі ступенем магістра приватного розшуку [22, с. 583].

Навчальний план включає юридичну підготовку, тактико-спеціальну, технічну, психологічну підготовку, навчання з надання першої допомоги та підсумкову атестацію.

Юридична підготовка включає: правові основи приватної детективної діяльності; основи кримінального права; кримінальний процес, судова експертиза; цивільне право; цивільне процесуальне право; адміністративне право; використання приватними детективами спеціальних засобів

Спеціальна тактична підготовка включає: види служб, дозволених у недержавній (приватній) розшуковій діяльності; організаційно-тактичні основи діяльності приватних детективів з надання пошукових послуг; використання технічних та інших засобів недержавної (приватної) розшукової діяльності, що не завдають шкоди життю та здоров’ю громадян та довкіллю.

Технічна підготовка включає вивчення та оволодіння: технічними засобами, які використовуються в детективній роботі; системи управління технічними засобами; засоби пожежогасіння, зв'язок та робота з ними.

Психологічна підготовка включає психологічні аспекти детективної роботи; стресові фактори та шляхи їх подолання.

Медична підготовка містить загальні відомості про будову тіла людини; основні ознаки травм і гострих захворювань; методи надання першої медичної допомоги, зокрема, при ударах, вивихах, переломах; правила надання першої медичної допомоги особам, пораненим вогнепальними пораненнями; надання першої медичної допомоги при травмах слізними та подразливими речовинами, ураження електричним струмом; реанімаційні методики

Підготовлені приватні детективи – це, як правило, колишні слідчі та оперативники правоохоронних органів. Зазвичай до них поширюються вимоги щодо несумісності, подібні до тих, що застосовуються до державних службовців.

Суб'єкти приватної детективної (розшукової) діяльності не мають права проводити зазначені в Законі оперативно-розшукові заходи до виключної компетенції оперативних підрозділів, передбачених ст. 5 Закону України «Про оперативно-розшукову діяльність».

Видача свідоцтв на право здійснення приватної детективної (розшукової) діяльності здійснюється Національною поліцією України з урахуванням вимог цього Закону.

Замовниками послуг приватного детектива або приватної детективної компанії можуть бути фізичні чи юридичні особи України, а також іноземні громадяни чи юридичні особи.

Суб'єкт, який здійснює приватну детективну (розшукову) діяльність, може надавати своїм клієнтам послуги, передбачені ст. 12 цього Закону після укладення з ними відповідного письмового договору (контракту).

Законодавець визначив такі види приватних детективних послуг:

1) збирання, облік і дослідження інформації, необхідної для розгляду справ у цивільному, господарському та адміністративному судочинстві, на договірних засадах зі сторонами судового розгляду;

2) дослідження ринку, пошук та збір інформації з відкритих джерел для підготовки ділових переговорів клієнта, з'ясування фінансової платоспроможності, майнового стану та надійності потенційних ділових партнерів;

3) уточнення біографічних та інших даних, що характеризують особу, щодо окремих громадян (за їх письмовою згодою) при укладенні ними трудових та інших договорів із замовником (замовником) послуг приватного детектива (розшуку) (займаючи відповідну вакантну посаду) , виявлення їх ділових відносин, у тому числі з конкурентами клієнта в регіонах та за кордоном;

4) розшук осіб, місцезнаходження яких невідоме, з’ясування причин та обставин зникнення, можливостей та умов їх повернення, розшук осіб, які втратили родинні та дружні зв’язки;

5) розшук зниклого (втраченого чи викраденого) майна, предметів та тварин;

6) пошук, збір та фіксація інформації у кримінальному провадженні на договірних засадах зі стороною кримінального провадження;

7) здійснення заходів щодо відтворення втраченої (відсутньої) інформації про законні права та інтереси клієнтів;

8) пошук та збір даних, які можуть бути приводом або підставою для звернення замовника приватних детективних (розшукових) послуг до правоохоронних органів або суду з метою захисту законних прав та інтересів такого замовника;

9) виявлення фактів незаконного (несанкціонованого) збору з метою використання інформації, що становить комерційну таємницю замовника, або її розголошення, а також фактів незаконного (несанкціонованого) збору конфіденційної інформації щодо фізичних осіб;

10) пошук, виявлення та фіксація фактів незаконного використання прав інтелектуальної власності, що належать клієнту, а також випадків недобросовісної конкуренції;

11) розшук боржників та осіб, які ухиляються від виконання своїх договірних зобов'язань, вирішення в порядку, встановленому законодавством України, питань стягнення заборгованості та виконання договірних зобов'язань;

12) забезпечення захисту з обмеженим доступом (комерційної, виробничої, професійної таємниці) замовника приватних детективних (розшукових) послуг.

Отже, хоча цей Закон № 3726 «Про приватну детективну (розшукову) діяльність» не розширює права приватних детективів, але це важливий крок українського законодавства у сфері розшукової діяльності.

**Висновки до розділу 2**

Проведення аналізу інформаційного забезпечення безпеки підприємства дозволило зробити ряд висновків.

ТОВ «Детективне агентство «Холмс» за формою власності є товариством з обмеженою відповідальністю.

Всі співробітники агентства є висококласними професіоналами, колишніми працівниками державних органів правопорядку.

В агентстві є такі фахівці: експерти- криміналісти, оперативні працівники, психологи, графологи, поліграфологи та інші.

Досвід і знання, відповідальне та уважне ставлення до роботи дозволяють розслідувати найскладніші справи, збирати важкодоступну інформацію та шукати людей. Під час роботи приватний детектив збирає інформацію, проводить розслідування та складає протокол, який особисто вручає замовнику, надсилає через Інтернет або іншим зручним для замовника способом.

Детективне агентство забезпечує своїм клієнтам повну конфіденційність.

Послуги приватного детектива розраховані як на юридичних, так і на фізичних осіб. Детективні послуги охоплюють дуже широкий спектр сфер: пошук автомобілів і людей, у тому числі за телефоном або даними в Інтернеті; збір інформації про організацію чи особу; проведення зовнішнього спостереження за автомобілем, нерухомістю або людиною; консультації юристів; розкриття крадіжок і крадіжок; проведення судово-медичної експертизи будь-якого виду.

Вважаємо, що, виявивши всі можливі загрози, які можуть пошкодити інформацію на підприємстві, і тим самим завдати певної шкоди, в першу чергу фінансову, а також проаналізувавши потенційних носіїв цих загроз, керівник підприємства отримає комплекс факторів на основі з яких можна сформувати політику інформаційної безпеки. Таким чином, викладена класифікація покликана спростити роботу з формування чітких моделей загроз і правопорушників, що дає можливість відкинути зайві фактори та зосередитися на тих, хто несе реальну загрозу. При цьому необхідно враховувати потенційно небезпечні впливи, тобто припускати ймовірність різних загроз.

**РОЗДІЛ 3**

**ШЛЯХИ УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА**

**3.1. Шляхи управління інформаційною безпекою підприємства**

Завдяки масовій комп’ютеризації та інформатизації ринку товарів і послуг суб’єкти господарювання мають доступ до різноманітної інформації, а тим самим полегшують процеси виробництва, управління та збуту продукції. Проте за останні роки почастішали випадки електронного шахрайства та кіберзлочинності, що негативно позначилося на бізнесі.

Гостра проблема інформаційної безпеки комерційних організацій набула актуальності в сучасних умовах масового використання комп'ютерних інформаційних систем. Відповідно, надійним засобом захисту підприємства від інформаційних загроз є створення ефективної та дієвої системи захисту.

Сучасні інформаційні системи призначені для забезпечення працездатності інформаційної інфраструктури підприємства, надання різних видів інформаційних послуг, автоматизації фінансової та виробничої діяльності, а також бізнес-процесів організації, що дозволяє знизити як фінансові, так і трудові витрати. Інформаційні системи зберігають та обробляють значні обсяги інформації різного ступеня секретності, тому гостро постає питання захисту цих інформаційних систем підприємства від різноманітних загроз інформаційній безпеці [7, с. 158].

Інформація може приймати різні форми. Його можна роздрукувати або написати на папері, зберігати в електронному вигляді, передавати поштою чи електронними засобами, відображати на плівці або висловлювати усно. Незалежно від форми, засобів поширення та зберігання інформація є цінним активом будь-якого підприємства [10].

Розвиток теорії менеджменту дозволяє розглянути нові самостійні напрямки управління, пов’язані з управлінням інформаційними ресурсами, впровадженням і використанням інформаційних технологій у діяльності підприємств і організацій, управлінням процесами обробки інформації в організаціях.

Розвиток комп’ютерних технологій та їх використання в багатьох сферах економіки є сьогодні одним із основних факторів його ефективності. Проте прогрес в інформаційно-технічній сфері створив потенційні загрози через розробку нових та вдосконалення вже відомих методів наукового шпигунства, що дозволяють швидко знаходити необхідну інформацію в ЕОМ [38, с. 349].

Інформаційна безпека підприємства насамперед стосується захисту інформаційних систем, особливо виконуваних функцій (табл. 3.1).

Таблиця 3.1

Функції інформаційних систем [32, с. 19].

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Системамаркетингу | ВиробничіСистеми | Фінансові системи та системи обліку | Системакадрів | Інші системи (напр., ІС керівництва) |
| Дослідження ринку і прогнозування продаж | Планування обсягів робіт і розробка календарних планів | Управлінняпортфелемзамовлень | Аналіз і прогнозування потреби у трудових ресурсах | Контроль за діяльністю організації |
| Управлінняпродажами | Оперативний контроль і управління виробництвом | Управліннякредитноюполітикою | Ведення архівів записів про персонал | Виявленняоперативнихпроблем |
| Рекомендації з виробництва нової продукції | Аналіз роботи обладнання | Розробкафінансовогоплану | Аналіз і планування підготовки кадрів | Аналіз управлінських і стратегічних ситуацій |
| Аналіз і встановлення ціни | Участь у формуванні замовлень постачальникам | Фінансовий аналіз і прогнозування | Забезпеченняпроцесукадровогоуправління | Виробленнястратегічнихрішень |
| Облікзамовлень | Управлінняресурсами | Контроль бюджету. Бухгалтерський облік і розрахунок заробітної платні |  |  |

Найбільш поширені види потенційних загроз і небезпек для комерційного підприємства у сфері інформаційної діяльності:

- відсутність копіювання важливих бухгалтерських та організаційно-розпорядчих документів на матеріальних носіях інформації;

- відсутність ведення протоколів змін у програмному забезпеченні;

- недобросовісного використання інформації працівниками підприємства;

- відсутність регламентації доступу користувачів до різних видів інформації та баз даних;

- відсутність схем інформаційного забезпечення рівнів управління;

можливість несанкціонованого втручання в програмне забезпечення та базу даних;

- крадіжка носіїв інформації;

- промислове шпигунство;

- хакерські атаки, шкідливе програмне забезпечення, комп'ютерні віруси;

- піратське програмне забезпечення, неліцензійні антивірусні програми, відсутність брандмауера від інтернет-атак;

- наявність у системі управління підприємством непідзвітних посадових осіб.

Отже, інформаційні системи виконують багато важливих функцій, які об'єднують систему управління.

Виникла необхідність створення інформаційної інфраструктури підприємства на основі парадигми єдиного інформаційного простору підприємства, що передбачає інтеграцію різноманітної науково-технічної, інженерної, фінансової, маркетингової та інших видів інформації в рамках єдиної системи. Створення єдиного інформаційного простору дозволяє реалізувати єдиний безперервний цикл інновацій підприємства, гнучко враховуючи ринкові сигнали в процесі вдосконалення продукції, що дозволяє найбільш повно задовольнити потреби клієнтів.

Інформаційну безпеку (ІБ) зазвичай розуміють як стан (власність) захищеності ресурсів інформаційної системи за наявності загроз в інформаційній сфері.

Інформаційний захист – це процес, спрямований на забезпечення інформаційної безпеки. Визначальними факторами інформаційної безпеки є загроза та ризик. Загроза — це потенційна причина (подія, порушення, інцидент), що знижує рівень інформаційної безпеки системи, тобто потенційно здатна призвести до негативних наслідків (впливу) та шкоди (втрат) для системи чи організації.

Інформаційна безпека - це механізм захисту, який забезпечує:

1) Конфіденційність: доступ до інформації мають лише авторизовані користувачі.

2) Цілісність: достовірність і повнота інформації та методів її обробки.

3) Доступність: доступ до інформації та пов'язаних активів для авторизованих користувачів, коли це необхідно.

Для побудови та ефективної роботи СПІБ (система інформаційної безпеки) А.В. Черевко рекомендує:

- виявити вимоги інформаційної безпеки, характерні для даного об'єкта захисту;

- враховувати вимоги національного та міжнародного законодавства;

- використовувати передовий досвід (стандарти, методології) для побудови аналогічного SPIB;

- визначити підрозділи, відповідальні за впровадження та підтримку ВОІВ;

- розподілити між підрозділами зони відповідальності за виконання вимог СПІБ;

- на основі управління ризиками інформаційної безпеки знайти загальні положення, технічні та організаційні вимоги, що складають політику інформаційної безпеки об'єкта, що охороняється;

- реалізовувати вимоги політики інформаційної безпеки шляхом впровадження відповідних програмно-технічних засобів і методів захисту інформації;

- впровадити систему управління інформаційною безпекою (СУІБ);

- за допомогою системи управління організовувати регулярний моніторинг ефективності СПІБ та, за потреби, переглядати та коригувати СПІБ [41].

Зміст роботи з контролю інформаційної безпеки підприємства повинен включати:

- процедури моніторингу та перевірки та інші засоби контролю ризиків (захисні заходи) для швидкого виявлення помилок в обробці результатів, швидкого виявлення порушень безпеки, надання інформації керівництву, допомоги у визначенні небезпечних подій та запобігання інцидентам загроз інформації та інших видів безпеки підприємства шляхом використання відповідних систем критеріїв;

- регулярні перевірки ефективності системи управління інформаційною безпекою (включаючи дотримання політики та досягнення цілей системи управління інформаційною безпекою, перевірку засобів контролю безпеки) з урахуванням результатів аудиту безпеки, інцидентів, результатів вимірювань ефективності. , пропозиції всіх зацікавлених сторін;

- перегляд оцінки рівня ризику через заплановані проміжки часу, а також виявлення залишкових ризиків та визначення прийнятних рівнів ризику відповідно до змін в організації та її операційному та бізнес-середовище;

- здійснення внутрішніх аудитів системи управління інформаційною безпекою;

- здійснення аудиту керівництвом системи управління інформаційною безпекою для підтвердження адекватності її обсягу та ефективності заходів щодо вдосконалення системи управління інформаційною безпекою [31, с. 158].

У таблиці 3.2 наведено характеристику основних міжнародних стандартів управління інформаційними ризиками на комерційному підприємстві.

Таблиця 3.2

Міжнародні стандарти з керування методів для визначення інформаційних ризиків та їх коротка характеристика [27, с. 223-224]

|  |  |  |
| --- | --- | --- |
| Стандарт | Назва стандарту | Коротка характеристика |
| ІБО/ІБС27002-2012 | Інструкція 3 менеджменту інформаційної безпеки для телекомунікаційних організацій | Цей стандарт надає додаткові рекомендації з реалізації та менеджменту ІБ в телекомунікаційних організаціях. Визначає цілі, вимоги оцінки ризику до системи ІБ та забезпечує контроль управління. Діючий Міжнародний стандарт пропонує рекомендації та основні принципи введення, реалізацію, поліпшення менеджменту ІБ |
| ІБО/ІБС27003-2012 | Інструкція з реалізації системи менеджменту ІБ | У цьому Міжнародному стандарті розглядаються найважливіші аспекти, необхідні для успішної розробки та впровадження в СМІБ відповідно зі стандартом ІБО/ІБС 27001:2005, який розглядає процес визначення та розробку СМІБ від початку до стану впровадження |
| ІБО/ІЕС27004-2011 | Менеджмент інформаційної безпеки вимірювання | Цей стандарт містить рекомендації з розробки та використання вимірювань і заходів вимірювання для проведення оцінки ефективності реалізованої СМІБ.Процес вимірювання реалізується у вигляді програми, пов’язаний з ІБ. Програма вимірювань надає допомогу користувачу у виявленні і оцінюванні вимог, яким не відповідає процес ефективності контролю і управління СМІБ, а також визначення пріоритетів дій, спрямованих на удосконалення або зміну цих процесів |
| ІБО/ІЕС27005-2010 | Менеджмент ризику інформаційної безпеки який конкретизує поняття інформаційного ризику | Цей стандарт поданий у вигляді додатку прикладу типових загроз, уразливостей та потреб інформаційної безпеки. Проблема оцінювання та дослідження інформаційних ризиків насамперед асоціюється з британським стандартом В Б 7799, а саме з його двома частинами: першою - В Б 7799-1 «Звіт правил з менеджменту безпеки інформації» та другою - ВБ 7799-2 «Системи менеджменту безпекою інформації», у яких вперше питання аналізу стану безпеки інформації та формування її захисту були напряму пов’язані з інформаційними ризиками. Однак, безпосередньо, аспекти оцінювання та управління ризиками були докладніше розглянуті у третій частині стандарту В Б 7799-3 «Настанови з менеджменту ризиками безпеки інформації» |
| ІБО/ІЕСТЯ13335-2:1997 | Настанови з керування безпекою інформаційних технологій (ІТ) | Надати рекомендації, а не конкретні рішення з керування безпекою інформаційних технологій (ІТ). Кваліфікація осіб, відповідальних за безпеку ІТ у межах організацій повинна бути достатньою для адаптування матеріалів, поданих у цьому стандарті, до конкретних потреб організацій |

ISO / IEC 27001: 2015 Інформаційні технології - Методи безпеки - Системи управління інформаційною безпекою - Вимоги. Цей стандарт був створений для визначення вимог до розробки, впровадження, експлуатації, моніторингу, перегляду, підтримки та постійного вдосконалення системи управління інформаційною безпекою (СУІБ). Прийняття системи управління інформаційною безпекою є стратегічним рішенням для організації. На розробку та впровадження системи управління інформаційною безпекою організації впливають потреби та цілі організації, вимоги безпеки, застосовувані організаційні процеси, а також розмір і структура організації.

Система управління інформаційною безпекою забезпечує збереження конфіденційності, цілісності та доступності інформації за допомогою впровадження процесу управління ризиками та надає зацікавленим сторонам впевненість у належному управлінні ризиками.

**3.2 Окремі засоби зміцнення інформаційної безпеки підприємства**

Основною метою будь-якої системи інформаційної безпеки є забезпечення коректної та безперебійної роботи захищеного об’єкта, запобігання можливим фінансовим втратам через загрози безпеці, розкриття таємниці бізнес-процесів, спотворення та знищення службової інформації. Іншою метою можна вважати забезпечення якості послуг та гарантії безпеки інтересів як власників інформаційних ресурсів, так і їх клієнтів, гарантуючи взаємну конфіденційність даних. Встановлений ступінь конфіденційності інформації, як правило, зберігається під час її обробки в інформаційних системах та під час передачі по телекомунікаційних мережах.

Для досягнення вищезазначених цілей необхідно вирішити ряд завдань:

- обмежити доступ до інформації, яка становить службову таємницю;

- визначати та здійснювати адміністративні заходи щодо виявлення загроз безпеці інформаційних ресурсів;

- з'ясувати можливі мотиви, спрямовані на заподіяння матеріальної та моральної шкоди;

- використання правових, організаційних і технічних засобів забезпечення безпеки;

- створення умов для максимальної локалізації можливих втрат: фінансових, матеріальних і моральних, що призводять до порушення нормального функціонування та розвитку організації.

Режим інформаційної безпеки в таких системах забезпечується:

- на адміністративному рівні політика безпеки організації, яка формулює цілі інформаційної безпеки та шляхи їх досягнення;

- на процесуальному рівні - шляхом розробки та впровадження розділів інструкцій для персоналу, присвячених інформаційній безпеці, а також заходам фізичного захисту;

- на програмно-технічному рівні - з використанням перевірених і сертифікованих рішень, стандартного набору контрзаходів: резервне копіювання, антивірусний і парольний захист, брандмауери, шифрування даних тощо.

При створенні системи інформаційної безпеки важливо не виключити жодного істотного аспекту – в цьому випадку застосовуваним інформаційним технологіям буде гарантований відповідний рівень інформаційної безпеки.

Для того, щоб система інформаційної безпеки була збалансованою, на початку процесу її формування проводиться аналіз можливих ризиків, які можуть загрожувати інформаційній системі підприємства. На основі аналізу загроз, ризиків, вразливостей, потенційних точок проникнення в систему, оцінки збитків формується обґрунтування вибору заходів протидії загрозам, які завдають шкоди підприємству чи організації у вигляді моральної чи матеріальної шкоди (Рис. 3.1).

Рис. 3.1. Модель реалізації загроз інформаційної безпеки [9, с. 95]

Загальний підхід до інформаційної безпеки передбачає наступні кроки [29]:

- визначити цілі забезпечення інформаційної безпеки АІС (наприклад, забезпечення технологічної незалежності та високої конкурентоспроможності технічного потенціалу підприємства/організації, захист інформаційного поля комерційної таємниці та досягнення необхідного рівня інформаційного забезпечення роботи всіх відділи);

- створити ефективну систему управління інформаційною безпекою (чинником ефективності системи управління інформаційною безпекою є її побудова на основі міжнародних стандартів ISO / IEC 17799: 2005 та ISO / IEC 27001: 2011 [45];

- оцінити відповідність запропонованих заходів із забезпечення інформаційної безпеки заявленим цілям (оцінка поточного рівня ефективності системи; локалізація вузьких місць у системі; оцінка відповідності системи підприємства існуючим стандартам у сфері інформації; охорона; розробка рекомендацій та нормативних документів щодо забезпечення безпеки об'єктів, що охороняються).

Прийняті вимоги до системи інформаційної безпеки, що розробляється, повинні враховувати відповідні заходи на всіх етапах життєвого циклу інформаційної системи, тобто протягом усього періоду існування системи від початку розробки до кінця її використання та утилізації комплексу автоматизації інформаційної системи. Таким чином, розробка відповідних заходів інформаційної безпеки відбувається після закінчення аналізу ризиків і вибору заходів, які повинні запобігти цим ризикам. Слід зазначити, що обов’язковою складовою цих заходів є періодична перевірка: наскільки існуючий режим інформаційної безпеки відповідає політиці безпеки, розробленій для певних умов функціонування конкретного підприємства.

Через відсутність надійного і водночас простого та доступного методичного інструментарію для створення адекватної системи захисту інформації виникає необхідність пошуку та визначення шляхів, які сприятимуть розвитку комплексу інформаційної безпеки в неоднорідному інформаційному підприємстві. системи [33]. Формування та реалізація рекомендацій/інструкцій політики інформаційної безпеки має стосуватися всіх етапів життєвого циклу інформаційної системи, бути комплексними та спиратися на перевірені методи та методи, які виявилися ефективними та надійними, з одного боку, та з іншого боку, використовувати перспективний підхід до побудови складних систем захисту інформації в комп'ютерних мережах, що дозволяє подолати деякі недоліки традиційних методів захисту, а саме технології інтелектуальних багатоагентних систем.

Серед таких методів можна виділити обов’язкове використання певних засобів ідентифікації та аутентифікації об’єктів та суб’єктів, засобів резервного копіювання, антивірусного контролю: для виявлення комп’ютерних вірусів і протидії їм, додавання структури цінності до опису об’єкта автоматизації. та провести аналіз ризиків, визначити правила для будь-якого процесу використання цього типу доступу до ресурсів об’єкта автоматизації, які мають такий ступінь цінності, тощо.

Прийоми та методи поділяються на групи заходів, спрямованих на забезпечення інформаційної безпеки організації, серед яких:

- управління персоналом;

- фізичний захист;

- підтримка продуктивності;

- реагування на порушення режиму охорони;

- планування реставраційних робіт.

Слід зазначити, що при розробці концепції інформаційної безпеки для підприємства слід не тільки спиратися на вищезазначені групи видів діяльності, але й враховувати сферу діяльності компанії/організації, яка формулюватиме конкретні вимоги до інформаційної безпеки, обсяг коштів, які планується витратити, а також рівень і кількість спеціалістів. що вони будуть залучені до розробки та реалізації політики щодо збереження конфіденційних даних, можуть бути збитки від можливого зниження репутації організації, дезорганізації її діяльності.

Система управління інформаційною безпекою повинна здійснювати управління ризиками, контролювати ефективність системи в цілому, коригувати управління персоналом, впорядковувати документацію та записи самої системи управління ІБ, з можливістю її перегляду та модернізації, нести відповідальність за безперервність діяльності та швидкість його відновлення після критичних (з точки зору інформаційної безпеки) перерв (рис. 3.2)

Рис. 3.2. Модель системи безпеки підприємства в інформаційній сфері [9, с. 96]

Вимоги, які диктує система управління інформаційною безпекою, виконуються або спеціальними працівниками відповідної служби, або відповідальними працівниками з досвідом роботи та повноваженнями, призначеними адміністрацією, і мають змогу ознайомити рядових працівників із правилами роботи з системою, навчання їх та своєчасне інформування.

При цьому використання технології інтелектуальних мультиагентних систем дає змогу порівняно з традиційними методами значно підвищити ефективність захисту інформації, зокрема її адекватність, відмовостійкість, стійкість до руйнівних дій, універсальність, гнучкість тощо. автономні об'єкти/агенти), здатні отримувати, зберігати, обробляти та передавати інформацію як в інтересах вирішення власних, так і корпоративних завдань аналізу та синтезу інформації. У подібних системах кожен агент розглядається як система, заснована на знаннях з додаванням компонентів, що забезпечують безпеку, якість обслуговування, взаємодію з мережевими ресурсами та користувачами. Поняття агента відповідає апаратно або програмно реалізованої сутності, яка здатна діяти в інтересах досягнення цілей, оскільки однією з особливостей багатоагентних систем є здатність вирішувати складні погано формалізовані задачі, що вимагають побудови оригінальний алгоритм рішення в залежності від конкретної ситуації, що характеризується невизначеністю і динамічністю вихідних даних. і знання.

Забезпечення інформаційної безпеки є присутнім фактором, обов'язковим і необхідним елементом цілеспрямованої діяльності багатоагентних систем для підтримки функціонування систем інформаційної безпеки на основі політик безпеки.

Досвід показує, що для боротьби з правопорушеннями у сфері обігу інформації на підприємстві необхідна цілеспрямована організація процесу захисту інформаційних ресурсів.

Джерелом цього виду загрози можуть бути внутрішні (власні працівники), зовнішні (наприклад, конкуренти) та змішані (замовники є зовнішніми, а виконавцем є працівник компанії). Як показує практика, більшість цих правопорушень вчиняють самі працівники підприємства.

Що є безпосереднім об’єктом правопорушень у сфері обігу інформації? Перш за все, це інформація (дані). Правопорушник отримує доступ до захищеної інформації без дозволу її власника або з порушенням встановленого порядку доступу. Способи такого несанкціонованого доступу до комп’ютерної інформації можуть бути різними – крадіжка носія інформації, порушення засобів захисту інформації, використання чужого імені, зміна коду чи адреси технічного пристрою, подання фіктивних документів на право доступу до інформації. , встановлення записуючого обладнання, підключеного до каналів передачі даних. доступ може здійснюватися в приміщеннях підприємства, де зберігаються носії інформації, з комп'ютера на робочому місці, локальної мережі, глобальної мережі. Усі загрози об’єктам інформаційної безпеки за методом впливу можна об’єднати у п’ять груп [19, с. 172]: власне інформаційні, фізичні, організаційно-правові, програмно-математичні, радіоелектронні.

Наслідки вчинених протиправних дій можуть бути різними:

- копіювання інформації (оригінал зберігається);

- зміна змісту інформації в порівнянні з тим, що був раніше;

- блокування інформації - неможливість її використання під час збереження інформації;

- знищення інформації без можливості її оновлення;

- несправність комп'ютера, комп'ютерної системи або їх мережі.

Правове регулювання обігу інформації на підприємстві та відповідальності за порушення у цій сфері ґрунтується на тому, що, відповідно до законодавства України, захисту підлягає будь-яка документована інформація, неправомірне використання якої може завдати шкоди її власнику, користувачеві. Захист здійснюється з метою витоку, крадіжки, втрати, спотворення, підробки інформації, а також для запобігання несанкціонованим діям щодо знищення, зміни, спотворення, копіювання, блокування інформації; недопущення інших форм незаконного втручання в інформаційні ресурси та інформаційні системи, забезпечення правового режиму документованої інформації як об’єкта права власності. Крім того, за зазначені протиправні дії передбачена як адміністративна, так і кримінальна відповідальність. І це не випадково, оскільки загрози інформаційним системам можуть призвести не тільки до значних фінансових втрат, а й до незворотних наслідків – ліквідації самого суб’єкта господарювання.

Забезпечення безпеки підприємств з боку інформаційних систем є одним із блоків проблеми безпеки. Захист від правопорушень у сфері обігу інформації слід розпочинати з розробки концепції інформаційної безпеки підприємства.

Способи захисту підприємства від правопорушень у сфері обігу інформації можна поділити на дві групи – організаційні та технічні. Методи організаційного захисту пов'язані з обмеженням можливого несанкціонованого фізичного доступу до інформаційних систем. Методи технічного захисту передбачають використання програмно-технічних засобів, спрямованих насамперед на обмеження доступу користувача, що працює з інформаційними системами підприємства, до інформації, на яку він не має права доступу.

Практики виділяють, наприклад, такі основні напрямки технічного захисту інформаційних систем [23]:

- захист інформаційних ресурсів від несанкціонованого доступу та використання - використовуються засоби контролю включення та завантаження програмного забезпечення, а також методи захисту паролем при вході в систему;

- захист від витоку по вторинних каналах електромагнітного випромінювання та перешкод - шляхом екранування обладнання, приміщень, використанням маскуючих генераторів шуму, додаткового випробування обладнання на наявність компрометуючого випромінювання;

- захист інформації в каналах зв'язку та вузлах комутації - використовуються процедури аутентифікації абонентів і повідомлень, шифрування та спеціальні протоколи зв'язку;

- захист правового значення електронних документів - при довірчих відносинах між двома суб'єктами господарювання та коли виникає необхідність передачі документів (платіжних доручень, договорів) через комп'ютерні мережі - для визначення правдивості адресата, документ доповнюється записом «цифровий підпис» - спеціальна мітка, логічно пов'язана з текстом і сформована за допомогою секретного криптографічного ключа;

- захист автоматизованих систем від комп'ютерних вірусів і незаконної модифікації - використовуються імуностійкі програми та механізми модифікації фактів програмного забезпечення.

Отже, на основі проведеного дослідження, як узагальнення, можна зазначити, що підприємства розглядаються як суб’єкти інформаційного права, а тому повинні вивчати інформаційні правовідносини, в які вони практично вступають, здійснюючи повноваження, врегульовані нормами різних галузей закону, їх статус як суб'єкта зазначеної галузі.

При цьому одним із фундаментальних аспектів, на якому слід зосередити увагу, є питання забезпечення інформаційної безпеки підприємства. Якщо процедури створення, отримання спеціальних статусів і дозволів, припинення діяльності та нагляду за такою діяльністю більше пов’язані з предметом інших галузей права, то забезпечення інформаційної безпеки, необхідність якого, як намагався показати автор, проявляється Сам по собі протягом усього існування підприємства та його взаємодія з іншими суб'єктами майже повністю пов'язаний з предметом інформаційного права. У той же час, оскільки неможливо повноцінно виділити інформаційну складову в діяльності підприємства, настільки важко розрізнити правове регулювання цієї сфери різними галузями права.

**Висновки до розділу 3**

Гостра проблема інформаційної безпеки комерційних організацій набула актуальності в сучасних умовах масового використання комп'ютерних інформаційних систем. Відповідно, надійним засобом захисту підприємства від інформаційних загроз є створення ефективної та дієвої системи захисту.

Сучасні інформаційні системи призначені для забезпечення працездатності інформаційної інфраструктури підприємства, надання різних видів інформаційних послуг, автоматизації фінансової та виробничої діяльності, а також бізнес-процесів організації, що дозволяє знизити як фінансові, так і трудові витрати. Інформаційні системи зберігають та обробляють значні обсяги інформації різного ступеня секретності, тому гостро постає питання захисту цих інформаційних систем підприємства від різноманітних загроз інформаційній безпеці.

Основною метою будь-якої системи інформаційної безпеки є забезпечення коректної та безперебійної роботи захищеного об’єкта, запобігання можливим фінансовим втратам через загрози безпеці, розкриття таємниці бізнес-процесів, спотворення та знищення службової інформації. Іншою метою можна вважати забезпечення якості послуг та гарантії безпеки інтересів як власників інформаційних ресурсів, так і їх клієнтів, гарантуючи взаємну конфіденційність даних. Встановлений ступінь конфіденційності інформації, як правило, зберігається під час її обробки в інформаційних системах та під час передачі по телекомунікаційних мережах.

Для досягнення вищезазначених цілей необхідно вирішити ряд завдань:

- обмежити доступ до інформації, яка становить службову таємницю;

- визначати та здійснювати адміністративні заходи щодо виявлення загроз безпеці інформаційних ресурсів;

- з'ясувати можливі мотиви, спрямовані на заподіяння матеріальної та моральної шкоди;

- використання правових, організаційних і технічних засобів забезпечення безпеки;

- створення умов для максимальної локалізації можливих втрат: фінансових, матеріальних і моральних, що призводять до порушення нормального функціонування та розвитку організації.

**ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ**

Аналіз теоретичних та практичних аспектів інформаційної компоненти забезпечення економічної безпеки дозволив зробити ряд висновків та пропозицій.

Найпоширенішим із тлумачень «економічної безпеки» є її розуміння як «системи захисту від негативних впливів зовнішнього та внутрішнього середовища». Така інтерпретація економічної безпеки ґрунтується на захисній властивості сукупності засобів, методів і засобів, що використовуються для забезпечення реалізації поставлених цілей, та визначенні сукупності загроз, небезпек і ризиків та визначенні напряму їх впливу на діяльності підприємства.

Загрози збереження, цілісності та конфіденційності інформаційних ресурсів обмеженого доступу практично реалізуються через ризик формування каналу несанкціонованого отримання (вилучення) кимось цінної інформації та документів. Відповідно, забезпечення інформаційної безпеки має починатися з визначення суб’єктів господарських відносин, пов’язаних із використанням інформаційних систем. Спектр їх інтересів можна розділити на такі основні категорії: доступність (можливість отримати необхідну інформаційну послугу в розумний час), цілісність (актуальність і несуперечливість інформації, її захист від знищення та несанкціонованого зміни), конфіденційність (захист від несанкціонованого знайомства). У зв'язку з цим інформаційна безпека є невід'ємним елементом системи економічної безпеки. Відповідно, комплексна інформаційна безпека є запорукою забезпечення економічної безпеки підприємства.

ТОВ «Детективне агентство «Холмс» за формою власності є товариством з обмеженою відповідальністю.

Всі співробітники агентства є висококласними професіоналами, колишніми працівниками державних органів правопорядку.

В агентстві є такі фахівці: експерти- криміналісти, оперативні працівники, психологи, графологи, поліграфологи та інші.

Досвід і знання, відповідальне та уважне ставлення до роботи дозволяють розслідувати найскладніші справи, збирати важкодоступну інформацію та шукати людей. Під час роботи приватний детектив збирає інформацію, проводить розслідування та складає протокол, який особисто вручає замовнику, надсилає через Інтернет або іншим зручним для замовника способом.

Детективне агентство забезпечує своїм клієнтам повну конфіденційність.

Послуги приватного детектива розраховані як на юридичних, так і на фізичних осіб. Детективні послуги охоплюють дуже широкий спектр сфер: пошук автомобілів і людей, у тому числі за телефоном або даними в Інтернеті; збір інформації про організацію чи особу; проведення зовнішнього спостереження за автомобілем, нерухомістю або людиною; консультації юристів; розкриття крадіжок і крадіжок; проведення судово-медичної експертизи будь-якого виду.

Вважаємо, що, виявивши всі можливі загрози, які можуть пошкодити інформацію на підприємстві, і тим самим завдати певної шкоди, в першу чергу фінансову, а також проаналізувавши потенційних носіїв цих загроз, керівник підприємства отримає комплекс факторів на основі з яких можна сформувати політику інформаційної безпеки. Таким чином, викладена класифікація покликана спростити роботу з формування чітких моделей загроз і правопорушників, що дає можливість відкинути зайві фактори та зосередитися на тих, хто несе реальну загрозу. При цьому необхідно враховувати потенційно небезпечні впливи, тобто припускати ймовірність різних загроз.

Гостра проблема інформаційної безпеки комерційних організацій набула актуальності в сучасних умовах масового використання комп'ютерних інформаційних систем. Відповідно, надійним засобом захисту підприємства від інформаційних загроз є створення ефективної та дієвої системи захисту.

Сучасні інформаційні системи призначені для забезпечення працездатності інформаційної інфраструктури підприємства, надання різних видів інформаційних послуг, автоматизації фінансової та виробничої діяльності, а також бізнес-процесів організації, що дозволяє знизити як фінансові, так і трудові витрати. Інформаційні системи зберігають та обробляють значні обсяги інформації різного ступеня секретності, тому гостро постає питання захисту цих інформаційних систем підприємства від різноманітних загроз інформаційній безпеці.

Основною метою будь-якої системи інформаційної безпеки є забезпечення коректної та безперебійної роботи захищеного об’єкта, запобігання можливим фінансовим втратам через загрози безпеці, розкриття таємниці бізнес-процесів, спотворення та знищення службової інформації. Іншою метою можна вважати забезпечення якості послуг та гарантії безпеки інтересів як власників інформаційних ресурсів, так і їх клієнтів, гарантуючи взаємну конфіденційність даних. Встановлений ступінь конфіденційності інформації, як правило, зберігається під час її обробки в інформаційних системах та під час передачі по телекомунікаційних мережах.

Для досягнення вищезазначених цілей необхідно вирішити ряд завдань:

- обмежити доступ до інформації, яка становить службову таємницю;

- визначати та здійснювати адміністративні заходи щодо виявлення загроз безпеці інформаційних ресурсів;

- з'ясувати можливі мотиви, спрямовані на заподіяння матеріальної та моральної шкоди;

- використання правових, організаційних і технічних засобів забезпечення безпеки;

- створення умов для максимальної локалізації можливих втрат: фінансових, матеріальних і моральних, що призводять до порушення нормального функціонування та розвитку організації.

**ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ**

1. Аніловська Г.Я. Інформаційна безпека підприємства в умовах використання сучасних інформаційних технологій. *Науковий вісник ЛНТУ України*. 2008. Вип. 18 (9). 270 с.
2. Баїк О. І. Поняття і категорії як основа науки по­даткового права України. *Вісник Національного уні­верситету «Львівська політехніка». Юридичні науки*. 2015. № 824. С. 10-13.
3. Василішин С. І. Теоретико-методологічні засади встановлення сутності, проявів та складових економічної безпеки підприємств як економічної категорії. *Економіка та держава*. 2019. № 9. С. 35-39.
4. Васильців Т. Г., Волошин В. І., Бойкевич О. Р., Каркавчук В. В. Фінансово-економічна безпека підприємств України: стратегія та механізми забезпечення: монографія. Львів: Новий світ, 2012. С. 12.
5. Велігура А.В., Дегтярьова Л.М., Степанова О.М. Дослідження шляхів розробки комплексів інформаційної безпеки. *Вісник Східноукраїнського національного університету імені В. Даля*. 2009. № 6(136). Ч. 1 С 154–161.
6. Верескун М.В. Методичне забезпечення системи інформаційної безпеки промислових підприємств. *Економiка i організація управлiння*. 2014. № 1 (17). С. 76–82.
7. Данілова Е. І. Семантико-морфологічний аналіз поняття «економічна безпека підприємства». *Формування ринкових відносин в Україні*. 2019. № 6(217). С. 90-99.
8. Данілова Е. І. Семантико-морфологічний аналіз поняття «економічна безпека підприємства». *Формування ринкових відносин в Україні*. 2019. № 6(217). С. 90-99.
9. Дегтярьова, Л. М., Ляшевський, В. Г. (2017). Практичні прийоми та керівні принципи розробки комплексів інформаційної безпеки. Системи управління, навігації та зв’язку. 2017. № 2(42). С. 94–97.
10. Дорофеев А. В., Марков А. С. Менеджмент информационной безопасности: основные концепции. Вопросы кибербезопасности. 2014. №1 (2). С. 67-73.
11. Єфімова Г. В., Марущак С. М. Планування безпечного розвитку підприємства на основі результатів діагностики рівня його економічної безпеки. *Економіка: реалії часу*. №3(8), 2013. С.44.
12. Зачосова Н. В. Формування системи економічної безпеки фінансових установ: монографія. Черкаси: ПП Чабаненко Ю.А., 2016. 375 с.
13. Зачосова Н. В. Формування системи економічної безпеки фінансових установ: монографія. Черкаси: ПП Чабаненко Ю.А., 2016. 375 с.
14. Іванюта Т.М., Заїчковський А.О. Економічна безпека підприємства: навч. посіб. Київ: Центр навч. літ., 2017. 256 с.
15. Кавин О. М., Кавин С. Я., Кавин Б. Я., Кавин Я. М. Сутність інформаційно-економічної безпеки підприємства. *Scientific collection «Interconf»*. № 76. С. 39-54
16. Колодяжна І. В., Букріна К. А. Економічна безпека в системі сталого функціонування підприємства. *Науковий вісник Ужгородського національного університету*. 2019. №23. С. 135-140.
17. Колодяжна І. В., Букріна К. А. Економічна безпека в системі сталого функціонування підприємства. *Науковий вісник Ужгородського національного університету*. 2019. №23. С. 135-140.
18. Корецька О. В. Теоретичні підходи до управління фінансово-економічною безпекою підприємств портової галузі*. Глобальні та національні проблеми еко­номіки*. 2017. Випуск 15. С. 225-229.
19. Курушин В. Д., Минаев В. А. Компьютерные преступления и информационная безопасность. М.: Новый юрист. 2012. 256 с.
20. Линник О. І. Артеменко Н. В. Стратегія економічної безпеки підприємства як фактор зменшення впли­ву зовнішніх та внутрішніх загроз. *Вісник НТУ «ХПІ»*. 2016. № 67 (1040). С. 159-169.
21. Маковський І.Ю. Аналіз вихідних даних для формування політики інформаційної безпеки на підприємстві. *Економіка, управління та адміністрування*. 2020. № 1(91). С. 38–42.
22. Мусиенко C.Г. Следователи и частные детективы: Защитники прав, имущества и жизни. Минск: Литература, 1996. 640 с.
23. Нашинець-Наумова А. Ю. Питання забезпечення інформаційної безпеки підприємства. *Юридичний вісник*. 2012. № 3(24). С. 58-62.
24. Небава М. І., Міронова Ю. В. Економічна безпе­ка підприємства: навчальний посібник URL: <https://web.posibnyky.vntu.edu.ua/fmib/33nebava_ekonomichna_bezpeka_pidpriyemstva/>
25. Небава М. І., Міронова Ю. В. Економічна безпе­ка підприємства: навчальний посібник URL: <https://web.posibnyky.vntu.edu.ua/fmib/33nebava_ekonomichna_bezpeka_pidpriyemstva/>
26. Орлова В.В. Ідентифікація загроз фінансовій без­пеці підприємства. *Науковий вісник НЛТУ України*. 2011. Випуск 21.13. С. 261-273.
27. Панченко В. А. Менеджмент інформаційної безпеки комерційного підприємства. Центральноукраїнський науковий вісник. Економічні науки. 2019. № 3 (36). С. 219-228.
28. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою КМУ від 29.03.2006 № 373
29. Про державну таємницю : Закон України від 21.09.99 № 1079-XIV. *Відомості Верховної Ради України*. 1994. № 16. 93 с.
30. Пуйда Г.В. Комплексний аналіз філософсько-економічної дефініції «інтелектуальна безпека підприємства». *Економічний аналіз*. 2017. Т. 27. № 4. С. 264.
31. Северина С. В. Інформаційна безпека та методи захисту інформації Вісник Запорізького національного університету. Економічні науки. 2016. №1. С. 155-161.
32. СпрінсянсВ., Бірюкова Т. Ресурси та технології інформаційного менеджменту : навчальний посібник. Одеса : ОНПУ, 2012. 248 с.
33. Степанова О.М., Дегтярьова Л.М. Інформаційна безпека в умовах розвитку інформаційної системи підприємства. *Інформаційна безпека.* 2009. № 1. С. 59-63.
34. Танцюра М.Ю. Забезпечення ефективності системи інформаційного забезпечення підприємства (на прикладі туристичних підприємств АР Крим) : автореф. дис. на здобуття наук. ступеня канд. екон. наук : 08.00.04 / М.Ю. Танцюра. Сімферополь, 2012. 21 с.
35. Терещенко Т. Теорія організації: навчальний посібник. Хмельницький: Хмельницький університет управління та права, 2015. 335 с.
36. Терещенко Т. Теорія організації: навчальний посібник. Хмельницький: Хмельницький університет управління та права, 2015. - 335 с.
37. Труш А. Ю. Принципи забезпечення інформаційної безпеки підприємств. *Геоекономічні та політико-правові виклики структурної перебудови міжнародних зв’язків України*: тези доповідей ІV Всеукр. студ. наук.-практ. конф. (Київ, 28 квітня 2020 р.) / відп. ред. С. В. Мельниченко. – Київ : Київ. нац. торг.-екон. у-т, 2020. С. 364-367.
38. Турчин О. І. Інформаційна безпека процесів менеджменту інтегрованих систем. Моделювання регіональної економіки. 2010. №2. С. 347-352.
39. Урба С.І., Івончак І.О. Теоретичні аспекти дослідження суті економічної безпеки. *Причорноморські економічні студії*. 2018. Вип. 34. С. 33-38.
40. Фальченко О. О. Глушач. Ю. С Стратегія забез­печення економічної безпеки підприємств. *Вісник НТУ «ХПІ». 2013.* № 66 (1039). С. 157-160.
41. Черевко О. В. Теоретичні засади поняття інформаційної безпеки та класифікація загроз системі Інформаційного захисту. Ефективна економіка. 2014. №5. URL: <http://nbuv.gov.ua/UJRN/efek_2014_5_103>
42. Ярославський А. О. Чинники економічної безпеки підприємства. *Економічний розвиток України в контексті впровадження прогресивних інформаційних технологій та систем управління*: матеріали ІІ Всеукр. наук.-практ. конф. (25 лютого 2019 р.; м. Київ). К.: ТОВ «ВІПО», 2019. С. 170-173.
43. Ярославський А. О. Чинники економічної безпеки підприємства. *Економічний розвиток України в контексті впровадження прогресивних інформаційних технологій та систем управління*: матеріали ІІ Всеукр. наук.-практ. конф. (25 лютого 2019 р.; м. Київ). К.: ТОВ «ВІПО», 2019. С. 170-173.
44. Avanesova N., Chuprin Y. Enterprise economic security: essential characteristics of the concept. *Innovative technologies and scientific solutions for industries*. Kharkiv, 2017. No. 1 (1). P. 98-102.
45. ISO 27001:2013. Information technology - Security techniques - Information security management systems - Requirements. URL: <http://www.teamprevent.com.ua/ua/poslugi/sistemi_menedzhmentu/iso_27001_sistema_menedzhmentu_informaciinoji_bezpeki.html>